Perlindungan Data Privasi Yang Dilakukan Perbankan Terhadap Penggunaan Layanan Mobile Banking

Dinda Novika Rahmahdhani[1*], Muhammad Irwan Padli Nasution[2], Sri Suci Ayu Sundari[3]
[1,2]Universitas Islam Negeri Sumatera Utara, Jl. William Iskandar Ps. V, Medan Estate, Kec. Percut Sei Tuan, Kab. Deli Serdang
Email: dindanovika1011@gmail.com [1*]

Abstrak

Pesatnya teknologi informasi , membuat bank meluncurkan layanan baru yang dinamakan layanan mobile banking (m-bangking). Dengan adanya layanan tersebut masyarakat/ nasabah jadi mudah dalam melakukan akses transaksi. Adanya kemudahan yang diberikan tidak menutup kemungkinan terdapat resiko keamanan dari data pribadi nasabah. Dengan adanya latar belakang tersebut tujuan penulis membuat paper ini yaitu untuk membahas tentang bagaimana perlindungan data privasi yang diberikan perbankan dan pemerintah dalam menjaga data privasi nasabah terhadap penggunaan m-banking. Penelitian ini menggunakan metode kepustakaan yang bersifat yuridis normatif dengan pendekatan peraturan perundang-undangan (statutory approach). Penulis juga mencari dan mengumpulkan informasi tentang perlindungan bank terhadap data pribadi melalui buku-buku dan artikel yang berkaitan. Hasil dari penelitian ini menunjukan bahwa terdapat model keamanan yang dilakukan perbankan dalam menjaga data nasabah atas penggunaan layanan m-banking. Contohnya yaitu dengan penerapan One-Time Password Tokens, One-Time Password cards, SSL, dan model keamanan lainnya. Untuk peraturan khusus mengenai perlindungan data pribadi pengguna layanan mobile banking sebenarnya belum terdapat di Indonesia, Namun terdapat aturan aturan yang terkait dengan perlindungan kerahasiaan data pribadi seperti yang tetera pada pasal 40 ayat (1) dan (2), Undang-undang Nomor 10 tahun 1998.

***Keyword**: Data privasi, Mobile banking, Perbankan, Perindungan*

PENDAHULUAN

Pada Undang-undang Nomor 10 Tahun 1998 tentang Perbankan, Bank disebutkan sebagai badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup masyarakat.

Dengan perkembangan teknologi informasi yang semakin berkembang. Tidak sedikit bank yang ingin memunculkan inovasi baru. Perbankan telah menyiapkan diri dengan menciptakan fitur-fitur finansial untuk menarik minat para nasabahnya. Salah satunya yaitu dengan diciptakannya layanan keuangan digital seperti alat pembayaran non tunai dengan fasilitas internet banking, mobile banking, dan short message service banking (sms banking). *Mobile-banking* adalah produk layanan perbankan yang memanfaatkan internet sebagai media untuk menyalurkan data keuangan dari bank kepada nasabah menggunakan smartphone, yang dapat diakses kapanpun dan diamanapun selama 24 jam (Nandavita, 2021).

Layanan mobile banking sendiri memiliki fasilitas, seperti layanan informasi (saldo, mutasi rekening, suku bunga, dan lokasi cabang/ATM terdekat); dan layanan

transaksi, seperti transfer, pembayaran tagihan (listrik, air, internet), Pembelian tiket, pembelian pulsa, dan berbagai fitur lainnya. Dengan fitur tersebut banyak orang merasakan kemudahan dalam melakukan transaksi.

Di balik keunggulan *(m-banking)* itu, ada risiko kamanan yang menjadi bahan pertimbangan nasabah. Kerahasiaan data konsumen adalah sesuatu yang bersifat privasi dan harus dilindungi dengan hati-hati. Perlindungan data konsumen sangat penting untuk melindungi konsumen dari pencurian data, peretasan, serta penyalahgunaan data untuk hal-hal yang melanggar hukum. Agar kepercayaan nasabah tetap terjaga mengenai amannya bertransaksi secara elektronik, industri perbankan mulai diharuskan untuk mampu menyediakan *security features*, selain dari menjaga kepercayaan yang telah diberikan oleh masyarakat, perlindungan hukum juga diberikan dalam rangka untuk melindungi hak-hak nasabah sebagai konsumen dalam jasa perbankan.

Dengan latar belakang tersebut maka tujuan dari paper ini yaitu untuk membahas tentang bagaimana perlindungan data *privacy* yang diberikan perbankan dalam menjaga data *privacy* nasabah terhadap penggunaan *m-banking* dan bagaimana perlindungan yang tertera dalam undang-undang mengenai data *privacy* nasabah terhadap penggunaan *m-bangking*.

METODE

Pada bagian perlindungan bank terhadap data pribadi, penulis mencari, mengumpulkan dan menganalisis informasi melalui buku-buku dan artikel yang berkaitan. Selain itu pada bagian perlindungan data pribadi berdasarkan undang-undang penulis menggunakan metode kepustakaan yang bersifat yuridis normatif dengan pendekatan peraturan perundang-undangan (statutory approach). Soerjono Soekanto dan Sri Mamudji mengatakan bahwa "penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder belaka, dapat dinamakan penelitian hukum normatif atau penelitian hukum kepustakaan". Jenis data yang digunakan dalam penelitian ini adalah data sekunder yang terdiri dari bahan hukum primer, sekunder, dan tersier. Data diambil dengan cara mengumpulkan data yang terdapat dalam peraturan perundangan, buku-buku, dan artikel yang ada hubungannya dengan masalah yang akan di teliti.

HASIL DAN PEMBAHASAN

Perkembangan Mobile Banking

Pada akhir 1995 *Mobile Banking (M-Banking)* diluncurkan pertama kali oleh *Excelcom*. Dengan respon yang beragam. Hampir semua bank-bank yang saat ini ingin mendapat kepercayaan dari setiap nasabahnya menjadi latar belakang di luncurkan nya *m-bangking* ini. Dan salah satu cara yang dilakukan yaitu dengan pemanfaatan teknologi.

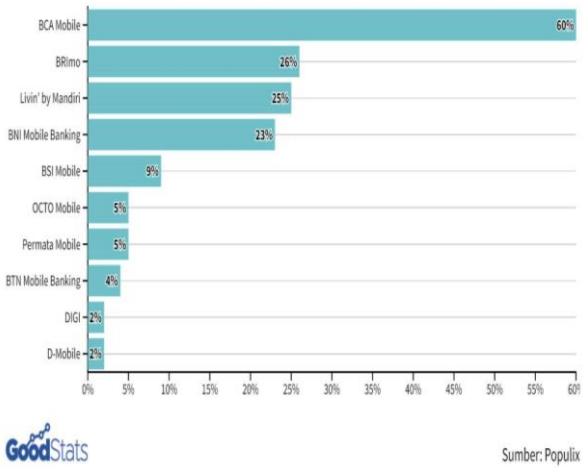
Berdasarkan hasil survei MARS Indonesia tahun 2012 di 5 kota (Jakarta, Bandung, Semarang, Surabaya, Medan) tingkat kesadaran nasabah terhadap mobile

banking melonjak tinggi mencapai 50,4%. Atau meningkat 14,9% dibanding tahun 2008 yang baru mencapai 35,5% dari 1.710 nasabah yang disurvei separuhnya mengaku telah mengetahui mobile banking (Afifah and Widyanesti, 2017).

Hal ini menunjukkan bahwa produk *e-banking* tersebut bukan sesuatuyang asing lagi bagi nasabah perbankan. Nasabah di Jakarta, Bandung dan Semarang relatif lebih mengetahui mobile banking dibandingkan dengan nasabah di Surabaya dan Medan.

Sementara itu data Bank Indonesia mencatatkan, volume transaksi *m-banking* mencapai 3,2 miliar sejak awal tahun hingga Mei 2022. Nilai itu mengalami pertumbuhan 67,87% yoy dari posisi yang sama tahun lalu sebesar 1,90 miliar kali transaksi. Penggunaan smartphone juga akan berpengaruh pada perkembangan mobile banking. Indonesia sebagai negara dengan angka penjualan smartphone tertinggi di asia tenggara menjadi pasar mobile banking yang menjanjikan. Menurut *survey Sharing Vision* kepada 68 orang, 65 persen telah menggunakan smartphone. Dari survey tersebut juga menunjukan bahwa mobile banking cukup sering diakses smartphone mereka. Berdasarkan data-data tersebut dapat dilihat bahwa mobile banking sebenarnya sudah mengalami peningkatan dibanding tahun-tahun sebelumnya.

Selain itu sebuah survei yang dirilis oleh Populix pada tahun 2022 menunjukkan bahwa *mobile banking* dan *e-Wallet* menjadi 2 aplikasi finansial yang paling sering digunakan oleh seluruh kalangan usia. Adapun sebesar 64 persen responden menggunakan aplikasi perbankan atau finansial di smartphone mereka. Secara spesifik, sebesar 91 persen di antaranya memiliki serta menggunakan aplikasi *m-banking* di perangkat masing-masing. Di sisi lain, temuan dari survei ini menunjukkan bahwa mayoritas pengguna aplikasi mobile banking berasal dari wilayah Jabodetabek.



Gambar 1. Hasil poling 10 Aplikasi mobile banking yang banyak digunakan masyarakat Indonesia Tahun 2022

Berdasarkan hasil survei Populix, BCA Mobile berhasil menempati peringkat pertama aplikasi *mobile banking* paling banyak digunakan oleh responden. Adapun persentasenya mencapai 60 persen pada tahun 2022 (Angelia, 2022).

Model sistem keamanan yang digunakan perbankan dalam keamanan data pribadi

Model yang saat ini diadopsi dalam sistem perbankan online didasarkan pada beberapa lapisan keamanan. terdiri dari beragam solusi dan mekanisme paralel yang bertujuan untuk melindungi aplikasi perbankan dan data pengguna, memberikan identifikasi, otentikasi, dan otorisasi.

1. *Digital Certificates*: Sertifikat digital digunakan untuk mengotentikasi pengguna dan sistem perbankan itu sendiri. Autentikasi semacam ini bergantung pada keberadaan Infrastruktur Kunci Publik (PKI) dan Otoritas Sertifikat (CA), yang mewakili pihak ketiga tepercaya yang menandatangani sertifikat yang membuktikan validitasnya.
2. *One-Time Password Tokens:* Perangkat Kata Sandi Satu Kali umumnya digunakan sebagai faktor otentikasi kedua, yang dapat diminta dalam situasi tertentu atau acak.Jenis perangkat ini membuat data autentikasi yang ditangkap tidak berguna untuk serangan di masa mendatang. Dilakukan dengan penggunaan kata sandi yang berubah secara dinamis yang hanya dapat digunakan sekali.
3. *One-Time Password Cards*: Kartu Kata Sandi Sekali Pakai merupakan metode yang lebih murah untuk menghasilkan kata sandi dinamis, juga menyediakan faktor autentikasi kedua. Namun, di beberapa sistem perbankan, kata sandi dihasilkan oleh kartu OTP dapat digunakan kembali beberapa kali sebelum dibuang, Hal ini membuat sistem ini rentan terhadap serangan ulangan jangka pendek.
4. *Browser Protection*: Dalam model ini, sistem diamankan di tingkat peramban Internet, yang digunakan untuk mengakses sistem perbankan. Pengguna browser dilindungi dari malware yang dilakukan dengan memantau area memori yang dialokasikan oleh browser untuk mendeteksi malware dan mencegah pencurian informasi sensitif.
5. *Virtual Keyboards*: Papan ketik virtual dikembangkan untuk menggagalkan penggunaan keylogger yang efisien (yang menangkap informasi yang diketik ke dalam perangkat). Perangkat ini biasanya berbasis Java dan kriptografi berbasis perangkat lunak, memungkinkan portabilitas antara perangkat yang berbeda.
6. *Device Registering*: Metode ini membatasi akses ke sistem perbankan melalui perangkat yang belum dikenal atau terdaftar pada sistem. Perangkat ini menggunakan scan sidik jari untuk identifikasi penggunanya.
7. *CAPTCHA*: Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) yaitu metode yang tujuannya adalah untuk membuat serangan otomatis terhadap sesi yang diautentikasi menjadi tidak efektif. Metode ini mengharuskan pengguna yang sah untuk memasukkan informasi yang disampaikan sebagai gambar acak yang sulit untuk diproses dan dikenali oleh robot otomatis.
8. *Short Message Service (SMS):* Metode ini bertujuan untuk memberi tahu pengguna tentang transaksi yang memerlukan otorisasi mereka. Ini menyediakan saluran otentikasi kedua untuk transaksi yang sesuai dengan karakteristik tertentu dengan

mengirimkan kepada pengguna serangkaian karakter yang harus diinformasikan untuk mengotorisasi dan memproses transaksi melalui sistem perbankan online.

9. *Device Identification*: Model ini biasanya diterapkan bersamaan dengan pendaftaran perangkat tetapi juga digunakan sebagai solusi yang berdiri sendiri dalam sistem perbankan online yang bertujuan untuk memfasilitasi akses pengguna. Model identifikasi ini didasarkan pada karakteristik fisik perangkat pengguna yang memungkinkan untuk mengidentifikasi informasi asal dan riwayatnya.
10. *Positive Identification*: Identifikasi positif adalah model di mana pengguna diminta untuk memasukkan beberapa informasi rahasia yang hanya diketahui olehnya untuk mengidentifikasi dirinya sendiri. Ini diterapkan sebagai metode otentikasi kedua.
11. *Pass-Phrase*: Model keamanan berdasarkan informasi yang dimiliki oleh pengguna. Biasanya digunakan sebagai metode otentikasi kedua dalam transaksi yang melibatkan pergerakan uang.
12. *Transaction Monitoring*: Saat ini model ini diterapkan di semua sistem perbankan online, masing-masing menggunakan teknik yang berbeda. Mulai dari teknik kecerdasan buatan, analisis riwayat transaksi dan metode lain yang digunakan untuk mengidentifikasi polapola penipuan dalam transaksi perbankan sebagai pendekatan untuk pemantauan transaksi perbankan (Peotta et al, 2011).
13. *Secure Socket Layer (SSL)*: merupakan bagian terpenting dari Digital Certificates dimana Digital Certificates salah satu model keamanan Internet Banking. SSL merupakan protokol standar web yang digunakan untuk menjaga keamanan web dengan cara mengenkripsi komunikasi data antara pengguna dengan website yang diakses. Enkripsi merupakan proses pengacakan data sehingga data tidak bisa dibaca oleh pihak lain. Kemudian proses mengembalikan data yang acak menjadi data asli disebut dengan dekripsi. Lalu lintas data melalui sambungan SSL akan selalu di enkripsi sehingga akan menghindari risiko sabotase atau pencurian data. Misalnya data username, password dan data-data penting lainnya. SSL mempunyai cara kerja tersendiri dimana dalam SSL terdapat suatu tanda tangan digital (digital signature). Tanda tangan digital tersebut digunakan untuk memastikan integritas data. Setiap data yang dipertukarkan melalui SSL memiliki tanda tangan digital yang melekat pada SSL tersebut. Tanda tangan digital tersebut juga digunakan untuk memproses data menggunakan algoritma enkripsi, hash dan informasi kunci publik yang ada pada komputer client dan server. Data yang telah melalui proses hash dengan menggunakan kunci publik tidak dapat dikembalikan seperti semula, karena proses hash merupakan

proses enkripsi satu arah. Kemudian data yang telah dihash baik dari komputer client maupun komputer server akan dicocokan (checksum), jika data cocok berarti saluran akses ke website aman, jika tidak cocok berarti sudah terjadi kerusakan atau kebocoran data (Hendarsyah, 2012).

14. *Token (One-Time Password Tokens)*: adalah autentikator lain dalam sistem perbankan online, yang bertanggung jawab untuk membuat kata sandi yang digunakan untuk mengautentikasi transaksi perbankan online dimana token berbentuk kalkulator. Sebelum menggunakan token, kata sandi harus dimasukkan untuk membuka kunci token, jadi token menggunakan kata sandi sebelum membuat kata sandi untuk memastikan keamanan. Sehingga dapat disebut alat otentikasi. Meskipun otentikasi secara garis besar dapat dibagi menjadi empat metode, yaitu:
    a. *Something You Know*: Ini adalah metode otentikasi yang paling umum. Metode ini didasarkan pada kerahasiaan informasi seperti kata sandi atau kode PIN. Teknik ini mengasumsikan bahwa tidak ada yang mengetahui rahasia tersebut kecuali pemilik asli hak akses tersebut.
    b. *Something You Have*: Metode ini merupakan elemen tambahan yang membuat autentikasi lebih aman. Metode ini didasarkan pada item unik, misalnya kartu magnetik/pintar, token perangkat keras, token USB, dll. Metode ini mengasumsikan bahwa tidak ada yang memiliki barang tersebut kecuali pemilik aslinya.
    c. *Something You Are*: Cara ini juga jarang digunakan karena faktor teknis dan manusia. Cara ini mengandalkan keunikan bagian tubuh asli pengguna yang
    mungkin tidak ada pada orang lain, seperti: sidik jari, sidik suara, sidik retina atau sidik bibir. Cara ini mengasumsikan bahwa bagian tubuh pemegang akses, seperti sidik jari, retina, atau bibir, tidak dapat identik dengan milik orang lain.
    d. *Something You Can*: metode ini mengasumsikan bahwa tidak seorang pun di dunia dapat melakukan hal yang sama seperti pemegang lisensi asli. Misalnya, tanda tangan materai. Faktanya, otentikasi tanda tangan didasarkan pada asumsi bahwa tidak seorang pun kecuali pemilik tanda tangan yang dapat merekam tanda tangan tersebut. Padahal sebenarnya ada orang yang sangat pandai meniru tanda tangan orang lain. Namun demikian, tanda tangan di atas kertas tetap diterima sebagai bukti otentik pemegang tanda tangan (Hendarsyah, 2018).

Perundang-Undangan yang berkaitan dengan perlindungan data pribadi terhadap pengguna layanan bangking.

Di Indonesia sendiri belum ada peraturan hukum perundang-undangan yang mengatur secara khusus tentang perlindungan

data pribadi pengguna layanan *mobile banking*. Namun aturan ini dapat ditemukan pada beberapa peraturan yang terkait dengan perlindungan kerahasiaan data pribadi nasabah. Adapun peraturan-peraturan yang terkait dengan pelindungan nasabah pengguna internet diantaranya:

1. Pada pasal 29 ayat (4) Undang-undang Nomor 10 tahun 1998 yang menyatakan bahwa untuk kepentingan nasabah, bank wajib menyediakan informasi mengenai kemungkinan timbul resiko kerugian sehubungan dengan transaksi nasabah yang dilakukan oleh bank. Dengan ketentuan tersebut sudah seharusnya penerapan ini dilakukan tidak hanya waktu diminta saja namun bank harus aktif dalam memberikan informasi-informasi yang berhubungan dengan resiko kerugian sehubungan dengan transaksi nasabah yang dilakukan oleh bank.(Astrini 2015)
2. Pasal 40 ayat (1) dan (2), Undang-undang Nomor 10 tahun 1998 yang menyatakan bahwa Bank diwajibkan untuk merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya, kecuali dalam hal sebagaimana dimaksud dalam Pasal 41, Pasal 41A, Pasal 42 Pasal 43, Pasal 44 dan Pasal 44A. Pasal-pasal pengecualian tersebut adalah apabila untuk kepentingan perpajakan, untuk penyelesaian piutang bank, untuk kepentingan peradilan dalam perkara pidana serta atas permintaan, persetujuan atau kuasa dari nasabah penyimpan, dimana bank dapat melanggar ketentuan mengenai rahasia bank ini tentunya dengan prosedur-prosedur tertentu.
3. Peraturan Bank Indonesia Nomor 7/6/PBI/2005 tentang transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah. Dalam hal ini bank wajib menerapkan transparansi informasi tentang produk bank dan penggunaan data pribadi nasabah. Bank diwajibkan memberi informasi kepada nasabah dan calon nasabah mengenai produk-produk yang diterbitkan oleh bank maupun lembaga keuangan lain yang di pasarkan memalui bank (Dewi 2017)
4. Pasal 4 huruf a, Undang-undang Nomor 8 Tahun 1999 yang menyatakan bahwa hak konsumen atas kenyamanan, keamanan dan keselamatan dalam mengkonsumsi barang dan/atau jasa. Menjadi tanggungjawab pihak bank sebagai penyedia jasa, bahkan bank akan memberikan yang terbaik dalam pelayanannya kepada nasabah dan konsumen pengguna berhak mendapatkan fasilitas terbaik terutama dalam hal ini, berkaitan dengan keamanan nasabah sendiri (Astrini 2015).
5. Pasal 4 huruf d Undang-undang Nomor 8 Tahun 1999 menyatakan bahwa “hak untuk didengar pendapat dan keluhannya atas barang dan/atau jasa yang digunakan”. Aturan ini memberikan kesempatan kepada konsumen untuk dapat menyampaikan kekurangan kekurangan dari pelayanan jasa internet banking yang diberikan oleh bank.

6. Pasal 4 huruf h, Undang-undang Nomor 8 Tahun 1999 yang menyatakan bahwa tentang hak konsumen untuk mendapatkan kompensasi dan/atau ganti rugi bila barang dan/atau jasa yang diterima tidak sesuai dengan perjanjian atau tidak sebagaimana mestinya pada pasal 19 Ayat (1) dan Ayat (2) yang juga berisi tentang kewajiban pelaku usaha untuk memberikan ganti rugi
7. Undang-undang Nomor 36 Tahun 1999 Tentang Telekomunikasi. Pasal 15 Undang-Undang Telekomunikasi mengatur tentang kesalahan dan kelalaian penyelenggara telekomunikasi yang menimbulkan kerugian, maka pihak-pihak yang dirugikan berhak menuntut ganti rugi. Ganti rugi wajib diberikan , Kecuali mereka dapat membuktikan bahwa kerugian yang muncul bukan karena kelalaian penyelenggara telekomunikasi (Pujiyono 2021).

Pasal 22 Undang-undang Telekomunikasi tersebut terdapat dalam Pasal 50 menyatakan bahwa:"Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam pasal 22, dipidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah)" (Astrini 2015).

KESIMPULAN

Berdasarkan survei yang dirilis oleh Populix pada tahun 2022 menunjukkan bahwa mobile banking dan e-Wallet menjadi 2 aplikasi finansial yang paling sering digunakan. Secara spesifik, sebesar 91 persen menggunakan aplikasi *m-banking* di perangkat seluler masing-masing. Untuk menjaga data nasabah, perbankan dalam layanan *m-banking* melakukan model keamanan seperti : menggunakan *One-Time Password Tokens, One-Time Password cards, SSL, Token (One-Time Password Tokens)* dan model keamanan lainnya. Di Indonesia belum terdapat peraturan hukum perundang-undangan yang mengatur secara khusus tentang perlindungan data pribadi pengguna layanan *mobile banking.* Namun terdapat aturan aturan yang terkait dengan perlindungan kerahasiaan data pribadi seperti yang tetera pada pasal 40 ayat (1) dan (2), Undang-undang Nomor 10 tahun 1998.

UCAPAN TERIMA KASIH

Dengan selesainya paper ini. Penulis mengucapkan terima kasih kepada semua pihak yang terlibat dalam membantu meneyelesaikan paper ini.

DAFTAR PUSTAKA

Afifah, Fadhilah, and Sri Widyanesti. (2017). Analisis Penggunaan Mobile Banking Dengan Mengadopsi Technology Acceptance Model (Tam) (Studi Kasus Pada Bank Central Asia Di Jakarta)." *e-Proceeding of Management* 4(1): 46–52.

Angelia, Diva. (2022). "Aplikasi Mobile Banking Paling Banyak Digunakan Masyarakat Indonesia. https://goodstats.id/article/aplikasi-mobile-banking-paling banyakdigunakanmasyarakat-indonesia-2022-Vb18i. (Diakses pada 2 Mei 2023 pukul 03:47wib).

Astrini, Dwi Ayu. (2015). Perlindungan Hukum Terhadap Nasabah Bank Pengguna Internet Banking Dari Ancaman Cybercrime. *Lex Privatum*

III(1): 149–60. file:///C:/Users/tania/Downloads/jak_lexprivatum,+14.+Dwi+Ayu+Astrini.pdf.

Dewi, Sinta. (2017). Principles of Personal Data Protection Customer Credit Card According To. *Sosiohumaniora* 19(3): 206–12.

Hendarsyah, Decky. (2012). Keamanan Layanan Internet Banking Dalam Transaksi Perbankan. *Iqtishaduna: Jurnal Ilmiah Ekonomi Kita* 1(1): 12–33.

Nandavita, Alva yenica. (2021). Analisis Pengaruh Kepercayaan Nasabah Terhadap Risiko Menggunakan Layanan E-Banking. : 28–38.

Peotta, Laerte et al. (2011). A Formal Classification of Internet Banking Attacks and Vulnerabilities. *International Journal of Computer Science and Information Technology* 3(1): 186–97.

Pujiyono, Agung Budiarto; (2021). Perlindungan Hukum Nasabah Pengguna Mobile Banking. *Jurnal Privat Law* 9(Vol 9, No 2 (2021): Juli-Desember): 300–308.