

PERLINDUNGAN HUKUM TERHADAP PENGGUNA LAYANAN PERBANKAN DIGITAL DALAM KAITANNYA DENGAN KEAMANAN DATA DAN PRIVASI¹

Oleh :

Andree Mark Bojoh²

Deasy Soeikromo³

Kathleen C. Pontoh⁴

ABSTRAK

Penelitian ini bertujuan untuk menilai efektivitas regulasi perlindungan hukum pengguna layanan dalam kaitannya dengan keamanan data dan privasi dan untuk menilai keadaan pengguna layanan perbankan digital dalam kaitannya dengan keamanan data dan privasi. Metode yang digunakan adalah yuridis normatif, dengan kesimpulan yaitu: 1. Pengaturan tentang pengguna layanan perbankan dalam kaitannya dengan keamanan data dan privasi diatur dalam, Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Pasal 40 ayat (1). Terdapat juga Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan, Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, UU Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, dan Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia. 2. Selanjutnya mengenai layanan perbankan digital berupa ATM, *call center*, *internet banking*, dan rekening ponsel. Adapun penjelasan mengenai Keamanan data dengan pengaturan dalam UU Nomor 27 Tahun 2022. Penjelasan mengenai Privasi dengan pengaturan dalam UU Nomor 39 Tahun 1999.

Kata Kunci : *pengguna layanan, perbankan, keamanan data dan privasi*

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi dan komunikasi pada era globalisasi telah membawa perubahan besar dalam berbagai aspek kehidupan manusia, termasuk dalam sektor keuangan dan perbankan. Digitalisasi telah menjadi kekuatan utama dalam mendorong efisiensi, transparansi, dan inklusi keuangan. Salah satu bentuk nyata dari transformasi ini adalah munculnya layanan

perbankan digital yang mengandalkan teknologi internet, perangkat lunak, dan kecerdasan buatan untuk menyediakan layanan keuangan kepada masyarakat secara cepat dan mudah. Layanan perbankan yang dahulu dilakukan secara konvensional di kantor-kantor cabang bank, kini dapat diakses melalui berbagai platform digital seperti aplikasi mobile banking, internet banking. Transformasi digital ini tidak hanya mengubah mekanisme kerja perbankan dari sisi internal, tetapi juga menciptakan paradigma baru dalam hubungan antara lembaga keuangan dan nasabah. Masyarakat kini dapat membuka rekening bank secara daring (*digital onboarding*), melakukan transaksi keuangan tanpa perlu datang ke kantor cabang, serta mengakses berbagai produk keuangan seperti pinjaman, investasi, atau asuransi melalui perangkat digital. Lembaga keuangan juga dituntut untuk terus berinovasi dalam menyediakan layanan yang cepat, aman, dan nyaman agar tetap relevan di tengah persaingan industri yang semakin ketat, termasuk dengan hadirnya perusahaan teknologi finansial (*fintech*) yang agresif dalam menawarkan solusi keuangan berbasis teknologi.

Transformasi ini didorong oleh beberapa faktor penting, antara lain meningkatnya penetrasi internet di Indonesia, pertumbuhan pengguna smartphone, serta perubahan preferensi konsumen yang menginginkan layanan keuangan yang praktis dan dapat diakses kapan saja. Pemerintah Indonesia melalui berbagai kebijakan dan program seperti Gerakan Nasional Non-Tunai (GNNT).⁵ Peraturan OJK terkait digital banking, serta dukungan terhadap startup fintech juga turut mempercepat digitalisasi di sektor ini. Selain itu, situasi pandemi COVID-19 yang berlangsung sejak tahun 2020 telah mempercepat adopsi teknologi digital dalam kehidupan sehari-hari, termasuk dalam hal pengelolaan keuangan. Selama masa pembatasan sosial, masyarakat secara luas mulai mengandalkan platform digital untuk memenuhi berbagai kebutuhan, termasuk dalam melakukan transaksi perbankan. Namun, perubahan yang cepat ini tidak hanya membawa dampak positif. Di balik kemajuan teknologi, terdapat tantangan besar yang perlu dihadapi, terutama dalam hal perlindungan konsumen. Layanan perbankan digital yang sepenuhnya berbasis sistem elektronik dan jaringan internet menjadi sangat rentan terhadap berbagai bentuk kejahatan siber dan pelanggaran hak konsumen. Oleh karena itu, meskipun digitalisasi

¹ Artikel Skripsi

² Mahasiswa Pascasarjana Unsrat, NIM 210711010508

³ Dosen Pascasarjana Unsrat, Doktor Ilmu Hukum

⁴ Dosen Pascasarjana Unsrat, Magister Ilmu Hukum

⁵ Bank Mega, Apa Itu Gerakan Nasional Non Tunai (GNNT) ?, <https://blog.bankmega.com/apa-itu-gerakan-nasional-non-tunai-gnnt-dan-manfaatnya-bagi-masyarakat/>, pukul 5.46 Wita, tanggal 25 Juli 2025.

memberikan banyak manfaat, tetap diperlukan pengawasan dan regulasi yang ketat agar transformasi ini berjalan secara adil, aman, dan bertanggung jawab bagi semua pihak.

Seiring dengan meningkatnya adopsi teknologi digital, penggunaan layanan perbankan digital di Indonesia menunjukkan pertumbuhan yang sangat pesat. Menurut data dari Bank Indonesia, nilai transaksi digital banking pada Agustus tahun 2023 mencapai Rp5,1 Kuadriliun.⁶ Meningkat secara signifikan dibandingkan tahun-tahun sebelumnya. Tren ini diproyeksikan akan terus berlanjut seiring meningkatnya literasi digital dan kemudahan akses terhadap layanan keuangan berbasis internet. Tidak hanya masyarakat di kota-kota besar, masyarakat di wilayah pedesaan pun mulai terpapar layanan keuangan digital, terutama dengan masuknya platform fintech yang menyediakan pinjaman mikro dan sistem pembayaran daring. Masyarakat kini semakin akrab dengan berbagai fitur layanan digital perbankan, seperti cek saldo, transfer dana antar bank, pembayaran tagihan, pembelian produk, hingga pengajuan pinjaman dan investasi digital. Penggunaan *QRIS* (*Quick Response Code Indonesian Standard*)⁷ juga menjadi tren baru dalam sistem pembayaran, yang menggantikan transaksi tunai dalam banyak kegiatan ekonomi, termasuk di pasar tradisional, UMKM, dan toko-toko kecil. Hal ini menunjukkan bahwa inklusi keuangan digital telah menyentuh berbagai segmen masyarakat, dari kelas menengah hingga masyarakat berpenghasilan rendah.

B. Rumusan Masalah

1. Bagaimana bentuk perlindungan hukum terhadap pengguna layanan perbankan digital dalam kaitannya dengan keamanan data dan privasi?
2. Bagaimana pelaksanaan perlindungan hukum terhadap pengguna layanan perbankan digital dalam kaitannya dengan keamanan data dan privasi?

C. Metode Penelitian

Jenis Penelitian yang akan digunakan dalam penelitian ini adalah metode penelitian normatif.

⁶ Adi Ahdiat, "Transaksi Digital Banking Capai Rp5,1 Kuadriliun pada Agustus 2023", dari: <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/ae217ecf13a93fa/transaksi-digital-banking-capai-rp51-kuadriliun-pada-agustus-2023>, pukul 6.52 Wita, tanggal 25 Juli 2025.

⁷ Tim Blog Amarta Apa Itu QRIS? Berikut Pengertian, Tujuan, dan Manfaatnya, dari: <https://amartha.com/en/blog/work-smart/apa-itu-qris-pengertian-tujuan-manfaat/>, pukul 6.58 Wita 25 Juli 2025.

PEMBAHASAN

A. Analisis Putusan Nomor 36/Pid.Sus/2020/PN Dps

Pengertian Putusan pidana sederhananya adalah keputusan yang diambil oleh pengadilan terhadap seseorang yang terbukti melakukan tindak pidana. Adapun dalam pembahasan kali ini mengenai analisis Putusan Nomor 36/Pid.Sus/PN Dps tentang pengguna mobile banking BCA mengalami kerugian dengan mentranfer uang akibat penipuan, dengan 98 hal yang berasal dari Pengadilan Negeri Denpasar, Bali. Kemudian, ada dua terdakwa yang tertulis dalam Putusan Nomor 36/Pid.Sus/PN Dps: Naufal Ibrahim Antonie dan Poppy Christiane V. Terdapat juga beberapa analisis mulai dari Perlindungan Hukum Terhadap Nasabah di dalam Putusan, Kronologi Kejadian, Saksi-Saksi dan Ahli, Hukuman Terdakwa, dan Para Hakim dan Panitera Pengganti serta Jaksa Penuntut Umum. Berikut Penjelasannya:

1. Perlindungan Hukum Terhadap Nasabah di dalam Putusan

Menimbang, bahwa para Terdakwa didakwa oleh Jaksa Penuntut Umum didakwa dengan dakwaan berbentuk Alternatif sebagai berikut :

- a. Pasal 28 ayat (1) *Jo* Pasal 45 A Undang-undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).

Pasal 28 ayat (1) *jo* pasal 45A Undang-undang Nomor 19 Tahun 2016 memberikan perlindungan hukum, terutama terhadap konsumen atau masyarakat dari penyebaran berita bohong/hoaks yang berpotensi merugikan secara digital. Pasal ini juga memperkuat penegakan hukum terhadap penyalahgunaan teknologi informasi.

2. Kronologi Kejadian

- a. Bahwa berawal pada hari Senin, tanggal 21 Oktober 2019, sekitar 16.00 Wita, ketika saksi berada di tempat kerja saksi (PT. Bali 66 Citrine yang beralamat di jalan Dewi Sri No. 23 Kuta, Badung) saksi diberitahu oleh salah seorang teman kerja atas nama saksi Ni Made Sri Handarini yang menyampaikan bahwa sebelumnya yang bersangkutan telah

menerima pesan melalui *WhatsApp (WA)* dari seseorang yang mengaku AKBP Bambang Tertianto selaku Wadir Reskrimsus Polda Bali dengan nomor 081259800269, yang isinya yaitu meminta bantuan karena Wadir Reskrimsus akan berangkat ke Jakarta untuk menghadiri undangan gelar perkara di Bareskrim. Selanjutnya saksi meminta kepada Ni Made Sri Handarini untuk menyampaikan kepada orang tersebut (dengan nomor 081259800269) Agar menghubungi nomor telepon milik saksi I Putu Oka Semadi;⁸

- b. Bahwa sekitar pukul 16.06 Wita, saksi I Putu Oka Semadi menerima yang saksi I Putu Oka Semadi terima dengan menggunakan HP saksi I Putu Oka Semadi dengan nomor 08123808313 yang isinya pada intinya yang bersangkutan mengaku sebagai AKBP Bambang Tertianto selaku Wadir Reskrimsus Polda Bali yang saat itu sedang bersama dengan Waka Polda Bali dan meminta bantuan untuk biaya operasional menghadiri gelar perkara di Bareskrim Polri di Jakarta bersama pimpinan, selanjutnya yang bersangkutan mengirimkan rekening Bank BCA dengan nomor 6590150191 atas nama Naufal Ibrahim A. yang mana menurut yang bersangkutan bahwa pemilik rekening adalah sebagai anggota bag ops;⁹
- c. Bahwa sekira pukul 17.36 wita, saksi mentransfer uang sebesar Rp5.000.000,00 (lima juta rupiah) ke rekening Bank BCA dengan nomor 6590150191 atas nama Naufal Ibrahim Antonie melalui *m.banking* rekening Bank BCA dengan nomor 0490295097 atas nama I Putu Oka Semadi, kemudian setelah itu, saksi I Putu Oka Semadi mengirimkan bukti transfer tersebut melalui aplikasi *Whatsapp (WA)* ke nomor +6281259800269 dan yang bersangkutan mengaku akan menyampaikan bantuan tersebut kepada Pak Waka Polda Bali serta menyampaikan bahwa Pak Waka Polda Bali akan menghubungi saksi I Putu Oka Semadi secara langsung;¹⁰
- d. Bahwa sekira pukul 19.07 Wita, saksi I Putu Oka Semadi menerima pesan melalui *WhatsApp (WA)* dengan nomor 08170796998 yang mengaku sebagai Wakapolda Bali, yang menyampaikan ucapan terima kasih atas bantuan yang saksi I Putu Oka Semadi berikan kepada AKBP Bambang Tertianto (Wadir Krimsus polda Bali) dan selanjutnya beliau meminta untuk ditinjau perihal bantuan terkait kegiatan beliau di Jakarta dan perihal

bantuan agar di koordinasikan dengan AKBP Bambang Tertianto (Wadir Krimsus polda Bali), melalui aplikasi *Whatsapp (WA)* dengan nomor +6281259800269, kemudian setelah itu, saksi I Putu Oka Semadi menerima telepon melalui *WhatsApp (WA)* dari nomor 081259800269 namun suaranya tidak jelas karena sinyalnya tidak bagus. Selanjutnya saksi I Putu Oka Semadi menerima pesan kembali melalui *WhatsApp (WA)* dari nomor 08170796998 yang isinya yaitu ketersinggungan yang bersangkutan terhadap saksi I Putu Oka Semadi, kemudian sekira pukul 19.16 wita, saksi I Putu Oka Semadi kembali mentransfer uang sebesar Rp20.000.000,00 (dua puluh juta rupiah) ke rekening Bank BCA dengan nomor 6590150191 atas nama Naufal Ibrahim Antonie melalui *m.banking* rekening Bank Mandiri dengan nomor 1450010128631 atas nama I Putu Oka Semadi. Setelah itu, saksi I Putu Oka Semadi mengirimkan bukti transfer tersebut kepada pemilik nomor *WhatsApp (WA)* 081259800269;¹¹

- e. Bahwa pada tanggal 22 Oktober 2019, sekira pukul 17.00 Wita, ketika saksi I Putu Oka Semadi berada di kantor, saksi I Putu Oka Semadi kembali dihubungi oleh nomor telepon 08170796998 melalui aplikasi *Whatsapp (WA)* yang mengaku sebagai Wakapolda Bali, dan mengirim photo Gelar Perkara yang dihadapinya dan di dalam foto tersebut terlihat bapak Kapolri dan Bapak Jokowi. Selanjutnya yang bersangkutan menyampaikan pesan untuk antisipasi saja apabila ada kepentingan tolong dibantu tergantung situasinya. Kemudian beberapa saat kemudian saksi I Putu Oka Semadi kembali menerima pesan dari nomor 08170796998 melalui aplikasi *Whastapp* bahwa yang bersangkutan mengaku akan meminjam uang sebesar Rp.45.000.000 (empat puluh lima juta rupiah) dan akan dikembalikan keesokan harinya ketika sudah sampai di Bali dan dananya akan diantar sendiri oleh anggotanya, untuk uang tersebut agar di transfer ke rekening BCA 7650634599 atas nama Murtiarani, hal ini dilakukan guna menghindari pemeriksaan dari BPK RI;¹²
- f. Bahwa selanjutnya sekira pukul 18.36 Wita, saksi I Putu Oka Semadi kembali mentransfer uang sebesar Rp45.000.000,00 (empat puluh lima juta rupiah) ke rekening bank BCA dengan nomor 7650634599 atas nama

⁸ *Ibid*, hal. 4-5.

⁹ *Ibid*, hal. 5.

¹⁰ *Ibid*.

¹¹ *Ibid*, hal. 5-6.

¹² *Ibid*, hal.6.

Murtiarani melalui m.banking rekening Bank Mandiri dengan nomor 1450010128631 atas nama I Putu Oka Semadi, kemudian sekira pukul 20.27 Wita, saksi I Putu Oka Semadi kembali menerima pesan melalui WhatsApp (WA) dari nomor 08170796998, yang isinya meminta tambahan pinjaman lagi sebesar Rp25.000.000,00 (dua puluh lima juta rupiah) sehingga total pinjaman menjadi Rp70.000.000,00 (tujuh puluh juta upiah) yang akan dikembalikan keesokan harinya setelah tiba di Bali. Sehingga sekira pukul 20.45 Wita, saksi I Putu Oka Semadi melakukan transfer uang sebesar Rp25.000.000,00 (dua puluh lima juta rupiah) ke rekening bank BCA dengan nomor 7650634599 atas nama Murtiarani melalui *m.banking* rekening Bank Mandiri dengan nomor 1450010128631 atas nama I Putu Oka Semadi;¹³

- g. Bahwa pada sekira awal bulan Oktober 2019, ayah kandung terdakwa. Naufal Ibrahim Antonie yang bernama Stevanus Abraham Antonie (diajukan dalam penuntutan terpisah) meminta nomor rekening terdakwa, karena ayah terdakwa Stevanus Abraham Antonie (diajukan dalam penuntutan terpisah) menyampaikan akan mengirimkan uang kepada terdakwa, sehingga terdakwa memberikan rekening Bank BCA dengan nomor 6590150191 atas nama Naufal Ibrahim Antonie kepada ayah terdakwa tersebut melalui pesan SMS dari nomor 081286066374 yang terdakwa kirimkan ke nomor 08170796997. Beberapa hari kemudian, terdakwa menerima pesan SMS dari ayah terdakwa bahwa ada uang masuk ke rekening terdakwa, yaitu rekening Bank BCA dengan nomor 6590150191 atas nama Naufal Ibrahim Antonie sebesar Rp20.000.000,00 (dua puluh juta rupiah) yang kemudian setelah terdakwa terima uangnya langsung terdakwa transfer kembali ke beberapa rekening orang lain sesuai dengan dengan permintaan dari ayah terdakwa yaitu Stevanus Abraham Antonie (diajukan dalam penuntutan terpisah);¹⁴
- h. Bahwa pada sekira bulan Oktober terdakwa II. Poppy Christiane V diminta oleh Stevanus Abraham Antonie (diajukan dalam penuntutan terpisah) untuk meminjam rekening orang lain dan terdakwa kemudian meminjam rekening atas nama Murtiarani di Bank BCA dengan nomor 7650634599, selanjutnya pada tanggal

22 Oktober 2019 melalui pesan *WhatsApp (WA)* Stevanus Abraham Antonie (diajukan dalam penuntutan terpisah) menyampaikan kepada terdakwa II. Poppy Christiane V bahwa ada uang Rp45.000.000,00 (empat puluh lima juta rupiah) masuk ke rekening atas nama Murtiarani tersebut, selanjutnya terdakwa II. Poppy Christiane V atas perintah dari Stevanus Abraham Antonie (diajukan dalam penuntutan terpisah) meminta kepada Murtiarani untuk mengirimkan uang tersebut sebesar Rp20.000.000,00 (dua puluh juta rupiah) ke rekening Bank BCA atas nama Olivia yang terdakwa II. Poppy Christiane V tidak ingat nomor rekeningnya dan sebesar Rp15.000.000,00 (lima belas juta rupiah) ke rekening Bank BRI dengan nomor 0534-01-009631-50-8 atas nama Teressa Linda S Gumay untuk kemudian ditransfer kembali ke rekening atas nama terdakwa I, Naufal Ibrahim Antonie sebesar Rp9.900.000,00 (sembilan juta sembilan ratus ribu rupiah), sedangkan sisanya sebesar Rp10.000.000,00 (sepuluh juta rupiah) terdakwa II. Poppy Christiane V minta untuk ditarik tunai dan diberikan kepada terdakwa.¹⁵

- i. Bahwa kemudian terdakwa II. Poppy Christiane V diberitahu lagi oleh Stevanus Abraham Antonie (diajukan dalam penuntutan terpisah) melalui pesan pesan *WhatsApp (WA)* yang isinya ada dana lagi ke rekening yang dipinjam oleh terdakwa II. Poppy Christiane V sebesar Rp25.000.000,00 (dua puluh lima juta rupiah). Selanjutnya terdakwa memberitahu Murtiarani dan meminta untuk mengirimkan uang tersebut sebesar Rp15.000.000,00 (lima belas juta rupiah) ke rekening Bank BRI dengan nomor 0534-01-009631-50-8 atas nama Teressa Linda S Gumay dan sisanya sebesar Rp10.000.000,00 (sepuluh juta rupiah) agar ditarik tunai dan diberikan kepada terdakwa. Setelah transaksi tersebut sudah dilakukan, terdakwa II. Poppy Christiane kemudian meminta Murtiarani untuk memblokir rekening miliknya yang dipinjam oleh terdakwa II. Poppy Christiane V tersebut.¹⁶
- j. Bahwa terdakwa terdakwa II. Poppy Christiane V juga diminta oleh Stevanus Abraham Antonie (diajukan dalam penuntutan terpisah) untuk mengirimkan uang sebesar Rp2.000.000,00 (dua juta rupiah) ke rekening Bank BCA dan uang sebesar Rp2.000.000,00 (dua juta rupiah) ke rekening bank BNI

¹³ *Ibid*, hal.6-7.

¹⁴ *Ibid*, hal.7.

¹⁵ *Ibid*, hal. 7-8.

¹⁶ *Ibid*, hal. 8.

namun terdakwa tidak ingat nomor dan atas nama siapa dan sisanya sebesar Rp1.000.000,00 (satu juta rupiah) terdakwa gunakan untuk keperluan sehari-hari;¹⁷

k. Bahwa terdakwa II. Poppy Christiane V juga mengirimkan uang atas permintaan dari Stevanus Abraham Antonie (diajukan dalam penuntutan terpisah) kepada:

- 1) Rekening Bank BNI dengan nomor 0682400343 atas nama I Ketut Suarsana sebesar Rp600.000,00 (enam ratus ribu rupiah) pada tanggal 28 Oktober 2019, yang terdakwa lakukan melalui *m. banking*.
- 2) Rekening Bank BNI dengan nomor 0682400343 atas nama I Ketut Suarsana sebesar Rp150.000,00 (seratus lima puluh ribu rupiah) dan sebesar Rp75.000,00 (tujuh puluh lima ribu rupiah) pada tanggal 29 Oktober 2019, yang terdakwa lakukan melalui *m. banking*.
- 3) Rekening Bank BNI dengan nomor 0682400343 atas nama I Ketut Suarsana sebesar Rp1.000.000,00 (satu juta rupiah) sebanyak 2 (dua) kali pada tanggal 04 November 2019, yang terdakwa lakukan warung transfer *online* dan melalui *m. banking*.
- 4) Rekening Bank BCA dengan nomor 8620383211 atas nama Alfin Adam sebesar Rp400.000,00 (empat ratus ribu rupiah) yang terdakwa lakukan pada tanggal 04 November 2019 melalui *m. banking*.¹⁸

l. Bahwa jumlah uang yang masuk ke rekening yang dipinjam oleh terdakwa II. Poppy Christiane V adalah sebesar Rp70.000.000,00 (tujuh puluh juta rupiah);¹⁹

m. Bahwa akibat perbuatan terdakwa I. Naufal Ibrahim Antonie bersama dengan terdakwa II. Poppy Christiane V. dan Stevanus Abraham Antonie (diajukan dalam penuntutan terpisah) tersebut saksi I Putu Oka Semadi mengalami kerugian materil sebesar Rp95.000.000,00 (sembilan puluh lima juta rupiah).²⁰

1. Para Saksi dan Ahli

- a. Ir. I Putu Oka Semadi, menerangkan 17 poin.
- b. Made Sri Handarini, menerangkan 9 poin.
- c. Anom Cahyadi, menerangkan 11 poin.
- d. Silvia Rosalina, menerangkan ada 10 poin.
- e. Andi Prasetyo, SH., menerangkan ada 10 poin.

- f. Stevanus Abraham Antonie, menerangkan ada 15 poin.
- g. Adityo Bagus Rihandono, ada 9 poin (keterangan dibacakan).
- h. Murtiarani, ada 16 keterangan (keterangan dibacakan).
- i. Ahli I Made Dwi Aritanaya, SH.,CCPA.,CCLO ada 6 poin.²¹

4. Hukuman kepada Terdakwa

Menjatuhkan pidana kepada terdakwa Naufal Ibrahim Antonie dan Poppy Christiane V oleh karena itu dengan pidana penjara masing-masing selama 3 (tiga) tahun dan denda masing-masing sejumlah Rp100.000.000,00 (seratus juta rupiah) dengan ketentuan apabila denda tersebut tidak dibayar diganti dengan pidana penjara masing-masing selama 4 (empat) bulan.²²

5. Para Hakim dan Panitera Pengganti serta Jaksa Penuntut Umum

Putusan diputuskan dalam rapat permusyawaratan Majelis Hakim Pengadilan Negeri Denpasar, pada hari Senin, tanggal Maret 2020, oleh I Ketut Kimiarsa, SH. selaku Hakim Ketua Majelis, I Wayan Kawisada, SH.,M.Hum. dan I Gusti Ngurah Putra Atmaja, SH., MH., masing-masing selaku Hakim Anggota, putusan mana pada hari itu juga diucapkan dalam persidangan yang terbuka untuk umum oleh Majelis Hakim Pengadilan Negeri Denpasar dengan dibantu oleh I Wayan Deresta, SH, selaku Panitera Pengganti, dan dihadiri pula oleh I Made Dipa Umbara, SH., Jaksa Penuntut Umum.²³

B. Tindak Pidana di Perbankan Digital

Pengertian Tindak Pidana di perbankan digital sederhananya adalah perbuatan melawan hukum di perbankan digital yang tidak harus hanya melawan hukum perbankan. Memang tindak pidana di perbankan digital,ada yang dapat di kenakan pasal di UU ITE (Informasi dan Transaksi Elektronik), ada yang dapat dikenakan pasal di KUHP, dan ada yang dapat dikenakan pasal di UU PDP (Perlindungan Data Pribadi). Terdapat beberapa tindak pidana di perbankan digital. Berikut beberapa tindak pidana di perbankan digital dan pasal dapat dikenakannya serta cara menghindarinya:

1. Phising

Phishing adalah teknik penipuan untuk mencuri informasi pribadi, melalui email atau tautan yang palsu. Modus ini biasanya mengarahkan korban ke situs web tiruan yang

¹⁷ *Ibid*.

¹⁸ *Ibid*, hal.8-9.

¹⁹ *Ibid*, hal.9.

²⁰ *Ibid*.

²¹ *Ibid*, hal. 49.

²² *Ibid*, hal.96

²³ *Ibid*, hal.98

menyerupai situs resmi. *Phising* dapat dikenakan dikenakan beberapa pasal. Berikut penjelasannya:

- a. Pasal 28 ayat (1) UU Nomor 1 Tahun 2024

Setiap orang dengan sengaja mendistribusikan dan/atau mentransmisikan informasi elektronik dan/atau dokumen elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian materiil bagi konsumen dalam transaksi elektronik.²⁴

- b. Pasal 378 KUHP:

Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan, dengan pidana penjara paling lama 4 tahun.²⁵

Kemudian, kasus *phising* pernah terjadi seperti yang dialami seorang pria berinisial MS yang merugi hingga Rp 261 juta akibat *phising*. Dua orang ditetapkan sebagai tersangka dalam kasus ini. Modus tersangka mengirimkan pesan ke *WhatsApp* korban dengan mengaku dari pihak bank. Isi pesannya meminta korban mengkonfirmasi transaksi sebesar Rp 3 juta dari kartu kreditnya. Konfirmasi dilakukan dengan mengisi formulir melalui link yang dikirimkan tersangka. Dalam formulir tersebut, korban mengisi nomor rekening, nama lengkap, pembukaan bank, nama orang tua, dan memberikan kode *OTP*. Isi formulir itu lah yang dijadikan pelaku untuk menggunakan menguras rekening korban. Korban baru tersadar saat ada pemberitahuan dari bank bahwa ada transaksi hingga ratusan juta rupiah. Selanjutnya terdapat cara menghindari *phising*.

2. *Cracking*

Cracking adalah salah satu bentuk kejahatan *cyber* dengan cara membobol keamanan sistem dengan berbagai tujuan kejahatan. Pelaku *cracking* biasa disebut dengan *Cracker*. Kemudian, terdapat pasal-pasal yang dapat dikenakan kepada pelaku *Cracking*. Berikut penjelasannya:

- a. Pasal 30 ayat (3) UU Nomor 11 Tahun 2008

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.²⁶

- b. Pasal 32 ayat (1) UU Nomor 11 Tahun 2008

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.²⁷

- c. Pasal 65 ayat (1) dan (3) UU Nomor 27 Tahun 2022

- 1) Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi.

- 3) Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya.²⁸

Kemudian, kasus *cracking* pernah terjadi di Indonesia yaitu: terjadi kejadian membobol *m-banking* perbankan. Mencuri uang Rp 120 Juta dari hasil membobol akun BRI *Mobile* dari telepon seluler (ponsel) yang ditemukan di Mampang pada Jumat (9/12/2022) membobol akun *mobile banking* pemilik ponsel hanya dengan cara menggunakan fitur lupa *password*. Selanjutnya terdapat beberapa cara mengatasi *cracking*. Berikut caranya:

- a. Gunakan *password* unik

Pastikan menggunakan *password* yang unik dan sulit digunakan untuk setiap akun. Jadi, ketika *cracker* berhasil meretas salah satu *password* akun, mereka tidak akan dapat mengakses akun lain. Bisa menggunakan *password generator* untuk membuat kata sandi yang aman dan sulit untuk diretas. Aplikasi *password manager* biasanya menawarkan fitur *password generator* dan *auto-fill password* untuk berbagai akun, jadi tak perlu mengingat seluruh kata sandi.

²⁴ Pasal 28 ayat (1) Undang-Undang 1 Tahun 2024.

²⁵ Pasal 378 KUHP.

²⁶ Pasal 30 ayat (3) UU Nomor 11 Tahun 2008

²⁷ Pasal 32 ayat (1) UU Nomor 11 Tahun 2008.

²⁸ Pasal 65 ayat (1) dan (3) UU Nomor 27 Tahun 2022.

- b. Jangan mengulang *password*
Jangan sekali-kali memiliki *password* yang sama pada setiap akun. *Cracker* akan dengan mudahnya membobol semua akun-akun bila berhasil menebaknya menggunakan teknik *password cracking*. Memang, mengulang *password* akan memudahkan pengguna untuk mengingat, tetapi risikonya sangatlah besar dan mengancam reputasi.

- c. Amankan ponsel
Jaga ponsel agar tidak kehilangan jika ada data penting. Kemudian supaya lebih aman pakai kata sandi atau pola di ponsel serta keamanan dengan sidik jari.

- d. Gunakan *VPN* (*Virtual Private Network*): *VPN*
Mengkripsi koneksi internet, menambahkan lapisan perlindungan ekstra dari *Cracker* yang mungkin mencoba mengakses data. Selain itu, *VPN* membantu melindungi informasi pribadi dari pelacakan oleh situs web dan aplikasi yang Anda kunjungi, sehingga meningkatkan privasi secara keseluruhan.

3. *DDoS Attack*

DDoS (*Distributed Denial of Service*) *Attack* atau Serangan *DDoS* bertujuan untuk menonaktifkan atau melumpuhkan situs web, aplikasi web, layanan *cloud*, atau sumber daya *online* lainnya dengan membanjiri situs tersebut dengan permintaan koneksi yang tidak berguna, paket palsu, atau lalu lintas berbahaya lainnya. Serangan *DDoS* dapat dikenakan:

- a. Pasal 30 ayat (3) UU Nomor 11 Tahun 2008
Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.²⁹
- b. Pasal 32 ayat (1) UU Nomor 11 Tahun 2008
Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.³⁰

- c. Pasal 33 UU Nomor 11 Tahun 2008

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.³¹

Kemudian, terdapat Kasus sistem penukaran uang bernama PINTAR dari Bank Indonesia (BI) mengalami kendala atau error akibat adanya kendala teknis berupa serangan *Distributed Denial of Service (DDoS)*. Deputy Gubernur BI Doni Primanto Joewono mengatakan *DDoS* tersebut membuat aplikasi PINTAR menjadi tidak bisa diakses atau down. Selanjutnya, terdapat cara menghindari *DDoS Attack* atau serangan *DDoS*:

- a. Meningkatkan kapasitas sumber daya server
- b. Batasi Akses *IP*
- c. Gunakan *firewall* yang Kuat
- d. Gunakan *CDN Content Delivery Network (CDN)*
- e. Melakukan *monitoring traffic*
- f. Gunakan layanan proteksi *DDoS*

4. *Ransomware Attack*

Ransomware Attack atau serangan *Ransomware* adalah jenis kejahatan dunia maya di mana penyerang menggunakan *ransomware* yang akan mengenkripsi data korban dan meminta pembayaran tebusan untuk melepaskannya. *Ransomware* adalah *malware* yang akan mengenkripsi file di komputer korban menggunakan algoritma enkripsi yang kompleks. File yang terinfeksi tidak dapat dibuka tanpa kunci dekripsi yang dimiliki oleh pelaku. *Ransomware attack* atau serangan *ransomware* dapat dikenakan:

- a. Pasal 30 ayat (3) UU Nomor 11 Tahun 2008
Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.³²
- b. Pasal 32 ayat (1) UU Nomor 11 Tahun 2008
Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan,

²⁹ Pasal 30 ayat (3) UU Nomor 11 Tahun 2008.

³⁰ Pasal 32 ayat (1) UU Nomor 11 Tahun 2008.

³¹ Pasal 33 UU Nomor 11 Tahun 2008.

³² Pasal 32 UU Nomor 11 Tahun 2008.

menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

Kemudian *ransomware attack* (serangan *ransomware*) pernah terjadi di Bank Indonesia. Pada 21 Januari 2022, BI mengumumkan telah terkena serangan ,yang mana *ransomware conti* adalah *ransomware*. Serangan *ransomware conti* ke BI sejatinya telah terjadi pada akhir 2021. Serangan menyasar 16 komputer personal di kantor BI Bengkulu, Data yang terkena mencakup pekerjaan personal di komputer kantor. Kelompok *Conti* mengklaim memiliki data dari BI dengan ukuran 487,09 MB, namun BI memastikan tidak ada data sensitif yang bocor. Selanjutnya terdapat cara menghindari *ransomware attack* (serangan *ransomware*):

- a. Memperbarui perangkat dan perangkat lunak
- b. Memasang perangkat lunak keamanan yang kuat
- c. Membuat cadangan data yang teratur
- d. Melakukan pemindaian berkala
- e. Hati-hati saat mengunduh dan menginstal aplikasi
- f. Menggunakan kata sandi yang kuat

5. *Skimming*

Skimming ATM adalah tindakan ilegal di mana penjahat mencuri informasi dari kartu ATM dengan cara memasang perangkat tambahan pada mesin ATM yang sah. Perangkat tambahan ini biasanya disebut "*skimmer*" dan memiliki kemampuan untuk membaca dan merekam data dari magnetik strip kartu ATM. Dasar hukum pada kejahatan tindak pidana *skimming* yaitu:

- a. Pasal 362 KUHP
Barangsiapa mengambil barang sesuatu, 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 sembilan ratus rupiah.³³
- b. Pasal 30 ayat (1) UU Nomor 11 Tahun 2008
Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
- c. Pasal 30 ayat (3) UU Nomor 11 Tahun 2008
Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses

Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Kemudian Kasus Ilegal Access (*Skimming*) pernah terjadi di indonesia.Yang Berhasil Curi Uang Lewat ATM Berhasil Diungkap Polres Pasuruan Kota. Lebih lanjut AKBP Arman mengatakan kedua pelaku ini berkewarganegaraan Bulgaria, dengan modus tersangka memasang alat *skimming* di beberapa daerah di Jawa Timur antara lain, Kediri, Madiun, Ngawi, Tulungagung dan juga Kota Pasuruan di salah satu ATM Bank Negara di jalan Sultan Agung. Tersangka memasang alat *skimming* ini mulai tanggal 26 Juli sampai 31 Juli 2021 dan tersangka tertangkap di Surabaya tanggal 2 Oktober 2021, jumlah korban 29 orang dengan jumlah uang yang berhasil di curi berjumlah Rp493.000.000,00. Yang bersangkutan memasang alat *skimming* dimulut ATM dan ada kamera kecil yang dipasang diatas tombol pin, sehingga tersangka bisa mengetahui identitas kartu ATM nasabah dan bisa mengetahui pin ATM saat dipencet. Data kemudian dikirim keserver oleh temannya di negaranya sana, kemudian dikirimkan kembali dengan analisa melalui nomer kartu dan pin ATM yang sama kemudian dipindahkan datanya sehingga menjadi ATM serupa yang baru yang bisa mengakses rekening nasabah untuk selanjutnya mencuri uang nasabah.³⁴ Selanjutnya terdapat menghindari *skimming*. Berikut caranya:

- a. Pilih dengan hati-hati lokasi ATM
Saat ingin menarik uang dari ATM, jangan sembarangan memilih mesin ATM. Pilihlah mesin ATM yang terletak di tempat ramai dan termonitor dengan baik, seperti pusat perbelanjaan atau cabang bank resmi. Hindari mesin ATM yang terpencil atau di tempat sepi, karena ini bisa memiliki risiko tinggi untuk *skimming*.
- b. Periksa kondisi mesin ATM
Sebelum menggunakannya, selalu periksa mesin ATM dengan seksama. Lihat apakah ada tanda-tanda yang mencurigakan, seperti perangkat tambahan yang tidak biasa. Jika ada yang tampak aneh, lebih baik hindari penggunaan mesin ATM tersebut. Bahkan dapat membandingkannya dengan mesin ATM lain di sekitarnya.

³³ Pasal 362 KUHP

³⁴ spbe, "Pelaku Ilegal Access (Skimming) Yang Berhasil Curi Uang Lewat ATM Berhasil Diungkap Polres Pasuruan Kota", diakses dari: <https://pasuraukota.go.id/2021/10/12/pelaku-ilegal-access-skimming-yang-berhasil-curi-uang-lewat-atm-berhasil-diungkap-polres-pasuruan-kota/>, pada tanggal Mei 16 2025, pukul 12.46 Wita.

- c. Gunakan layanan transaksi *cardless*
Beberapa bank saat ini menawarkan layanan transaksi tanpa kartu, yang memungkinkan melakukan transaksi di mesin ATM tanpa perlu menggunakan kartu fisik. Cukup dengan menggunakan layanan perbankan seluler (*m-banking*), dapat melakukan transaksi tanpa kartu, yang merupakan cara lain untuk menghindari *skimming* ATM.³⁵
- d. *Upgrade* ke kartu dengan teknologi *chip*
Jika kartu ATM masih menggunakan *magnetic stripe*, saatnya untuk menggantinya dengan kartu yang dilengkapi dengan teknologi *chip*. Kunjungi bank dan minta kartu baru yang lebih aman. Meskipun teknologi keamanan terus berkembang, tetap waspada terhadap risiko *skimming*.

PENUTUP

A. Kesimpulan

1. Adanya kemajuan digital menjadi penyebab timbul layanan perbankan digital yang dibuat oleh bank konvensional dan bank digital. Kemudian timbulah pengguna layanan perbankan digital dengan membuat data mereka disitu. Selanjutnya pengaturan tentang pengguna layanan perbankan dalam kaitannya dengan keamanan data dan privasi diatur dalam, Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Pasal 40 ayat (1). Terdapat juga Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan, Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, UU Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, dan Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia. Kemudian mengenai sejarah bank dimulai abad ke-18 sebelum masehi, bank di Italia, bank di Jerman, bank di Inggris, bank di Skotlandia, bank di Spanyol, bank di Belanda, dan bank di Indonesia.
2. Selanjutnya mengenai layanan perbankan digital berupa ATM, *call center*, *internet banking*, dan rekening ponsel. Adapun penjelasan mengenai Keamanan data dengan pengaturan dalam UU Nomor 27 Tahun 2022. Penjelasan mengenai Privasi dengan

pengaturan dalam UU Nomor 39 Tahun 1999. Kemudian, Mengenai Analisis Putusan Nomor 36/Pid.Sus/2020/PN Dps berupa Perlindungan Hukum Terhadap Nasabah di dalam Putusan, Kronologi Kejadian, Saksi-Saksi dan Ahli, Hukuman Terdakwa, dan Para Hakim dan Panitera Pengganti serta Jaksa Penuntut Umum. Lalu Pembahasan Tindak Pidana di Perbankan Digital, Pasal yang dapat dikenakan Tindak Pidana di Perbankan, dan cara menghindari Tindak Pidana di Perbankan Digital.

B. Saran

1. Bagi pemerintah perlu mengadakan edukasi kepada masyarakat tentang apa saja tindak pidana di perbankan digital dan jelaskan. Kemudian informasikan kalau sudah banyak kasus tindak pidana di perbankan digital yang merugikan. Selanjutnya berikan edukasi bagaimana cara menghindari dari tindak pidana di perbankan digital.
2. Bagi Pengguna Layanan Perbankan (Nasabah), Nasabah perlu lebih aktif dalam menjaga keamanan data pribadinya dengan tidak sembarangan memberikan informasi sensitif. Kemudian Menggunakan fitur keamanan tambahan yang disediakan bank, seperti *OTP*. Jika terjadi kebocoran data atau transaksi mencurigakan, segera melaporkannya kepada pihak bank untuk ditindak lanjuti secara hukum.

DAFTAR PUSTAKA

Buku

- Abdullah, T & Wahjusaputri, S. 2018. *Bank dan Lembaga Keuangan*. Jakarta: Mitra Wacana Media.
- Anwar, M. 1986. *Tindak pidana di bidang Perbankan*. Bandung: Penerbit Alumni.
- Fahmi, I. 2014. *Pengantar Perbankan Teori & Aplikasi*. Bandung: Penerbit Alfa
- Hasan, N. 2014. *Pengantar Perbankan*. Jakarta: Gaung Persada Press Group.
- Herlina, R. 2017. *Tanggung Jawab Negara Terhadap Perlindungan Konsumen Ditinjau dari Hukum Perdata*. Jakarta: Puslitbang Hukum dan Peradilan Mahkamah Agung RI.
- Kristyanti, C. 2018. *Hukum Perlindungan Konsumen*. Jakarta: Sinar Grafika.
- Marbawi. 2017. *Bank & Lembaga Keuangan Lainnya, Teori dan Kebijakan*. Lhokseumawe: Unimal Press.
- Rahmawati, T. & Supraptiningsih, U. 2020. *Pengantar Ilmu Hukum dan Pengantar Hukum Indonesia*. Pamekasan: Duta Media Publishing.

³⁵ TEMPO, "Mengenal Apa Itu Skimming dan Cara Menghindarinya", diakses dari: <https://www.tempo.co/ekonomi/mengenal-apa-itu-skimming-dan-cara-menghindarinya-132926>, 16 Mei 2025, pukul 1.42 Wita.

- Rusli, T. 2017. *Pengantar Ilmu Hukum*. Bandar Lampung: Universitas Bandar Lampung.
- Soeroso, R. 2017. *Pengantar Ilmu Hukum*. Jakarta: Sinar Grafika.
- Tim Pengajar. 2007. *Hukum Perbankan*. Manado: FH UNSRAT.
- Tjiptoadinugroho, R. 1974. *Perbankan masalah Permodalan Dana dan Potensi*. Jakarta: PT Pradnya Paramita.
- Wibowo, A. 2022. *Perbankan Digital (Digital Banking)*. Semarang: Yayasan Prima Agus Teknik Bekerja Sama Dengan Universitas Sains & Teknologi Komputer Universitas STEKOM.
- Yuhelson, 2018. *Pengantar Hukum Perbankan di Indonesia*. Ideas Publishing.
- Yunasril, A. 2018. *Dasar-Dasar Ilmu Hukum*. Jakarta: Sinar Grafika.

Peraturan Dan Perundang-Undangan

- Putusan Nomor 36/Pid.Sus/2020/PN Dps.
- Peraturan Bank Indonesia Nomor 3 Tahun 2023 Tentang Perlindungan Konsumen Bank Indonesia.
- Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 Tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum.
- Peraturan Otoritas Jasa Keuangan Nomor 21 Tahun 2023 tentang Layanan Digital oleh Bank Umum.
- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan.
- Undang-Undang Nomor 26 Tahun 2000 Tentang Pengadilan Hak Asasi Manusia.
- Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.
- Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia.
- Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik
- Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen.

Website / Internet

- Ahdiat, 2023, Oktober, 26. *Transaksi Digital Banking Capai Rp5,1 Kuadriliun pada Agustus 2023*, dari: <https://databoks.katadata.co.id/teknologitelek/omunikasi/statistik/ae217ecf13a93fa/transaksi-digital-banking-capai-rp51-kuadriliun-pada-agustus-2023>.

- Bank Mega, 2024, September, 12. *Apa Itu Gerakan Nasional Non Tunai (GNNT) ?*, dari: <https://blog.bankmega.com/apa-itu-gerakan-nasional-non-tunai-gnnt-dan-manfaatnya-bagi-masyarakat/>.
- Cermati.com, 2024, September 5. *Internet Banking: Pengertian, Kelebihan, dan Kekurangannya*”, diakses dari, cermati.com: <https://www.cermati.com/artikel/Internet-banking-fitur-kelebihan-dan-kekurangannya>.
- Cermati.com. 2024, oktober 1. *Mandiri Call: Layanan Call Center 24 Jam Bank Mandiri*, cermati.com, diakses dari: <https://www.cermati.com/artikel/mandiri-call-layanan-call-center-24-jam-bank-mandiri>.
- Databoks. 2017, Mei 8. *Separuh Transaksi Bank Mandiri via Mobile dan Internet Banking*, databoks.katadata.co.id, diakses dari: <https://databoks.katadata.co.id/keuangan/statistik/5a28d4e68055398/separuh-transaksi-bank-mandiri-via-mobile-dan-internet-banking>.
- Elitery. *Langkah Perlindungan Data Pribadi di Sektor Perbankan* ,dari <https://elitery.com/articles/langkah-perlindungan-data-pribadi-di-sektor-perbankan/>.
- Firlyana. F. 2023, Mei 12. *ATM: Pengertian, Fungsi, dan Jenisnya*. diambil dari dailysocial.id: <https://dailysocial.id/post/atm-adalah>.
- Hariato. A. 2017, Januari 9. *Perlindungan Data Pribadi di Indonesia*. diambil dari, combine.or.id, : <https://www.combine.or.id/2017/01/09/perlindungan-data-pribadi-di-indonesia/>.
- OCBC, 2022, September, 27. *Nasabah Adalah: Pengertian, Manfaat, dan Jenis-Jenisnya*, dari: <https://www.ocbc.id/article/2022/09/27/nasabah-adalah>.
- Prabawati, 2024, Januari 22. *BI Catat Nilai Transaksi Digital Banking 2023 Rp 58.478,24 Triliun*, diskominfo.kaltimprov.go.id ,di akses dari <https://diskominfo.kaltimprov.go.id/ekonomi/bi-catat-nilai-transaksi-digital-banking-2023-rp-5847824-triliun>.
- Pujiati. 2024, Maret 19. *4 Perbedaan Penelitian Normatif dan Empiris*”. diambil dari penerbitdeepublish.com: <https://penerbitdeepublish.com/perbedaan-penelitian-normatif-dan-empiris/>.
- Renata, 2022, Juli, 27. *3 Prinsip dan 5 Asas Hukum Perlindungan Konsumen*, dari: <https://www.hukumonline.com/klinik/a/3-prinsip-dan-5-asas-hukum-perlindungan-konsumen-lt62e0d9cc75e23/>.

spbe, 2021, Oktober, 12. Pelaku Illegal Access (Skimming) Yang Berhasil Curi Uang Lewat ATM Berhasil Diungkap Polres Pasuruan Kota, dari: <https://pasuruankota.go.id/2021/10/12/pelaku-ilegal-access-skimming-yang-berhasil-curi-uang-lewat-atm-berhasil-diungkap-polres-pasuruan-kota>.

Team Amarthia Blog. 2021, Agustus 9. *Rekening Ponsel: Definisi, Kelebihan, dan Cara Membuatnya*”, diambil dari amarthia.com: <https://amartha.com/blog/pendana/lifestyle/rekening-ponsel/>.

Tim Blog Amarthia, 2024, Mei, 25. *Apa Itu QRIS? Berikut Pengertian, Tujuan, dan Manfaatnya*, dari: <https://amartha.com/en/blog/work-smart/apa-itu-qris-pengertian-tujuan-manfaat/>.

VIDA, 2025, Juli, 28. *Penyalahgunaan Data Pribadi: Contoh Kasus dan Kerugiannya* dari: <https://vida.id/id/blog/penyalahgunaan-data-pribadi>.

Willa, 2023, Juli, 3. *8 Prinsip Hak Privasi dalam Aturan Pelindungan Data Pribadi*, dari: <https://www.hukumonline.com/berita/a/8-prinsip-hak-privasi-dalam-aturan-pelindungan-data-pribadi-lt64a2dcec71359/?page=2>.

Sumber Lain

Al Fahri, Syafiq Muhammad. 2023. Implementasi Kebijakan Privasi Terhadap Data Pribadi Pengguna E-Commerce Ditinjau dari UU No 27 Tahun 2022 Tentang Perlindungan Data Pribadi (Studi Kasus Lazada). (Skripsi: Universitas Islam Negeri, Jakarta).

Rosnawan, Dadan. 2011. Aplikasi Algoritma RSA untuk Keamanan Data pada Sistem Informasi Berbasis Web. (Skripsi: Universitas Negeri Semarang).

Wulandari, Novita. 2023. Perlindungan Hukum terhadap Konsumen Makanan dan Minuman dengan Informasi Tidak Jujur perspektif Undang-Undang Nomor 8 Tahun 1999. (Skripsi: Institut Agama Islam Negeri, Metro).