ANALISIS PIDANA TERHADAP PENIPUAN DAN PENGGELAPAN DANA MELALUI M-BANKING DI KOTA MEDAN

Daniel Limbong
Universitas Prima Indonesia
E-mail: daniellimbong@unprimdn.ac.id

Samuel Siahaan
Universitas Prima Indonesia
Email: samuelsihaan04@gmail.com

Feby Yolanda Saragih
Universitas Prima Indonesia
Email: febyolanda16@gmail.com

Elni Puspitasari Zendrato
Universitas Prima Indonesia
Email: sarizendrato22@gmail.com.

Abstract

The advancement of digital technology has brought about a significant transformation in the banking sector, particularly through mobile banking (m-banking) services that facilitate various financial transactions. However, this convenience also poses a serious challenge in the form of increasing fraud and embezzlement crimes through the platform. This research aims to analyze the factors causing such crimes in Medan City and evaluate mitigation strategies that can be effectively implemented. The methods used are normative juridical and sociological juridical approaches, with data collection through literature study of laws and regulations, scientific literature, and observation of related social dynamics. The results show that low digital literacy, weak supervision of financial institutions, and the rapid development of technology without the support of an adequate security system are the main factors. In addition, the lack of public understanding of digital risks increases the potential for cybercrime. Therefore, a comprehensive mitigation strategy is needed, including the implementation of multi-factor authentication, strengthening artificial intelligence-based security systems, and continuous digital education. Collaboration between banking institutions, law enforcement officials, government, and the public is key in creating a safe and reliable digital ecosystem.

Keywords: *Fraud, embezzlement of funds, mobile banking, legal protection, Electronic Information and Transaction Law*

Abstrak

Kemajuan teknologi digital telah membawa transformasi signifikan dalam sektor perbankan, khususnya melalui layanan mobile banking (m-banking) yang mempermudah berbagai transaksi keuangan. Namun, kemudahan ini juga menimbulkan tantangan serius berupa meningkatnya kejahatan penipuan dan penggelapan dana melalui platform tersebut. Penelitian ini bertujuan untuk menganalisis faktor-faktor penyebab tindak pidana tersebut di Kota Medan serta mengevaluasi strategi mitigasi yang dapat diterapkan secara efektif. Metode yang digunakan adalah pendekatan yuridis normatif dan yuridis sosiologis, dengan pengumpulan data melalui studi pustaka terhadap peraturan perundang-undangan, literatur ilmiah, serta observasi dan analisis kriminologis terhadap fenomena sosial dan pola kejahatan digital yang relevan. Hasil penelitian menunjukkan bahwa rendahnya literasi digital, lemahnya pengawasan lembaga keuangan, dan pesatnya perkembangan teknologi tanpa dukungan sistem keamanan yang memadai menjadi faktor utama. Selain itu,

kurangnya pemahaman masyarakat terhadap risiko digital memperbesar potensi terjadinya kejahatan siber. Oleh karena itu, strategi mitigasi yang komprehensif diperlukan, mencakup penerapan otentikasi multi-faktor, penguatan sistem keamanan berbasis kecerdasan buatan, serta edukasi digital secara berkelanjutan. Kolaborasi antara institusi perbankan, aparat penegak hukum, pemerintah, dan masyarakat menjadi kunci dalam menciptakan ekosistem digital yang aman dan terpercaya.

Kata Kunci: *Penipuan, penggelapan dana, mobile banking, perlindungan hukum, Undang-Undang Informasi dan Transaksi Elektronik*.

I. PENDAHULUAN

Perkembangan teknologi digital, khususnya di era Revolusi Industri 4.0, telah membawa perubahan signifikan dalam berbagai sektor, termasuk sektor keuangan dan perbankan. Salah satu manifestasi utama dari transformasi ini adalah layanan mobile banking (m-banking), yang memungkinkan masyarakat melakukan transaksi keuangan secara cepat dan efisien. Namun, kemudahan tersebut juga membuka peluang terjadinya penyalahgunaan teknologi untuk tujuan kriminal, khususnya dalam bentuk tindak pidana penipuan dan penggelapan dana secara daring.[1]

Fenomena kejahatan siber yang berkaitan dengan layanan perbankan digital, seperti penipuan melalui SMS banking dan penggelapan dana melalui m-banking, menunjukkan tren peningkatan, terutama di kota-kota besar seperti Medan. Para pelaku memanfaatkan celah keamanan teknologi dan rendahnya literasi digital masyarakat untuk melakukan kejahatan yang semakin canggih dan sulit dideteksi. Kompleksitas modus operandi ini menimbulkan tantangan hukum yang serius, yang menuntut peningkatan kapasitas aparat penegak hukum dalam mengidentifikasi, membuktikan, dan menindak para pelaku secara efektif..[2]

Secara eksplisit, tindak pidana penipuan diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP), yang menjelaskan bahwa setiap orang yang dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan menggunakan nama palsu, martabat palsu, tipu muslihat, atau rangkaian kebohongan, dapat dipidana.[3] Adapun penggelapan diatur dalam Pasal 372 KUHP, yakni perbuatan mengambil barang milik orang lain yang telah berada dalam penguasaan pelaku secara sah, kemudian

[1] Elvira Fitriyani Pakpahan, Lionel Ricky Chandra, and Ananta Aria Dewa, "Perlindungan Hukum Terhadap Data Pribadi Dalam Industri Financial Technology," *Veritas et Justitia* 6, no. 2 (2020): 298323, https://doi.org/10.25123/vej.3778.

[2] Jevlin Solim et al., "Upaya Penanggulangan Tindak Pidana Penipuan Situs Jual Beli Online Di Indonesia," *Jurnal Hukum Samudra Keadilan* 14, no. 1 (2019): 97 110, https://doi.org/10.33059/jhsk.v14i1.1157.

[3] Renata Christha Auli., "Bunyi Dan Unsur Pasal 378 KUHP Tentang Penipuan," Hukum Online, 2023, https://www.hukumonline.com/klinik/a/pasal-378-kuhp-tentang-penipuan-lt6571693c4c627/.

disalahgunakan untuk kepentingan pribadi secara melawan hukum.[4]

Penipuan dan penggelapan memiliki karakteristik berbeda, baik dari segi unsur delik maupun motif. Penipuan berfokus pada adanya unsur tipu daya untuk memperoleh sesuatu dari korban, sedangkan penggelapan menitikberatkan pada penyalahgunaan keperc ayaan yang telah diberikan sebelumnya. Meskipun demikian, keduanya merupakan kejahatan terhadap harta benda yang dapat terjadi dalam konteks transaksi digital melalui m-banking.[5]

Seiring meningkatnya kasus kejahatan siber yang melibatkan transaksi perbankan digital di wilayah Sumatera Utara, Kepolisian Daerah (Polda) Sumut merespons dengan membentuk Direktorat Reserse Siber (Ditreskrimsiber) pada September 2024. Direktorat ini dibentuk untuk memperkuat penanganan tindak pidana siber yang kian kompleks, termasuk kasus penipuan dan penggelapan berbasis digital. Fokus utama Ditreskrimsiber tidak hanya mencakup penyebaran informasi palsu dan ujaran kebencian di dunia maya, tetapi juga penguatan kapasitas dalam mengungkap dan menindak kejahatan keuangan digital. Pembentukan unit ini menandai komitmen aparat penegak hukum dalam mengantisipasi eskalasi kejahatan siber di Sumatera Utara, khususnya menjelang momentum politik dan meningkatnya penggunaan layanan digital di masyarakat.[6]

Fakta ini menunjukkan pentingnya pendekatan kriminologis dalam memahami motif, modus, dan pola kejahatan yang terjadi, selain pendekatan yuridis normatif yang mengkaji aspek peraturan perundang-undangan. Analisis ini tidak hanya bertujuan untuk memahami konteks hukum yang berlaku, tetapi juga untuk menggali akar sosial dan psikologis dari pelaku kejahatan berbasis teknologi. Dalam rangka mengarahkan analisis secara sistematis, penelitian ini merumuskan dua pokok permasalahan utama sebagai berikut:

1. Apakah faktor penyebab terjadinya kejahatan penipuan dan penggelapan dana yang dilakukan pelaku melalui mobile banking (m-banking) dari korban di kota Medan?
2. Bagaimanakah upaya penanggulangan dari tindak pidana penipuan dan penggelapan dana terhadap pelaku dengan menggunakan aplikasi mobile banking (m-banking) di Kota Medan?

[4] sonya arini batu bara. mazmur rumapea, dewi ervina suryani, "Upaya Penanggulangan Tindak Pidana Penggelapan Pada Koperasi Kredit," *Jurnal Ilmu Hukum Prima* 11, no. 1 (2019): 1–14.

[5] Muhammad Raihan Nugraha, "Perbedaan Pasal Penipuan Dan Penggelapan," Hukum Online, 2024, https://www.hukumonline.com/klinik/a/pasal-penipuan-dan-penggelapan-lt4ceb3048897ea/.

[6] Polda Sumut, "Perkuat Penanganan Kejahatan Siber, Polda Sumut Kini Punya Direktorat Reserse Siber," Heta News, 2024, https://www.hetanews.com/article/291301/perkuat-penanganan-kejahatan-siber-polda-sumut-kini-punya-direktorat-reserse-siber.

Penelitian ini bertujuan untuk menganalisis fenomena penipuan dan penggelapan dana melalui aplikasi mobile banking di Kota Medan dari sudut pandang kriminologi. Fokus utama penelitian adalah memahami karakteris tik pelaku, pola kejahatan, serta faktor-faktor yang memengaruhinya. Selain itu, penelitian ini mengevaluasi strategi dan tantangan yang dihadapi aparat penegak hukum serta efektivitas langkah pencegahan yang diterapkan. Hasil penelitian diharapkan dapat memberikan kontribusi terhadap pengembang an ilmu kriminologi dan kebijakan publik dalam menghadapi kejahatan berbasis teknologi digital.

Secara teoritis dan pragmatis, penelitian ini diharapkan memberikan kontribusi besar dalam pengembangan ilmu hukum pidana serta solusi nyata dalam menghadapi maraknya kejahatan penipuan dan penggelapan dana melalui mobile banking (m-banking). Secara teoritis, temuan penelitian ini dapat memperkaya wawasan para akademisi hukum pidana mengenai faktor-faktor penyebab kejahatan berbasis teknologi, baik dari aspek individu, sosial, maupun teknologi itu sendiri. Pemahaman ini diharapkan mendorong lahirnya teori-teori hukum baru yang relevan dengan tantangan digital saat ini.

Secara praktis, hasil penelitian ini dapat dijadikan referensi penting bagi pembuat kebijakan, aparat penegak hukum, serta lembaga terkait dalam menyusun strategi yang lebih efektif untuk mencegah dan menangani kejahatan m-banking. Dengan adanya pemahaman yang lebih baik terhadap modus dan karakteristik kejahatan ini, diharapkan upaya penegakan hukum dapat ditingkatkan sehingga kepercayaan masyarakat terhadap sistem perbankan digital semakin kuat dan aman.

Dalam pelaksanaan penelitian ilmiah, khususnya dalam ranah ilmu hukum, kerangka teori menjadi unsur yang sangat penting sebagai landasan berpikir dan titik tolak analisis. Kerangka teori berfungsi sebagai abstraksi dari berbagai pemikiran yang mendasari penelitian. Dalam penelitian ini digunakan dua teori utama, yaitu:

1. Teori Penyebab Terjadinya Kejahatan

Abdulsyani menyatakan bahwa kejahatan merupakan fenomena sosial yang memiliki banyak penyebab dan dapat ditinjau dari berbagai sudut pandang, yakni hukum, sosial, dan ekonomi.

a. Aspek hukum: Kejahatan dipandang sebagai perbuatan yang melanggar hukum positif dan pelakunya dinyatakan bersalah oleh pengadilan.

b. Aspek sosial: Kejahatan muncul sebagai bentuk penyimpangan terhadap norma sosial yang berlaku, baik secara sengaja maupun tidak.

c. Aspek ekonomi: Kejahatan terjadi karena individu menghalangi kepentingan ekonomi orang lain demi keuntungan pribadi, sehingga menimbulkan kerugian bagi pihak lain.

2. Teori Upaya Penanggulangan Kejahatan

Menurut Ende Hasbi Nasaruddin, upaya pencegahan kejahatan mencakup tindakan-

tindakan yang dilakukan baik sebelum maupun sesudah tindak pidana terjadi. Pendekatan ini melibatkan pengendalian terhadap lingkungan fisik dan sosial serta perhatian terhadap pelaku maupun korban kejahatan.[7]

II. METODE PENELITIAN

Kajian ini berfokus pada hukum positif sebagai objek utama analisis, yang menempatkannya dalam ranah penelitian hukum normatif.[8] Penelitian ini bertumpu pada pemahaman mendalam terhadap berbagai peraturan perundang-undangan yang relevan, serta didukung oleh teori-teori hukum, pemikiran akademis, dan literatur ilmiah yang membahas isu-isu seputar kejahatan dalam konteks penggunaan teknologi, khususnya mobile banking. Seluruh kerangka pemikiran tersebut menjadi fondasi konseptual dan metodologis dalam menggali, menelaah, serta menafsirkan norma hukum yang berlaku guna menjawab persoalan hukum yang diangkat dalam penelitian ini.

Bahan hukum di kumpulkan melalui studi pustaka (*library research*) yang mencakup penelusuran melalui berbagai sumber yang valid, antara lain Jaringan Dokumentasi dan Informasi Hukum (JDIH), situs resmi Mahkamah Agung dan Kepolisian RI, Google Scholar, Perpustakaan Nasional RI (Perpusnas), serta perpustakan universitas pri ma indonesia. Pengumpulan dilakukan secara selektif dan sistematis untuk memastikan relevansi dan validitas bahan hukum yang digunakan sebagai dasar analisis dalam penelitian ini. Bahan hukum di gunakan antara meliputi:

a. Bahan hukum primer: peraturan perundang-undangan seperti Kitab Undang-Undang Hukum Pidana (KUHP), Kitab Undang-Undang Hukum Acara Pidana (KUHAP), Undang-Undang No. 2 Tahun 2022 tentang Kepolisian Negara Republik Indonesia, serta peraturan pelaksana terkait.
b. Bahan hukum sekunder: buku ajar, jurnal hukum, artikel kriminologi, dan pendapat ahli hukum pidana.
c. Bahan hukum tersier: kamus hukum, ensiklopedia hukum, dan dokumen penunjang lainnya.

Metode Analisis

Penelitian ini menggunakan metode analisis sistematis dan interpretasi hukum gramatikal dalam menelaah bahan hukum yang dikumpulkan. Analisis sistematis dilakukan untuk mengkaji keterkaitan antar norma dalam sistem hukum pidana Indonesia, dengan menyusun pasal-pasal yang relevan secara runtut dan terstruktur dalam kerangka logika hukum. Analisis ini bertujuan

[7] Mar'ah Shaleha, "Tinjauan Kriminologis Fenomena Penggunaan Senjata Tajam Oleh Anak Di Kabupaten Bantaeng," *FIS Universitas Negeri Makassar* 5, no. 2 (2018): 1–12.

[8] Soerjono Soekanto and Sri Mamudji, "Penelitian Hukum Normatif Suatu Tinjauan Singkat" (Jakarta: Raja Grafindo Persada, 2010), hlm 13.

memastikan bahwa pemahaman terhadap norma hukum dilakukan secara utuh, tidak parsial, dan sesuai dengan asas-asas hukum pidana yang berlaku.[9]

Sementara itu, interpretasi hukum gra matikal digunakan untuk memahami bunyi pasal-pasal hukum, khususnya Pasal 372 dan Pasal 378 KUHP, berdasarkan makna bahasa normatifnya. Metode ini dipilih karena pentingnya ketepatan dalam menafsirkan istilah hukum seperti "tipu muslihat", "dengan melawan hukum", atau "penguasaan yang sah" yang menjadi unsur-unsur delik dalam kasus penipuan dan penggelapan melalui mobile banking.[10] Dengan pendekatan ini, penelitian diharapkan dapat memberikan pemahaman yang jelas dan terukur terhadap norma hukum yang berlaku, serta relevansi penerapannya dalam konteks kejahatan digital di Kota Meda n.

III. HASIL PENELITIAN DAN PEMBAHASAN

3.1 Faktor Penyebab Terjadinya Kejahatan Penipuan Dan Penggelapan Dana Melalui M-Banking Di Kota Medan

Ketika aktivitas kriminal terutama meng gunakan komputer atau jaringan komputer, istilah"kejahatan dunia maya" terkadang digu nakan untuk mengkarakterisasikannya.[11] Keja hatan klasik yang memanfaatkan komputer ataujaringan untuk memungkinkan atau memf asilitasi tindakanya juga dapat di sebut sebagai kejahatan e-commerce.[12] Salah satu jenis kejahatan e-commerce adalah penipuan daring. Istilah "penipuan daring" didefinisikan dalam konteks perdagangan elektronik sebagai praktik melakukan transaksi bisnis sepenuhnya secara daring, bukan melalui lokasi fisik yang lebih konvensional.

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) tahun 2008 tidak hanya mengatur penipuan daring, tetapi juga mengatur penipuan menggunakan Short Massage Service (SMS).[13] 13 Kasus penipuan SMS sering kali menggunakan telepon seluler, yang merupakan media elektronik sebagaimana dimaksud dalam UU ITE. Menurut Pasal 1 angka 2 UU ITE, penipuan yang dilakukan melalui media sosial atau pesan singkat tergolong kejahatan telekomunikasi karena teknologi informasi meliputi penggunaan komputer, jaringan komputer, dan media elektronik lainnya.

Indonesia telah memberlakukan UU ITE untuk memerangi kejahatan dunia maya dan bentuk-bentuk kejahatan dunia maya lainnya

[9] Muwahid -, "Metode Penemuan Hukum (Rechtsvinding) Oleh Hakim," *Al-Hukama'* 7, no. 1 (2017):hal 236-237, https://doi.org/10.15642/alhukama.2017.7.1.224-248.

[10] *Ibid*, hal 235.

[11] Rena Yulia Edi Setiadi, *Hukum Pidana Ekonomi* (Yogyakarta: Graha Ilmu, 2010), hlm 40.

[12] Harianto Rantesalu, "Penanggulangan Kejahatan Penipuan Belanja Online Di Wilayah Kepolisian Daerah Jawa Timur," *Janaloka* 1, no. 2 (2022): 70–94.

[13] Eveline Ivanca and Hery Firmansyah, "Perlindungan Hukum Pengguna Mobile Banking Sebagai Korban Kejahatan Melalui Internet Ditinjau Dari Hukum Positif," *UNES* 6, no. 2 (2023): 6166, 74, https://review unes.com/https://creativecommons.org/licenses/by/4.0/ .

dengan mengatur masalah-masalah yang berkaitan dengan teknologi informasi dan komunikasi. Ekosistem digital yang lebih aman dapat terwujud melalui pemberantasan kejahatan siber secara global dan domestik, yang sangat dipengaruhi oleh kriminalisasi kejahatan siber dalam regulasi di Indonesia.

Dalam era digital, layanan mobile banking (m-banking) memudahkan transaksi keuangan masyarakat, namun juga membuka peluang terjadinya kejahatan siber seperti penipuan dan penggelapan dana. Di Kota Medan, modus kejahatan ini marak dilakukan oleh pelaku yang memanfaatkan celah keamanan sistem dan kelalaian pengguna. Dalam konteks hukum positif, perlindungan terhadap korban tercantum dalam Pasal 28 ayat (1) UU ITE yang mengatur sanksi pidana atas penyebaran informasi bohong yang merugikan konsumen dalam transaksi elektronik, serta Pasal 40 ayat (1) yang menegaskan kewajiban menjaga kerahasiaan data nasabah oleh penyelenggara sistem elektronik.

Perlindungan ini diperkuat oleh Pasal 28D ayat (1) UUD 1945 dan Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen. Meski regulasi telah tersedia, lemahnya pengawasan internal lembaga keuangan memungkinkan terjadinya penyalahgunaan wewenang. Oleh karena itu, penguatan pengawasan dan kepastian hukum menjadi sangat penting dalam mencegah dan menanggulangi kejahatan perbankan digital.

Dilansir dari TEMPO.CO berikut adalah sederet modus kejahatan yang sering dilakukan melalui internet atau mobile banking dan cara menghindarinya:

1. *Pharming*

   Penyerang mengalihkan pengguna dari situs resmi ke situs palsu yang menyerupai aslinya. Tujuannya adalah untuk mencuri informasi pribadi seperti ID pengguna, PIN, atau nomor rekening.

2. *Spoofing*

   Pelaku menyamarkan identitasnya dengan menampilkan alamat email, nama, atau nomor telepon palsu. Hal ini menciptakan kesan seolah-olah berinteraksi dengan pihak yang terpercaya misalnya pihak bank.

3. *Keylogger*

   Perangkat lunak ini dapat merekam setiap tombol yang ditekan pada keyboard tanpa sepengetahuan pengguna. Dengan demikian, informasi sensitif seperti PIN atau password dapat dicuri.

4. *Phishing*

   Metode penipuan melalui email, situs web, atau komunikasi elektronik lainnya yang mengaku berasal dari bank atau lembaga keuangan resmi. Tujuannya adalah untuk memperoleh informasi pribadi seperti user ID, password/PIN, nomor kartu kredit, dan CVV.

5. *Sniffing*

   Kejahatan ini dilakukan dengan mengintersep paket data yang melewati jaringan. Penyerang dapat mengakses

informasi yang sedang ditransmisikan tanpa sepengetahuan pengirim atau penerima.[14]

Tabel 1

Data Kasus Kejahatan Di Medan

Jenis Kejahatan/Pelanggaran	2021	2022	2023
Kejahatan Politik	-	-	-
Kejahatan Terhadap Kepala Negara	2	-	-
Kejahatan Terhadap Ketertiban Umum	1	-	-
Pembakaran	111	79	107
Kebakaran	158	155	56
Penyuapan	2	-	26
Kejahatan Mata Uang	21	8	8
Kejahatan Materai dan Merk	7	5	16
Melanggar Kesopanan, Perzinahan	565	425	330
Perkosaan	211	216	203
Perjudian	1.069	581	514
Penculikan	19	25	28
Pembunuhan	107	106	96
Penganiayaan Berat	2.536	2.254	2.260
Penganiayaan Ringan	2.779	2.569	1.176
Pencurian Ringan	2.015	1.618	28
Pencurian dengan Kekerasan	716	681	532
Pencurian dengan Pemberatan	4.679	3.908	4.738
Penghinaan	415	278	457
Pemerasan	697	590	715
Penggelapan	2.667	2.555	2.531
Penipuan	2.450	2.379	2.736
Pengrusakan	776	608	723
Penadahan	55	13	4
Kejahatan Ekonomi	-	-	3
Pencurian Kendaraan Bermotor	2.982	2.634	2.620
Melarikan Wanita dibawah Umur	104	89	-
Kejahatan Narkotik	6.376	6.218	5.950
Penyelundupan	11	4	4
Korupsi	29	27	12
Penyalahgunaan Senjata Api	24	11	15
Kejahatan Surat-surat Sejenis	-	222	322
Sengketa Tanah	201	186	375
Ilegal Logging	25	29	18
Kejahatan Digital Perbankan (Skimming, Phishing, phraming dan sejenisnya)	70	250	80
Lain-lain Kejahatan	5.564	5.180	10.023
Jumlah	**37.444**	**33.903**	**36.715**

Sumber: Badan Pusat Statistik Sumatera Utara[15]

Data dari Badan Pusat Statistik Sumatera Utara (BPS Sumut) menunjukkan peningkatan kasus kejahatan siber, terutama yang melibatkan M-banking. Pada tahun 2021-2023, tercatat lebih dari 300 kasus kejahatan siber di seluruh Sumatera Utara, dengan sebagian besar kasus berasal dari Kota Medan. Meskipun masyarakat semakin menyadari manfaat M-banking, banyak yang tidak menyadari bahwa platform ini bisa menjadi sasaran empuk bagi pelaku kejahatan yang memanfaatkan kelemahan dalam sistem dan kurangnya kewaspadaan pengguna.

Kurangnya literasi digital di kalangan masyarakat kota medan menjadi faktor

[14] Tim redaksi tempo, "Kenali 5 Modus Kejahatan Mobile Banking Dan Cara Menghindarinya," Tempo, 2023, https://www.tempo.co/digital/kenali-5-modus-kejahatan-mobile-banking-dan-cara-menghindarinya-187128.

[15] Kepolisian Daerah Sumatera Utara, "Banyaknya Peristiwa Kejahatan/Pelanggaran Yang Dilaporkan Menurut Jenis Kejahatan/Pelanggaran, 2019-2021," *Badan Pusat Statistik SUmatera Utara*, vol. 75, 2021.

pendukung lainnya. Banyak nasabah yang belum memahami risiko keamanan dalam penggunaan m-banking, sehingga mudah menjadi target penipuan.[16] Banyak pengguna yang tidak sepenuhnya memahami pentingnya menjaga data pribadi, seperti PIN, kata sandi, dan informasi transaksi lainnya. Mereka lebih fokus pada kemudahan transaksi dan sering mengabaikan langkah-langkah pengamanan dasar, seperti autentikasi dua faktor (2FA) atau memperbarui kata sandi secara berkala.

Berdasarkan informasi dari BPS Sumut, peningkatan kasus kejahatan siber di Medan yang tercatat pada tahun 2022 adalah masalah serius yang tidak bisa diabaikan. Sangat penting bagi masyarakat untuk meningkatkan literasi digital dan tetap waspada terhadap potensi ancaman. Dengan adanya program edukasi yang lebih intensif serta langkah-langkah pencegahan dari pihak bank dan pemerintah, diharapkan masyarakat dapat lebih terlindungi dan tidak menjadi korban kejahatan yang memanfaatkan kemajuan teknologi.[17]

Beberapa faktor utama yang menyebabkan lonjakan kasus ini meliputi rendahnya literasi digital, kurangnya pengawasan dari pihak bank, dan perkembangan teknologi yang cepat tanpa diimbangi dengan upaya mitigasi yang memadai.[18]

1. **Rendahnya Literasi Digital**

   Rendahnya literasi digital menyebabkan maraknya penipuan digital seperti phishing dan vishing, di mana pelaku menyamar sebagai pihak resmi untuk mencuri data pribadi korban. Di Medan, 38% kasus kejahatan siber tahun 2022 terkait modus ini, menunjukkan perlunya peningkatan edukasi dan kewaspadaan digital masyarakat.[19]

2. **Kurangnya Pengawasan Dari Bank**

   Kurangnya pengawasan dari pihak bank turut memicu meningkatnya kejahatan terkait M-banking. Sekitar 40% kasus tahun 2022 di Sumut disebabkan oleh lemahnya deteksi transaksi mencurigakan. Beberapa pelaku bahkan berhasil melakukan transaksi besar melalui perangkat tidak dikenal tanpa verifikasi tambahan dari sistem perbankan.

3. **Perkembangan Teknologi Yang Terus Berkembang.**

[16] Najla Amaly and Armiah Armiah, "Peran Kompetensi Literasi Digital Terhadap Konten Hoaks Dalam Media Sosial," *Alhadharah: Jurnal Ilmu Dakwah* 20, no. 2 (2021): 43, https://doi.org/10.18592/alhadharah.v20i2.6019.

[17] Syfa Tasya Zahwani, Muhammad Irwan, and Padli Nasution[2], "Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi Di Era Digital,"*Analisis Kesadaran Masyarakat (Zahwani, Dkk.) JoSES: Journal of Sharia Economics Scholar* 2, no. 2 (2023): 105-9, https://doi.org/10.5281/zenodo.12608751.

[18] Sindy Ariyaningsih et al., "Korelasi Kejahatan Siber Dengan Percepatan Digitalisasi Di Indonesia," *Justisia: Jurnal Ilmu Hukum* 1, no. 1 (2023): 1–11, https://doi.org/10.56457/jjih.v1i1.38.

[19] Nirwansyah Sukartara et al., "Optimalisasi Literasi Digital Sebagai Upaya Menanggulangi Hoax Dan Pembangunan Masyarakat Kritis Pada Perkumpulan Pemuda Pemudi Kampung Sejahtera," *Indonesian Journal of Emerging Trends in Community Empowerment* 2, no. 1 (2024): 29–34, https://ejournal.pabki.org/index.php/ETCE/article/view/26.

Mahir dalam memanfaatkan teknologi untuk melakukan tindakan kriminal. Salah satu contohnya adalah penggunaan malware dan keylogger, yang memungkinkan mereka mencuri informasi pribadi korban tanpa terdeteksi. Menurut data dari BPS Sumut, sekitar 39% dari total kasus kejahatan yang tercatat di Medan pada tahun 2022 melibatkan penggunaan malware dan keylogger untuk mencuri data korban. Ini menunjukkan bahwa kemajuan teknologi yang cepat juga menjadi tantangan besar bagi masyarakat dan bank dalam menjaga keamanan data serta transaksi digital.[20]

4. **Kurangnya Kesadaran Masyarakat tentang Ancaman Digital**

   Sebanyak 30% kasus kejahatan siber di Sumut tahun 2023 disebabkan oleh kelalaian masyarakat dalam menjaga keamanan perangkat. Minimnya kewaspadaan terhadap ancaman digital membuat pengguna rentan diserang. Ketertarikan pada kemudahan transaksi sering mengabaikan risiko, sehingga kesadaran akan keamanan digital menjadi sangat penting.[21]

5. **Kurangnya Pengawasan Lembaga Keuangan**

   Lemahnya pengawasan internal dan eksternal lembaga keuangan di Medan serta aturan hukum yang ambigu membuka celah bagi kejahatan siber. Transaksi mencurigakan sering lolos tanpa deteksi akibat sistem bank yang tidak optimal. Hal ini dimanfaatkan pelaku untuk mencuri dana dan memanipulasi data tanpa terdeteksi.[22]

3.2 Upaya Penanggulangan Tindak Penipuan dan Penggelapan Dana Terhadap Pelaku Menggunakan Aplikasi M-Banking di Kota Medan

Di era digital, penggunaan layanan mobile banking oleh masyarakat semakin meingkat karena kepraktisanya. Namun, hal ini turut meingkatkan risiko kejahatan siber. Oleh karena itu, peningkatan sistem keamanan dalam M-Banking menjadi prioritas utama untuk melindungi nasabah dari ancaman kejahatan siber. Akan tetapi, kemudahan ini juga meningkatkan resiko berupa kejahatan siber seperti penipuan dan penggelapan dana oleh pelaku kejahatan. Kejahatan ini sering kali memanfaatkan kelemahan sistem keamanan dan kelalaian nasabah dalam menjaga data pribadi mereka.[23]

[20] Komang Maysa Surya Aditya I Gusti Ngurah Nyoman Krisnadi Yudiantara, "ANALISIS KRIMINO LOGI DALAM TINDAK PIDANA" 3, no. 2 (2025).

[21] Harya Nugroho et al., "Edukasi Keamanan Digital Untuk Meningkatkan Kewaspadaan Masyarakat Terhadap Link Phising," *Jurnal Pengabdian Masyara kat Multidisiplin (ECOS-PRENEURS)* 1, no. 2 (2023): 28–40.

[22] F. A Gusti, "Kelalaian Bank Dalam Menjaga Rahasia Bank Pada Perjanjian Baku Terhadap Tindakan Phising Yang Dialami Nasabah Akibat Social Engineering Ditinjau Dari Hukum Positif Indonesia (Doctoral Dissertation)," *FAKULTAS HUKUM UNIVERSITAS PASUNDAN*, 2023.

[23] Ivanca and Firmansyah, "Perlindungan Hukum Pengguna Mobile Banking Sebagai Korban

Sejumlah studi menunjukkan bahwa metode yang sering digunakan oleh pelaku adalah phishing, sniffing, dan malware berbasis aplikasi palsu yang menyamar sebagai layanan resmi perbankan. Salah satu cara yang dapat dilakukan adalah dengan menerapkan teknologi autentikasi berlapis atau multi-factor authentication (MFA), seperti kombinasi PIN, sidik jari, pengenalan wajah, dan kode OTP (One-Time Password).[24] Sistem ini akan mempersempit peluang bagi pelaku kejahatan untuk mengakses akun nasabah secara ilegal. sistem keamanan berbasis blockchain dapat diterapkan untuk meningkatkan transparansi dan akurasi dalam pencatatan transaksi, sehingga mengurangi kemungkinan manipulasi data oleh pihak yang tidak bertanggung jawab.

Keamanan m-banking dapat ditingkatkan melalui penerapan teknologi seperti enkripsi data dan otentikasi dua faktor (2FA).[25] Enkripsi data dan autentikasi dua faktor (2FA) merupakan langkah penting untuk melindungi transaksi mobile banking dari akses tidak sah. Selain itu, pendekatan non-penal yang menekankan edukasi dan pemberdayaan masyarakat dianggap lebih efektif dalam mencegah kejahatan dibandingkan hanya mengandalkan sanksi pidana.[26]

Dalam konteks kejahatan cyber, kebijakan ini mencakup kerjasama internasion al untuk menangani kejahatan lintas negara, pengembangan teknologi dan jaringan informasi, pelatihan personel penegak hukum, harmonisasi hukum antar negara, dan penyebarluasan kesepakatan internasional.

1. Kronologi Kasus Pembobolan Rekening Lewat AplikasiMobile Banking

Salah satu contoh kasus konkret terkait dengan tindak pidana m-banking yaitu kasus buk butet (bukan nama sebenarnya), pada tanggal 9 juli tahun 2022 nasabah bank Bri yaitu buk butet secara tiba-tiba tidak bisa mengakses akun BRI Mobile (Brimo) saat ingin mengisi pulsa. Beberapa menit setelahnya, dia menerima telfon dari seorang pria yang mengaku sebagai kantor BRI Sumat era Utara (Sumut) bahwasanya sedang ada perbaikan sistem.

Setelah itu, Buk Butet juga mendapat pesan berisi tautan dari nomor yang sama, beserta permintaan untuk mengubah data login. Meski awalnya mengabaikan, karena pria tersebut mengetahui masalah login-nya, ia akhirnya mempercayainya dan mengklik tautan tersebut serta memberikan kode OTP

Kejahatan Melalui Internet Ditinjau Dari Hukum Positif."

[24] Mar'atun Tursinah and Muhammad Iqbal Fasa, "Analisis Peran Keamanan Data Dalam Meningkatkan Kepuasaan Nasabah Pada Penggunaan Mobile Banking," *JIEMAS*, 2024, 481–86.

[25] Yuyun Prastiwi, Erico Yuan Varel, and Holland Nainggolan, "Analisis Keamanan Data Pribadi Dalam Aplikasi Mobile " Dana "," 2024, 584–88.

[26] Angela Gabriela Bupu, Karolus Kopong Medan, and Heryanto Amalo, "Analisis Yuridis Cyber Crime Pembobolan Dana Nasabah Pada Aplikasi Mobile Banking Dengan Modus Pembobolan Jalur Undangan Pernikahan Palsu," *Jurnal Ilmu Hukum Dan Sosial* 2, no. 2 (2024): 367–83, https://doi.org/10.51903/hakim.v2i2.1829.

yang diminta. Setelah berhasil masuk ke akunnya, saldo rekening Buk Butet sebesar Rp 112 juta perlahan-lahan berkurang secara cepat dalam waktu kurang dari 10 menit melalui beberapa kali transfer ke rekening dan aplikasi e-wallet yang tidak dikenal. Ia kemudian melaporkan kejadian tersebut ke kantor BRI di Medan untuk mencari tahu penyebab hilangnya dana, namun pihak bank menyatakan bahwa kasus tersebut merupakan kesalahan nasabah karena memberikan kode OTP kepada pihak lain.

Wesly Simanjuntak, suami Buk Butet, menilai kejadian itu bukan semata-mata kelalaian nasabah, melainkan juga akibat lemahnya sistem keamanan aplikasi BRImo yang sudah diretas sejak awal, sehingga memudahkan pencurian saldo. Kekecewaan bertambah ketika pihak BRI cabang Medan menyatakan bahwa penyelidikan kasus adalah kewenangan kantor pusat dan hampir setahun berlalu tanpa kejelasan atau tindak lanjut dari pihak berwenang.

2. Laporan Ke Polisi Dan Respon BRI

Merasa tidak mendapat pelayanan yang memuaskan dari Bank BRI, Butet bersama suaminya melaporkan kasus pembobolan rekening yang dialaminya ke Polda Sumut pada 11 Juli 2022. Dalam proses pelaporan, mereka mengetahui bahwa kasus serupa ternyata juga dialami oleh banyak nasabah lain, namun enggan melapor karena merasa pesimis kasus akan terungkap.

Butet mengaku sangat kecewa terhadap BRI, karena bank yang selama ini dianggap sebagai tempat penyimpanan uang yang aman justru gagal melindungi nasabahnya. Namun, hingga hampir setahun setelah laporan dibuat, kasus tersebut belum juga menunjukkan perkembangan, bahkan sang suami yang semestinya menjadi saksi belum pernah dipanggil oleh pihak kepolisian.

Parboaboa yang berupaya mengonfirma si kasus ini kepada Manajer Senior Bank BRI Sumut, Nartha Simamora, awalnya tidak mendapat tanggapan. Setelah akhirnya berhasil bertemu langsung di Menara BRI Medan, Nartha tidak memberikan klarifikasi dan justru bersikap tidak kooperatif dengan menyamakan upaya konfirmasi wartawan sebagai tindakan premanisme. Dia bahkan menantang wartawan untuk adu kekuatan secara fisik, sebelum akhirnya mengatakan bahwa ia tidak memiliki wewenang untuk menjelaskan kasus tersebut dan menyarankan agar wartawan menghubungi bagian humas. Sayangnya, nomor kontak humas pun tidak diberikan. Hingga kini, upaya untuk mendapatkan kejelasan terkait kasus pembobolan rekening nasabah BRI itu belum membuahkan hasil.

Kejadian yang dialami Butet bukanlah kasus pertama. Sebelumnya, pada Februari 2023, sebanyak 70 rekening nasabah Bank BRI Unit Tanjung Sakti, Cabang Kota Pagar Alam, Sumatera Selatan, juga dibobol, dengan total kerugian mencapai Rp5,2 miliar. Ironisnya, seperti dijelaskan oleh Wakil Direktur Ditreskrimsus Polda Sumsel, AKBP I

Putu Yudha Prawira, pelaku pembobolan adalah dua mantan pegawai bank tersebut.

Pakar keamanan siber dan forensik digital dari Vaksincom, Alfons Tanujaya, mengungkapkan bahwa pembobolan m-banking kini semakin canggih, dengan modus menggunakan undangan pernikahan palsu yang mengandung aplikasi berbahaya dari luar Play Store. Jika korban menginstalnya dan memberikan kode OTP, maka pelaku dapat dengan mudah meretas akun m-banking maupun e-wallet seperti OVO dan Gopay.

Menurut Alfons, aplikasi berbahaya tersebut tidak bisa langsung mengakses m-banking tanpa kombinasi user ID, password, dan OTP. Namun, jika korban sudah memberikan OTP, maka aplikasi tersebut bisa mengakses berbagai layanan finansial digital. Ia menduga, dalam kasus pembobolan rekening salah satu warga Medan senilai Rp112 juta, pelaku mendapatkan data dari jaringan kriminal phishing yang saling berbagi database, atau dari kebocoran data pengguna m-banking.

Dia menekankan, jika bank menjalanka n prosedur keamanan dengan baik, maka meski pelaku mendapatkan OTP, mereka tetap akan kesulitan membobol akun. Karena itu, ia menyarankan agar bank menggunakan verifikasi ganda berbasis "What You Have" seperti verifikasi melalui kartu ATM, KTP asli, atau fisik pemilik rekening bukan hanya "What You Know" seperti password dan OTP.

Sebagai langkah antisipasi, pengguna disarankan segera mengganti password dan PIN persetujuan transaksi jika menduga terjadi kebocoran data. Ia juga mendorong pemerintah dan regulator keuangan untuk menetapkan standar keamanan transaksi digital yang ketat demi menjaga kepercayaan publik terhadap sistem keuangan digital.[27]

3. Analisis Terhadap Kasus Pembobolan Bri M-Banking (BRIMO).

Kasus pembobolan rekening yang dialami Bu Butet menyoroti sejumlah kelemahan serius dalam sistem perlindungan mobile banking. Peretasan terjadi bahkan sebelum korban menyadarinya, menunjukkan adanya celah dalam sistem keamanan aplikasi. Pelaku menggunakan metode phishing sebagai teknik utama, yakni dengan menipu korban agar menyerahkan kode OTP melalui tautan palsu yang dikirim lewat pesan. Selain itu, pelaku juga memanfaatkan spoofing, dengan menyamar sebagai petugas resmi Bank BRI untuk membangun kepercayaan korban melalui panggilan telepon.

Kasus ini semakin sulit untuk di proses diakrenakan kurangnya tanggung jawab dan transparansi dari pihak bank dalam menangani laporan, serta lambannya proses penanganan oleh aparat kepolisian yang hingga kini belum menunjukkan tindak lanjut yang jelas.

[27] PARBOABOA, "Rekening Nasabah BRI Di Medan Dibobol, Uang Raib Hingga Rp 112 Juta: Hampir Setahun Kasus Dilaporkan, Tak Ada Kejelasan," TIM PARBOABOA, 2022, https://parboaboa.com/kasus-rekening-nasabah-bri-di-medan-yang-dibobol-tak-kunjung-selesai?

Hal ini menandakan perlunya peningkat an literasi digital bagi nasabah, penerapan standar keamanan yang lebih ketat seperti verifikasi berbasis "What You Have" selain "What You Know", serta reformasi sistem penegakan hukum dan pelayanan bank agar kepercayaan masyarakat terhadap layanan keuangan digital dapat terjaga dan kasus serupa tidak terulang kembali.

Dan kejadian pembobolan m-banking seperti ini tidak hanya terjadi keapada buk butet tapi banyak kasus serupa lainya dengan berbagai modus kejahatan digital. Sulit menangkap pelaku pembobolan rekening seperti kasus Buk Butet disebabkan beberapa faktor, antara lain pelaku sering menggunakan teknologi canggih yang memanfaatkan metode phishing dan malware sehingga jejak digitalnya sulit dilacak.

Selain itu, pelaku sering beroperasi dari lokasi yang berbeda atau bahkan luar negeri, membuat koordinasi antar aparat penegak hukum menjadi kompleks. Data nasabah yang bocor juga bisa disebarkan dalam jaringan kriminal yang luas, sehingga korban dan pelaku tidak langsung saling terhubung. Kelemahan sistem keamanan aplikasi dan kurangnya standar pengamanan ketat dari pihak bank juga mempersulit proses identifikasi dan pembuktian tindak kejahatan. Ditambah lagi, proses penyelidikan yang terkadang lambat dan birokrasi yang berbelit membuat kasus sulit diselesaikan dengan cepat. Semua hal ini menjadikan penangkapan pelaku dan pemulihan dana nasabah menjadi tantangan besar bagi aparat penegak hukum.

4. Rekomedasi dan Upaya Penanggulangan

Tiga tujuan utama dari kemitraan ini adalah untuk meningkatkan keamanan digital, menstandardisasi proses di seluruh dunia, dan memperkuat respons internasional terhadap kejahatan dunia maya. Untuk memerangi penipuan perbankan daring secara efektif, berbagai lembaga harus bekerja sama. Untuk memastikan bahwa semua bank mematuhi standar keamanan, Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI) bekerja sama untuk mengawasi dan mengatur industri perbankan.[28] Untuk lebih menjamin keamanan data dan mengawasi infrastruktur telekomunikasi, diperlukan kolaborasi dengan Kementerian Komunikasi dan Informasi (Kominfo).

Tidak ada satu lembaga pun yang dapat secara efektif memerangi kejahatan dunia maya di industri perbankan daring. Satu-satunya cara untuk mengamankan sistem dan memastikan korban memiliki perlindungan hukum adalah dengan bekerja sama dengan beberapa lembaga. Untuk menyelesaikan masalah ini, organisasi-organisasi berikut harus bekerja sama:

1. Peran Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI)

OJK berperan mengawasi penerapan sistem keamanan siber di sektor jasa keuangan,

[28] Finantier, *"Tantangan Dan Potensi Open Finance Di Indonesia"* (Katadata Insight Center, 2024).

sementara Bank Indonesia menjaga stabilitas sistem pembayaran digital. Melalui regulasi terkait enkripsi data, autentikasi, dan transaksi berbasis teknologi, BI memastikan keamanan dan kelancaran transaksi elektronik seperti mobile banking, dompet digital, dan QRIS.[29]

2. Peran Badan Siber dan Sandi Negara (BSSN)

BSSN bertugas mendeteksi potensi serangan siber seperti peretasan, malware, dan DDoS yang mengancam sistem perbankan. Lembaga ini juga memberikan rekomendasi kebijakan, pedoman tata kelola keamanan data, serta strategi mitigasi dan koordinasi antar-lembaga untuk menjaga stabilitas sektor keuangan nasional.[30]

3. Peran Kepolisian Republik Indonesia (Polri)

Polri, melalui Direktorat Tindak Pidana Siber, menangani kejahatan digital seperti pencurian data nasabah, skimming, phishing, dan peretasan sistem perbankan. Selain melakukan investigasi dan penangkapan, Polri juga berkolaborasi dengan berbagai lembaga untuk meningkatkan kesadaran masyarakat terhadap ancaman kejahatan siber.[31]

4. Peran Kejaksaan dalam proses Penegakan Hukum

Kejaksaan berperan dalam menyiapkan tuntutan hukum terhadap pelaku berdasarkan bukti yang dikumpulkan selama investigasi. Jaksa akan memastikan bahwa pelaku kejahatan siber diadili sesuai dengan peraturan perundang-undangan yang berlaku, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP).[32]

5. Kolaborasi Bank dengan Perusaahan teknologi

Bank juga dapat bekerja sama dengan perusahaan teknologi untuk mengembangkan sistem deteksi dan pencegahan kejahatan berbasis kecerdasan buatan (Artificial Intelligence/AI) dan machine learning. Teknologi ini memungkinkan bank untuk mengenali pola transaksi yang mencurigakan, seperti aktivitas yang tidak biasa dalam akun nasabah, serta memberikan peringatan dini sebelum kejahatan terjadi. Dengan demikian, risiko pencurian identitas atau akses ilegal terhadap rekening nasabah dapat diminimalkan.

6. Peran Bank BRI dalam Penanganan dan Pencegahan Kejahatan Siber

Bank BRI memiliki tanggung jawab dalam melindungi data dan dana nasabah

[29] Alfi zakki Alfarhani, "Peran Otoritas Jasa Keuangan (Ojk) Dalam Penegakan Hukum Investasi Bodong," *JURIDICA : Jurnal Fakultas Hukum Universitas Gunung Rinjani* 4, no. 1 (2022):13, 31,https://doi.org/10.46601/juridica.v4i1.213.

[30] Sukoharjo, "Waspadai Upaya Penipuan Mengatasnamakan Badan Siber Dan Sandi Negara," Sukoharjokab.go.id, 2024, https://portal.sukoharjokab.go.id/2024/06/29/waspadai-upaya-penipuan-mengatasnamakan-badan-siber-dan-sandi-negara/.

[31] Hasbuddin Khalid Annastasyia Mukrimah Yusuf, Ma'ruf Hafidz, "EfektivitasPeran Kepolisan Terhadap Penegakan Hukum Tindak Pidana Penipuan OnlineDiDuniaMaya," *Journal of Lex Philosophy (JLP)* 5, no. 1 (2024): 260–75.

[32] Ervian Ridho Mawlidy, Rieswandha Dio, and Like Lorensa, "Kemampuan Artifical Intelligence Terhadap Pendeteksian Fraud: Studi Literatur," *Akurasi : Jurnal Studi Akuntansi Dan Keuangan* 7, no. 1 (2024): 89–104, https://doi.org/10.29303/akurasi.v7i1.488.

melalui penerapan sistem keamanan digital yang baik. Dalam kasus kejahatan siber, BRI seharusnya bertanggung jawab untuk segera merespons laporan nasabah, melakukan investigasi internal, serta memberikan informasi yang dibutuhkan oleh aparat penegak hukum. Selain itu, Bank BRI juga wajib memastikan sistem mobile banking-nya mematuhi standar keamanan yang ketat, serta aktif memberikan pemberitahuan (*announcem ent*) kepada nasabah mengenai ancaman digital seperti phishing dan spoofing. Sebagai bentuk tanggung jawab, BRI juga diharapkan memberikan transparansi dalam penanganan kasus serta mendampingi nasabah selama proses hukum berlangsung.

Sebagai upaya pencegahan dan penindakan terhadap kejahatan siber seperti ini, Polri telah melakukan berbagai langkah strategis, termasuk sosialisasi kepada masyarakat, tokoh agama, dan pelajar guna meningkatkan kesadaran dan kewaspadaan publik. Di samping itu, patroli siber dilakukan selama 24 jam penuh untuk memantau aktivitas di media sosial. Polri juga menjalankan pendekatan preventif dan represif, melalui edukasi daring, penegakan hukum terhadap pelaku kejahatan digital, serta menjalin kerja antar instansi untuk memperku at sistem keamanan digital nasional.[33]

IV. KESIMPULAN

Penelitian ini menyimpulkan bahwa kejahatan penipuan dan penggelapan dana melalui layanan m-banking di Kota Medan disebabkan oleh lemahnya pengawasan lembaga keuangan, rendahnya literasi digital masyarakat, integritas individu yang rendah, serta belum memadainya regulasi yang berlaku. Temuan ini memperlihatkan bahwa infrastruktur keamanan digital yang lemah dan lambatnya respons dari bank serta aparat penegak hukum turut memperbesar risiko. Kasus seperti yang dialami oleh Buk Butet menunjukkan bagaimana pelaku dengan mudah memanfaatkan celah teknis dan kelalaian pengguna untuk melakukan pembobolan rekening.

Penanggulangan kejahatan ini menuntut strategi terpadu yang melibatkan kolaborasi antar lembaga seperti OJK, Bank Indonesia, BSSN, Kepolisian, dan Kejaksaan, serta kerja sama antara perbankan dan penyedia teknologi. Penggunaan sistem deteksi berbasis kecerdasan buatan (AI), penerapan autentikasi multi-lapis (MFA), dan edukasi digital masyarakat merupakan komponen krusial dalam pencegahan. Meskipun penelitian ini memperkaya pemahaman tentang kejahatan digital perbankan di Indonesia, cakupannya masih terbatas secara geografis. Penelitian lanjutan disarankan untuk mengeksplorasi dampak psikologis terhadap korban serta

[33] Tursinah and Fasa, "Analisis Peran Keamanan Data Dalam Meningkatkan Kepuasaan Nasabah Pada Penggunaan Mobile Banking."

mengkaji efektivitas kebijakan keamanan digital lintas wilayah dalam rangka memperkuat perlindungan konsumen secara nasional.

DAFTAR PUSTAKA

1. Buku

Edi Setiadi, Rena Yulia. *Hukum Pidana Ekonomi*. Yogyakarta: Graha Ilmu, 2010.

Finantier. *"Tantangan Dan Potensi Open Finance Di Indonesia"*. Katadata Insight Center, 2024.

Soekanto, Soerjono, and Sri Mamudji. "Penelitian Hukum Normatif Suatu Tinjauan Singkat," hlm 13. Jakarta: Raja Grafindo Persada, 2010.

2. Jurnal

Muwahid. "Metode Penemuan Hukum (Rechtsvinding) Oleh Hakim." *Al-Hukama'* 7, no. 1 (2017): 224–48. https://doi.org/10.15642/alhukama.2017.7.1.224-248.

Alfarhani, Alfi zakki. "peran otoritas jasa keuangan (ojk) dalam penegakan hukum investasi bodong."*Juridica : Jurnal Fakultas Hukum Universitas Gunung Rinjani* 4, no. 1 (2022): 13-31. https://doi.org/10.46601/juridica.v4i1.213.

Amaly, Najla, and Armiah Armiah. "Peran Kompetensi Literasi Digital Terhadap Konten Hoaks Dalam Media Sosial." *Alhadharah: Jurnal Ilmu Dakwah* 20, no. 2 (2021): 43. https://doi.org/10.18592/alhadharah.v20i2.6019.

Annastasyia Mukrimah Yusuf, Ma'ruf Hafidz, Hasbuddin Khalid. "EfektivitasPeran Kepolisan Terhadap Penegakan Hukum Tindak Pidana Penipuan Online Di Duni a Maya." *Journal of Lex Philosophy (JLP)* 5, no. 1 (2024): 260–75.

Ariyaningsih, Sindy, A. Ari Andrianto, Adri Surya Kusuma, and Rina Arum Prastyanti. "Korelasi Kejahatan Siber Dengan Percepatan Digitalisasi Di Indonesia." *Justisia: Jurnal Ilmu Hukum* 1, no. 1 (2023): 1–11. https://doi.org/10.56457/jjih.v1i1.38.

Bupu, Angela Gabriela, Karolus Kopong Medan, and Heryanto Amalo. "Analisis Yuridis Cyber Crime Pembobolan Dana Nasabah Pada Aplikasi Mobile Banking Dengan Modus Pembobolan Jalur Undangan Pernikahan Palsu." *Jurnal Ilmu Hukum Dan Sosial* 2, no. 2 (2024): 367–83. https://doi.org/10.51903/hakim.v2i2.1829.

Ivanca, Eveline, and Hery Firmansyah. "Perlindungan Hukum Pengguna Mobile Banking Sebagai Korban Kejahatan Melalui Internet Ditinjau Dari Hukum Positif." *UNES* 6, no. 2 (2023): 6166–74. https://review unes.com/https://creativecommons.org/licenses/by/4.0/.

Mawlidy, Ervian Ridho, Rieswandha Dio, and Like Lorensa. "Kemampuan Artifical Intelligence Terhadap Pendeteksian Fraud: Studi Literatur." *Akurasi : Jurnal Studi Akuntansi Dan Keuangan* 7, no. 1 (2024): 89–104. https://doi.org/10.29303/akurasi.v7i1.488.

mazmur rumapea, dewi ervina suryani, sonya arini batu bara. "Upaya Penanggulangan Tindak Pidana Penggelapan Pada Koperasi Kredit." *Jurnal Ilmu Hukum Prima* 11, no. 1 (2019): 1–14.

Nugroho, Harya, Mohamad Nur Ihsan, Annisa Haryoko, Fauzan Màarif, and Fatiya Alifah. "Edukasi Keamanan Digital Untuk Meningkatkan Kewaspadaan Masyarakat Terhadap Link Phising." *Jurnal Pengabdian Masyarakat Multidisiplin (ECOS-PRENEURS)* 1, no. 2 (2023): 28–40.

Pakpahan, Elvira Fitriyani, Lionel Ricky Chandra, and Ananta Aria Dewa. "Perlindungan Hukum Terhadap Data Pr ibadi Dalam Industri Financial Technology." *Veritas et Justitia* 6, no. 2 (2020): 298–323.

https://doi.org/10.25123/vej.3778.

Prastiwi, Yuyun, Erico Yuan Varel, and Holland Nainggolan. "Analisis Keamana n Data Pribadi Dalam Aplikasi Mobile " Dana "," 2024, 584–88.

Rantesalu, Harianto. "Penanggulangan Kejaha tan Penipuan Belanja Online Di Wilayah Kepolisian Daerah Jawa Timur." *Janaloka* 1, no. 2 (2022): 70–94.

Shaleha, Mar'ah. "Tinjauan Kriminologis Fenomena Penggunaan Senjata Tajam Oleh Anak Di Kabupaten Bantaeng." *FIS Universitas Negeri Makassar* 5, no. 2 (2018): 1–12.

Solim, Jevlin, Mazmur Septian Rumapea, Agung Wijaya, Bella Monica Manurung, and Wendy Lionggodinata. "Upaya Penanggulangan Tindak Pidana Penipuan Situs Jual Beli Online Di Indonesia." *Jurnal Hukum Samudra Keadilan* 14, no. 1 (2019): 97–110. https://doi.org/10.33059/jhsk.v14i1.1157

Sukartara, Nirwansyah, M. Rifqi Ramadhona, Eka Syafrina Monika, Akbar Idaman, and Tar Muhammad Raja Gunung. "Optimalisasi Literasi Digital Sebagai Upaya Menanggulangi Hoax Dan Pembangunan Masyarakat Kritis Pada Perkumpulan Pemuda Pemudi Kampung Sejahtera." *Indonesian Journal of Emerging Trends in Community Empowerment* 2, no. 1 (2024): 29–34. https://ejournal.pabki.org/index.php/ETCE/article/view/26.

Tursinah, Mar'atun, and Muhammad Iqbal Fasa. "Analisis Peran Keamanan Data Dalam Meningkatkan Kepuasaan Nasabah Pada Penggunaan Mobile Banking." JIEMAS, 2024, 481–86.

Yudiantara, Komang Maysa Surya Aditya I Gusti Ngurah Nyoman Krisnadi. "Analisis Kriminologi Dalam Tindak Pidana" 3, no. 2 (2025).

Zahwani[1], Syfa Tasya, Muhammad Irwan, and Padli Nasution[2]. "Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi Di Era Digital." *Analisis Kesadaran Masyarakat (Zahwani, Dkk.) JoSES: Journal of Sharia Economics Scholar* 2, no. 2 (2023): 105–9. https://doi.org/10.5281/zenodo.12608751.

3. Disertasi/Skripsi

Gusti, F. A. "Kelalaian Bank Dalam Menjaga Rahasia Bank Pada Perjanjian Baku Terhadap Tindakan Phising Yang Dialami Nasabah Akibat Social Engineering Ditinjau Dari Hukum Positif Indonesia (Doctoral Dissertation)." *FAKULTAS HUKUM UNIVERSITAS PASUNDAN*, 2023.

4. Website

Kepolisian Daerah Sumatera Utara. "Banyakn ya Peristiwa Kejahatan/Pelanggaran Yan g Dilaporkan Menurut Jenis Kejahatan/P elanggaran, 2019-2021." *Badan Pusat Statistik SUmatera Utara*. Vol. 75, 2021.

Muhammad Raihan Nugraha. "Perbedaan Pasal Penipuan Dan Penggelapan." Hukum Online, 2024. https://www.huku monline.com/klinik/a/pasal-penipuan-dan-penggelapan-lt4ceb3048897ea/.

PARBOABOA. "Rekening Nasabah BRI Di Medan Dibobol, Uang Raib Hingga Rp 112 Juta: Hampir Setahun Kasus Dilaporkan, Tak Ada Kejelasan." TIM PARBOABOA, 2022. https://parboaboa.com/kasus-rekening-nasabah-bri-di-medan-yang-dibobol-tak-kunjung-selesai?

Polda Sumut. "Perkuat Penanganan Kejahatan Siber, Polda Sumut Kini Punya Direktorat Reserse Siber." Heta News, 2024. https://www.hetanews.com/article/291301/perkuat-penanganan-kejahatan-siber-polda-sumut-kini-punya-direktorat-reserse-siber.

Renata Christha Auli. "Bunyi Dan Unsur Pasal 378 KUHP Tentang Penipuan." Hukum Online, 2023. https://www.hukumonline.com/klinik/a/pasal-378-kuhp-tentang-penipuan-lt6571693c4c627/.

Sukoharjo. "Waspadai Upaya Penipuan Mengatasnamakan Badan Siber Dan

Sandi Negara." Sukoharjokab.go.id, 2024. https://portal.sukoharjokab.go.id/2024/06/29/waspadai-upaya-penipuan-mengatasnamakan-badan-siber-dan-sandi-negara/.

Tim redaksi tempo. "Kenali 5 Modus Kejahatan Mobile Banking Dan Cara Menghindarinya." Tempo, 2023. https://www.tempo.co/digital/kenali-modus-kejahatan-mobile-banking-dan-cara-menghindarinya-187128.