Perlindungan Konsumen di Sektor Jasa Keuangan pada Kasus Serangan Siber *Ransomware* yang Menimpa Perbankan

Diana Afifah
Universitas Indonesia
E-mail : dianaffh@yahoo.com

Article Info
Article History
Received: 2023-09-17
Revised: 2023-10-23
Published: 2023-11-04

Keywords:
Consumer Protection;
Financial Services;
Ransomware;
Customer Protection.

Abstract
This paper focuses on the ransomware cyber attack that affected PT Bank Syariah Indonesia (Bank BSI) and its impact on consumer protection in the financial services sector. The research method used is a normative juridical approach, employing secondary data and literature study techniques. By examining the Consumer Protection Act No. 8 of 1999 and the Financial Services Authority Regulation (POJK) 6/2022, this paper highlights the importance of information transparency in the financial services sector and the legal protection that should be provided to consumers. In the context of Bank BSI, the lack of information transparency provided to customers in addressing cyber attacks leads to losses and damages consumer trust. Furthermore, this paper also emphasizes Bank BSI's responsibility in managing customers' personal data by ensuring the security of the information technology used. As a result, the cyber attack on Bank BSI underscores the need for improvements in information transparency and legal consumer protection in the financial services sector.

Artikel Info
Sejarah Artikel
Diterima: 2023-09-17
Direvisi: 2023-10-23
Dipublikasi: 2023-11-04

Kata kunci:
Perlindungan Konsumen;
Jasa Keuangan;
Ransomware;
Perlindungan Nasabah.

Abstrak
Tulisan ini berfokus pada serangan siber ransomware yang menimpa PT Bank Syariah Indonesia (Bank BSI) dan dampaknya terhadap perlindungan konsumen di sektor jasa keuangan. Metode penelitian yang digunakan adalah pendekatan yuridis normatif dengan menggunakan data sekunder dan teknik studi kepustakaan. Melalui tinjauan terhadap Undang-Undang Perlindungan Konsumen No. 8 Tahun 1999 dan Peraturan Otoritas Jasa Keuangan (POJK) 6/2022, tulisan ini menyoroti pentingnya transparansi informasi dalam sektor jasa keuangan dan perlindungan hukum yang harus diberikan kepada konsumen. Dalam konteks Bank BSI, kurangnya transparansi informasi yang disampaikan kepada nasabah dalam mengatasi serangan siber menimbulkan kerugian dan merusak kepercayaan konsumen. Selain itu, tulisan ini juga menekankan tanggung jawab Bank BSI dalam mengelola data pribadi nasabah dengan memastikan keamanan teknologi informasi yang digunakan. Implikasinya, serangan siber pada Bank BSI menunjukkan perlunya perbaikan dalam aspek transparansi informasi dan perlindungan hukum konsumen dalam sektor jasa keuangan.

I. PENDAHULUAN

Dalam era digital yang semakin maju, serangan siber menjadi ancaman serius bagi berbagai sektor, termasuk diantaranya sektor perbankan. Serangan siber dapat merusak keamanan dan privasi data, mengganggu operasional perusahaan, dan merugikan nasabah bank secara finansial. Salah satu bentuk serangan yang cukup umum adalah serangan siber *ransomware*. Serangan siber *ransomware* melibatkan peretas yang mengenkripsi data penting nasabah dan meminta tebusan dalam bentuk mata uang digital agar data tersebut dapat dikembalikan. Serangan ini tidak hanya memengaruhi nasabah perorangan, tetapi juga dapat berdampak pada bisnis kecil, perusahaan besar, dan bahkan institusi keuangan. Cara kerja Ransomware yaitu dengan cara menyalurkan malware melalui rekayasa sosial dan interaksi antar pengguna. Ransomware adalah malware untuk pencurian data melakukan enkripsi data korban dan juga membatasi pengguna untuk melakukan akses kepada data yang dicuri.

Beberapa waktu lalu terjadi serangan siber yang cukup meresahkan masyarakat Indonesia dialami oleh salah satu Bank BUMN yaitu PT Bank Syariah Indonesia (Bank BSI) dan sempat melumpuhkan sistem perbankan Bank BSI selama kurang lebih 1 minggu. Serangan siber yang terjadi pada tanggal 8 hingga 11 Mei 2023 tersebut membuat nasabah Bank BSI sama sekali tidak dapat mengakses dan melakukan transaksi keuangan baik melalui layanan *mobile banking*, kantor cabang, dan ATM Bank BSI. Sistem perbankan Bank BSI benar-benar lumpuh dikarenakan serangan siber ini.

Berdasarkan *press release* yang dibuat oleh Bank BSI pada 8 Mei 2023, disampaikan juga

bahwa pada tanggal tersebut Bank BSI sedang melakukan maintenance sistem guna meningkatkan pelayanan dan akan kembali normal secepatnya. Rilis ini disampaikan oleh Bank BSI pada akun media sosial Instagram Bank BSI @banksyariahindonesia. Hal yang sama juga disampaikan oleh *Corporate Secretary* BSI, Gunawan Arief Hartoyo yang dikutip dari laman liputan 6, Gunawan menyampaikan:

> *"BSI berkomitmen untuk terus meningkatkan pelayanan kepada nasabah, dan tentunya sangat berterima kasih atas kepercayaan yang telah diberikan nasabah kepada Bank Syariah Indonesia. Sebagai bentuk peningkatan layanan, saat ini sedang dilakukan maintenance sistem di BSI sehingga tidak dapat diakses untuk sementara waktu. Kami memohon maaf, untuk sementara waktu nasabah terkendala dalam mengakses layanan BSI dan kami memastikan dana nasabah tetap aman. Untuk itu seluruh nasabah agar tetap waspada dan berhati-hati atas segala bentuk modus penipuan yang mengatasnamakan Bank Syariah Indonesia"*

Namun hal yang sangat disayangkan dari Bank BSI, ternyata perbaikan sistem tersebut tidak kunjung selesai hingga muncul pernyataan dari Menteri BUMN, Erick Thohir, pada tanggal 10 Mei 2023 bahwa telah terjadi serangan siber terhadap system Bank BSI yang membuat sistem perbankan mereka down. Menindaklanjuti hal tersebut kemudian Bank BSI akhirnya mengakui bahwa telah terjadi serangan siber tersebut berupa *ransomware* dan sistem perbankan mulai berangsur pulih.

Dalam konteks perlindungan konsumen, nasabah bank yang terkena serangan siber *ransomware* menghadapi berbagai masalah dan risiko. Pertama, kerahasiaan data pribadi nasabah dapat terancam, seperti informasi identitas, nomor rekening bank, dan data keuangan sensitif lainnya. Kedua, akses ke akun bank dan transaksi keuangan dapat terhalang, menyebabkan ketidaknyamanan dan gangguan dalam kegiatan keuangan sehari-hari. Ketiga, nasabah juga berpotensi mengalami kerugian finansial yang signifikan akibat tebusan yang harus dibayarkan kepada peretas.

Hal ini juga terjadi dalam kasus serangan siber ke Bank BSI dimana dampak dari lumpuhnya system Bank BSI sangat dirasakan oleh warga Aceh. Sebagaimana diketahui bahwa di Provinsi Aceh yang menerapkan Otonomi Khusus dan mengacu pada Qanun Aceh No. 11 Tahun 2018 tentang Lembaga Keuangan Syariah maka seluruh layanan yang perbankan dan produk keuangan lainnya yang dapat diakses di Provinsi Aceh hanyalah yang memiliki skema syariah. Sehingga akibat dari serangan siber yang menimpa Bank BSI sebagai bank syariah terbesar yang beroperasi di Aceh ini nyaris melumpuhkan system perekonomian di Aceh dimana sebagian besar masyarakat, pebisnis, dan UMKM merupakan nasabah Bank BSI yangh tidak dapat melakukan aktivitas perbankan, termasuk menggambil uang tunai di Bank maupun ATM.

Isu keamanan data pribadi juga menjadi hal yang esensial dalam kasus serangan siber ke Bank BSI ini. Pihak yang menyatakan bertanggung jawab atas serangan siber ini yaitu Grup Peretas asal Rusia yaitu LockBit. Grup peretas (*hacker*) ini telah mengumumkan bahwa mereka berhasil mencuri data-data dari sistem Bank BSI dengan jumlah 1,5 terabyte termasuk didalamnya data pribadi dari nasabah dan pegawai Bank BSI yang meliputi nama, nomor telepon, alamat, informasi dokumen, jumlah isi rekening, nomor kartu, histori transaksi, dll yang berjumlah kurang lebih 15 juta data pribadi. Hacker ini memberi tenggat waktu hingga 15 Mei pukul 21:09 UTC (16 Mei, 04:09 WIB) untuk pihak Bank BSI mengontak mereka dan memberikan uang tebusan yang diminta. Bila tidak, mereka mengancam akan membocorkan semua data tersebut. Dalam hal ini, perlindungan konsumen terhadap nasabah bank yang terkena serangan siber ransomware menjadi sangat penting. Nasabah bank membutuhkan perlindungan hukum yang memastikan bahwa bank bertanggung jawab atas keamanan dan pemulihan data mereka. Selain itu, perlindungan konsumen juga harus mencakup pencegahan serangan siber, pendidikan nasabah tentang risiko serangan, serta mekanisme kompensasi dan pemulihan jika serangan terjadi.

Di banyak negara, termasuk Indonesia, regulator dan otoritas terkait mengeluarkan kebijakan dan peraturan untuk melindungi nasabah bank dari serangan siber ransomware. Tujuan utama peraturan ini adalah memastikan bahwa bank melaksanakan langkah-langkah yang diperlukan untuk mencegah serangan siber dan memberikan perlindungan yang memadai kepada nasabah yang menjadi korban. Dalam konteks Indonesia, Otoritas Jasa Keuangan (OJK) memiliki peraturan yang mengatur perlindungan konsumen dalam sektor jasa keuangan, termasuk perlindungan terhadap nasabah bank yang

terkena serangan siber. Peraturan OJK ini mendorong bank untuk meningkatkan keamanan sistem mereka, memberikan informasi yang jelas kepada nasabah tentang risiko serangan siber, dan memberikan bantuan yang diperlukan jika serangan terjadi.

Dengan diterbitkannya POJK No. 6/POJK.07/ 2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan yang memperbarui POJK sebelumnya No. 1/POJK.07/ 2013 (POJK 6/2022), diharapkan mampu untuk menjadi solusi bagi konsumen di sektor jasa keuangan dalam hal ini nasabah bank untuk mendapatkan perlindungan terhadap jasa yang mereka terima dari pelaku usaha. Dalam POJK 6/2022 antara lain diatur mengenai penerapan dari perlindungan konsumen sejak tahap perencanaan produk, pelayanan, hingga cara penyelesaian sengketa. Hal yang paling penting juga dalam POJK 6/2022 ini yaitu dengan POJK 6/2022 akan memperjelas kewajiban PUJK untuk menerapkan prinsip keterbukaan dan transparansi informasi produk serta meningkatkan perlindungan data dan informasi bagi nasabah.

Lebih lanjut, pengaturan terkait dengan perlindungan konsumen nasabah bank yang diatur dalam POJK /2022 pada Pasal 11 ayat (5) menyebutkan "Dalam hal PUJK menggunakan teknologi informasi untuk mengelola data dan/atau informasi pribadi Konsumen, PUJK wajib menggunakan teknologi informasi yang andal serta menjamin keamanan data dan/atau informasi pribadi Konsumen dengan melakukan pengecekan kelayakan dan/atau keamanan secara berkala."

II. METODE PENELITIAN

Pendekatan penelitian ini adalah pendekatan yuridis normative. Dalam penelitian hukum normative, maka jenis data yang digunakan adalah data sekunder atau disebut dengan bahan hukum. Bahan hukum terdiri dari bahan hukum primer dan bahan hukum sekunder. Teknik pengumpulan data yang digunakan dalam penelitian ini adalah melalui teknik studi kepustakaan. Teknik pengolahan data adalah kegiatan merapikan data hasil dari pengumpulan data sehingga siap dipakai untuk dianalisis secara kualitatif. Setelah melalui proses pengolahan yang selektif, kemudian data tersebut dijabarkan secara deskriptif analisis, yaitu dijabarkan dalam bentuk uraian–uraian yang nantinya dapat menjawab permasalahan yang dibahas.

III. HASIL DAN PEMBAHASAN

Sebagaimana yang telah diuraikan dalam latar belakang, maka dalam penelitian ini terdapat 2 (dua) isu krusial dalam kasus serangan siber kepada Bank BSI yaitu pertama terkait dengan transparansi informasi dari pelaku usaha sektor jasa keuangan (dalam hal ini Bank BSI) kepada nasabah dan kedua mengenai bentuk perlindungan hukum kepada konsumen di sektor jasa keuangan yang mengalami kasus peretasan *ransomware*. Mengacu pada Pasal 3 huruf d Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen (Undang-Undang No. 8/1999) disebutkan bahwa "Perlindungan Konsumen bertujuan: …d. menciptakan sistem perlindungan konsumen yang mengandung unsur kepastian hukum dan keterbukaan informasi serta akses untuk mendapatkan informasi…". Lebih lanjut Pasal 4 huruf c Undang-Undang No. 8/1999 juga menyebutkan "Hak konsumen adalah hak atas informasi yang benar, jelas, dan jujur mengenai konsidi dan jaminan barang dan/atau jasa"

Undang-Undang No. 8/1999 Pasal 7 huruf b juga menyatakan bahwa "Kewajiban pelaku usaha adalah memberikan informasi yang benar, jelas dan jujur mengenai kondisi dan jaminan barang dan/atau jasa serta memberi penjelasan penggunaan, perbaikan dan pemeliharaan". Sehingga pada prinsipnya Undang-Undang perlindungan konsumen di Indonesia senantiasa mengedepankan transparansi informasi dari pelaku usaha kepada konsumen guna menjamin adanya kepastian hukum.

Pentingnya transparansi informasi diperlukan dalam hal memberikan pemahaman kepada konsumen mengenai risiko dan keamanan yang terkait dengan produk atau layanan keuangan yang mereka gunakan. Pelaku usaha harus menyampaikan informasi mengenai risiko investasi, perlindungan asuransi, atau keamanan transaksi keuangan dengan jelas dan jujur. Hal ini memungkinkan konsumen untuk membuat keputusan yang informasional dan memahami risiko yang mungkin terkait dengan keputusan finansial mereka. Dalam kasus serangan siber yang menimpa Bank BSI ini, dapat terlihat dari komunikasi publik awal yang disampaikan dalam rilis resmi Bank BSI bahwa mereka tidak memberikan informasi yang jelas dan akurat mengenai gangguan pada sistem pelayanan Bank yang terjadi mulai tanggal 8 Mei 2023. Terlebih lagi, Bank BSI menyampaikan pada nasabah bahwa gangguan system yang terjadi tersebut

akibat sedang adanya perbaikan (*maintenance*) guna peningkatan layanan. Padahal setelah keluar pernyataan dari Menteri BUMN, Bank BSI baru memberikan statement baru terkait adanya serangan siber ke system jaringan perbankan mereka.

Konsumen atau nasabah dalam hal ini tentunya berhak atas informasi yang benar terhadap layanan yang diberikan oleh Bank BSI. Sehingga pernyataan yang disampaikan oleh Bank BSI ini dapat mengarah kepada pemberian informasi yang tidak benar dan terkesan menutup-nutupi. Konsumen tentunya merasa dirugikan atas Tindakan Bank BSI yang tidak transparan dalam memberikan informasi kepada nasabah. Terlebih lagi akibat yang ditimbulkan karena adanya pemberian informasi yang tidak benar ini membuat sebagian nasabah dirugikan dari segi ekonomi karena merasa bahwa jaringan Bank BSI akan kembali normal dalam waktu dekat, namun nyatanya jaringan pelayanan baru pulih secara keseluruhan dalam waktu kurang lebih 1 minggu. Kepercayaan nasabah kepada Bank BSI juga tentu akan berkurang akibat adanya informasi yang tidak transparan, terlebih lagi kasus serangan siber ini juga mengincar informasi dan data pribadi nasabah.

Selain Undang-Undang No. 8/1999, aspek transparansi ini juga ditekankan dalam POJK 6/2022. Dalam POJK 6/2022 dinyatakan bahwa Pelaku Usaha Jasa Keuangan harus mematuhi prinsip-prinsip Perlindungan Konsumen dan Masyarakat yang meliputi edukasi yang memadai, transparansi dan keterbukaan informasi mengenai produk dan layanan, perlakuan yang adil dan bertanggung jawab dalam bisnis, perlindungan terhadap aset, privasi, dan data konsumen, serta penanganan pengaduan dan penyelesaian sengketa yang efektif dan efisien. Prinsip-prinsip ini harus diwujudkan dalam proses desain, penyediaan dan penyampaian informasi, kegiatan pemasaran, penyusunan perjanjian, pemberian layanan kepada pengguna produk dan/atau layanan, serta penanganan dan penyelesaian pengaduan dan juga sengketa konsumen.

Terkait dengan perlindungan hukum bagi konsumen, sebagaimana yang diketahui bahwa hukum perlindungan konsumen adalah salah satu kajian hukum ekonomi yang berada pada lingkup hukum privat dan hukum publik (hukum pidana dan administrasi negara). Sejalan dengan tujuan dari perlindungan konsumen dalam Undang-Undang No. 8/1999 yaitu Menciptakan sistem perlindungan konsumen yang mengandung unsur kepastian hukum dan keterbukaan informasi serta akses untuk mendapatkan informasi, maka implementasi UUPK telah menetapkan sejumlah hak dan tanggung jawab bagi konsumen dan pelaku usaha. Hak dan tanggung jawab ini menjadi pedoman yang harus diikuti dengan penuh ketentuan oleh konsumen dan pelaku usaha. Pelanggaran terhadap ketentuan UUPK dapat berakibat pada kemungkinan adanya gugatan baik dari individu atau kelompok konsumen, Lembaga Perlindungan Konsumen Swadaya Masyarakat (LPKSM), atau pemerintah dan instansi terkait. UUPK juga memberikan kemudahan dan akses untuk penyelesaian sengketa konsumen melalui Badan Penyelesaian Sengketa Konsumen (BPSK), selain proses penyelesaian sengketa konsumen di pengadilan.

Lebih lanjut dalam Pasal 11 ayat (5) POJK 6/2022 "Dalam hal PUJK menggunakan teknologi informasi untuk mengelola data dan/atau informasi pribadi Konsumen, PUJK wajib menggunakan teknologi informasi yang andal serta menjamin keamanan data dan/atau informasi pribadi Konsumen dengan melakukan pengecekan kelayakan dan/atau keamanan secara berkala." Teknologi informasi yang andal dapat diartikan yaitu teknologi informasi yang dapat memberikan layanan yang akurat dengan memastikan informasi input, proses, dan output yang terotorisasi, yang dilakukan secara aman, benar dan lengkap.

Mengacu kepada pengertian yang diatur dalam POJK 6/2022 tersebut maka dapat dikatakan bahwa terdapat tanggung jawab dari PUJK untuk mengelola data dan/atau informasi pribadi dari nasabah dengan penuh kehati-hatian dan menjamin keamanan data dan/atau informasi pribadi konsumen dalam lingkup teknologi informasi yang andal. Selain itu PUJK juga diwajibkan untuk melakukan pengecekan dan kelayakan teknologi informasi tersebut secara berlaka. Serangan siber yang menimpa Bank BSI beberapa waktu lalu tersebut telah nyata menjadi sebuah bentuk kelalaian dari PUJK dalam mengelola data dan/atau informasi pribadi konsumen, dimana seharusnya PUJK dalam hal ini melakukan pengecekan dan kelayakan teknologi informasi tersebut secara berlaka. Bentuk kelalaian yang dilakukan oleh PUJK ini memiliki konsekuensi dapat diberikannya sanksi administratif kepada PUJK mengacu pada Pasal 45 POJK 6/2022 dengan denda yang

dapat dikenakan paling banyak sebesar Rp15.000.000.000,00 (lima belas miliar rupiah). Sanksi administratif tersebut dapat berupa:

1. peringatan tertulis,
2. denda,
3. larangan sebagai pihak utama sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penilaian kembali bagi pihak utama Lembaga Jasa Keuangan,
4. pembatasan produk dan/atau layanan dan/atau kegiatan usaha;
5. pembekuan produk dan/atau layanan dan/atau kegiatan usaha;
6. pencabutan izin produk dan/atau layanan; dan pencabutan izin usaha.

IV. SIMPULAN DAN SARAN

A. Simpulan

Kesimpulan dari pembahasan tulisan ini adalah bahwa transparansi informasi dari pelaku usaha sektor jasa keuangan kepada konsumen merupakan aspek penting dalam perlindungan konsumen. Undang-Undang Perlindungan Konsumen No. 8 Tahun 1999 dan POJK 6/2022 mengatur prinsip-prinsip perlindungan konsumen, termasuk edukasi yang memadai, transparansi informasi, perlakuan yang adil, perlindungan aset dan privasi konsumen, serta penanganan pengaduan dan penyelesaian sengketa yang efektif dan efisien.

Dalam kasus serangan siber yang menimpa Bank BSI, terdapat pelanggaran terhadap transparansi informasi kepada nasabah. Bank BSI tidak memberikan informasi yang jelas dan akurat mengenai gangguan pada sistem pelayanan bank mereka akibat serangan siber. Hal ini berdampak pada kerugian nasabah yang mengharapkan pemulihan sistem dengan cepat. Informasi yang tidak transparan juga dapat mengurangi kepercayaan nasabah kepada Bank BSI dan meningkatkan risiko kebocoran data pribadi.

Selain itu, perlindungan hukum bagi konsumen dalam sektor jasa keuangan juga penting. Undang-Undang Perlindungan Konsumen menetapkan hak dan tanggung jawab bagi konsumen dan pelaku usaha, serta memberikan akses untuk penyelesaian sengketa melalui Badan Penyelesaian Sengketa Konsumen. Pelaku usaha juga memiliki kewajiban dalam mengelola data dan informasi pribadi konsumen dengan menggunakan teknologi informasi yang andal dan menjaga keamanannya.

Dalam kasus Bank BSI, terjadi kelalaian dalam mengelola data dan informasi pribadi konsumen, yang menunjukkan ketidaktepatan dalam pengecekan dan kelayakan teknologi informasi yang digunakan. Kelalaian tersebut dapat dikenai sanksi administratif sesuai dengan POJK 6/2022.

B. Saran

Berdasarkan pembahasan di atas, saran yang dapat diberikan adalah Bank BSI perlu memperbaiki transparansi informasi kepada nasabah, memberikan informasi yang jelas dan akurat mengenai gangguan yang terjadi, serta meningkatkan keamanan data dan informasi pribadi nasabah melalui pengecekan dan pemeliharaan teknologi informasi yang andal. Otoritas terkait juga perlu melakukan pengawasan yang lebih ketat terhadap pelaku usaha sektor jasa keuangan guna memastikan kepatuhan terhadap prinsip-prinsip perlindungan konsumen dan memberikan sanksi yang tegas dalam kasus pelanggaran. Dalam menghadapi serangan siber ransomware, penting bagi bank dan otoritas terkait untuk terus beradaptasi dan mengembangkan solusi yang lebih baik. Perlindungan konsumen terhadap nasabah bank harus menjadi fokus utama dalam upaya melawan serangan siber dan meminimalkan dampak negatifnya terhadap nasabah dan sistem keuangan secara keseluruhan.

DAFTAR RUJUKAN

Artha, Yohana, “Layanan BSI "Error", Erick Thohir Akui Ada Serangan Siber”, https://money.kompas.com/read/2023/05/10/140408326/layanan-bsi-error-erick-thohir-akui-ada-serangan-siber , diakses pada 15 Juni 2023

Baderi, Firdaus, “Aturan Baru Perlindungan Konsumen: - OJK: Perjelas Prinsip Transparansi dan Layanan”, https://www.neraca.co.id/article/163064/aturan-baru-perlindungan-konsumen-ojk-perjelas-prinsip-transparansi-dan-layanan, diakses pada 16 Juni 2023

Bank Syariah Indonesia, https://www.instagram.com/p/Cr-MIIari8H/, diakses pada 15 Juni 2023

BBC, "BSI diduga kena serangan siber, pengamat sebut sistem pertahanan bank 'tidak kuat'", https://www.bbc.com/indonesia/articles/cn01gdr7eero, diakses pada 15 juni 2023

Indonesia, Undang-Undang Perlindungan Konsumen, UU No. 8 Tahun 1999, LN No. 22 Tahun 1999, TLN No. 3821

Istianur, Ilyas, "Aplikasi BSI Mobile Error Tenyata Gara-Gara Maintenance", https://www.liputan6.com/bisnis/read/5280278/aplikasi-bsi-mobile-error-tenyata-gara-gara-maintenance , diakses pada 15 Juni 2023

Miru, Ahmadi & Sutarman Yado, *Hukum Perlindungan Konsume*n. (Jakarta: Raja Grafindo Persada, 2004)

Otoritas Jasa Keuangan Republik Indonesia, Peraturan Otoritas Jasa Keuangan tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan, POJK 6/POJK.07/2022 LN. No. 99 Tahun 2022, TLN No. 6788

Zalavadiya & Priyanka, "A Metodology of malware Analysis, tools, and Technique for windows platform – RAT analysis", *International Journal of Innovative Research in Computer and Communication Engineering* (Vol. 5 Maret 2017)