Das Sollen: Jurnal Kajian Kontemporer Hukum dan Masyarakat (2023) 02:02, 1-25
ISSN 1111-1111 | DOI: 10.11111/dassollen.xxxxxxx
Diterbitkan oleh FORIKAMI (Forum Riset Ilmiah Kajian Masyarakat Indonesia)
Tersedia online Pada Bulan Juni 2024.

Implementasi Pasal 362 KUHP dan Pasal 30 Undang-Undang Informasi dan Transaksi Elektronik Terkait Pertanggung Jawaban Pelaku Pembobolan Rekening Nasabah

Muhammad Gerda Fadhilah. Fakultas Hukum, Universitas Pasundan**,** **muhammadgerdaf11@gmail.com**

ABSTRACT: Nowadays, hacking of customer accounts via internet banking is becoming increasingly common, this is of course very disturbing to the public as customers, in the case of criminal acts of burglary committed by these individuals, of course they must be held accountable. In positive legal regulations, there are no specific and clear regulations regarding internet banking. However, researchers want to look at cases of burglary of customer accounts via internet banking from the perspective of Article 362 of the Criminal Code and Article 30 of Law Number 19 of 2016 concerning Information and Electronic Transactions. This research is descriptive sociological in nature using normative juridical methods where the research results focus on positive law and legal rules. The results of the research conclude that the implementation of Article 362 of the Criminal Code and Article 30 of Law Number 19 of 2016 concerning Information and Electronic Transactions regarding the responsibility of perpetrators in cases of burglary of customer accounts via internet banking is the right step for victims to take with proof in Article 184 of the Criminal Code accompanied by tools. electronic evidence as evidence specified in the article.

KEYWORDS: Responsibility, Burglary, Internet Banking.

ABSTRAK: Pembobolan rekening nasabah melalui internet banking sedang marak terjadi, hal ini sangat meresahkan masyarakat sebagai nasabah, dalam hal tindak pidana pembobolan yang dilakukan oleh oknum tersebut tentu harus dipertanggung jawabkan. Didalam peraturan hukum positif, belum ada pengaturan yang khusus dan jelas mengenai internet banking. Namun peneliti ingin melihat kasus pembobolan rekening nasabah melalui internet banking dari perspektif "Pasal 362 KUHP" dan "Pasal 30 Undang Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik". Penelitian ini bersifat deskriptif yang menggunakan metode yuridis normatif dimana dalam hasil penelitian berfokus pada hukum positif dan kaidah hukum. Hasil penelitian menyimpulkan bahwa implementasi "Pasal 362 KUHP" dan "Pasal 30 Undang Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik" terkait pertanggung jawaban pelaku dari kasus pembobolan rekening nasabah melalui internet banking merupakan langkah yang tepat untuk diupayakan oleh korban dengan pembuktian dalam "Pasal 184 KUHP" disertai alat bukti elektronik sebagai alat bukti yang ditentukan dalam pasal tersebut.

KATA KUNCI: Pertanggung Jawaban, Pembobolan, Internet Banking.

I. PENDAHULUAN

Teknologi dewasa ini berkembang dengan kian pesat seiring dengan zaman. Ini adalah sesuatu yang tidak dapat dihindari. Perkembangan teknologi ini pasti memiliki dampak yang signifikan pada semua sektor ekonomi, termasuk sektor perbankan. Perkembangan teknologi telah membawa perubahan besar dan terbukti memberikan banyak keuntungan, seperti meningkatkan keamanan, meningkatkan kecepatan, dan meningkatkan kenyamanan dalam menjalankan berbagai aktivitas (Dikdik, 2005). Internet banking adalah tanda perkembangan teknologi di dunia perbankan. Ini menjadi alat alternatif untuk usaha bank untuk memanjakan nasabah, memungkinkan mereka melakukan transaksi dengan mudah, cepat, dan kapan saja mereka mau (Kurniawan, 2013).

Internet banking sendiri berbeda dengan perbankan konvensional, hal ini tentu membuat banyak pertanyaan salah satunya bagaimana perlindungan hukum data pribadi para nasabah (Hermansyah, 2000). Dalam transaksi internet banking, tidak hanya antara pihak bank dan nasabah, tetapi juga antara berbagai pihak, seperti penyedia layanan internet, penjual, dan nasabah, hal ini diatur dalam "Undang-Undang RepubIik lndonesia Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan Pasal 1 angka (28)" (Riswandi, 2005).

Namun berkembangnya teknologi sering dimanfaatkan beberapa oknum untuk kepentingan individual dan merugikan orang lain, hal ini dapat kita lihat maraknya kasus pembobolan rekening nasabah melalui *internet banking*, oknum yang tidak memiliki wewenang tersebut tersebut menggunakan data pribadi nasabah dan menggunakannya untuk kepentingan pribadi dan bisnis yang dapat merugikan nasabah sebenarnya.

Beberapa jenis modus yang digunakan pelaku diantaranya mengirim pesan melalui whatsapp berupa dokumen digital yang ternyata itu merupakan aplikasi yang apabila didownload otomatis terinstal

aplikasi dan pada saat itulah pelaku tersebut melakukan aksinya yaitu membobol rekening nasabah, selain itu ada juga yang banyaknya pesan singkat atau layanan pesan singkat (SMS) dan panggilan telepon yang digunakan dalam industri keuangan seperti asuransi, kredit, voucher rekreasi, dan produk lainnya juga mengirim link yang apabila diakses maka pelaku dapat membobol rekening nasabah tersebut (VioIina & Zahrani, 2021).

Di Indonesia terdapat "Undang Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik" tetapi undang-undang tersebut tidak secara khusus dan jelas mengatur terkait *internet banking* itu sendiri. Namun apabila ditinjau dari hukum pidana, kasus pembobolan rekening nasabah melalui internet banking ini dapat dijerat dengan "pasal 362 KUHP" tentang pencurian. Pelaku pembobolan tersebut tentu harus mempertanggungjawabkan tindakan melawan hukum yang dilakukan sehingga mengakibatkan kerugian materil maupun immateril yang dialami oleh korban. Berdasarkan uraian diatas, peneliti disini akan membahas mengenai bagaimana impelementasi "Pasal 362 Hukum Pidana Republik Indonesia" dan "Pasal 30 Undang-undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik" terkait pertanggungjawaban pelaku terhadap pembobolan rekening nasabah melalui internet banking dan bagaimana pembuktian menurut "Pasal 184 KUHAP". Kasus pembobolan dana nasabah melalui internet banking sering kali terjadi dan menelan banyak korban dengan jumIah uang yang tidak main-main, kasus yang menimpa seorang yang bernama irwan gema yakni pemboboIan rekening sebesar Rp. 594.000.000,00 merupakan saIah satu kasus yang mencuat ditahun 2023. Maka dari itu, penulis tertarik mengkaji lebih dalam mengenai fenomena pemboboIan internet banking yang sedang marak ini khususnya bagaimana pertanggungjawaban pelaku pembobolan rekening nasabah tersebut.

II. METODE

Metode penelitian yang digunakan oleh peneliti untuk menemukan kebenaran dan solusi dari masalah yang ada adalah metode yuridis normatif. Dalam konteks ini, peneliti mengumpulkan data melalui studi kepustakaan dan data tersebut dianalisis secara tidak langsung melalui bahan tertulisnya (Soekanto, 2001). Dalam hal spesifikasi penulisan, peneliti menggunakan metode analisis deskriptif, yang menghubungkan aturan saat ini dengan permasalahan yang telah dijelaskan di atas, dengan mempertimbangkan pendapat serta temuan dari sarjana hukum dan implementasi hukum saat ini yang relevan dengan permasalahan yang diteliti (Soemitro, 1990).

DaIam penuIisan yang diteIiti, peneIiti menganaIisis bagaimana pertanggungjawaban pelaku terkait pembobolan rekening nasabah melalui internet banking serta bagaimana pembuktian atas tindakan yang telah dilakukan oleh oknum tersebut berdasarkan kepada Pasal 184 KUHAP. Untuk memenuhi data yang diperIukan, peneIiti meIakukan peneIitian kepustakaan (Library Research), yakni peneIitian pada data sekunder yakni data yang diambiI secara tidak Iangsung meIaIui objeknya baik daIam bentuk tuIisan sehingga dapat membantu peneIiti untuk mengetahui sedaIam-daIamnya, menguraikan serta memecahkan persoaIan yang ada.

III. HASIL PENELITIAN & PEMBAHASAN

Dalam Kamus Besar Bahasa Indonesia (KBBI) online, bobol diartikan sebagai jebol atau rusak, juga bisa diartikan sebagai tembus. Pembobol adalah pelaku yang menyebabkan terjadinya bobol. Pembobolan merujuk pada proses, cara, atau perbuatan untuk membobol.

Membobol berarti menjebol, merusak, menembus, atau membongkar dengan paksa. Jika kita mengacu pada makna harfiah dan denotatif kata bobol menurut KBBI, kita dapat menyimpulkan bahwa

kata ini digunakan dalam konteks yang melibatkan tindakan fisik yang memaksa. Dalam konteks kejahatan, istilah bobol hampir sama dengan rampok atau pencuri, yang sama-sama mengambil milik orang lain tanpa izin, dengan melakukan tindakan yang memaksa dan fisik. Namun, kejahatan perbankan, menurut Direktur II Ekonomi Khusus Bareskrim Mabes Polri, Brigadir Jenderal Polisi Arief Sulistyo, tidak dilakukan secara fisik seperti merampok atau mencuri.

Pembobolan dilakukan dengan berbagai cara, seperti pegawai bank mencairkan dan mentransfer dana nasabah tanpa izin, menggunakan berita teleks palsu untuk membuka rekening pinjaman modal kerja, serta memberikan kartu kredit dengan identitas palsu dan jaminan fiktif. Dalam konteks pembobolan ATM, pelaku umumnya memindai nomor PIN ATM untuk digunakan tanpa izin nasabah. Modus operandi ini jelas memanfaatkan sistem operasional bank.

Kerugian keuangan dalam pembobolan tidak terjadi secara fisik, melainkan melalui manipulasi dalam sistem operasional bank. Namun, mengapa media sering kali menggunakan kata "pembobol" atau "pembobolan"? Sebelum istilah ini populer, kita sudah mengenal kata "penggelapan". Kata-kata "pembobolan" dan "penggelapan" digunakan sebagai eufemisme. Eufemisme sering kali menciptakan istilah yang keliru dan menjadi umum.

KBBI telah mengadaptasi makna konotatif dari "penggelapan" yang tidak hanya berarti kegelapan secara harfiah, tetapi juga perilaku penyelewengan dan korupsi. Namun, jika KBBI harus mengakomodasi perkembangan bahasa, istilah "pembobolan" hingga saat ini masih dianggap keliru dan tidak sesuai dengan kaidah sebelum makna konotatifnya dimasukkan dalam KBBI. Seharusnya kita, khususnya media, tidak menggunakan istilah "pembobolan" untuk menggantikan makna "penggelapan" sebelum KBBI melakukan penyesuaian. Dalam kasus kejahatan perbankan, pelaku pembobolan bank sering kali adalah mereka yang memiliki kedudukan sosial dan status yang tinggi, yang dikenal sebagai "*white collar criminal*".

Rekening adalah instrumen untuk mencatat transaksi keuangan yang terkait dengan aktiva, kewajiban, modal, pendapatan, dan biaya. Penggunaan rekening bertujuan untuk mencatat data yang menjadi dasar penyusunan laporan keuangan. Jumlah rekening yang dibutuhkan dalam pembukuan suatu perusahaan bergantung pada kebutuhan. Sekelompok rekening yang digunakan dalam pembukuan suatu perusahaan dikenal sebagai Buku Besar atau *General Ledger*.

Nasabah, menurut "Undang-Undang Nomor 10 Tahun 1998" yang telah diubah oleh "Undang-Undang Nomor 7 Tahun 1992", adalah individu atau entitas yang menggunakan layanan dari bank. Nasabah penyimpan adalah nasabah yang menyetor dananya di bank dalam bentuk simpanan berdasarkan perjanjian antara bank dan nasabah. Nasabah debitur adalah nasabah yang memperoleh fasilitas kredit atau pembiayaan sesuai dengan prinsip syariah atau yang setara dengan itu, berdasarkan perjanjian antara bank dan nasabah yang bersangkutan.

Internet banking adalah sebuah layanan inovatif yang disediakan oleh bank untuk memungkinkan pengguna melakukan transaksi perbankan melalui *smartphone*. *M-Banking*, atau yang lebih dikenal sebagai internet banking, adalah fasilitas perbankan yang memanfaatkan perangkat komunikasi bergerak seperti handphone, dengan menyediakan aplikasi unggulan untuk melakukan transaksi perbankan. Dengan adanya handphone dan layanan *m-Banking* ini, transaksi perbankan yang sebelumnya harus dilakukan secara manual dengan mengunjungi kantor bank, kini dapat dilakukan secara online. Hal ini membantu nasabah menghemat waktu dan biaya, serta menjaga agar mereka tetap terhubung dengan teknologi modern dalam menggunakan media elektronik. Selain itu, *internet banking* juga memungkinkan nasabah untuk memanfaatkan *handphone* mereka tidak hanya untuk berkomunikasi, tetapi juga untuk berbisnis atau melakukan transaksi lainnya.

Internet banking memberikan kemudahan kepada nasabah untuk melakukan berbagai transaksi perbankan seperti pengecekan saldo dan transfer antar rekening dengan cepat dan efisien. Dengan fasilitas ini,

siapa pun yang memiliki ponsel dapat melakukan transaksi kapan saja dan di mana saja. Bank-bank berlomba-lomba menyediakan layanan internet banking guna meningkatkan kepuasan nasabah dan jumlah pengguna layanan tersebut.

Internet banking adalah layanan perbankan yang dapat diakses langsung oleh nasabah melalui handphone dengan menggunakan menu yang tersedia di SIM Card atau dikenal juga sebagai SIM Toolkit. Kemajuan teknologi juga membawa dampak negatif seperti peningkatan kejahatan yang terkait dengan penggunaan internet. Penyalahgunaan internet seringkali digunakan sebagai sarana untuk melakukan kejahatan atau tindak pidana, yang semula dilakukan secara konvensional seperti pencurian, pengancaman, atau pembobolan ATM, dapat beralih menggunakan internet untuk mengurangi risiko tertangkap dan menggunakan situs web sebagai media transaksi. Kejahatan semacam ini dapat mengancam ketertiban masyarakat dan keamanan secara keseluruhan. Oleh karena itu, hukum memiliki peran penting dalam menangani benturan-benturan yang muncul dalam situasi seperti ini (Wahid, 2015).

Cybercrime adalah salah satu bentuk kejahatan modern yang mendapat perhatian global yang luas. Volodymyr Golubev menggambarkannya sebagai bentuk baru dari perilaku anti-sosial yang muncul dalam era teknologi saat ini. Kejahatan ini merupakan sisi gelap dari kemajuan teknologi yang memiliki dampak negatif yang sangat luas di berbagai aspek kehidupan modern saat ini (Arief, 2006).

Cybercrime merujuk pada tindak pidana yang dilakukan melalui jaringan sistem komputer dan komunikasi, baik lokal maupun global seperti internet. Pelaku kejahatan ini memanfaatkan teknologi informasi yang berbasis sistem komputer, yang bisa diakses secara virtual, dan sering kali melibatkan pengguna internet sebagai korban. Contoh kejahatan tersebut antara lain manipulasi data (*trojan horse*), spionase (*hacking*), penipuan kartu kredit online (*carding*), merusak sistem (*cracking*), skimming ATM, dan berbagai tindak kejahatan lainnya. Para pelaku *cybercrime* sering kali memiliki keahlian teknis yang tinggi

sehingga sulit untuk dilacak dan diberantas sepenuhnya (Suhariyanto, 2013).

Hukum pidana Indonesia yang mengatur mengenai cybercrime terdapat dalam "Undang-undang Nomor 19 tahun 2016 atas perubahan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik" atau yang biasa kita sebut dengan UU ITE. Kejahatan yang marak terjadi saat ini adalah kejahatan di bidang perbankan dimana banyak nasabah pemilik suatu rekening bank dibobol oleh oknum tertentu melalui internet banking namun belum dapat ditangani dengan baik, hal ini dapat kita lihat bahwa semakin banyak oknum yang melakukan pembobolan terhadap rekening nasabah, yang berarti dari penanganan kasus yang sudah inkrah tidak membuat efek jera baik terhadap pelaku maupun oknum-oknum diluar sana.

Tindak pidana pencurian uang pada rekening nasabah melalui internet banking sesuai dengan ketentuan "Pasal 362 KUHP Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik" Selama ini penyalahgunaan komputer di Indonesia hanya dijerat dengan ketentuan hukum pidana, yaitu "Pasal 362 tentang pencurian", "Pasal 378 tentang penggelapan dana public", dan "Pasal 263 tentang pemalsuan". Namun dengan berkembangnya zaman, tentunya kualitas kegiatan kriminal dengan menggunakan komputer sebagai sarana atau alat juga semakin meningkat, dan diperlukan aturan khusus untuk meredam ancaman penyalahgunaan komputer.

Penyusunan peraturan mengenai internet bertujuan untuk memberikan kepastian hukum kepada pengguna internet serta mengurangi dampak negatif dari perkembangan internet yang cepat, termasuk untuk menghindari penyalahgunaan komputer oleh para *hacker*. Indonesia memiliki beberapa undang-undang yang saat ini mengatur penanganan pelaku kejahatan komputer (*cracker*). seperti "Pasal 362 KUHP" dan "Undang-Undang Nomor 12 Tahun 1997 tentang Hak Cipta", serta "Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik". "Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP)" dan "Pasal 30 Undang-Undang

Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE)" merupakan dasar hukum yang dapat digunakan dalam menjerat pelaku kejahatan pembobolan rekening nasabah melalui internet banking. Berikut adalah implementasi kedua pasal tersebut terkait dengan pertanggungjawaban pelaku:

a. Pasal 362 KUHP: Pencurian

Pasal 362 KUHP menyatakan:

"Barang siapa mengambil sesuatu barang, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak enam puluh rupiah."

Dalam konteks pembobolan rekening melalui internet banking, tindakan pelaku dapat dikategorikan sebagai pencurian. Unsur-unsur yang perlu dibuktikan meliputi:

1. Barang: Uang dalam rekening nasabah.
2. Pengambilan: Transfer atau penarikan uang secara ilegal.
3. Kepemilikan Orang Lain: Rekening milik nasabah.
4. Maksud untuk Memiliki secara Melawan Hukum: Niat pelaku untuk mengambil uang tanpa hak.

b. Pasal 30 UU ITE: Akses Ilegal

"Pasal 30 UU ITE" menyatakan:

1. "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun".
2. "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan

cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik".

3. "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan".

Untuk menjerat pelaku pembobolan rekening melalui internet banking dengan Pasal 30 UU ITE, unsur-unsur yang harus dibuktikan antara lain:

1. Akses Tanpa Hak atau Melawan Hukum: Pelaku mengakses sistem internet banking nasabah tanpa izin.
2. Sengaja: Ada niat atau kesengajaan dalam melakukan akses tersebut.
3. Sistem Elektronik: Sistem perbankan yang digunakan oleh nasabah.

c. Pertanggungjawaban Pelaku

Pelaku yang terbukti melakukan pembobolan rekening melalui internet banking dapat dikenakan sanksi berdasarkan kedua pasal di atas:

1. Sanksi Pidana Pencurian (Pasal 362 KUHP): Penjara maksimal 5 tahun atau denda maksimal enam puluh rupiah (jumlah ini perlu disesuaikan dengan peraturan terbaru yang relevan).
2. Sanksi UU ITE (Pasal 30 UU 19/2016):
    a) Penjara maksimal 6 tahun atau denda maksimal Rp600 juta untuk pelanggaran Pasal 30 ayat (1).
    b) Penjara maksimal 7 tahun atau denda maksimal Rp700 juta untuk pelanggaran Pasal 30 ayat (2).

c) Penjara maksimal 8 tahun atau denda maksimal Rp800 juta untuk pelanggaran Pasal 30 ayat (3).

d. Proses Penegakan Hukum

Proses penegakan hukum terhadap pelaku pembobolan rekening nasabah melalui internet banking mencakup beberapa tahap:

1. Pelaporan: Nasabah melaporkan kasus kejahatan ke pihak berwenang (kepolisian).
2. Penyelidikan dan Penyidikan: Polisi melakukan penyelidikan dan penyidikan untuk mengumpulkan bukti-bukti yang relevan.
3. Penuntutan: Jaksa penuntut umum menyusun dakwaan berdasarkan hasil penyidikan.
4. Persidangan: Pengadilan memeriksa, mengadili, dan memutus perkara berdasarkan bukti dan dakwaan yang diajukan.
5. Putusan: Jika terbukti bersalah, hakim menjatuhkan hukuman sesuai dengan ketentuan dalam KUHP dan UU ITE.

e. Pembuktian Dalam Tindak Pidana Pembobolan Rekening Nasabah Melalui Internet Banking Dengan Teknologi Informasi

Menurut Undang-Undang ITE, pembuktian menyatakan bahwa informasi elektronik atau arsip elektronik beserta salinan cetaknya merupakan alat bukti hukum yang sah, yang merupakan kelanjutan dari alat bukti hukum yang diatur dalam hukum acara Indonesia saat ini.

Undang-undang ITE mendefinisikan dokumen elektronik sebagai setiap informasi elektronik yang dibuat, ditransmisikan, dikirim, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optik, atau bentuk lainnya, yang dapat dilihat, ditampilkan, dan/atau didengar oleh komputer atau sistem elektronik. Dokumen ini bisa berupa kata-kata, suara, gambar, peta, desain, foto, huruf, tanda, angka, kode akses, simbol, atau perforasi yang memiliki arti atau dapat dipahami oleh orang yang dapat memahaminya. Informasi elektronik merujuk pada

satu atau sekelompok data elektronik, termasuk teks, suara, gambar, peta, desain, foto, electronic data interchange (EDI), surat elektronik (email), telegram, teleks, huruf, tanda, angka, kode akses, simbol, atau perforasi yang diproses secara analog dan memiliki arti atau dapat dipahami oleh orang yang memahaminya.

Penggunaan alat bukti elektronik untuk melegalkan penggunaan media online untuk mengungkap pasal pidana antara lain:

Pasal 44 yang berbunyi:

1. Alat bukti penyidikan, penuntutan, dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut:

2. Alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan;

3. Alat bukti lain berupa Informasi Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

Pasal-pasal tersebut dianggap memberikan pedoman kepada penyidik dalam mengumpulkan barang bukti elektronik untuk mengungkap pelaku kejahatan internet, terutama yang terkait dengan penggunaan internet untuk mencuri dana melalui rekening bank. Barang bukti elektronik ini seringkali digunakan sebagai pelengkap alat bukti yang diatur dalam alinea pertama "Pasal 184 KUHAP", yang mengatur bahwa alat bukti yang sah dapat digunakan sebagai alat bukti dalam proses penyidikan dan persidangan:

1. Keterangan Saksi;

2. Keterangan Ahli;

3. Surat;

4. Petunjuk;

5. Keterangan Terdakwa.

IV. KESIMPULAN

Berdasarkan hasil pembahasan, dapat disimpulkan bahwa kejahatan pencurian uang dari rekening bank melalui internet dapat dianalisis dari perspektif "Pasal 362 KUHP dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik" di Indonesia. Peraturan hukum terkait pencurian uang di bank dengan menggunakan internet di Indonesia telah memiliki dasar yang memadai. Pembuktian dalam kasus pencurian uang dari rekening bank melalui internet menggunakan teknologi informasi memerlukan alat bukti elektronik untuk melengkapi alat-alat bukti yang dijelaskan dalam "Pasal 184 ayat (1) KUHAP", termasuk keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan dari terdakwa.

Penegakan hukum pidana harus dilakukan sesuai dengan peraturan perundang-undangan yang berlaku di Indonesia untuk menciptakan kepastian hukum, meningkatkan kepercayaan masyarakat, dan memastikan kepatuhan terhadap hukum. Untuk mewujudkan proses peradilan pidana yang baik, penting bahwa aparat penegak hukum profesional dan ditempatkan sesuai dengan keahlian mereka. Selain itu, perlu ditingkatkan sumber daya manusia melalui pelatihan yang sesuai serta ditingkatkan sarana dan prasarana untuk menunjang kinerja aparat penegak hukum.

DAFTAR REFERENSI

Arief, B. N. (2006). Tindak Pidana Mayantara Perkembangan Kajian Cyber crime di Indonesia. Rajawali Pers.

Dikdik, M. A. M. (2005). Cyber Law Aspek Hukum Teknologi Informasi. Refika Aditama.

Hermansyah. (2000). Hukum Perbankan Nasional Indonesia. Kencana Prenada Media Group.

Kurniawan, R. (2013). Perkembangan E-Banking Indonesia. Jurnal Ilmuti (Ilmu Teknologi Informasi, 4(2), 10.

Riswandi, B. A. (2005). Aspek Hukum Internet Banking. PT. Raja Grafindo.

Soekanto, S. & S. mamuji. (2001). Penelitian Hukum Normatif (Suatu Tinjauan Singkat). Rajawali Pers.

Soemitro, R. H. (1990). Metode Penulisan Hukum dan Jurimetri. Ghalia Indonesia.

Suhariyanto, B. (2013). Tindak Pidana Teknologi Informasi (cyber crime). Rajawali Pers.

VioIina, D., & Zahrani, H. T. (2021). Perlindungan Data Pribadi Bagi Nasabah Korban Pembobolan Rekening Melalui Internet Banking Ditinjau Dari Hukum Positif Indonesia. Jurnal Kepastian Hukum Dan Keadilan, 2(1), 69. https://doi.org/10.32502/khdk.v2i1.3048.

Wahid, A. & M. L. (2015). Kejahatan Mayantara. Refika Aditama.