



LEMAHNYA KEAMANAN BANK PEMERINTAH DI INDONESIA: STUDI KASUS PERETASAN BANK BRI TERHADAP NASABAHNYA

Jonathan Jordan Sianipar

jonathansianipar93@students.unnes.ac.id

Fakultas Hukum, Universitas Negeri Semarang

Marta Solavide Naibaho

martasolavide@students.unnes.ac.id

Fakultas Hukum, Universitas Negeri Semarang

Sekaran, Gunungpati

Kota Semarang, Jawa Tengah, 50229

Korespondensi penulis: jonathansianipar93@students.unnes.ac.id

Abstract *A government bank is a bank that is partially or wholly owned by the Indonesian government. All profits of state-owned banks also belong to the government. The types of government banks include Bank Rakyat Indonesia (BRI), Bank Mandiri, Bank Negara Indonesia (BNI), Bank Tabungan Negara (BTN), and Bank Syariah Indonesia (BSI). In the past in the banking world, to conduct all forms of transactions must go through a bank teller, and now because of the changing times, then all forms of transactions can be accessed easily through m-banking, which we can access on our handphone, but behind the ease of accessing it, on the other hand, it also has negative impacts such as the ease with which our bank accounts can be hacked by others. For this reason, the purpose of this paper is to understand what factors cause weak bank security and how banks should handle hacking cases that occur to their customers, by using empirical juridical research methods, namely raising case studies about Bank BRI hacking that actually occur in society.*

Keyword: *Bank BRI; Bank Security; Hacking*

Abstrak Bank pemerintah adalah bank yang sebagian atau seluruh sahamnya dimiliki oleh pemerintah Indonesia. Seluruh keuntungan bank pemerintah juga menjadi milik pemerintah. Jenis-jenis dari bank pemerintah antara lain yaitu Bank Rakyat Indonesia (BRI), Bank Mandiri, Bank Negara Indonesia (BNI), Bank Tabungan Negara (BTN), dan Bank Syariah Indonesia (BSI). Dahulu dalam dunia perbankan, untuk melakukan segala bentuk transaksi harus melalui teller bank, dan sekarang karena adanya perubahan zaman, maka segala bentuk transaksi dapat diakses dengan mudah melalui *m-banking* yang bisa kita akses di *handphone* saja, namun dibalik mudahnya pengaksesan tersebut, disisi lain juga memiliki dampak negatif seperti mudahnya akun bank kita diretas oleh orang lain. Untuk itu tujuan dari penulisan ini adalah memahami faktor apa saja yang menyebabkan masih lemahnya keamanan bank dan bagaimana seharusnya pihak bank menangani kasus peretasan yang terjadi pada nasabahnya, dengan menggunakan metode penelitian yuridis empiris yaitu mengangkat studi kasus tentang peretasan Bank BRI yang benar-benar nyata terjadi di masyarakat.

Kata Kunci: Bank BRI; Keamanan Bank; Peretasan

PENDAHULUAN

Peretasan merupakan tindakan untuk mengakses sistem komputer atau jaringan secara tidak sah dengan cara mengeksploitasi kelemahannya. Biasanya tujuan dari peretasan ini untuk mencuri data pribadi atau finansial, memperoleh keuntungan finansial untuk pribadi, dan lain sebagainya.¹ Peretasan biasanya terjadi melalui aplikasi yang di dalamnya memiliki nilai berharga, seperti *mobile banking* atau yang disingkat dengan *m-banking* atau seperti dompet

¹ <https://www.bola.com/ragam/read/5658489/arti-peretasan-beserta-macam-macam-aspek-pentingnya>

digital. Peretasan ini sudah cukup banyak terjadi di Indonesia dan sangat merugikan masyarakat. Seperti salah satu contoh kasus yang terjadi pada salah satu *followers* akun Tiktok @realmrbert, *followers*-nya itu mengadu dan menceritakan kepada Mr. Bert (si pemilik akun @realmrbert) melalui chat di aplikasi Tiktok tentang apa yang dialaminya. Bermula pada bulan Maret tahun 2022, seorang nasabah BRI kita sebut saja namanya Hengky, ia mendapatkan pesan dari akun Bank BRI yang asli melalui WhatsApp, isi pesan tersebut tertulis bahwa Hengky telah merubah nama serta nomor teleponnya di Kantor BRI dan perubahan tersebut sudah berhasil, yang menjadi permasalahan di sini adalah Hengky tidak pernah melakukan perubahan tersebut, hal itu terjadi secara tiba-tiba tanpa sepengetahuan Hengky, padahal ketika seorang nasabah ingin mengganti nama atau nomor telepon, wajib menunjukkan KTP, buku tabungan, dan nomor kartu debit.

Karena Hengky merasa tidak pernah melakukan perubahan nama atau nomor telepon, ia segera menelepon CS (*Costumer Service*) BRI dan menghubungi Sabrina (nomor telepon CS resmi BRI), serta mengirimkan *e-mail* ke Bank BRI untuk solusi dari permasalahan ini, namun jawaban dari CS BRI hanya menyarankan Hengky untuk *uninstall* BRI-mo (BRI *mobile*), jawaban tersebut hanya normatif, sama sekali tidak menyelesaikan masalah karena walaupun di *uninstall* nanti masih bisa terjadi lagi. Dari permasalahan tersebut apakah ada oknum di dalamnya, atau ada sistem yang salah dalam menjaga keamanan data nasabah Bank BRI. Inilah gambaran potrait dari keamanan Bank Pemerintah di Indonesia terutama Bank BRI, padahal Bank BRI mendapatkan keuntungan dari nasabahnya. Untuk contoh yang dilansir pada infobank.news tertulis dalam artikel tersebut bahwa laba BRI tahun 2023 tembus Rp60,4 Triliun, melesat 17,5%.² Namun, dengan Bank BRI mendapat keuntungan sebesar itu, seharusnya bisa memberikan dana yang cukup untuk menambah keamanan dari Bank BRI, karena ini adalah hak kita, kelayakan kita sebagai nasabah Bank BRI untuk mendapatkan keamanan yang sebanding. Ternyata ada ribuan kasus serangan *cyber* yang lolos, dan Bank BRI adalah bank yang paling banyak jebol dan kasusnya dianggap kesalahan/kelalaian dari pihak nasabah, ketika nasabah mengadu, tidak ada tanggapan dari pihak Bank BRI, semuanya dilemparkan kepada nasabah karena suatu bank tidak pernah merasa bersalah.

KAJIAN TEORI

Teori merupakan alat yang digunakan untuk membantu orang memahami dan menjelaskan dunia sekeliling kita. Dari latar belakang yang sudah dijabarkan di atas, maka penulis mendapat kajian teori berupa teori kriminologi. Teori kriminologi sangat erat kaitannya dengan perubahan masyarakat, perubahan tersebut terjadi akibat dari adanya kemajuan teknologi yang berkembang, hal itu bisa menimbulkan terjadinya kejahatan. Menurut Hartanto (2015), dilihat dari aspek sosiologi bisa ditarik suatu kesimpulan bahwa kejahatan merupakan salah satu jenis gejala sosial yang terjadi pada individu atau masyarakat. Dalam kriminologi, teori ini membantu kita memahami cara kerja sistem peradilan pidana dan siapa yang berperan dalam sistem peradilan. Teori kejahatan bisa digunakan dalam penegakan hukum pidana karena memberikan jawaban dari pertanyaan terkait kenapa dan bagaimana orang atau suatu perbuatan dianggap jahat di masyarakat.

Beberapa penelitian sebelumnya yang relevan dan memberikan penjabaran tentang kejahatan *cyber* di Indonesia, yakni penelitian terkait pencurian data yang diperbuat oleh *hacker* (Sulirudatin, 2018; Widayanti, 2018). Dalam penelitian tersebut dijelaskan tentang tindak pidana untuk pelaku kejahatan *cyber*, tetapi belum adanya artikel yang menjelaskan teori-teori

² <https://infobanknews.com/cetak-rekor-laba-bri-2023-tembus-rp604-triliun-melesat-175-persen/>

kriminologi pada kejahatan *cyber* tersebut. *M-banking* dan *internet banking* membuat adanya kemungkinan dari masyarakat untuk melakukan transaksi jual-beli melalui aplikasi perbankan. Sudah pasti, berdasarkan kemudahan tersebut ada resiko dan ancaman yang besar untuk pengguna layanan teknologi informasi tersebut. Pada beberapa kasus, bank bisa mendapat gangguan pelayanan digital karena serangan *hacker*. Penjahat *cyber* akan mencuri data-data pribadi nasabah dan nantinya data itu bisa dipakai sebagai alat pencucian uang dan juga terorisme.

RUMUSAN MASALAH

Dari penjabaran latar belakang yang sudah dirunut di atas, maka penulis mendapat rumusan masalah sebagai berikut:

1. Faktor apa saja yang menyebabkan masih lemahnya keamanan pada Bank Pemerintah?
2. Bagaimana langkah atau solusi yang dilakukan oleh suatu bank jika nasabahnya mengalami peretasan bank?

METODE PENELITIAN

Metode penelitian sebenarnya diambil dari bahasa Yunani, yakni '*methodos*' yang memiliki arti "langkah/cara menuju suatu jalan". Metode adalah aktivitas akademis, relevansinya terhadap suatu prosedur (tersusun) guna mendapatkan pemahaman suatu subjek atau objek dari penelitian kita sebagai usaha guna mendapatkan jawaban yang bisa dipertanggungjawabkan melalui akademis serta keasliannya³, sedangkan arti dari penelitian merupakan suatu cara untuk mengumpulkan dan menganalisis suatu data yang dilakukan dengan cara kerja yang baik guna mencapai tujuan tertentu.⁴ Jadi, berdasarkan penjabaran di atas tentang metode dan penelitian, artinya suatu proses guna memecahkan masalah ataupun proses mengembangkan ilmu pengetahuan dengan memakai metode ilmiah. Metode penelitian hukum empiris (yuridis empiris) adalah metode penelitian hukum yang meneliti aturan hukum apa yang terjadi dan berlaku pada realita di masyarakat, penelitian ini dilakukan terhadap kondisinya yang sesungguhnya terjadi di masyarakat dengan maksud untuk mendapatkan fakta-fakta yang dipergunakan menjadi data penelitian yang selanjutnya data tersebut dianalisis guna menentukan masalah yang akan dibuat menjadi rumusan masalah dan pada akhirnya menuju pada penyelesaian masalah.⁵

PEMBAHASAN

Faktor yang Menyebabkan Masih Lemahnya Keamanan pada Bank Pemerintah

Maraknya kasus ancaman *cyber* yang terjadi dikarenakan macam-macam faktor, salah satunya adalah semakin meningkatnya akses pengguna *online*. Banyaknya informasi data pribadi yang masuk dan lemahnya sistem keamanan pada teknologi *online* tersebut memudahkan penyerangan pencurian informasi data. Semakin tingginya pemanfaatan teknologi internet justru juga menjadi tantangan baru dalam melindungi data pribadi, apalagi pada pengumpulan, pemanfaatan, dan penyebaran data pribadi seseorang.⁶ Ancaman yang sering terjadi adalah penipuan yang memanfaatkan celah penggunaan teknologi digital. Dengan cepatnya teknologi

³ Rosady Ruslan, *Metode Penelitian Public Relations dan Komunikasi*, Jakarta: Rajawali Pers, 2003. hlm. 24.

⁴ Dr. Jonaedi Efendi, S.H.I., M.H., Prof. Dr. Johnny Ibrahim, S.H., S.E., M.M., M.Hum., *Metode Penelitian Hukum: Normatif dan Empiris*, Depok: Prenadamedia Group, 2006. hlm. 3.

⁵ Muhammad Hendri Yanova, Parman Komarudin, Hendra Hadi, *Metode Penelitian Hukum: Analisis Problematika Hukum Dengan Metode Penelitian Normatif dan Empiris*, Badamai Law Journal, Vol. 8, No. 2, 2023

⁶ Sahat Parulian, Devi Anassalifa Pratiwi, Meiliya Cahya Yustina, *Ancaman dan Solusi Serangan Siber di Indonesia*, Jurnal UPI, Vol. 1, No. 2, 2021.

dan informasi berkembang untuk mendukung inisiatif *e-government*, permintaan untuk arsip digital pada instansi pemerintah semakin tinggi, membuat keamanan data menjadi perhatian penting yang tidak bisa dihindari.⁷ Apalagi, saat ini Bank di Indonesia mendorong digitalisasi semua layanan perbankan untuk mewujudkan masyarakat tanpa uang tunai atau *cashless society*. Beberapa hal yang masih menyebabkan keamanan bank itu rentan diretas: (1) Keamanan yang tidak berlapis. Penyebab ini berkaitan dengan kurangnya tingkat keamanan yang dimiliki Indonesia. Seharusnya diperlukan keamanan berlapis untuk keamanan server database, salah satu contohnya menggunakan *firewall* untuk mengontrol lalu lintas jaringan yang masuk dan keluar dari server dan database, serta menerapkan kebijakan akses yang cukup ketat. (2) *Backup* data. *Membackup* data merupakan hal yang cukup penting dan jangan sampai disepelekan setelah data terlindungi. *Backup* data bukan hanya memiliki fungsi ketika server mendapat serangan *cyber*, namun juga bencana alam dan kejadian yang tak diduga kapan terjadinya. Sebaiknya back up data dilakukan secara berkala. (3) Minimnya rencana merespon serangan. Hal ini disebut dengan *crisis preparedness* atau persiapan krisis. Mungkin masih ada beberapa bank di Indonesia yang belum mempersiapkan rencana untuk menanggapi serangan dari *hacker*. (4) Kurangnya perhatian/pengawasan dari manajemen internal bank. Faktor ini juga menjadi salah satunya karena kurangnya pengawasan dari dewan direksi atau manajemen yang menjadi permasalahan yang signifikan bagi banyak bank yang gagal diantaranya adalah kurangnya jaminan kepatuhan sistem terhadap kebijakan-kebijakan internal atau undang-undang perbankan dan/atau kurangnya kontrol atau pengawasan dari pejabat utama bank atau departemen.

Mungkin itulah beberapa faktor yang bisa dijabarkan, perlu menjadi perhatian khusus untuk kita menjaga keamanan akun *m-banking* kita, apalagi di zaman sekarang dengan banyaknya kemudahan dalam membobol sistem jaringan.

Langkah/Solusi yang Dilakukan oleh Suatu Bank jika Nasabahnya Mengalami Peretasan Bank

Mengapa penulis melihat dan menuntut dari sudut pandang pihak bank, karena “berdasarkan riset F5, masih banyak nasabah Indonesia yang meragukan keamanan siber di sektor perbankan. Hanya sekitar 57% saja nasabah yang percaya bahwa perbankan cukup efektif dalam menjaga keamanan siber” kata Surung SInamo, Country Manager F5, dalam acara konferensi pers virtual pada Rabu (3/3), padahal bank selaku badan usaha sekaligus penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap sistem elektronik sebagaimana mestinya. Berdasarkan ketentuan di atas, maka suatu bank harus mempunyai sistem keamanan yang mencukupi pada sistem elektroniknya. Tujuannya adalah guna melindungi data dan transaksi nasabah dari pengaksesan yang tidak sah serta ancaman keamanan lainnya. Apabila suatu bank tidak bisa memenuhi aturan tersebut, maka bisa dikenakan sanksi administratif oleh OJK berupa teguran berbentuk tulisan, larangan untuk menerbitkan produk baru, pembekuan kegiatan usaha tertentu, dan/atau penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan bank. Bank yang terkena serangan *cyber* sehingga membuat transaksi nasabah tersumbat dan menyebabkan hilangnya uang nasabah, merupakan bentuk kelalaian bank dalam melaksanakan kewajibannya berdasarkan peraturan perundang-undangan yang berlaku. Langkah/solusi yang bisa dilakukan oleh suatu bank ketika nasabahnya mengalami peretasan akun bank adalah dapat disepakati oleh nasabah dan bank, contohnya dalam bentuk ganti rugi, untuk tambahan, jika bank ditimpa oleh serangan *cyber* dan

⁷ Eko Jhony Pranata, Lukman Ependi, *Phising Terhadap Website Bank BCA*, Jurnal Trends, Vol. 1, No. 1, 2023.

menyebabkan data pribadi nasabah menjadi bocor, maka berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, nasabah berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi, sebab dalam UU Perlindungan Data Pribadi, bank dapat digolongkan sebagai pengendali data pribadi yakni tiap-tiap orang, badan publik, dan organisasi internasional yang bertindak secara sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan data pribadi. Dan dalam kasus di atas, karena bank tidak menjaga akun bank nasabahnya dengan benar, jadi tolong lebih teliti lagi untuk perubahan data yang dilakukan karena semua akun bank dipegang oleh pihak bank, jangan biarkan data berubah-ubah seenaknya, pihak bank bisa mengatasi masalah tersebut dengan mengecek perubahan data tersebut dan mengganti lagi kembali seperti semula, karena kita tidak tahu siapa oknum dibalik kasus tersebut, apalagi dalam hal perubahan data apakah ada yang meretas atau memang pihak bank yang sengaja merubahnya.

PENUTUP

Kesimpulan

Sistem perbankan yang sudah berubah pasti memiliki dampak positif yaitu segala bentuk transaksi bisa lebih cepat dan efisien, seperti transfer, membayar pengeluaran, dll, namun dibalik itu pasti ada dampak negatifnya juga seperti mudahnya akun bank diretas, faktor-faktor tersebut bisa berasal dari dalam (internal) pihak bank seperti sistem keamanan yang masih harus diperbaiki agar memiliki progres yang baik untuk keamanan akun bank nasabah dan masih kurangnya perhatian dari manajemen bank, faktor dari luar bisa dari pihak kominfo untuk lebih memperketat keamanan dalam bidang komunikasi dan informasi. Langkah atau solusi yang bisa dijadikan jalan keluar oleh pihak bank jika akun bank nasabah diretas, mulanya nasabah dan pihak bank bisa melakukan kesepakatan, maka akan ada ganti rugi dari pihak bank, karena kita sebagai nasabah menabung di bank, maka seluruh keuangan kita menjadi tanggung jawab pihak bank, apalagi pihak bank mendapat keuntungan dari nasabah dalam bentuk bunga, dan sebagai tambahan, jika bank ditimpa oleh serangan *cyber* dan menyebabkan data pribadi nasabah menjadi bocor, maka berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, nasabah berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi, sebab dalam UU Perlindungan Data Pribadi, bank dapat digolongkan sebagai pengendali data pribadi yakni tiap-tiap orang, badan publik, dan organisasi internasional yang bertindak secara sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan data pribadi.

DAFTAR PUSTAKA

Buku

Ruslan R., *Metode Penelitian Public Relations dan Komunikasi*, Jakarta: Rajawali Pers, 2003.

Efendi, J., Ibrahim, J., *Metode Penelitian Hukum: Normatif dan Empiris*, Depok: Prenadamedia Group, 2006.

Jurnal

Yanova, M., H., Komarudin, P., Hadi, H., *Metode Penelitian Hukum: Analisis Problematika*

Hukum Dengan Metode Penelitian Normatif dan Empiris, Badamai Law Journal, Vol.

8, No. 2, 2023.

Pranata, E., J., Ependi, L., *Phising Terhadap Website Bank BCA*, Jurnal Trends, Vol. 1, No.

1, 2023.

Parulian, S., Pratiwi, D., A., Yustina, M., C., Meiliya Cahya Yustina, *Ancaman dan Solusi Serangan Siber di Indonesia*, Jurnal UPI, Vol. 1, No. 2, 2021.

Duana, G., R., Masyar, A., Wulandari, C., *Tinjauan Teori Kriminologi Dalam Kejahatan Siber (Kasus Kebocoran Data Nasabah)*, Journal Trisaksi, Vol. 11, No. 2, 2024.

Novira, E., *Faktor-Faktor Esensial Bank Gagal*, Jurnal Jurisprudencia, Vol. 5, No. 2, 2023.

Undang-Undang

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Undang-Undang Nomor 11 Tahun 2022 tentang Peraturan Otoritas Jasa Keuangan

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Website

Yulianto, H. S., *Arti Peretasan beserta Macam-Macam Aspek Pentingnya*, bola.com, <https://www.bola.com/ragam/read/5658489/arti-peretasan-beserta-macam-macam-aspek-pentingnya>, 2024.

Ibrahim, M., *Cetak Rekor! Laba BRI 2023 Tembus Rp60,4 Triliun, Melesat 17,5 Persen*, infobanknews.com, <https://infobanknews.com/cetak-rekor-laba-bri-2023-tembus-rp604-triliun-melesat-175-persen/>, 2024.

Salim, F., M., *Tanggung Jawab Bank Jika Terkena Serangan Siber*, hukumonline.com, <https://www.hukumonline.com/klinik/a/tanggung-jawab-bank-jika-terkena-serangan-siber-lt64c399574869f/>, 2023