ISSN (P): (2580-8656)
ISSN (E): (2580-3883)

LEGAL STANDING
JURNAL ILMU HUKUM

Vol.8 No.1, April 2024

ANALISA *CYBERCRIME* PENCURIAN DATA PRIBADI MODUS APLIKASI PINJAMAN ONLINE DAN *DIGITAL BANKING*

***Evan Sugiarto[1], Vincentius Oscar[2], Dewi Sartika Simanungkalit[3]**
[1,2,3]Universitas Wijaya Kusuma Surabaya, Jl. Dukuh Kupang XXV No.54, Surabaya, Jawa Timur, Indonesia
*evan.sugiarto@gmail.com

ABSTRACT

These technological advances have resulted in tremendous efficiency for the economy. Financial institutions have changed approaches and practices. His financial business. However, rapid technological progress has resulted in negative consequences, such as an increase in more sophisticated cyber crimes. This research aims to examine technology-based crimes involving data theft using online lending and digital banking modes. This research uses a normative juridical type with data collection using literature studies, as well as correlative analysis. The results of this research show that criminals collaborate with financial service institutions. Using sophisticated information technology and computers to steal client online loan application data. Financial service institutions usually only commit document falsification, embezzlement and corruption as victims. Efforts to prevent these crimes include the ITE Law which regulates formal cyber crimes.

Kemajuan teknologi ini telah menghasilkan efisiensi yang luar biasa bagi ekonomi. Lembaga keuangan telah mengubah pendekatan dan praktik. Bisnis keuangannya. Namun, kemajuan teknologi yang begitu cepat telah menghasilkan konsekuensi negatif, seperti peningkatan kejahatan *cyber* yang lebih canggih. Penelitian ini bertujuan untuk meneliti kejahatan berbasis teknologi pencurian data dengan modus pinjaman online dan *digital banking*. Penelitian ini menggunakan jenis *yuridis normative* dengan pengumpulan data secara studi pustaka, serta analisis korelatif. Hasil penelitian ini menunjukkan bahwa pelaku kejahatan bekerja sama dengan lembaga jasa keuangan. Menggunakan kecanggihan teknologi informasi dan komputer untuk mencuri data aplikasi pinjaman online klien. Lembaga jasa keuangan biasanya hanya melakukan pemalsuan dokumen, penggelapan, dan korupsi sebagai korban. Upaya pencegahan tindak pidana kejahatan ini yaitu dengan UU ITE yang mengatur tindak pidana *cyber formil*.

Kata Kunci: *Cybercrime, Pencurian Data, Pinjaman Online, Digital Banking.*

A. PENDAHULUAN

Lembaga jasa keuangan merupakan suatu lembaga ekonomi yang menyalurkan bantuan berupa dana kepada masyarakat guna untuk menunjang kelangsungan hidupnya. Sebagai wadah perputaran uang, lembaga sering dijumpai penyalahgunaan wewenang, baik oleh pihak dalam maupun luar lembaga untuk menutupi kejahatannya (Melati, 2023; Purnama et al., 2020; Sari, 2019). Oleh sebab itu diperlukan sistem

keamanan yang tidak hanya berkaitan dengan SDM saja, akan tetapi juga infrastruktur yang memadai (Raden et al., 2023; Takalamingan, 2021).

Kejahatan yang terjadi di era sekarang ini didukung oleh perkembangan teknologi yang semakin berkembang pesat sehingga dinamai dengan kejahatan elite karena hanya bisa dilakukan oleh orang-orang tertentu. Dengan perkembangan IPTEK ini kejahatan kelas elite ini hanya membutuhkan tenaga yang sedikit dan mengandalkan pola pikir. Dengan pola pikir ini para penjahat memanfaatkan media-media teknologi yang sudah berkembang pesat dan tersebar luas di seluruh dunia sehingga berakibat munculnya kejahatan komputer (*cybercrime*) (Curry, 2023; Febriansyah et al., 2023).

Istilah *cybercrime* merujuk menunjukkan hubungan pada tindakan kejahatan dengan menggunakan media teknologi yang terjadi di dunia maya. sederhananya *cybercrime* merupakan aktivitas kejahatan dengan memanfaatkan media teknologi seperti komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan (Fissel & Lee, 2023). *Cybercrime* ini memiliki banyak bentuknya, seperti penipuan aplikasi peminjaman online, pemalsuan cek, lelang online, dan yang semisalnya. Indonesia sendiri tercatat sebagai salah satu negara yang mengalami *cybercrime* paling banyak (Hapsari & Pambayun, 2023).

Contoh *cybercrime* yang sering terjadi di dalam lembaga jasa keuangan yang menggunakan sarana internet dan berbasis sistem transaksi adalah jasa pinjaman dana online. Penipuan pinjaman dana online ini biasanya diawali dengan *carding*, yaitu pelaku *carding* memperoleh data aplikasi pinjaman online korban secara ilegal dan kemudian menggunakan aplikasi pinjaman online tersebut untuk berbelanja online (*forgery*). Indonesia sendiri termasuk negara yang sering terjadi kasus seperti ini meskipun secara data Indonesia berada di posisi kedua terendah se-Asia Tenggara. Sedangkan berdasarkan data Visa, Indonesia menduduki posisi ketiga terendah se-Asia Tenggara. Menurut data terakhir yang sudah dikumpulkan oleh OJK (Otoritas Jasa Keuangan Indonesia) telah tercatat banyak tindak kejahatan pembobolan (*fraud*) yang merugikan negara (OJK, 2023; Sulisrudatin, 2014).

Direktur kriminal umum polda metro jaya kombes pol Khrisna Murti pernah berhasil menangkap pelaku penipuan aplikasi pinjaman online yang berhasil menggasak uang dari lembaga jasa keuangan swasta melalui aplikasi pinjaman dana online korban sebanyak ratusan juta (Agustina, 2021; Mansur & Yulianto, 2022; Rassat, 2022). Modus yang digunakan yaitu dengan membeli data daftar nasabah pemegang aplikasi pinjaman online tersebut dari pihak *marketing*. Kemudian pelaku kejahatan tersebut menghubungi nomor telepon para nasabah dan mengaku dari pusat lembaga pinjaman online tersebut. Kemudian pelaku menjelaskan sesuatu dan menggunting aplikasi pinjaman online korban dengan modus akan diganti dengan aplikasi yang terbaru dengan tambahan limit yang lebih besar. Para korban juga dimintai foto KTP guna untuk menyesuaikan identidas atau identitas dari pemilik aplikasi pinjaman online tersebut. Dengan adanya aplikasi pinjaman dana online milik nasabah beserta KTP nasabah tersebut, para pelaku

menggunakannya untuk melakukan transaksi di toko untuk membeli barang-barang mewah. Akibat dari perbuatannya tersebut tersangka dikenai sanksi sesuai dengan Passal 379 dan Pasal 362 KUHP dengan ancaman hukuman penjara paling lama 4 dan 5 tahun.

Beberapa penelitian terdahulu, perlindungan hukum terhadap korban penyalahgunaan data pribadi pada aplikasi pinjaman online (Nurfadilah et al., 2023), perlindungan hak keamanan data pribadi konsumen pinjaman online dana cair (Anwar & Kerti, 2022), perlindungan hukum terhadap penyalahgunaan data pribadi pada aplikasi pinjaman online ilegal menurut undang-undang no 27 tahun 2022 tentang perlindungan data pribadi (Muzakkie & Juarsa, 2023), pentingnya perlindungan data pribadi dalam transaksi pinjaman online (Priliasari, 2019), perlindungan terhadap korban pencurian data pribadi melalui media digital (Triadi, 2023) dan masih banyak lagi penelitian serupa, namun berdasarkan hal tersebut, belum ada yang berfokus pada kejahatan yang menyangkut *cybercrime*, sehingga menjadi keunikan dalam penelitian ini.

B. METODE

Penelitian ini dilaksanakan menggunakan model penelitian yuridis normatif, yaitu penelitian dengan melakukan analisis bahan hukum primer, bahan hukum sekunder dan tersier secara normative dengan pendekatan konseptual dan PERPU. Konsep ini menganggap hukum identik dengan standar perundang-undangan. Mereka yakin bahwa hukum adalah sistem normatif yang mandiri, tertutup, dan terpisah dari masyarakat. Data pada penelitian ini dikumpulkan secara studi pustaka, yakni mengumpulkan data dengan mencari dan menelaah bahan pustaka seperti jurnal ilmiah, majalah, artikel ilmiah, ataupun penelitian-penelitian terdahulu. Kemudian data yang telah diperoleh dianalisis secara kualitatif, yakni menghasilkan data deskriptif dari objek yang diteliti yaitu Undang-Undang Nomor 27 Tahun 2022. Data yang diperolehdikorelasi untuk menggambarkan secara sistematis mengenai penegakkan dan perlindungan hukum terkait data pribadi dan pencurian data pribadi melalui media sosial. Hasil analisis korelatif ditarik ke dalam pembahasan yang lebih khusus mengenai perlindungan hukum dalam pencurian data pribadi melalui media social (Ibrahim, 2013; Rideng, 2013).

C. HASIL DAN PEMBAHASAN

Pengertian kejahatan di bidang lembaga jasa keuangan sangat luas dan mencakup kejahatan apapun yang berhubungan dengan lembaga jasa keuangan, seperti memeriksa lembaga jasa keuangan atau transfer rekening secara tidak sah. Namun kejahatan lembaga jasa keuangan adalah tindakan yang dilarang oleh undang-undang lembaga jasa

keuangan, seperti mendirikan lembaga jasa keuangan ilegal dan pembocoran rahasia lembaga keuangan.

Karena hanya mencakup tindak pidana yang dilakukan oleh orang yang berada di dalam atau di luar lembaga jasa keuangan, tindak pidana di bidang lembaga jasa keuangan tampaknya lebih netral dan lebih luas. Tindak pidana lembaga jasa keuangan tidak didefinisikan oleh UU No. 10 Tahun 1998; itu hanya mengkategorikan beberapa pelanggaran yang termasuk ke dalam kategori kejahatan dan di satu sisi dapat dianggap sebagai pelanggaran. Namun, ada beberapa peraturan yang membedakan tindak pidana lembaga jasa keuangan dengan tindak pidana di bidang lembaga jasa keuangan.

Lembaga keuangan dapat berperan sebagai korban atau pelaku dalam tindak pidana. Institusi keuangan dapat bertindak sebagai korban penipuan, pemalsuan dokumen, atau pelaku. Untuk mengetahui apakah seseorang atau perusahaan menjadi korban, mereka terlebih dahulu harus mengetahui perbuatan apa yang dianggap sebagai kejahatan atau tindak pidana. Perbuatan pidana yang telah diatur oleh hukum dan dapat dikategorikan sebagai kejahatan lembaga jasa keuangan adalah; pertama, pasal 244, 245, 246, 249, dan 250 KUHP; kedua, UU No. 7 tahun 1992 dan UU No 10 tahun 1998; dan ketiga, tindak pidana yang diatur dalam UU tentang lembaga jasa keuangan sentral.

Cybercrime menggunakan teknologi internet jelas sangat membantu menyelesaikan masalah yang kompleks. Namun, kemajuan teknologi ini juga dapat mendorong orang untuk melakukan hal-hal yang tidak etis. *Cybercrime* adalah salah satu dimensi baru dari kejahatan modern yang mendapat perhatian luas di seluruh dunia. Dalam arti sempit, *cybercrime* mencakup semua jenis kejahatan yang ditujukan pada komputer, jaringan komputer, dan penggunaannya. Dengan demikian, *cybercrime* meliputi kejahatan yang dilakukan:

1. *By means of a computer system or network*, yaitu dengan sarana dari sistem ataupun jaringan komputer.
2. *In a computer system or network*, yaitu dengan sistem atau jaringan yang ada dalam komputer itu sendiri.
3. *Against a computer system or network*, yaitu terhadap sistem atau jaringan komputer tersebut.

Tempat-tempat berikut dapat menjadi sasaran *cybercrime* dalam operasi lembaga jasa keuangan. Seperti layanan pembayaran dengan aplikasi pinjaman online pada situs-situs tertentu dan layanan lembaga jasa keuangan online (online lembaga jasa keuanganing). Menurut aktivitasnya, dapat diketahui bahwa *cybercrime* memiliki beberapa jenis, yaitu sebagai berikut:

1. *Carding*, yaitu berbelanja menggunakan identitas dan nomor aplikasi pinjaman orang lain yang dicuri secara ilegal, biasanya melalui pencurian data online.
2. *Hacking*, yaitu mengambil alih program komputer orang lain atau pihak lain.

3. *Cracking*, yaitu hacking dengan maksud jahat. "Hacker bertopi hitam" adalah sebutan lain untuk "*cracker*". Berbeda dengan "*carder*", yang hanya melihat aplikasi pinjaman online, "*cracker*" melihat simpanan klien di berbagai lembaga jasa keuangan.
4. *Defacing*, yaitu mengubah halaman web pihak lain.
5. *Phising*, yaitu upaya untuk memaksa pengguna komputer (user) untuk memberikan data pribadi mereka (username dan password) pada website yang telah dimodifikasi. Pengguna layanan keuangan online biasanya ditargetkan untuk phising.
6. *Spamming*, yaitu pengiriman iklan atau berita melalui surat elektronik (e-mail) yang tidak diinginkan.
7. *Malware*, yaitu program komputer untuk membobol operating system.

Namun, berdasarkan modus operandinya, cybercrime terbagi menjadi:

1. *Unauthorized Access to Computer System and Service*, kesalahan yang dilakukan dengan masuk ke sistem jaringan secara ilegal tanpa diketahui.
2. *Illegal Contents*, merupakan pelanggaran memasukkan data atau informasi yang tidak benar atau tidak etis ke Internet, seperti menyebarkan informasi palsu atau fitnah yang dapat merusak martabat atau harga diri seseorang.
3. *Data Forgery*, memalsukan data pada dokumen penting, seperti dokumen tanpa skrip di Internet.
4. *Cyber Espionage*, merupakan pelanggaran yang melakukan kegiatan mata-mata terhadap orang lain dengan memanfaatkan jaringan Internet.
5. *Cyber Sabotage and Extortion*, biasanya kejahatan ini dilakukan dengan menyusupkan virus.
6. *Offense Against Intellectual Property*, kejahatan ini merusak hak kekayaan intelektual pihak lain di internet. Sebagai contoh, menampilkan konten pada situs web yang dimiliki oleh orang lain secara ilegal, menyebarkan informasi di Internet yang ternyata merupakan rahasia dagang orang lain.
7. *Infringements of Privacy*, kejahatan ini biasanya berfokus pada informasi pribadi yang disimpan dalam komputer.

1. Modus Pencurian Data Aplikasi Pinjaman Online

Secara umum pencurian data aplikasi pinjaman online ini dapat diketahui dengan ciri-ciri: Pertama tanpa menggunakan kekerasan, kedua sedikit kontak tubuh, ketiga menggunakan teknologi, keempat memanfaatkan jaringan telematika. Lembaga jasa keuangan biasanya dapat dilihat pada KUHP pasal 263, 264, dan 378 sebagai korban, tetapi sebagai pelaku, undang-undang lembaga jasa keuangan.

Lembaga jasa keuangan biasanya hanya melakukan pemalsuan dokumen, penggelapan, dan korupsi sebagai korban. Mereka yang melakukannya biasanya individu, bukan korporasi, dan modus operandinya beragam. Kejahatan ini selalu dilakukan secara sistematis dan termasuk dalam kategori kriminal lembaga jasa keuangan.

Dalam sistem layanan yang pertama, pelanggaran yang dikenal sebagai *carding* harus diwaspadai. Prosesnya adalah sebagai berikut: pelaku *carding* mengambil data aplikasi pinjaman online korban secara ilegal dan menggunakannya untuk berbelanja di toko online. Sistem autentikasi yang digunakan untuk memastikan bahwa orang yang membeli barang di toko online adalah orang yang benar dapat menyebabkan modus ini terjadi. Lembaga keuangan online adalah kegiatan yang kedua.

Di Indonesia, modus operandi yang disebut "*typosite*" menggunakan kesalahan pelanggan yang salah menulis alamat web perusahaan keuangan online yang mereka inginkan. Pelaku membuat situs web palsu yang mirip dengan situs web asli perusahaan keuangan online. Jika pelanggan salah ketik dan masuk ke situs web palsu, pelaku akan merekam ID dan password pelanggan untuk mengakses situs web yang sebenarnya, yang pada gilirannya akan berdampak negatif pada pelanggan. Adapun contoh cara kerja modus pencurian data aplikasi pinjaman online yaitu:

a. Membeli data nasabah senilai 20.000 rupiah dari oknum.
b. Pelaku kemudian menghubungi setiap pelanggan aplikasi pinjaman melalui telepon menggunakan identitas lembaga jasa keuangan dan mengatakan bahwa mereka akan menawarkan *upgrade*.
c. Kemudian jika disetujui pelaku akan mendatangkan kurir.
d. Kemudian setelah kurir datang mereka akan meminta data lengkap korban.
e. Setelah itu selesai, si pelaku akan membuat duplikat kartu kredit korban dan kembali ke rumah korban untuk memberikan kartu kredit baru. Kemudian, si pelaku akan mengedit kartu kredit korban agar terlihat lebih percaya.
f. Mereka mengambil kartu kredit palsu, tetapi yang asli sudah mereka bawa.

Pelaku kemudian menggunakan data ini untuk melakukan transaksi atas nama pelanggan. Metode yang paling umum digunakan pelaku pencurian data korban biasanya pelaku menelpon korban untuk memperbarui data kartu kredit korban sebagai perwakilan dari bank, atau bisa dengan membuat situs belanja online palsu dan skimming yaitu penyalin data pada mesin ATM atau mesin EDC dengan alat tertentu.

2. Upaya Pencegahan Tindak Pidana

Kriminalitas, juga dikenal sebagai tindak pidana, adalah perbuatan yang menyebabkan penderitaan dan harus dicegah atau ditanggulangi. Meskipun

demikian, langkah-langkah yang diambil untuk mencegah atau menangani kejahatan tidaklah mudah atau sama untuk setiap kejahatan. Misalnya, tindak pidana yang berkaitan dengan lembaga jasa keuangan tidak dapat dicegah atau ditangani dengan cara yang biasa digunakan untuk tindak pidana. Dalam kebanyakan kasus, pihak interent atau pihak afiliasi lembaga keuangan terlibat dalam pembobolan lembaga keuangan. Karena memiliki karakteristik yang membedakan mereka dari tindak pidana lain, tindak pidana yang melibatkan lembaga jasa keuangan harus dicegah dan ditangani dengan cara yang berbeda. Oleh karena itu, hambatan terus muncul dalam upaya mencegah dan menanggulangi kejahatan yang berkaitan dengan lembaga jasa keuangan. Penanganan tindak pidana lembaga jasa keuangan menghadapi beberapa hambatan, diantaranya tidak ada kesepakatan tentang penggunaan dokumen fotokopi sebagai barang bukti dan penetapan undang-undang yang melanggar tindak pidana lembaga jasa keuangan, tingkat pemahaman penegak hukum tentang operasi dan kegiatan lembaga jasa keuangan yang berbeda yang tidak seragam dan tidak terkoordinasi, dan lemahnya tingkat keberhasilan penyelidikan kasus oleh penyidik.

Kebijakan kriminal dapat melakukan pencegahan serta penanggulangan tindak pidana dengan dua cara: kebijakan kriminal atau kebijakan non-kriminal. Politik hukum lebih menekankan upaya represif penegak hukum yang dilakukan sebelum undang-undang ada. Polisi, jaksa, hakim, dan tentu saja lembaga keuangan Indonesia bertanggung jawab atas pelanggaran administrasi. Namun, kebijakan non-hukum dilakukan oleh aparat penegak hukum, lembaga keuangan Indonesia, lembaga keuangan pemerintah dan swasta, dan masyarakat. Di Indonesia, definisi "tindak pidana *cyber*" didefinisikan secara luas dan sempit. Secara umum, tindak pidana yang menggunakan sarana atau dengan bantuan Sistem Elektronik dianggap sebagai tindak pidana *cyber*. Ini berarti bahwa setiap tindak pidana konvensional yang tercantum dalam Kitab Undang-Undang Hukum Pidana (KUHP), termasuk pembunuhan dan perdagangan orang, dapat termasuk dalam kategori tindak pidana *cyber* dalam arti luas.

Selain itu, ada tindak pidana seperti UU Transfer Dana Nomor 3 Tahun 2011, tindak pidana lembaga jasa keuangan, dan tindak pidana pencucian uang. Namun, UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mengatur tindak pidana *cyber* dalam arti yang lebih sempit.

a. Tindak pidana yang berhubungan dengan aktivitas illegal, yaitu:
    1) Pasal 27 ayat 1-4 UU ITE, Pasal 28 ayat 1-2 UU ITE, dan Pasal 29 UU ITE, terkait penyebaran, transmisi ilegal.
    2) Pasal 30 UU ITE terkait akses ilegal.
    3) Pasal 31 UU ITE terkait intersepsi informasi atau dokumen secara ilegal.
b. Tindak pidana yang berhubungan dengan gangguan (*interferensi*), yaitu:

1) Pasal 32 UU ITE, terkait gangguan terhadap informasi dan e-dokumen.
2) Pasal 33 UU ITE, terkait gangguan terhadap sistem.

c. Pasal 34 UU ITE, terkait memfasilitasi kejahatan.
d. Pasal 35 UU ITE, pemalsuan dokumen atau informasi.
e. Pasal 36 UU ITE, pidana tambahan.
f. Pasal 52 UU ITE, perberatan terhadap ancaman pidana.

Sebagaimana diketahui, UU ITE mengatur tindak pidana *cyber formil*, terutama selama penyidikan. Menurut Pasal 42 UU ITE, ketentuan tentang penyidikan dalam Undang-Undang No. 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP) berlaku untuk penyidikan terhadap tindak pidana yang diatur dalam UU ITE, sepanjang tidak diatur dengan cara lain dalam UU ITE. Khususan UU ITE untuk penyidikan termasuk, tetapi tidak terbatas pada, hal-hal berikut:

a. Penyidik yang menangani tindak pidana *cyber* berasal dari kepolisian atau Kementerian Komunikasi dan Informatika.
b. Penelitian dilakukan dengan mempertimbangkan perlindungan privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data.
c. Dengan izin ketua pengadilan negeri setempat, sistem elektronik yang terkait dengan dugaan tindak pidana harus diselidiki dan disita.
d. Penyidik harus memastikan bahwa kepentingan pelayanan umum terpelihara selama penggeledahan dan penyitaan sistem elektronik.

Untuk penyidikan tindak pidana *cyber* secara keseluruhan, ketentuan penyidikan UU ITE berlaku. Sebagai contoh, sebelum penggeledahan atau penyitaan server lembaga jasa keuangan, penyidik harus memastikan kelancaran layanan publik dan mempertahankan kepentingan pelayanan umum yang diatur dalam UU ITE. Jika mematikan server lembaga jasa keuangan akan mengganggu layanan publik, hal itu tidak boleh dilakukan. Peraturan pelaksana UU ITE dan peraturan teknis penyidikan instansi penyidik merupakan landasan dalam penanganan kasus *cybercrime* di Indonesia. Pencegahan dan penanggulangan kejahatan akan lebih efektif jika dikaitkan langsung dengan ciri-ciri khusus tindak pidana daripada hanya melakukan upaya hukum yang seringkali bersifat represif.

Tindak pidana yang melibatkan lembaga jasa keuangan dapat dicegah secara lebih dini melalui penilaian yang tepat dari bidang ini. Secara khusus, disebutkan bahwa tindakan yang harus diambil untuk penegakan hukum dan pencegahan pelanggaran oleh lembaga jasa keuangan adalah:

a. Kemampuan penyidik *akunting* dan keuangan harus ditingkatkan.

b. Sistem pengawasan lembaga keuangan yang efektif dapat dicapai jika rekruitmen karyawan lebih berfokus pada psikologi.

c. Dalam melakukan pekerjaannya, penyidik harus memiliki keahlian yang luas, bukan hanya dalam hal rahasia lembaga jasa keuangan.

d. Undang-undang yang mengatur lembaga jasa keuangan harus diubah.

Namun, UU ITE berfungsi sebagai dasar untuk penegakan hukum terhadap kejahatan maka harus: *Pertama*, tanggung jawab penyelenggara sistem elektronik harus dibatasi agar tidak melampui kapasitas. *Kedua*, semua tanda tangan dan informasi elektronik yang dibuat oleh sistem informasi harus dapat digunakan sebagai bukti di pengadilan. *Ketiga*, diperlukan perlindungan hukum untuk lembaga jasa keuangan sentral dan lembaga lainnya. *Keempat*, perlu ada ancaman pidana yang mencegah tindak kejahatan elektronik (*cybercrime*) yang sesuai dan membuat jera.

D. SIMPULAN

Selama ini, kejahatan pencurian data aplikasi pinjaman online dilakukan oleh oknum-oknum yang memahami mekanisme transaksi dan teknis jaringan lembaga jasa keuangan yang dituju sebagai objek pembobolan, sehingga ada pihak terafiliasi (pihak dalam lembaga jasa keuangan) yang turut andil dalam pencurian data aplikasi pinjaman online. Pencurian data aplikasi pinjaman online ini memanfaatkan. Kejahatan lembaga keuangan merupakan ancaman besar terhadap kesehatan lembaga keuangan dan kepercayaan masyarakat, sehingga perlu dilakukan pencegahan segera. Karena sifat unik dari kegiatan lembaga jasa keuangan, semua pihak yang terlibat harus bekerja sama. Kejahatan lembaga jasa keuangan tidak dapat dilakukan hanya oleh satu pihak penegakan hukum. Akibatnya, bukan hanya masalah simptomatik atau kausatif yang dapat diatasi, tetapi masalah yang lebih luas dan dapat diatasi secara keseluruhan. Dalam kasus ini, pemerintah harus melakukan tindakan tegas dan hukuman yang berat terhadap pelaku dan mewajibkan mereka untuk mengganti semua kerugian yang dialami oleh lembaga jasa keuangan dan nasabahnya. Ini akan membuat orang lain berhenti melakukan kejahatan serupa.

E. DAFTAR RUJUKAN

Agustina, D. (2021). *Cerita Brigjen Krishna Murti dan Wakil Gubernur Diteror Pinjol Ilegal Meski Tak Pernah Pinjam Uang*. Tribunnews.Com. https://www.tribunnews.com/nasional/2021/10/31/cerita-brigjen-krishna-murti-dan-wakil-gubernur-diteror-pinjol-ilegal-meski-tak-pernah-pinjam-uang

Anwar, A., & Kerti, N. G. N. (2022). Perlindungan Hak Keamanan Data Pribadi Konsumen Pinjaman Online Dana Cair. *Reformasi Hukum Trisakti*, *4*(5), 1227–1240. https://doi.org/10.25105/refor.v4i5.15130

Curry, T. (2023). Cybercrime Perpetration Theories. In *Oxford Research Encyclopedia of*

Criminology and Criminal Justice. https://doi.org/10.1093/acrefore/9780190264079.013.787

Febriansyah, F. I., Indiantoro, A., & Ikhwan, A. (2023). Model Kejahatan Dunia Maya (Cybercrime) Sebagai Upaya Pembentukan Hukum Nasional. *Legal Standing : Jurnal Ilmu Hukum*, *7*(2), 183–196. https://news.detik.com/berita/d-3567290/polling-58-masyarakat-puas-kinerja-kpk,

Fissel, E., & Lee, J. (2023). The Cybercrime Illusion: Examining the Impact of Cybercrime Misbeliefs on Perceptions of Cybercrime Seriousness. *Journal of Criminology*, *56*(2), 263380762311746. https://doi.org/10.1177/26338076231174639

Hapsari, R., & Pambayun, K. G. (2023). Ancaman Cybercrime di Indonesia: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*, *5*(1), 1–17. https://doi.org/10.33701/jk.v5i1.3208

Ibrahim, J. (2013). *Teori dan Metodologi Penelitian Hukum Normatif*. Bayumedia Publishing.

Mansur, A., & Yulianto, A. (2022). *Ditreskrimsus Polda Metro Jaya Bekuk Lima Orang Terkait Pinjol*. Republika.Co.Id. https://news.republika.co.id/berita/rdioac396/ditreskrimsus-polda-metro-jaya-bekuk-lima-orang-terkait-pinjol

Melati, P. (2023). Perlindungan Hukum Terhadap Konsumen Lembaga Jasa Keuangan Berdasarkan Peraturan NO. 1/POJK.07/2013. *Journal Civics and Social Studies*, *7*(1), 101–106. https://doi.org/10.31980/civicos.v7i1.2981

Muzakkie, S., & Juarsa, E. (2023). Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Pada Aplikasi Pinjaman Online Ilegal Menurut Undang-Undang No 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Bandung Conference Series: Law Studies*, *3*(2), 984–987. https://doi.org/10.29313/bcsls.v3i2.7284

Nurfadilah, N., Diab, A., & Djaoe, A. (2023). Perlindungan Hukum Terhadap Korban Penyalahgunaan Data Pribadi Pada Aplikasi Pinjaman Online. *FAWAID: Sharia Economic Law Review*, *4*(2). https://doi.org/10.31332/flr.v4i2.4424

OJK. (2023). *Siaran Pers: OJK Minta Bank Blokir 85 Rekening Pinjol Ilegal*. Ojk.Go.Id. https://ojk.go.id/id/berita-dan-kegiatan/siaran-pers/Pages/OJK-Minta-Bank-Blokir-85-Rekening-Pinjol-Ilegal.aspx

Priliasari, E. (2019). Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online. *Majalah Hukum Nasional*, *49*(2), 1–27. https://doi.org/10.33331/mhn.v49i2.44

Purnama, R., Siregar, E., Sintha, L., & Tobing, F. (2020). Peningkatan Literasi Terhadap Lembaga Jasa Keuangan Bank Pada Masyarakat Kelurahan Cawang Jakarta Timur. *Jurnal ComunitÃ Servizio*, *2*(2), 429–436. https://doi.org/10.33541/cs.v2i2.1938

Raden, M., Jatmika, B., & Hasya, S. (2023). Tindak Pidana Penyuapan Dalam Pemberian Fasilitas Kredit Bank Yang Diterapkan Melalui Pengawasan Lembaga Otoritas Jasa Keuangan. *Padjadjaran Law Review*, *11*(2), 226–237. https://doi.org/10.56895/plr.v11i2.1413

Rassat, F. S. (2022). *Polda Metro sebut pimpinan pinjaman online ilegal berada di luar*

negeri. Antaranews.Com. https://lampung.antaranews.com/berita/630697/polda-metro-sebut-pimpinan-pinjaman-online-ilegal-berada-di-luar-negeri

Rideng, I. W. (2013). Metode Penelitian Hukum Normatif. *Kertha Widya*.

Sari, A. (2019). Peran Otoritas Jasa Keuangan Terhadap Pengawasan Lembaga Keuangan Di Indonesia. *Jurnal Gagasan Hukum*, *1*(2), 177–188. https://doi.org/10.31849/jgh.v1i02.7698

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

Takalamingan, F. (2021). Peran Otoritas Jasa Keuangan Dalam Melakukan Pengawasan Dan Pencegahan Terhadap Pendirian Perusahaan Investasi Ilegal Di Tinjau Dari Undang-Undang Nomor 21 Tahun 2011. *Lex Et Societatis*, *9*(1). https://doi.org/10.35796/les.v9i1.32052

Triadi, M. (2023). Perlindungan Terhadap Korban Pencurian Data Pribadi Melalui Media Digital. *REUSAM: Jurnal Ilmu Hukum*, *11*(1), 45. https://doi.org/10.29103/reusam.v11i1.10178