

ANALISIS PENIPUAN *ONLINE* DALAM BENTUK *PHISING* MENURUT PERSPEKTIF HUKUM INDONESIA

Amanda Faizah Nurfahda¹, Annasyanda Jelita Putri²,
Nayottama Aryasuta Yardi³, Fitra Deni⁴

^{1, 2, 3, 4} Fakultas Ilmu Sosial dan Ilmu Politik,

Universitas Islam Negeri Syarif Hidayatullah Jakarta,

¹amanda.nurfahda23@mhs.uinjkt.ac.id, ²annasyanda.jelitaputri23@mhs.uinjkt.ac.id,

³nayottama.aryasutayardi23@mhs.uinjkt.ac.id, ⁴fitra.deni@staff.uinjkt.ac.id

ABSTRACT

The rapid flow of technology has brought so many impacts to various spheres of life, especially the rapid growth in the digital sphere. This technological development also brings a variety of positive contributions. However, along with the benefits, there are also new threats that need to be anticipated. Especially the threat of personal data leakage or misuse of data by irresponsible parties. This paper examines the phenomenon of cybercrime in the form of phishing from the perspective of Indonesian law. This paper uses normative juridical research methods. The researcher proves that phishing crime is a threat to the flow of digital development in Indonesia. Phishing crime no longer relies on one pattern, but comes in various motives and methods. Despite its various challenges and limitations, Indonesian law has been able to create a set of rules to tackle and anticipate phishing crimes.

Keywords: Phising, Law, Indonesia.

ABSTRAK

Derasnya arus teknologi membawa begitu banyak dampak bagi berbagai ruang kehidupan, salah satunya pertumbuhan pesat di lingkup digital. Perkembangan teknologi ini, turut membawa berbagai macam kontribusi positif. Namun, seiring dengan manfaatnya, muncul pula ancaman-ancaman baru yang perlu diantisipasi. Terlebih ancaman dari kebocoran data pribadi ataupun penyalahgunaan data oleh para oknum yang tidak bertanggung jawab. Tulisan ini mengkaji fenomena kejahatan siber (*cybercrime*) dalam bentuk *phising* dari sudut pandang hukum di Indonesia. Penelitian ini menggunakan metode penelitian yuridis normatif. Peneliti membuktikan bahwa kejahatan *phising* menjadi ancaman bagi berjalannya arus perkembangan digital di Indonesia. Kejahatan *phising* tidak lagi bertumpu pada satu pola, namun hadir dalam berbagai motif dan metode. Terlepas dari berbagai tantangan dan keterbatasannya, hukum Indonesia telah mampu menciptakan seperangkat aturan untuk menanggulangi dan mengantisipasi kejahatan *phising*.

Kata-kata Kunci: *Phising*, Hukum, Indonesia.

I. PENDAHULUAN.

Teknologi informasi dan komunikasi telah berkembang dengan sangat pesat. Dalam prosesnya, internet menjadi bagian yang sangat penting dari perkembangan teknologi. Internet juga telah menjadi bagian penting dalam hidup manusia. Hal ini dikarenakan internet menjadi perantara untuk memfasilitasi komunikasi antar manusia di seluruh belahan dunia bahkan mampu membentuk budaya baru. Namun, perkembangan ini tidak hanya membawa dampak positif terhadap kehidupan masyarakat tetapi dampak negatif juga. Salah satu contoh dampak buruk yang muncul karena perkembangan teknologi adalah *cybercrime* dalam bentuk *phising* (Malunsenge, et al., 2022). *Phising* adalah pencurian data online yang dilakukan dengan cara mengelabui korban untuk memberikan informasi pribadinya. *Phising* berasal dari istilah dalam bahasa inggris, yaitu *fishing* yang artinya “memancing”. Informasi yang dicuri sering kali dimanfaatkan untuk melakukan tindakan ekonomi yang ilegal seperti membeli barang menggunakan identitas curian dan transaksi *online* ilegal.

Serangan *phising* memang sederhana tetapi sangat efektif dalam mencuri data korban (Ludl, et al., 2007). Biasanya pelaku *phising* akan membuat pesan yang terlihat meyakinkan sehingga memancing korban untuk percaya dan memasukan informasi pribadinya. Pelaku biasanya juga mengubah nama domain suatu web supaya lebih meyakinkan (Khonji, et al., 2013). Selain itu, pelaku juga merubah tampilan web semirip mungkin dengan website aslinya supaya korban terkecoh. Pelaku biasanya mengirimkan link *phising* lewat e-mail atau aplikasi pengirim pesan lainnya dengan tujuan untuk mengelabui korban supaya korban mau memberikan

informasi pribadinya. *Phising* merupakan bentuk *cybercrime* yang paling sering terjadi. Menurut data dari IDAX, sejak tahun 2018, telah terjadi 106.806 serangan *phising*. Menurut data dari IDADX, pada kuartal keempat tahun 2023, serangan *phising* lewat media sosial memiliki persentase sebesar 64,34 persen dari total semua serangan *phising* yang terjadi. Dari data tersebut dapat kita ketahui kalau mayoritas serangan *phising* terjadi di sektor media sosial (IDADX, 2023). Maka dari itu, tulisan ini akan menganalisis bagaimana hukum di indonesia memandang masalah ini. Contoh kasus terawal dari serangan *phising* pernah terjadi pada tahun 2001. serangan ini menargetkan pengguna bank BCA. Pada saat itu, bank BCA masih terbilang baru dalam menggunakan internet sebagai sarana untuk menjalankan layanan transaksi perbankan. Pelaku penyerangan membeli enam domain dan menamainya sama persis dengan website resmi bank BCA.

Dengan menggunakan website tiruan ini, pelaku mengelabui para nasabah karena mengira website tiruan tersebut merupakan website bank BCA yang asli. alhasil, nasabah pun terkecoh lalu memasukan pin dan identitasnya untuk login di website tiruan ini. Data pin dan identitas nasabah pun tercatat di *hard disk* pelaku. Kejadian ini memperlihatkan betapa berbahayanya *cybercrime* berjenis *phising* apabila dibiarkan. Oleh karena itu, perlu adanya tindakan hukum untuk melindungi hak masyarakat. Sanksi terhadap pelaku serangan *phising* sangatlah diperlukan untuk memberikan efek jera (Malunsenge, et al., 2022). UU ITE dan KUHP merupakan salah satu perangkat hukum yang bisa digunakan sebagai dasar hukum dalam peradilan tindak pidana *phising* (Muhammad & Harefa, 2023). Oleh karena itu, tulisan ini akan membahas *cybercrime* berjenis

phising dari sudut pandang hukum pidana yakni UU ITE.

II. METODE PENELITIAN.

Penelitian ini bertujuan untuk menganalisis fenomena penipuan *online* dalam bentuk *phising* dari kaca mata hukum di Indonesia. Artikel jurnal ini diteliti menggunakan metode penelitian yuridis normatif. Metode penelitian yuridis normatif adalah metode penelitian yang berbasis kepustakaan dengan menggali serta mengkaji sumber-sumber kepustakaan atau data sekunder (Soekanto & Mamudji, 2009). Data sekunder adalah informasi atau data yang diperoleh dari penelitian kepustakaan yang mengacu pada penelitian sebelumnya dengan tujuan untuk mengumpulkan informasi, teori, juga gagasan konseptual. Ini termasuk peraturan perundang-undangan dan karya ilmiah lainnya yang berkaitan dengan kejahatan teknologi informasi atau *cybercrime*, serta penegakan undang-undang lainnya yang berkaitan dengan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam menindak fenomena tindakan kejahatan dalam wujud *phising*.

III. HASIL DAN PEMBAHASAN PENELITIAN.

III.1 Metode dan Motif *Phising* Di Indonesia.

Phising merupakan salah satu kejahatan siber berjenis *cybersquatting*. *Cybersquatting* adalah salah satu bentuk kejahatan siber yang memanfaatkan nama situs atau domain. Modus kejahatan *phising* dilakukan dengan cara membuat situs tiruan untuk menipu korban. Pelaku kejahatan *phising* memanfaatkan situs tiruan ini untuk menjebak korban supaya

memberikan data pribadinya. Korban yang terkecoh akhirnya memasukan informasi pribadinya karena mengira situs palsu tersebut merupakan situs yang asli. Data korban ini selanjutnya dimanfaatkan oleh pelaku *phising* dengan maksud dan tujuan tertentu. *phising* sendiri memiliki beberapa bentuk. salah satunya adalah *phising* yang disebarakan lewat *e-mail*. Pelaku menyebarkan *e-mail* yang berisi situs tiruan kepada calon-calon korban dengan tujuan untuk menjebak mereka.

Menurut pakar di bidang teknologi dan informasi Dendy Eka Puspawadi, *phising* merupakan salah satu bentuk penipuan dengan tujuan untuk mencuri akun korban. pencurian akun korban ini dilakukan dengan menjebak korban untuk memberikan data pribadinya seperti *username* dan *password* lewat situs tiruan yang disebarakan lewat *e-mail*. *phising* dengan penyebaran lewat email ini dapat disebut juga dengan *filter evasion*. Bentuk *phising* selanjutnya adalah Manipulasi Link. Pelaku *phising* berjenis manipulasi link membuat link dengan ejaan yang sama persis dengan link situs aslinya sehingga korban menjadi terkecoh karena mengira link palsu tersebut merupakan yang asli. bentuk *phising* yang ketiga adalah *Website Forgery*. Pelaku *website forgery* menanamkan link tiruan pada file multimedia lewat celah keamanan situs yang asli. Selanjutnya, bentuk *phising* keempat adalah *Website Phising*. pelaku *website phising* membuat situs dengan domain yang sama menyerupai situs resmi perusahaan atau organisasi. hal ini dilakukan untuk menjebak korban supaya memberikan data pribadinya seperti *username* dan *password*. Bentuk *phising* selanjutnya adalah *Malware Phising*. Pelaku *malware phising* akan memancing korban untuk mendownload sebuah file yang berisi virus. Setelah korban mendownload file tersebut dan membukanya, pelaku akan mendapatkan

akses terhadap komputer korban dan mengeksploitasinya.

Dalam melakukan aksinya, pelaku *phishing* memiliki motif dan targetnya masing-masing. Motif yang pertama adalah *Whaling*. Pelaku *phishing* dengan motif *whaling* menargetkan orang dengan status yang tinggi seperti pejabat. Pelaku biasanya menggunakan dokumen yang berisi panggilan kepada korban untuk ke pengadilan dengan tujuan untuk memberi rasa takut kepada korban. Selanjutnya adalah *Spear Phishing*. Pelaku *spear phishing* memiliki target yang spesifik seperti *whaling*. Motif yang ketiga adalah *Clone Phishing*, motif ini menggunakan *e-mail* sebagai media untuk menyebarkan link *phishing*. Motif ini merupakan salah satu motif *phishing* yang paling sering terjadi. Motif selanjutnya adalah *Covert Redirect*. Pelaku *phishing* dengan motif *covert redirect* membuat link tiruan yang menyerupai website resmi lewat *pop up login*. Motif ini cenderung sulit dideteksi karena pelaku membuat *pop up* yang dimodifikasi pada situs resmi (Putra, 2021).

III.2. Perangkat Hukum di Indonesia terkait *Phishing*.

Masyarakat Indonesia harus menaruh perhatian lebih terhadap proteksi data pribadi. Perlindungan ini ditujukan untuk mengantisipasi terjadinya pelanggaran hukum. Rentannya keamanan di ranah siber didukung oleh pesatnya perkembangan teknologi di era digital berakibat pada besarnya potensi kemungkinan oknum pelaku kejahatan mengambil kesempatan untuk mengakses data personal seseorang. Adapun hukum Indonesia menyediakan beberapa perangkat peraturan yang merefleksikan perlindungan terhadap data pribadi sebelum diterbitkannya UU Perlindungan Data Pribadi (PDP). Meskipun belum dapat dijelaskan secara spesifik, Undang-

Undang Nomor 23 Tahun 2006 mengenai Administrasi Kependudukan telah menggarisbawahi betapa pentingnya perlindungan data pribadi (Sutarli & Kurniawan, 2023).

Pada tahun 2016, pemerintah kembali meluncurkan peraturan pendukung dalam upaya perlindungan data pribadi, melalui Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE) yang dikeluarkan oleh Kementerian Komunikasi dan Informatika RI. Walaupun, UU ITE tersebut belum memberikan definisi yang jelas terkait data pribadi itu sendiri. Namun, Pasal 26 dalam UU tersebut telah memuat beberapa pernyataan seperti, penegasan pentingnya kesepakatan dari pihak-pihak terkait dalam pemakaian data pribadi seseorang yang dimuat oleh Pasal 26 ayat (1). Lalu, pasal 26 ayat (2) menekankan apabila terjadi pelanggaran terhadap penggunaan data pribadi tanpa persetujuan pemilik data, maka pelaku dapat dikenakan gugatan karena pemilik memiliki hak hukum keperdataan. Berikutnya, terdapat pernyataan bahwa terdapat hak untuk menyampaikan permintaan penghapusan data pribadi yang tidak memiliki keterkaitan terhadap penyedia sistem elektronik, yang merujuk pada konsep "*right to be forgotten*", yang diatur dalam Pasal 26 ayat (3) (Yuniarti, 2019).

Adapun, terdapat undang-undang lainnya yang turut mengatur data pribadi. Namun, pengaturan tersebut masih bersifat general dan tidak memberikan perlindungan yang komprehensif. Selain itu, ketiadaan undang-undang yang menjamin pemulihan bagi korban pelanggaran privasi memperlihatkan bahwa perlindungan data pribadi belum sepenuhnya terpenuhi (Rizal, 2019).

UU PDP mengambil andil yang sangat besar dalam penanganan berbagai bentuk kejahatan siber, termasuk

phising. Dikarenakan UU PDP menetapkan perlindungan terhadap data pribadi individu dan memberikan sanksi yang tegas kepada para pelakunya. Penanganan *phising* di Indonesia sangat bergantung pada Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Pemerintah berkewajiban untuk memastikan bahwa peraturan dalam UU PDP diimplementasikan dengan semestinya untuk memproteksi data pribadi masyarakat. Pemerintah juga harus memberlakukan UU PDP untuk menindak dan mencegah pelaku *phising*. Pemerintah harus menjalin kolaborasi dengan lembaga-lembaga terkait yang memang memiliki kewenangan juga komitmen dalam memproteksi ruang digital, seperti, Badan Siber dan Sandi Negara (BSSN) juga Kepolisian Republik Indonesia (Sutarli & Kurniawan, 2023).

UU PDP mengatur sanksi administratif dan pidana bagi pelaku kejahatan siber yang terbukti melakukan pelanggaran terhadap perlindungan data pribadi, termasuk *phising*. *Phising* adalah aksi kejahatan siber (*cybercrime*) dengan melakukan pemalsuan informasi identitas atau data pribadi seseorang untuk mendapatkan keuntungan atau data pribadi korban. Sanksi administratif yang dapat dijatuhkan antara lain berupa peringatan, teguran, denda administratif, pencabutan izin usaha, maupun pembekuan kegiatan usaha. Pelaku *phising* dapat dijatuhi hukuman pidana sesuai dengan Pasal 67 UU PDP, dengan ancaman kurungan penjara tidak lebih dari 5 tahun dan/atau denda tidak lebih dari 5 miliar rupiah. Jika tindakan *phising* melibatkan pemerolehan atau pengambilan data pribadi korban secara ilegal, hal tersebut jelas melanggar Pasal 67 Undang-Undang Perlindungan Data Pribadi tahun 2022 (Sutarli & Kurniawan, 2023).

III.3. Perlindungan Hukum bagi Korban Penipuan *Phising*.

Penegakan hukum bermaksud mewujudkan keteraturan dan kedamaian pada masyarakat. Korban kejahatan membutuhkan perlindungan agar merasa tenang dan tentram saat menjalani kehidupannya. Sebagai negara hukum, perlindungan ini merupakan tanggung jawab negara kepada masyarakat Indonesia. Namun, dalam kasus kejahatan siber seperti *phising*, peraturan perundang-undangan belum memberikan perlindungan yang jelas bagi korban yang mengalami kerugian materiil, seperti kehilangan data pribadi dan kerugian ekonomi. (Leticia M. Malunsenge, et al., 2022).

Berikut ini adalah beberapa peraturan undang-undang yang relevan terkait penegakan hukum serta perlindungan bagi korban:

1. Pasal 28D ayat (1) Undang-Undang Dasar 1945: "Setiap orang berhak atas pengakuan, jaminan, perlindungan, dan kepastian hukum yang adil serta perlakuan yang sama di hadapan hukum".
2. Pasal 3 ayat (2) UU Nomor 39 Tahun 1999 tentang Hak Asasi Manusia: "Setiap orang berhak atas pengakuan, jaminan, perlindungan, perlakuan hukum yang adil serta kepastian hukum yang sama di hadapan hukum".
3. Pasal 40 ayat (2) UU ITE: "Pemerintah melindungi kepentingan umum dari gangguan akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum".
4. Pasal 1 angka 8 UU Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban: "Perlindungan adalah segala upaya pemenuhan hak dan pemberian bantuan untuk

memberikan rasa aman kepada saksi dan/atau korban yang diberikan oleh LPSK atau lembaga lainnya sesuai dengan ketentuan undang-undang". (Leticia M. Malunsenge, et al., 2022).

Meskipun UU ITE lebih berfokus pada pidana pelaku, hal ini seringkali tidak cukup untuk melindungi dan memulihkan hak-hak korban. Korban kejahatan siber, termasuk *phising*, memiliki hak untuk mendapatkan perlindungan dan kompensasi melalui Undang-Undang Perlindungan Saksi Korban (UUPSK). UU ini membahas mengenai kompensasi, pemulihan, dan bantuan bagi korban kejahatan. Dalam UUPSK disebutkan bahwa pemulihan merupakan salah satu cara yang sejalan dengan UU Nomor 31 Tahun 2014 tentang Perubahan atas UU Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, yang meliputi:

1. Pasal 1 angka 11: "Restitusi adalah ganti kerugian yang diberikan kepada korban atau keluarganya oleh pelaku atau pihak ketiga".
2. Pasal 7A ayat (1): "Korban tindak pidana berhak memperoleh restitusi berupa ganti kerugian atas kehilangan kekayaan atau penghasilan, ganti kerugian untuk penderitaan yang diderita, dan penggantian biaya perawatan medis dan/atau psikologis". (Leticia M. Malunsenge, et al., 2022)

Agar mendapatkan penggantian rugi dari pelaku, korban perlu menyerahkan berkas kepada Lembaga Perlindungan Saksi dan Korban (LPSK). Berkas ini harus memenuhi persyaratan tertentu dan dapat diajukan sebelum atau sesudah kasus diputuskan oleh pengadilan. LPSK akan memutuskan apakah permohonan tersebut diterima atau ditolak melalui Rapat Paripurna Anggota.

Jika Permohonan diterima, maka korban akan mendapatkan perlindungan dan kompensasi. (Leticia M. Malunsenge, et al., 2022)

III.4. Upaya Mengantisipasi Penipuan *Phising*.

Untuk mengantisipasi kejahatan *phising online*, peran publik sangatlah penting. Minimnya pengetahuan tentang keamanan data membuat masyarakat rentan menjadi korban *phising*. (Octo Iskandar, 2024) Meningkatkan kesadaran ini dapat dilakukan melalui sosialisasi dan simulasi praktik *social engineering (phising)* yang dapat membantu dalam meningkatkan pemahaman dan kewaspadaan terhadap risiko dan pencegahan kejahatan siber. Sosialisasi melalui webinar, simulasi, penyebaran poster, dan video edukasi mampu masyarakat luas dan mampu meningkatkan wawasan yang lebih baik tentang keamanan siber. (Eko Wahyu Tyas Darmaningrat, et al., 2022)

Dengan meningkatkan kesadaran dan pemahaman tentang teknik *phising*, masyarakat dapat mengambil langkah-langkah pencegahan seperti berhati-hati terhadap email dan situs web yang tidak dikenal, memverifikasi alamat yang sah, menggunakan kata sandi yang kuat, memasang perangkat lunak antivirus, dan melaporkan aktivitas phishing kepada pihak berwenang seperti Badan Siber dan Sandi Negara (BSSN). Mempelajari tentang *phising* dan membagikan informasi ini kepada teman dan keluarga sangat penting untuk melindungi mereka. Dengan memahami keamanan siber, Anda bisa membantu orang memahami risiko dan taktik *phising* yang sering digunakan. (Octo Iskandar, 2024).

IV. SIMPULAN.

Phising adalah salah satu kejahatan siber yang memanipulasi korban agar menyerahkan data pribadi mereka melalui situs tiruan yang menyerupai aslinya. Beberapa metode dan motif *phising* antara lain *phising* melalui email, manipulasi link, website *forgery*, website *phising*, dan *malware phising*. Di Indonesia, UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi berisi tentang sanksi administratif dan pidana bagi pelaku *phising*, dengan ancaman hukuman penjara hingga lima tahun dan/atau denda paling tinggi 5 miliar rupiah. Perlindungan hukum bagi korban *phising* meliputi pengakuan yang adil, jaminan, perlindungan, dan kepastian hukum sebagaimana diatur dalam berbagai undang-undang terkait, termasuk UUD 1945, UU Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, dan UU ITE. Namun, peraturan saat ini belum sepenuhnya memberikan perlindungan yang komprehensif bagi korban yang mengalami kerugian materiil akibat *phising*.

DAFTAR PUSTAKA

- Laporan aktivitas phishing domain. (2023). Retrieved July 7, 2024, from https://api.idadx.id/documents/uploads/1705892888_Laporan%20Q4%202023.pdf.pdf.
- Iskandar, O. (2024). Analisis Kejahatan Online Phising pada Masyarakat. Leuser: *Jurnal Hukum Nusantara*.
- Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: A literature survey. *IEEE Communications Surveys & Tutorials*, 15(4), 2091–2121. <https://doi.org/10.1109/surv.2013.032213.00009>.
- Ludl, C., McAllister, S., Kirda, E., & Kruegel, C. (2007). On the effectiveness of techniques to detect phishing sites. In *Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 20–39). Berlin, Heidelberg: Springer Berlin Heidelberg. Retrieved from http://dx.doi.org/10.1007/978-3-540-73614-1_2.
- Malunsenge, L., Massie, C., & Rorie, R. (2022). Penegakan Hukum terhadap Pelaku dan Korban Tindak Pidana Cyber Crime Berbentuk Phising di Indonesia.
- Muhammad, F. E., & Harefa, B. (2023). Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phising Berbasis web. *JURNAL USM LAW REVIEW*, 6(1), 226. <https://doi.org/10.26623/julr.v6i1.6649>.
- Putra Y, V. F. (2021). Modus operandi tindak pidana phising menurut UU ITE. *Jurist-Diction*, 4(6), 2525. <https://doi.org/10.20473/jd.v4i6.31857>.
- Rizal, M. S. (2019). Perbandingan Perlindungan Data Pribadi

- Indonesia dan Malaysia. *Jurnal Cakrawala Hukum*, 10(2). <https://doi.org/10.26905/idjch.v10i2.3349>.
- Soekanto, Soerjono, Mamudji, & Sri. (2009). *Penelitian Hukum Normatif..*
- Sutarli, A. F., & Kurniawan, S. (2023). Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia. *Innovative: Journal Of Social Science Research*, 3(2). <https://doi.org/10.31004/innovative.v3i2>.
- Tyas Darmaningrat, E. W., Noor Ali, A. H., Herdiyanti, A., Subriadi, A. P., Muqtadiroh, F. A., Astuti, H. M., & Susanto, T. D. (2022). Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi. *Sewagati*, 6(2). <https://doi.org/10.12962/j26139960.v6i2.92>.
- Yuniarti, S. (2019). PERLINDUNGAN HUKUM DATA PRIBADI DI INDONESIA. *Business Economic, Communication, and Social Sciences (BECOSS) Journal*, 1(1), 147–154. <https://doi.org/10.21512/becossjournal.v1i1.6030>.