

Kejahatan Pencurian Data Pribadi melalui Cyber Phishing dan Sistem Pembuktiannya dalam Persidangan: Studi Putusan No. 697/Pid.Sus/2024/PN.Sda.

Filda Evangelista Nababan, Benny Sumardiana
Fakultas Hukum, Universitas Negeri Semarang

Corresponding Author:
fildaevangelistafh21@students.unnes.ac.id

ISSN 2964-3848
QRCBN 62-6861-0144-710

ABSTRAK

Penelitian ini bertujuan untuk menganalisis kejahatan pencurian data pribadi di Indonesia, dengan fokus pada pengaturan hukum yang berlaku dan mekanisme penanganan serta penegakan hukum yang efektif. Kejahatan ini, yang sering kali dilakukan melalui metode cyber phishing, telah menjadi isu serius di era digital saat ini. Metode penelitian yang digunakan adalah yuridis normatif, dengan pendekatan studi kasus berdasarkan Putusan Nomor 697/Pid.Sus/2024/PN.Sda. Kajian ini menyoroti regulasi utama yang mengatur tindak pidana pencurian data pribadi, terutama yang tercantum dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya. Penanganan kasus ini melibatkan pelacakan digital dan pengumpulan alat bukti elektronik yang menjadi dasar pembuktian di persidangan. Peran kepolisian dan jaksa sangat penting dalam proses penyidikan dan penuntutan, di mana koordinasi dengan penyedia layanan digital diperlukan untuk memperoleh data teknis yang relevan. Putusan pengadilan yang mengedepankan perlindungan korban dan pengembalian

barang bukti mencerminkan penerapan hukum yang berpihak pada keadilan. Kesimpulannya, penegakan hukum yang efektif dalam menghadapi kejahatan pencurian data pribadi memerlukan pemahaman yang mendalam tentang hukum dan teknologi, serta kerja sama yang erat antar lembaga penegak hukum untuk menciptakan sistem perlindungan yang lebih baik bagi masyarakat.

Kata kunci: Cyber Phishing, Pencurian Data Pribadi, Penegakan Hukum.

PENDAHULUAN

Era sekarang ini, yang dikenal dengan Era Globalisasi, Percepatan penyebaran media transportasi dan elektornik telah mengubah struktur masyarakat lokal menjadi global. Internet telah menjadi fenomena yang memberikan kesan menyenangkan dalam menjelajahi setiap sudut jaringan tanpa batas.⁴¹¹ Internet sudah menjadi bagian yang tidak terpisahkan dari kehidupan manusia. Hampir seluruh kebutuhan sehari-hari manusia dapat dilakukan hanya dengan bantuan perangkat pintar yang dilengkapi dengan jaringan internet. Selain itu, kemudahan yang ditawarkan dan minimnya biaya, menjadikan internet sebagai sarana yang sangat menguntungkan karena dapat mengakses segala jenis situs.⁴¹²

Oleh kemudahan dan kebebasan akses dalam menyelami dunia maya, banyak orang yang menyalahgunakan internet untuk mendapatkan keuntungan personal yang bisa merugikan orang lain ataupun pihak lain. Kejahatan dunia maya dapat diartikan sebagai aktivitas kriminal yang terjadi di atau melalui media komputer maupun

⁴¹¹ Maskun, *Kejahatan Siber (Cyber Crime) Suatu Pengantar* (Jakarta: Kencana, 2013).

⁴¹² Siti Rohaya, "Internet: Pengertian, Sejarah, Fasilitas Dan Koneksinya," *Fihris Jurnal* 3, no. 1 (April 1, 2008).

internet atau dengan teknologi lain yang diakui oleh Undang-Undang. Kejahatan dunia maya telah menghadirkan suatu kontinum yang berkisar dari kejahatan yang hampir seluruhnya bersifat teknologi dimana kejahatan yang dilakukan sepenuhnya terkait dengan manusia.

Terdapat beberapa jenis kejahatan siber yang menggunakan media komputer di Indonesia, yaitu penyelundupan gambar porno melalui internet, spam, dan penyadapan. Salah satu jenis kejahatan siber adalah pencurian data pribadi atau yang lebih dikenal dengan cyber phishing. Biasanya pelaku akan membuat akun palsu, kemudian membuat link palsu dan dikirimkan melalui email kepada korban. Setelah korban membuka link yang dikirimkan, dan memberikan informasi pribadinya, si pelaku akan mengumpulkan data tersebut untuk diperjual belikan secara online ataupun untuk digunakan oleh pelaku itu sendiri.

Dilihat dari kemudahan bertransaksi online, kejahatan ini juga sangat mengancam stabilitas ekonomi dan keamanan digital suatu negara. Kejahatan ini menjadi sangat marak dan menimbulkan kekhawatiran yang sangat serius, karena keahlian para peretas yang mampu mengelabui sistem keamanan. Dengan ini, maka sangat diperlukan pengembangan yang berkesinambungan dan berkelanjutan untuk mencegah dan meningkatkan sistem perlindungan yang efisien untuk melindungi pengguna dan meminimalisasi jumlah korban skema penipuan kejahatan phishing.⁴¹³ Meskipun begitu, masih banyak kendala yang menjadi tantangan dalam sistem pembuktian tindak pidana kejahatan mayantara ini di persidangan, khususnya validitas bukti yang dihasilkan dari teknologi yang semakin berkembang.

⁴¹³ Octo Iskandar, "Analisis Kejahatan Online Phishing Pada Masyarakat," *Leuser: Jurnal Hukum Nusantara* 1, no. 2 (July 1, 2024).

Rumusan masalah dalam kajian ini mencakup tiga pokok bahasan utama, yakni keberadaan kejahatan pencurian data pribadi di Indonesia beserta pengaturannya dalam sistem hukum nasional, mekanisme penanganan atas kejahatan tersebut, serta strategi penegakan hukum yang tepat untuk menghadapinya. Adapun tujuan penulisan dari penelitian berjudul kejahatan pencurian data pribadi melalui cyber phishing dan sistem pembuktiannya dalam persidangan: studi putusan no. 697/Pid.Sus/2024/PN.Sda adalah untuk menganalisis eksistensi tindak pidana pencurian data pribadi dan regulasi yang mengatur kejahatan berbasis cyber phishing, mengevaluasi proses penegakan hukum terhadap kasus-kasus tersebut, serta mengidentifikasi langkah hukum yang paling efektif dalam upaya penanggulangannya.

TINJAUAN PUSTAKA

Landasan Konseptual

Pencurian Data Pribadi

Pencurian data pribadi merupakan Tindakan ilegal yang bertujuan untuk mendapatkan atau memperoleh data pribadi seseorang secara tidak sah untuk disalahgunakan dalam berbagai jenis kejahatan.⁴¹⁴ Tindakan yang menggunakan modus penipuan di dunia maya ini bertujuan tujuan untuk mengelabui korban agar memberikan informasi sensitif seperti username, password, dan bahkan data keuangan.

Sistem Pembuktian

Rangkaian Prosedur Hukum yang digunakan dalam Persidangan untuk membuktikan suatu tindak pidana , termasuk dalam hal ini menggunakan alat bukti elektronik. Klasifikasi alat elektronik sebagai alat bukti dalam persidangan pidana telah ditentukan muatannya dalam UU

⁴¹⁴ Fiqqih Anugerah and Tantimin Tantimin, "Pencurian Data Pribadi Di Internet Dalam Perspektif Kriminologi," *Jurnal Komunikasi Hukum (JKH)* 8, no. 1 (February 1, 2022): 419–35, <https://doi.org/10.23887/jkh.v8i1.45434>.

ITE. Kemudian dalam RUU-KUHAP juga direncanakan akan diakomodirnya pengaturan alat elektronik sebagai alat bukti dalam persidangan pidana.⁴¹⁵ Menurut penjelasan pasal 177 ayat (1) huruf c RUU KUHAP yang dimaksud dengan “bukti elektronik” adalah informasi yang diucapkan, dikirim, diterima atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu, termasuk setiap rekaman data atau informasi yang dapat dilihat, dibaca dan atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana baik yang tertuang diatas kertas, benda fisik apapun selain kertas maupun terekam secara elektronik yang berupa tulisan, gambar, peta, rancangan, foto, huruf, tanda, angka, atau perforasi yang memiliki makna. Namun terkait dengan perlindungan data pribadi, Indonesia belum memiliki pengaturan khusus mengenai perlindungan data pribadi pada level Undang-Undang.⁴¹⁶

a. Cyber Phishing

Pidana Cyber phishing merupakan kejahatan siber yang mengandalkan teknik rekayasa sosial, pelaku secara sengaja memanipulasi korban dengan mengirimkan pesan atau email yang tampak berasal dari sumber resmi, seperti bank, perusahaan telekomunikasi, atau lembaga pemerintah. Pesan tersebut biasanya berisi permintaan untuk melakukan verifikasi data, pembaruan informasi akun, atau pemberitahuan adanya masalah yang membutuhkan tindakan segera. Korban akan diarahkan untuk mengakses

⁴¹⁵ Rachelya Putri Audrian, “Kendala Penerapan Pembuktian Dokumen Elektronik Dalam Pemeriksaan Di Pengadilan,” *Causa: Jurnal Hukum Dan Kewarganegaraan* 6, no. 6 (June 6, 2024).

⁴¹⁶ Siti Yuniarti, “Perlindungan Hukum Data Pribadi Di Indonesia,” *Business Economic, Communication, and Social Sciences (BECOSS) Journal* 1, no. 1 (September 30, 2019): 147–54, <https://doi.org/10.21512/becossjournal.v1i1.6030>.

situs web palsu yang dirancang menyerupai situs asli agar merasa aman saat memasukkan data pribadi.

Informasi yang sering diminta meliputi nomor identitas, username, password, nomor kartu kredit, serta data finansial lainnya. Setelah berhasil memperoleh data tersebut, pelaku dapat melakukan berbagai tindakan kriminal seperti pembobolan rekening, penipuan, hingga penyalahgunaan identitas korban. Selain itu, kejahatan ini memberikan efek psikologis berupa rasa takut dan ketidakpercayaan terhadap layanan digital. Pelaku cyber phishing terus mengembangkan metode agar lebih sulit terdeteksi, seperti menggunakan email dengan domain yang mirip, teknik spoofing, hingga memanfaatkan media sosial dan aplikasi pesan instan.⁴¹⁷

b. Hacking

Hacking adalah tindakan ilegal yang dilakukan dengan cara masuk ke dalam sistem komputer atau jaringan tanpa izin dari pemiliknya. Pelaku hacking memanfaatkan berbagai teknik dan metode, termasuk eksploitasi celah keamanan yang ada pada sistem, pemanfaatan perangkat lunak khusus untuk menembus pertahanan digital. Aksi ini bertujuan untuk mendapatkan akses tidak sah ke data atau informasi yang tersimpan di dalam sistem tersebut. Data yang menjadi target adalah data pribadi, seperti informasi identitas, data keuangan, hingga dokumen penting lain.

Fokus utama dalam hacking data pribadi adalah untuk memperoleh data untuk tujuan kriminal, seperti pencurian identitas, penipuan keuangan, hingga penyebaran malware atau ransomware. Hacking data pribadi tidak hanya merugikan korban secara langsung, tetapi juga menimbulkan

⁴¹⁷ Akbar Galih Hariyono and Frans Simangunsong, "Perlindungan Hukum Korban Pencurian Data Pribadi (Phishing Cybercrime) Dalam Perspektif Kriminologi," *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 3, no. 1 (March 1, 2023).

ancaman bagi keamanan nasional dan stabilitas sosial jika data tersebut disalahgunakan untuk kepentingan yang lebih luas, seperti spionase atau sabotase.⁴¹⁸

c. Skimming

Skimming merupakan jenis kejahatan pencurian data yang dilakukan dengan cara menyalin informasi kartu debit atau kredit secara ilegal dengan alat khusus yang disebut skimmer. Alat ini biasanya dipasang secara tersembunyi pada mesin ATM, mesin pembayaran di toko, atau perangkat lain yang membaca kartu. Ketika korban memasukkan kartu ke dalam mesin yang sudah dipasang skimmer, data yang tersimpan di dalam strip magnetik kartu tersebut secara otomatis disalin oleh alat tersebut tanpa disadari korban. Selain itu, pelaku juga sering memasang kamera kecil atau alat perekam untuk merekam PIN yang dimasukkan oleh korban. Informasi yang berhasil dicuri ini akan dipakai membuat kartu tiruan untuk transaksi tanpa persetujuan pemilik kartu.

d. Penggunaan Malware

Malware adalah perangkat lunak berbahaya yang secara diam-diam dipasang pada perangkat korban. Malware dapat melakukan berbagai aktivitas berbahaya, seperti merekam aktivitas pengguna, mencuri informasi sensitif, atau mengendalikan perangkat dari jarak jauh. Malware ini biasanya menyebar melalui lampiran email berbahaya, tautan palsu, atau perangkat lunak yang tidak resmi. Dampak dari serangan malware tidak hanya merugikan secara finansial, tetapi juga berpotensi mengancam privasi

⁴¹⁸ Justinus Andjarwirawan, Leo Willyanto Santoso, and Kartika Gunadi, "Cybersecurity Threats through Phishing Attacks Targeting Internal Staff, Mitigation and Prevention," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering* 10, no. 156 (2024).

dan keamanan data pribadi pengguna. Malware dapat dengan cepat menyebar ke perangkat lain melalui jaringan yang sama, sehingga meningkatkan risiko pencurian data secara massif.⁴¹⁹

Kajian Teori

a. Teori Pidanaan

Dalam ranah ilmu hukum, berkembang beragam teori mengenai tujuan pidana yang berupaya menjelaskan dasar dan arah dari penjatuhan pidana terhadap pelaku kejahatan. Tiga teori utama yang mendominasi diskursus ini adalah teori absolut (retributive), teori relatif (deterrence/utilitarian), dan teori penggabungan (integrative). Teori absolut berpandangan bahwa pidana dijatuhkan semata-mata sebagai bentuk pembalasan atas perbuatan jahat yang telah dilakukan, tanpa mempertimbangkan dampaknya di masa depan. Sementara itu, teori relatif menekankan fungsi pidana sebagai sarana pencegahan, baik secara umum untuk menimbulkan efek jera bagi masyarakat, maupun secara khusus untuk mencegah residivisme pada pelaku. Adapun teori penggabungan merupakan pendekatan yang menyatukan unsur pembalasan dan pencegahan secara seimbang, dengan mempertimbangkan keadilan sekaligus efektivitas sosial dari pidana. Ketiga teori ini menjadi landasan penting dalam merumuskan kebijakan pidana yang tidak hanya represif, tetapi juga adaptif terhadap konteks sosial dan tujuan hukum yang lebih luas.

b. Teori Pembuktian

Pembuktian, menurut Kamus Besar Bahasa Indonesia (KBBI), diartikan sebagai suatu perbuatan atau cara untuk

⁴¹⁹ Fiqqih Anugerah and Tantimin Tantimin, "Pencurian Data Pribadi Di Internet Dalam Perspektif Kriminologi," *Jurnal Komunikasi Hukum (JKH)* 8, no. 1 (February 1, 2022): 419–35, <https://doi.org/10.23887/jkh.v8i1.45434>.

membuktikan, yaitu usaha yang dilakukan guna menentukan benar atau salahnya seorang terdakwa dalam suatu sidang pengadilan. Dalam konteks hukum pidana, pembuktian merupakan aspek fundamental yang menentukan apakah seseorang dapat dipertanggungjawabkan secara hukum atas suatu perbuatan pidana. Sistem pembuktian yang digunakan dalam hukum pidana sendiri terbagi ke dalam tiga pendekatan utama, yaitu pembuktian positif, pembuktian negatif, dan keseimbangan pembuktian. Sistem pembuktian positif mewajibkan terpenuhinya syarat pembuktian secara formil berdasarkan alat-alat bukti yang telah ditentukan undang-undang. Sementara itu, sistem pembuktian negatif tidak hanya mensyaratkan terpenuhinya alat bukti, tetapi juga mewajibkan keyakinan hakim sebagai faktor penentu dalam memutus perkara. Adapun sistem keseimbangan pembuktian mencoba menggabungkan unsur objektif dan subjektif dari kedua sistem sebelumnya, dengan menekankan keseimbangan antara alat bukti dan keyakinan hakim untuk mencapai keadilan yang seimbang. Ketiga sistem ini menjadi kerangka penting dalam memastikan proses peradilan pidana berjalan sesuai prinsip-prinsip hukum yang adil dan proporsional.

METODE

Penelitian ini menggunakan metode yuridis normatif, yaitu pendekatan penelitian hukum yang berfokus pada analisis terhadap peraturan perundang-undangan tertulis dan bahan hukum sekunder untuk memecahkan isu hukum tertentu, dengan menelaah hukum positif yang berlaku beserta aspek normatifnya yang telah diundangkan secara resmi.⁴²⁰ Penelitian ini mengombinasikan metode analisis perundang-undangan, kajian preseden kasus, dan evaluasi kritis untuk menganalisis regulasi dan praktik hukum terkait isu hukum yang diangkat. Penelitian ini mengombinasikan metode

⁴²⁰ Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana, 2005).

statute approach (pendekatan peraturan) dan case approach (pendekatan kasus) dengan menggunakan tiga jenis bahan penelitian: (1) bahan hukum primer berupa peraturan perundang-undangan, (2) bahan hukum sekunder berupa literatur hukum, dan (3) bahan non-hukum yang relevan. Proses analisis dilakukan melalui tahapan sistematis meliputi identifikasi, inventarisasi, pencatatan, pengutipan, dan kajian mendalam terhadap bahan-bahan tersebut untuk menjawab permasalahan penelitian sesuai tujuan yang telah ditetapkan.

PEMBAHASAN

Kejahatan Pencurian Data di Indonesia dan Pengaturannya dalam Sistem Hukum di Indonesia

a. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang kemudian direvisi menjadi Undang-Undang Nomor 19 Tahun 2016, merupakan regulasi kunci dalam penanganan tindak pidana yang terjadi di ranah elektronik di Indonesia. UU ini mengatur berbagai bentuk kejahatan siber, termasuk akses tanpa izin ke sistem elektronik serta pencurian data pribadi secara ilegal. Selain itu, UU ITE juga mengatur sanksi bagi pelaku kejahatan tersebut, yang meliputi ancaman pidana penjara serta denda yang signifikan. Sanksi ini bertujuan memberikan efek jera agar tindak kejahatan di dunia maya dapat diminimalisir.

Pengaturan mengenai proses pembuktian dan penggunaan bukti elektronik dalam persidangan juga disertakan dalam UU ini, sehingga memberikan kemudahan dalam penegakan hukum di ranah digital yang memiliki karakteristik berbeda dari tindak pidana konvensional.⁴²¹

⁴²¹ Prigel Aditama, Elisabeth Aprilia Sinaga, and Citra Anjelika Putri, "Perbandingan Hukum Pidana Cyber Crime Dan

Penindakan terhadap kejahatan pencurian data pribadi di Indonesia secara tegas mengacu pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahan terakhir melalui Undang-Undang Nomor 1 Tahun 2024. Terdapat pasal-pasal yang secara spesifik mengatur larangan pengaksesan sistem elektronik secara ilegal dan sanksi hukum bagi pelaku. Pasal 30 mengatur tentang larangan mengakses komputer, sistem elektronik, atau dokumen elektronik tanpa hak.⁴²²

Selanjutnya, Pasal 36 UU ITE mengatur larangan bagi siapa saja yang dengan sengaja dan tanpa hak atau melawan hukum melakukan pengubahan, penghilangan, pemindahan, pengrusakan, atau membuat tidak dapat diaksesnya informasi elektronik atau dokumen elektronik yang berada dalam sistem elektronik. Pasal 51 ayat (2) UU ITE memberikan ancaman pidana bagi pelaku, dengan sanksi yang cukup berat berupa pidana penjara dan/atau denda, yang menunjukkan keseriusan pemerintah dalam menangani kejahatan ini. Perubahan yang dilakukan dalam Undang-Undang Nomor 1 Tahun 2024 semakin memperkuat ketentuan tersebut dengan memperjelas jenis perbuatan dan memperberat sanksi bagi pelaku.

Penuntut umum harus mampu membuktikan bahwa pelaku dengan sengaja dan tanpa hak melakukan akses atau manipulasi terhadap sistem elektronik yang mengakibatkan kerugian materiil atau immateriil. Pembuktian ini memerlukan keahlian teknis dalam mengumpulkan dan

Pengaruhnya Dalam Penegakan Hukum Antara Indonesia Dan Amerika," *Jurnal Kompilasi Hukum* 10, no. 1 (January 1, 2025).

⁴²² Muhammad Yudistira and Ramadani, "Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominformasi," *UNES Law Review* 5, no. 4 (July 13, 2023).

menganalisis alat bukti elektronik seperti log aktivitas, data transaksi, serta perangkat yang digunakan pelaku.

Undang-Undang Perlindungan Data Pribadi (UU PDP)

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan regulasi terbaru yang khusus mengatur perlindungan hukum atas data pribadi warga negara Indonesia yang menegaskan hak-hak subjek data, yaitu individu yang memiliki data pribadi, serta menetapkan kewajiban bagi pengelola data untuk menjaga keamanan, kerahasiaan, dan integritas data tersebut. UU PDP juga mengatur sanksi administratif dan pidana bagi pelanggar yang terbukti melakukan pencurian, kebocoran, atau penyalahgunaan data pribadi. Regulasi ini tidak hanya mewajibkan perusahaan, lembaga pemerintah, dan pelaku usaha untuk menerapkan standar keamanan data yang lebih ketat, tetapi juga memberikan dasar hukum yang jelas untuk penindakan hukum terhadap pelaku kejahatan pencurian data secara sistematis.⁴²³

Pelacakan Digital dan Pengumpulan Alat Bukti Elektronik

Metode digital forensik diterapkan secara sistematis untuk mengungkap jejak digital pelaku, mulai dari identifikasi alamat IP yang digunakan saat mengakses sistem elektronik hingga analisis log aktivitas pada akun yang terlibat. Alamat IP berfungsi sebagai indikator lokasi dan identitas perangkat yang mengakses data secara ilegal, sehingga keberadaannya dapat menghubungkan pelaku dengan tindakan kriminal yang dilakukan. Log aktivitas akun menjadi bukti penting karena merekam setiap interaksi, termasuk

⁴²³ Fauzan Prasetyo Eka Putra et al., "Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study," *Brilliance: Research of Artificial Intelligence* 4, no. 1 (August 9, 2024): 413–21, <https://doi.org/10.47709/brilliance.v4i1.4357>.

waktu dan jenis akses yang dilakukan, yang dapat digunakan untuk membuktikan keterlibatan seseorang dalam tindak pidana pencurian data.⁴²⁴

Selain itu, pengumpulan bukti berupa tangkapan layar transaksi dan riwayat pembayaran digital juga menjadi bukti pendukung yang sangat vital. Misalnya, bukti pembayaran atas barang elektronik yang dibeli menggunakan data yang dicuri dapat menjadi petunjuk kuat bahwa data tersebut telah digunakan tanpa izin. Bukti-bukti ini memperkuat dakwaan penuntut umum dan membantu hakim dalam mengambil keputusan berdasarkan fakta yang ada.⁴²⁵

Pengumpulan alat bukti elektronik juga meliputi penyitaan perangkat komunikasi seperti handphone, komputer, atau gadget lain yang digunakan oleh pelaku saat melakukan tindak pidana. Perangkat ini dianalisis secara forensik untuk mendapatkan data digital yang relevan seperti pesan, email, file yang tersimpan, dan aplikasi yang digunakan. Proses ini harus dilakukan oleh tenaga ahli yang memiliki keahlian di bidang digital forensik dan dilaksanakan sesuai standar hukum, sehingga hasilnya bisa menjadi bukti yang diterima di pengadilan.⁴²⁶

⁴²⁴ Diyu Sulaeman and Anyelir Puspa Kemala, "Analisis Hukum Terhadap Tindak Pidana Pencurian Identitas Di Indonesia," *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 3, no. 2 (February 21, 2025): 133–48, <https://doi.org/10.59246/aladalah.v3i2.1258>.

⁴²⁵ Yazid Haikal Lokapala, Fuad Januar Nurfauzi, and Yeni Widowaty, "Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia," *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 5, no. 1 (June 11, 2024), <https://doi.org/10.18196/ijclc.v5i1.19853>.

⁴²⁶ Vita Fajrin Jahriyah et al., "Kebebasan Berekspresi Di Media Elektronik Dalam Perspektif Pasal 27 Ayat (3) Undang- Undang Nomor 19 Tahun 2016 Perubahan Atas Undang- Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Pelayanan Transaksi Elektronik (UU ITE)," *Sosio Yustisia: Jurnal Hukum Dan Perubahan Sosial* 1, no. 2 (November 30, 2021): 65–87, <https://doi.org/10.15642/sosyus.v1i2.96>.

Peran Kepolisian dan Jaksa dalam Penyidikan dan Penuntutan

Penyidik Kepolisian bertugas melakukan penyelidikan secara mendalam untuk mengumpulkan bukti-bukti digital dan fisik yang sah.⁴²⁷ Dalam proses ini, penyidik harus menjalin kerja sama yang erat dengan penyedia layanan digital, seperti perusahaan telekomunikasi, penyedia platform pembayaran elektronik, dan pengelola sistem teknologi informasi lainnya. Kerja sama ini bertujuan untuk memperoleh data teknis yang diperlukan, misalnya alamat IP, log aktivitas sistem, serta riwayat transaksi digital yang dilakukan pelaku. Selain itu, penyidik juga harus berkoordinasi dengan lembaga pengawas data dan keamanan siber untuk memastikan proses pengumpulan bukti sesuai dengan prosedur hukum dan tidak melanggar hak privasi yang dilindungi oleh peraturan perundang-undangan.⁴²⁸

Setelah tahap penyidikan selesai, peran Jaksa dalam proses penuntutan menjadi krusial untuk menentukan kelanjutan kasus ke pengadilan. Jaksa bertugas menyusun dakwaan yang jelas dan terstruktur berdasarkan hasil penyidikan yang telah dilakukan oleh Kepolisian. Penyusunan dakwaan harus menguraikan unsur-unsur tindak pidana yang dilakukan pelaku secara sistematis, seperti bagaimana pelaku mengakses sistem elektronik secara ilegal, unsur kesengajaan, tanpa hak, serta akibat yang ditimbulkan berupa kerugian materiil bagi korban.

Jaksa juga bertugas memastikan bahwa tuntutan pidana yang diajukan sesuai dengan ketentuan undang-undang

⁴²⁷ Fadhila Rahman Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia," *AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dah Hukum* 2, no. 1 (January 11, 2024): 8–16, <https://doi.org/10.32520/albahts.v2i1.3044>.

⁴²⁸ Iskandar, "Analisis Kejahatan Online Phishing Pada Masyarakat."

yang berlaku, khususnya Undang-Undang Informasi dan Transaksi Elektronik serta perubahannya, sehingga proses hukum berjalan efektif dan adil.⁴²⁹ Penyidik Kepolisian bertanggung jawab mengumpulkan dan melengkapi bukti-bukti yang diperlukan secara akurat dan terperinci, sementara Jaksa memiliki peran strategis untuk mengajukan dakwaan yang kuat dan mempresentasikan kasus di pengadilan.⁴³⁰

Analisis Putusan Nomor 697/Pid.Sus/2024/PN Sda

a. Latar Belakang Kasus

Putusan Kasus ini berawal dari hubungan profesional antara Terdakwa Muchammad Yufianto, seorang sales handphone merek VIVO yang bekerja di toko Eraphone Jalan Raya Gading Fajar, Candi-Sidoarjo, dengan Saksi Devi Nuri Khayati Putri R. yang telah dikenal sebelumnya. Pada Sabtu, 31 Agustus 2024, sekitar pukul 21.00 WIB, Terdakwa menghubungi Saksi Devi dan meminta bantuan untuk memenuhi target penjualan bulanan di toko tempat ia bekerja. Terdakwa mengaku hanya memerlukan data pribadi saksi untuk keperluan pendaftaran akun pada aplikasi pembiayaan kredit elektronik bernama “Akulaku”, dan menjanjikan bahwa transaksi tidak akan dilakukan atas nama saksi. Karena rasa percaya dan tidak curiga, Saksi Devi menyanggupi permintaan tersebut dan menyerahkan handphone miliknya, sebuah VIVO V27E warna hitam, kepada Terdakwa di warung angkringan depan Perumahan

⁴²⁹ Akhmad Fery Hasanudin and A Basuki Babussalam, “Perlindungan Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking,” *Jurnal Gagasan Hukum* 6, no. 01 (June 30, 2024): 16–29, <https://doi.org/10.31849/jgh.v6i01.18827>.

⁴³⁰ Elfian Fauzi and Nabila Alif Radika Shandy, “Hak Atas Privasi Dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi,” *Jurnal Lex Renaissance* 7, no. 3 (July 1, 2022): 445–61, <https://doi.org/10.20885/JLR.vol7.iss3.art1>.

Citra Mandiri Regency, Sukodono, Sidoarjo. Di lokasi itu, Terdakwa kemudian mendaftarkan akun Akulaku menggunakan identitas pribadi milik Saksi Devi tanpa penjelasan lebih lanjut terkait penggunaannya.⁴³¹

Setelah akun Akulaku berhasil dibuat, Terdakwa mengaksesnya tanpa sepengetahuan dan persetujuan dari Saksi Devi. Ia kemudian menghubungi rekannya, Saksi Dina Natalia Mardiana, yang merupakan sales dari leasing Paylater Akulaku, dan menyampaikan bahwa terdapat “customer” (padahal menggunakan identitas Saksi Devi) yang hendak melakukan pembelian handphone iPhone 15 secara kredit tanpa uang muka (DP) melalui fasilitas paylater tersebut. Saksi Dina kemudian menindaklanjuti dan memproses pengajuan kredit atas nama akun Akulaku milik Saksi Devi, tanpa menjelaskan detail transaksi kepada pemilik asli identitas. Transaksi tersebut akhirnya disetujui oleh pihak leasing, dan satu unit handphone iPhone 15 warna pink dengan harga Rp14.449.000,- disiapkan di toko Eraphone Gading Fajar. Namun, handphone tersebut tidak diserahkan kepada Saksi Devi sebagai pemilik akun, melainkan langsung diambil oleh Terdakwa Muchammad Yufianto sendiri. Artinya, Terdakwa secara sengaja dan melawan hukum telah mengakses akun elektronik orang lain dan memanfaatkan data pribadi tersebut untuk transaksi komersial yang merugikan.⁴³²

Tidak hanya sampai di sana, Terdakwa kembali melakukan tindakan penipuan dan penggelapan dengan menjual unit handphone iPhone 15 yang diperoleh melalui akun Saksi Devi dalam keadaan masih tersegel kepada seseorang bernama Eko melalui platform Facebook. Transaksi penjualan dilakukan dengan harga

⁴³¹ Mahkamah Agung Republik Indonesia, “Putusan Nomor 697/Pid.Sus/2024/PN Sda,” Pengadilan Negeri Sidoarjo § (2024).

⁴³² Mahkamah Agung Republik Indonesia.

Rp10.000.000,-. Uang hasil penjualan tersebut tidak disampaikan atau diserahkan kepada Saksi Devi, melainkan digunakan seluruhnya untuk kepentingan pribadi Terdakwa. Selain melakukan pembelian handphone secara ilegal melalui akun Akulaku milik orang lain, Terdakwa juga menggunakan akun tersebut untuk melakukan peminjaman dana tunai sebesar Rp1.000.000,-, kembali tanpa sepengetahuan dan persetujuan dari Saksi Devi. Dengan demikian, total kerugian materiil yang diderita oleh Saksi Devi mencapai Rp15.449.000,-, yang terdiri dari harga handphone yang dibeli atas namanya serta dana pinjaman yang harus dibayarkan oleh Saksi Devi ke pihak leasing.⁴³³

Perbuatan Terdakwa baru terungkap pada tanggal 18 September 2024, saat Saksi Devi dihubungi oleh tim Akulaku melalui sambungan telepon. Dalam komunikasi tersebut, pihak Akulaku menagih pembayaran cicilan atas transaksi pembelian unit iPhone 15 serta peminjaman dana tunai, yang semuanya terdaftar atas akun milik Devi. Merasa tidak pernah melakukan transaksi tersebut, Saksi Devi pun terkejut dan melakukan penelusuran terkait lokasi pembelian dan pihak-pihak yang terlibat. Dari penelusuran tersebut, ditemukan bahwa orang yang telah mengambil handphone serta memproses transaksi pinjaman adalah Terdakwa Muchammad Yufianto. Saksi kemudian melaporkan tindakan ini kepada pihak berwenang karena merasa identitas dan akun elektroniknya telah digunakan secara melawan hukum untuk tindakan kriminal yang merugikannya secara materiil.⁴³⁴

b. Pertimbangan Hukum Hakim terkait Pencurian Data Pribadi

Dalam kasus pencurian data pribadi yang melibatkan terdakwa Muchammad Yufianto, Majelis Hakim

⁴³³ Mahkamah Agung Republik Indonesia.

⁴³⁴ Mahkamah Agung Republik Indonesia.

mempertimbangkan berbagai bukti dan keterangan saksi yang diajukan oleh Penuntut Umum. Berdasarkan Pasal 30 ayat (2), Pasal 36, dan Pasal 51 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, tindakan terdakwa yang mengakses akun Akulaku milik Devi Nuri Khayati Putri tanpa izin dan melakukan transaksi fiktif senilai Rp14.449.000 jelas merupakan pelanggaran hukum. Bukti-bukti yang diajukan, termasuk handphone merek VIVO V27E, akun Akulaku, serta screenshot tagihan dan bukti pembayaran, menunjukkan adanya akses ilegal terhadap sistem elektronik dan penyalahgunaan data pribadi. Keterangan dari saksi-saksi, seperti Devi dan Dina, memberikan gambaran yang jelas tentang modus operandi terdakwa, di mana terdakwa meminjam data pribadi saksi untuk membuat akun dan melakukan transaksi tanpa sepengetahuan korban.⁴³⁵

Majelis Hakim juga mempertimbangkan dampak dari tindakan terdakwa terhadap korban, yang tidak hanya mengalami kerugian finansial tetapi juga kehilangan kepercayaan terhadap sistem digital.⁴³⁶ Dalam menanggapi tuntutan pidana yang diajukan oleh Jaksa Penuntut Umum, yaitu penjara selama 1 tahun 6 bulan, Hakim menilai bahwa hukuman tersebut sebanding dengan sifat melawan hukum dari perbuatan terdakwa dan kerugian yang ditimbulkan. Keputusan ini diharapkan dapat memberikan efek jera dan mendorong penegakan hukum yang lebih tegas terhadap kejahatan siber di Indonesia, serta melindungi hak-hak individu dalam era digital yang semakin kompleks.

c. Analisis Pencurian Data Pribadi

Penindakan pencurian data pribadi di Indonesia diatur tegas dalam UU ITE dan perubahannya melalui UU No. 1 Tahun 2024, khususnya Pasal 30 yang melarang akses

⁴³⁵ Mahkamah Agung Republik Indonesia.

⁴³⁶ Mahkamah Agung Republik Indonesia.

ilegal terhadap sistem elektronik dan menetapkan sanksi bagi pelanggar.⁴³⁷ Pasal 36 dan 51 ayat (2) UU ITE, yang diperkuat melalui perubahan dalam UU No. 1 Tahun 2024, menegaskan larangan dan sanksi tegas terhadap tindakan manipulasi sistem elektronik tanpa hak, sementara proses pembuktiannya menuntut keahlian teknis guna membuktikan unsur kesengajaan serta dampak kerugian yang ditimbulkan. Metode digital forensik digunakan secara sistematis untuk menelusuri jejak pelaku melalui analisis alamat IP dan log aktivitas akun, yang berfungsi sebagai bukti penting dalam menghubungkan identitas pelaku dengan tindakan pencurian data secara ilegal.⁴³⁸

Hakim berkewajiban menilai keabsahan dan kredibilitas bukti secara objektif serta mempertimbangkan secara menyeluruh unsur-unsur tindak pidana yang telah terbukti secara sah dan meyakinkan. Dalam hal ini, fokus utama adalah pada pemulihan hak korban yang mengalami kerugian materiil maupun immaterial akibat tindakan pelaku. Oleh karena itu, hakim tidak hanya menilai aspek hukum formil, tetapi juga mengedepankan aspek keadilan substantif yang menjamin perlindungan dan pemulihan hak korban.⁴³⁹

Dalam perkara Nomor 697/Pid.Sus/2024/PN Sda, pengadilan mengambil langkah konkret dengan menjatuhkan pidana penjara selama satu tahun enam bulan kepada terdakwa yang terbukti bersalah melakukan pencurian data pribadi melalui akses sistem elektronik secara ilegal. Selain hukuman penjara, pengadilan juga memerintahkan pengembalian barang bukti yang telah disita kepada korban.

⁴³⁷ Yudistira and Ramadani, "Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominfo."

⁴³⁸ Diyu Sulaeman and Anyelir Puspa Kemala, "Analisis Hukum Terhadap Tindak Pidana Pencurian Identitas Di Indonesia."

⁴³⁹ Khanifah Jannatul Diniyah, "Perlindungan Hukum Bagi Korban Tindak Pidana Cyber Crime Phishing" (Malang, December 28, 2021).

Hakim harus memastikan bahwa keputusan yang diambil memiliki dasar yang kuat dan tidak menimbulkan ketidakpastian hukum, agar putusan tersebut dapat memberikan kepastian hukum dan kepercayaan masyarakat terhadap sistem peradilan.⁴⁴⁰

Analisis terhadap pertimbangan hakim dalam perkara pencurian data pribadi yang melibatkan terdakwa Muchammad Yufianto menunjukkan bahwa penindakan terhadap kejahatan ini diatur secara tegas dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan perubahannya melalui UU No. 1 Tahun 2024. Pasal 30 UU ITE melarang akses ilegal terhadap sistem elektronik dan menetapkan sanksi bagi pelanggar, sementara Pasal 36 dan 51 ayat (2) menegaskan larangan dan sanksi tegas terhadap manipulasi sistem elektronik tanpa hak. Proses pembuktian yang melibatkan metode digital forensik, seperti analisis alamat IP dan log aktivitas akun, menjadi krusial dalam menghubungkan identitas pelaku dengan tindakan pencurian data. Dalam hal ini, hakim tidak hanya menilai keabsahan dan kredibilitas bukti secara objektif, tetapi juga mempertimbangkan pemulihan hak korban yang mengalami kerugian materiil dan immaterial. Dengan menjatuhkan pidana penjara selama satu tahun enam bulan dan memerintahkan pengembalian barang bukti kepada korban, pengadilan menunjukkan komitmennya terhadap keadilan substantif dan perlindungan hak-hak individu. Keputusan ini diharapkan dapat memberikan kepastian hukum dan meningkatkan kepercayaan masyarakat terhadap sistem peradilan, serta mendorong penegakan hukum yang lebih efektif terhadap kejahatan siber di Indonesia.

⁴⁴⁰ Adinda Lola Sariani Dinda, "Efektivitas Penegakan Hukum Terhadap Kejahatan Siber Di Indonesia," *AL-DALIL: Jurnal Ilmu Sosial, Politik, Dan Hukum* 2, no. 2 (July 18, 2024): 69–77, <https://doi.org/10.58707/aldalil.v2i2.777>.

SIMPULAN

Kesimpulan dari analisis putusan Nomor 697/Pid.Sus/2024/PN Sda menunjukkan bahwa tindakan pencurian data pribadi oleh terdakwa Muchammad Yufianto, melalui akses ilegal terhadap akun Akulaku milik Saksi Devi Nuri Khayati Putri, melanggar ketentuan Pasal 30 ayat (2), Pasal 36, dan Pasal 51 ayat (2) UU ITE serta UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Dalam perkara ini, terdakwa menggunakan identitas korban untuk mendaftarkan akun dan melakukan transaksi tanpa izin, yang mengakibatkan kerugian materiil sebesar Rp15.449.000,-. Putusan pengadilan yang menjatuhkan hukuman penjara selama satu tahun enam bulan serta mengembalikan barang bukti kepada korban mencerminkan upaya serius dalam menegakkan hukum dan memberikan efek jera terhadap pelaku kejahatan siber. Proses pembuktian melalui digital forensik, seperti analisis alamat IP dan log aktivitas akun, menunjukkan kemajuan sistem hukum Indonesia dalam melindungi hak individu di era digital. Oleh karena itu, pemerintah perlu meningkatkan sosialisasi UU ITE dan UU PDP, memperkuat kerja sama antara aparat penegak hukum dan penyedia layanan digital, serta memberikan pelatihan teknis terkait digital forensik kepada aparat. Di sisi lain, masyarakat juga perlu diedukasi agar lebih waspada dalam membagikan data pribadi serta memahami risiko penggunaan layanan digital secara sembarangan.

DAFTAR PUSTAKA

Aditama, Prigel, Elisabeth Aprilia Sinaga, and Citra Anjelika Putri. "Perbandingan Hukum Pidana Cyber Crime Dan Pengaruhnya Dalam Penegakan Hukum Antara Indonesia Dan Amerika." *Jurnal Kompilasi Hukum* 10, no. 1 (January 1, 2025).

Akhmad Fery Hasanudin, and A Basuki Babussalam. "Perlindungan Hukum Bagi Korban Kejahatan Phising Yang

Menguras Saldo M-Banking.” *Jurnal Gagasan Hukum* 6, no. 01 (June 30, 2024): 16–29. <https://doi.org/10.31849/jgh.v6i01.18827>.

Andjarwirawan, Justinus, Leo Willyanto Santoso, and Kartika Gunadi. “Cybersecurity Threats through Phishing Attacks Targeting Internal Staff, Mitigation and Prevention.” *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering* 10, no. 156 (2024).

Anugerah, Fiqqih, and Tantimin Tantimin. “Pencurian Data Pribadi Di Internet Dalam Perspektif Kriminologi.” *Jurnal Komunikasi Hukum (JKH)* 8, no. 1 (February 1, 2022): 419–35. <https://doi.org/10.23887/jkh.v8i1.45434>.

———. “Pencurian Data Pribadi Di Internet Dalam Perspektif Kriminologi.” *Jurnal Komunikasi Hukum (JKH)* 8, no. 1 (February 1, 2022): 419–35. <https://doi.org/10.23887/jkh.v8i1.45434>.

Audrian, Rachelya Putri. “Kendala Penerapan Pembuktian Dokumen Elektronik Dalam Pemeriksaan Di Pengadilan.” *Causa: Jurnal Hukum Dan Kewarganegaraan* 6, no. 6 (June 6, 2024).

Dinda, Adinda Lola Sariani. “Efektivitas Penegakan Hukum Terhadap Kejahatan Siber Di Indonesia.” *AL-DALIL: Jurnal Ilmu Sosial, Politik, Dan Hukum* 2, no. 2 (July 18, 2024): 69–77. <https://doi.org/10.58707/aldalil.v2i2.777>.

Diniyah, Khanifah Jannatul. “Perlindungan Hukum Bagi Korban Tindak Pidana Cyber Crime Phishing.” Malang, December 28, 2021.

Diyu Sulaeman, and Anyelir Puspa Kemala. “Analisis Hukum Terhadap Tindak Pidana Pencurian Identitas Di Indonesia.” *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 3, no. 2 (February 21, 2025): 133–48. <https://doi.org/10.59246/aladalah.v3i2.1258>.

Fauzi, Elfian, and Nabila Alif Radika Shandy. “Hak Atas Privasi Dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.” *Jurnal Lex*

Renaissance 7, no. 3 (July 1, 2022): 445–61. <https://doi.org/10.20885/JLR.vol7.iss3.art1>.

Hariyono, Akbar Galih, and Frans Simangunsong. “Perlindungan Hukum Korban Pencurian Data Pribadi (Phishing Cybercrime) Dalam Perspektif Kriminologi.” *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 3, no. 1 (March 1, 2023).

Iskandar, Octo. “Analisis Kejahatan Online Phishing Pada Masyarakat.” *Leuser: Jurnal Hukum Nusantara* 1, no. 2 (July 1, 2024).

Jahriyah, Vita Fajrin, Moch. Tommy Kusuma, Kuni Qonitazzakiah, and Muh. Ali Fathomi. “Kebebasan Berekspresi Di Media Elektronik Dalam Perspektif Pasal 27 Ayat (3) Undang- Undang Nomor 19 Tahun 2016 Perubahan Atas Undang- Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Pelayanan Transaksi Elektronik (UU ITE).” *Sosio Yustisia: Jurnal Hukum Dan Perubahan Sosial* 1, no. 2 (November 30, 2021): 65–87. <https://doi.org/10.15642/sosyus.v1i2.96>.

Lokapala, Yazid Haikal, Fuad Januar Nurfauzi, and Yeni Widowaty. “Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia.” *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 5, no. 1 (June 11, 2024). <https://doi.org/10.18196/ijclc.v5i1.19853>.

Mahkamah Agung Republik Indonesia. Putusan Nomor 697/Pid.Sus/2024/PN Sda, Pengadilan Negeri Sidoarjo § (2024).

Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Kencana, 2005.

Maskun. *Kejahatan Siber (Cyber Crime) Suatu Pengantar*. Jakarta: Kencana, 2013.

Putra, Fauzan Prasetyo Eka, Ubaidi Ubaidi, Achmad Zulfikri, Goffal Arifin, and Revi Mario Ilhamsyah. “Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study.” *Brilliance: Research of Artificial*

Intelligence 4, no. 1 (August 9, 2024): 413–21. <https://doi.org/10.47709/brilliance.v4i1.4357>.

Rahman Najwa, Fadhila. “Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia.” *AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dah Hukum* 2, no. 1 (January 11, 2024): 8–16. <https://doi.org/10.32520/albahts.v2i1.3044>.

Rohaya, Siti. “Internet: Pengertian, Sejarah, Fasilitas Dan Koneksinya.” *Fihris Jurnal* 3, no. 1 (April 1, 2008).

Yudistira, Muhammad, and Ramadani. “Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominfo.” *UNES Law Review* 5, no. 4 (July 13, 2023).

Yuniarti, Siti. “Perlindungan Hukum Data Pribadi Di Indonesia.” *Business Economic, Communication, and Social Sciences (BECOSS) Journal* 1, no. 1 (September 30, 2019): 147–54. <https://doi.org/10.21512/becossjournal.v1i1.6030>.