DOI: https://doi.org/10.62017/syariah

PERLINDUNGAN HUKUM BAGI KORBAN PENCURIAN DATA DAN INFORMASI PRIBADI DI ERA KEJAHATAN SIBER

Saptaning Ruju Paminto*[1]
Ahdi Hidayat[2]
Bilkis Nabila[3]
M. Raihan Husaeni[4]
Resna Amelia Putri[5]
Siti Jenar Maharani[6]

[1,2,3,4,5,6] Fakultas Hukum, Universitas Suryakancana
*e-mail: bilkisnabila15@gmail.com, Msitijenar8@gmail.com

Abstrak

Pencurian data dan informasi pribadi di era digital menjadi salah satu bentuk kejahatan siber yang semakin meresahkan di Indonesia. Kejahatan ini dipengaruhi oleh berbagai faktor, seperti pesatnya perkembangan teknologi informasi, kelalaian individu dalam menjaga data pribadi, serangan malware, social engineering, serta rendahnya kesadaran masyarakat terhadap keamanan siber. Dampak dari kejahatan ini mencakup kerugian finansial, kerusakan reputasi, gangguan emosional, hingga potensi ancaman terhadap keamanan nasional. Penelitian ini bertujuan untuk mengidentifikasi faktor-faktor penyebab pencurian data dan informasi pribadi, menganalisis dampaknya terhadap korban, serta mengevaluasi upaya perlindungan hukum yang dilakukan oleh pemerintah Indonesia. Penelitian ini menggunakan metode yuridis normatif, yaitu pendekatan yang berfokus pada studi terhadap aturan hukum yang berlaku, bahan kepustakaan, dan dokumen-dokumen resmi lainnya. Metode ini dilakukan dengan cara menganalisis peraturan perundang-undangan, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), serta berbagai kebijakan dan regulasi terkait perlindungan data pribadi di Indonesia. Selain itu, upaya pemerintah mencakup peningkatan kesadaran masyarakat, penegakan hukum, serta penyediaan mekanisme penyelesaian sengketa bagi korban kejahatan siber. Dengan adanya regulasi yang lebih ketat dan penguatan perlindungan hukum, diharapkan pencurian data dapat diminimalkan, dan korban mendapatkan perlindungan serta keadilan yang layak.

***Kata kunci**: Pencurian Data; Kejahatan Siber; Perlindungan Hukum; UU PDP.*

Abstract

Heft of data and personal information in the digital era is a form of cyber crime that is increasingly disturbing in Indonesia. This crime is influenced by various factors, such as the rapid development of information technology, individual negligence in protecting personal data, malware attacks, social engineering, and low public awareness of cyber security. The impact of this crime includes financial loss, reputation damage, emotional disturbance, and potential threats to national security. This research aims to identify the factors that cause data and personal information theft, analyze its impact on victims, and evaluate legal protection efforts carried out by the Indonesian government. This research uses a normative juridical method, namely an approach that focuses on the study of applicable legal regulations, library materials and other official documents. This method is carried out by analyzing statutory regulations, such as Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), as well as various policies and regulations related to personal data protection in Indonesia. In addition, government efforts include increasing public awareness, law enforcement, and providing dispute resolution mechanisms for victims of cyber crime. With stricter regulations and strengthening legal protection, it is hoped that data theft can be minimized, and victims will receive proper protection and justice.

***Keywords**: Data Theft; Cyber Crime; Legal Protection; PDP Law.*

PENDAHULUAN

Latar Belakang

Seiring dengan perkembangan zaman masyarakat dapat dengan mudah mendapatkan informasi yang diinginkan dengan mudah dan cepat melalui berbagi teknologi yang semakin maju dan canggih. Hal ini membuat teknologi menjadi kebutuhan sehari-hari yang harus ada dan ikut

DOI: https://doi.org/10.62017/syariah

serta dalam kehidupan masyarakat Indonesia untuk meningkatkan kemudahan dalam memperoleh informasi dengan cepat.[1] Kemajuan teknologi dan informasi juga dapat mengubah pola hidup dan pemicu adanya transmutasi masyarakat, budaya, ekonomi, keamanan, dan penegakkan hukum di masyarakat Indonesia. Perkembangan teknologi waktu dan jarak bukan lagi menjadi masalah utama setiap individu, termasuk pemerintah. Setiap individu dapat berkomunikasi satu sama lain tanpa bertemu di ruang fisik.[2]

Teknologi informasi dapat meningkatkan kemajuan dalam pandangan hidup manusia, namun juga bisa menjadi sarana melakukan tindak criminal hukum yang dikenal sebagai *"cybercrime". Cyber crime* merupakan tindak kejahatan atau kegiatan ilegal yang dilakukan melalui jaringan dunia elektronik. Kriminalitas melalui jaringan internet semakin berbahaya dikarenakan ruang lingkup tindakan tersebut sangat luas. Tindakan kriminal dalam internet merupakan kejahatan yang berhubngan dengan dunia maya yang dapat membahayakan privasi seseorang. Kejahatan di dunia internet semakin meningkat dan semakin banyak jenis kejahatannya. Para pelaku dengan mudah melakukan tindak kejahatan dengan memakai kemajuan teknologi dan informasi. Contoh dari kejahatannya seperti pornografi, perjudian *online,* terorisme, *hacking, carding, phishing,* ATM/EDC *skimming,* dan kejahatan lainnya yang membahayan korbannya.[3]

Pencurian data dalam internet disebut sebagai istilah *phishing,* merupak tindakan kejahatan mendapatkan informasi pribadi atau privasi nomor kartu kredit, PIN, *user ID,* nomor telepon, nomor rekening dan informasi data pribadi lainnya. Dari tindakan tersebut pelaku memanfaatkan kejahatan yang dapat merugikan bagi korban yang dicuri datanya dan korban lainnya yang akan dijadikan sebagai target dari pelaku untuk menipu. Tingkat ancaman kejahatan eksploitasi informasi atau data pribadi di Indonesia sudah sangat berbahaya ketika pemerintah menetapkan kebijakan Kartu Tanda Penduduk elektronik (e-KTP) yang sebagai metode pendataan informasi dana data pribadi masyarakat oleh pemerintah yang pertama kali dijalankan saat awal tahun 2011, yakni pelaksanaan dari metode Nomor Induk Kependudukan (NIK).

Kasus kebocoran informasi pribadi sangat sering terjadi di Indonesia. Di perbankan, pertukaran data pribadi dapat mencakup pertukaran informasi tentang data pribadi pelanggan antar card center, pengungkapan informasi kepada pihak ketiga, termasuk transaksi yang terkait dengan pemilik kartu kredit, atau transaksi antar bank, dilakukan melalui sistem umum atau melalui pihak ketiga, baik individu atau perusahaan yang mengumpulkan data dan memperdagangkan data pribadi pelanggan. Di sektor medis, data pasien diperdagangkan atau diungkapkan tanpa sepengetahuan pasien untuk tujuan asuransi, kesempatan kerja, atau penerimaan program dukungan pemerintah.

Pada platform transportasi online, detail telepon konsumen tidak digunakan untuk tujuan awal pengumpulan data, tetapi bahkan untuk mengancam konsumen karena ulasan penumpang yang buruk. Alternatifnya, hal ini mengacaukan kenyamanan konsumen dengan menyampaikan pesan pribadi yang tidak relevan dengan pemakaian pengiriman online. Untuk transaksi jual beli via pasar online, teknologi cookies menggunakan teknologi cookies untuk menyalahgunakan informasi pengenal pribadi seperti preferensi belanja, lokasi belanja, data komunikasi, dan bahkan pelacakan transaksi online di mana alamat konsumen berada.[4]

Mengingat banyaknya kejadian pencurian data yang terjadi di Indonesia, maka pemerintah Indonesia perlu mengantisipasi atau meminimalisir kejadian tersebut dengan membuat perlindungan hukum yang kuat agar segera keluar dari kejadian pencurian data ini.

[1] Disemadi, 2021, *Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia,* Jurnal Wawasan Yuridika, Vol. 5 No. 2, Fakultas Hukum, Universitas Internasional Batam, Batam, hlm. 177-199.

[2] Alhakim, 2022, *Urgensi Perlindungan Hukum Terhadap Jurnalis Dari Risiko Kriminalisasi UU Informasi Dan Transaksi Elektronik Di Indonesia*, Jurnal Pembangunan Hukum Indonesia, Vol. 4 No. 1, Fakultas Hukum, Universitas Internasional Batam, Batam, hlm. 89-106.

[3] Alhakim and Sofia, 2021, *Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia,* Jurnal Komunitas Yustisia, Vol. 4 No. 2, Fakultas Hukum, Universitas Internasional Batam, Batam, hlm. 377-385.

[4] Fiqqih Anugerah and Tantimin, 2022, *Pencurian Data Pribadi Di Internet Dalam Perspektif Kriminologi,* Jurnal Komunikasi Hukum, Vol. 8 No. 1, Fakultas Hukum, Universitas Internasional Batam, Indonesia, hlm. 421-422.

DOI: https://doi.org/10.62017/syariah

Kasus tersebut sangat dapat sangat merugikan korban secara material dan immaterial. Pada kasus pencurian informasi atau data pribadi juga dapat menimbulkan korban terus-menerus, tidak hanya pengunjung situs web dan sistem elektronik, tetapi juga perusahaan yang memiliki sistem elektronik dan bank yang menjadi mitra pembayaran dapat mencuri data. Dapat diartikan bahwa korban pencurian data dapat mencakup tidak hanya individu tetapi juga komunitas dan rakyat Indonesia.

Ketentuan mengenai perlindungan data pribadi tidak diatur secara khusus oleh hukum Indonesia, oleh karena itu, regulasi terkait data pribadi masih bersifat parsial atau sektoral dan masih bersifat duplikasi. Peraturan ini secara individual terkandung dari beberapa undang-undang dan hanya mencerminkan aspek umum dari perlindungan data pribadi. Terutama tentang regulasi sistem elektronik, Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah dirubah oleh Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE).[5]

Rumusan Masalah

Penulis sudah menyusun sebagian permasalahan yang hendak dibahas dalam jurnal ini. Ada pula permasalahan yang hendak dibahas dalam karya tulis ini adalah diantaranya :

1) Apa yang melatarbelakangi faktor-faktor terjadinya kejahatan pencurian data dan informasi pribadi di Indonesia?
2) Apa dampak pencurian data dan informasi pribadi terhadap korban kejahatan siber di Indonesia?
3) Bagaimana upaya pemerintah dalam melakukan perlindungan hukum bagi korban pencurian data dan informasi pribadi di era kejahatan siber?

METODE

Metode yang digunakan dalam penulisan ini menggunakan metode yuridis normatif, yaitu penelitian hukun dengan cara meneliti bahan kepustakaan dan peraturan perundang-undangan yang berlaku. Dimana penelitian ini berfokus pada perlindungan hukum bagi korban pencurian data dan informasi pribadi di era kejahatan siber, dengan tujuan untuk menganalisis regulasi yang ada serta meminimalisasi dampak dari kejahatan siber terhadap individu, masyarakat, dan pemerintah.

HASIL DAN PEMBAHASAN

Faktor yang melatarbelakangi terjadinya kejahatan pencurian data dan informasi pribadi di Indonesia.

Perkembangan masyarakat zaman sekarang semakin maju dan didukung oleh pertumbuhan teknologi telekomunikasi, hingga ikatan antar negara sudah bersifat mendunia sehingga menghasilkan tatanan dunia baru. Perkembangan teknologi informasi dan komunikasi terus berkembang pesat, kini dimungkinkan untuk menggunakan teknologi informasi dan komunikasi melalui perangkat mobile.

Kegiatan yang biasanya dilakukan di dunia nyata kini banyak diperdagangkan melalui gadget. Transaksi berpindah dengan menggunakan i-Pad, smartphone, handphone, laptop. Pesatnya perkembangan teknologi informasi dan komunikasi juga diiringi dengan meluasnya penyalahgunaan teknologi informasi dan komunikasi, sehingga menjadi masalah yang sangat meresahkan yaitu terjadinya kejahatan yang dilakukan di dunia maya atau biasa dikenal dengan istilah "*cybercrime*".[6]

Mengacu pada Kitab Hukum Pidana (KUHP), pengertian secara luas mengenai tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan sistem

[5] *Ibid,* hlm. 423.

[6] Miftakhur Rokhman, 2020, *Kejahatan Teknologi Informasi (Cyberr Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia,* Jurnal Al-Qanun : Jurnal Pemikiran dan Pembaharua Hukum Islam, Vol. 23 No. 2, UIN Sunan Ampel, Surabaya, hlm. 401.

DOI: https://doi.org/10.62017/syariah

elektronik, artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana (KUHP) sepanjang dengan bantuan atau sarana sistem elektronik seperti pembunuhan, perdagangan orang dapat termasuk dalam kategori tindak kejahatan siber secara luas.[7] Teknologi merupakan kegiata yang dilahirkan oleh manusia dengan merencakan dan menciptakan benda-benda material yang bernilai praktis, seperti mobil, pesawat, televisi adalah hasil dari perkembanga teknologi.

John Perry Barlow pada tahun 1990 mengaplikasikan istilah siber yang dihubungkan pada jaringan internet. Dalam perkembangannya, siber dapat membawa dampak positif dan negatif yang dapat menimbulkan suatu kejahatan dalam perkembangan dunia siber. Kejahatan yang lahir sebagai suau dampak negatif dari perkembangan aplikasi pada internet ini disebut dengan kejahatan siber (*cybercrime)* yang mencakup semua jenis kejahatan beserta modus operasinya yang dilakukan sebagai dampal negatif aplikasi internet.

Menurut pendapat **Mcdonnell** dan **Sayers,** ancaman siber terdiri atas tiga jenis yaitu :

a. Ancaman perangkat keras (*hardware threat),* ancaman ini merupakan ancaman yang disebabkan oleh pemasangan perangkat tertentu yang berfungsi untuk melakukan kegiatan tertentu didalam suatu sistem, sehingga peralatan tersebut merupakan gangguan terhadap sistem jaringan dan perangkat keras lainnya.
b. Ancaman perangkat lunak (*software threat),* ancaman ini merupakan ancaman yang disebabkan masuknya perangkat lunak tertentu yang berfungsi untuk melakukan kegiatan pencurian, perusakan, dan manipulasi informasi.
c. Ancaman data/informasi (*data/information threat),* ancaman ini merupakan ancaman yang diakibatkan oleh penyebara data/informasi tertentu yang bertujuan untuk kepentingan tertentu.

Dalam kajian strategis Keamanan Siber Nasional, mendefinisikan ancaman kejahatan siber (*cyber crime)* sebagai setiap kondisi dan situasi serta kemampuan yang dinilai dapat melakukan tindakan atau gangguan atau serangan yang mampu merusak atau segala sesuatu yang merugikan sehingga mengancam kerahasiaan (*confidentialty),* integritas (*integrity),* dan ketersediaan (*Availibility)* sistem dan informasi. Ancaman siber dapat terjadi karena adanya kepentingan dari berbagai individu atau kelompok tertentu dalam aspek kehidupan masyarakat dapat menimbulkan berbagai ancaman fisik, baik nyata maupun yang tidak nyata dengan menggunakan kode-kode komputer (*software)* untuk melakukan pencurian informasi (*information theft),* kerusakan sistem (*system destruction),* manipulasi informasi (*information corruption),* atau perangkat keras (*hardware)* untuk melakukan gangguan terhadap sistem (*network intrction)* ataupun penyebaran data dan informasi tertentu untuk melakuakn kegiatan propaganda.[8]

Kejahatan siber adalah setiap kegiatan criminal yang dilakukan menggunakan komputer, jaringan komputer atau internet. Hal ini berarti menggunakan teknologi untuk melakukan aktivitas ilegal, jaringan komputer, atau internet. Kejahatan siber seringkali merupakan kejahatan klasik (misalnya penipuan, pencrian identitas, pornografi anak), meskipun dilakukan dengan cepat dan terhadap sejumlah besar calon korban, seperti penggunaan yang tidak sah, kerusakan, dan gangguan sistem komputer.

Jenis kejahatan siber diantaranya :

1. Rekayasa sosial dan tipu daya (*social engineering and trickery),* yang melibatkan penerapan metode curang untuk memaksa individu agar berperilaku dengan cara tertentu atau melakukan beberapa tugas.
2. Pelecehan daring serupa dengan jenis yang lain dan menjelaskan contoh dimana orang yang daring merasa terganggu/dilecehkan dan disiksa oleh orang lain.

[7] Muhammad Anthony Aldrino and Mas Agus Priyambodo, 2022, *Cyber Crime Dalam Sudut Pandang Hukum Pidana, Jurnal Kewarganegaraan,* Vol. 6 No. 1, Sekolah Tinggi Ilmu Hukum IBLAM, Jakarta Pusat, hlm. 2171.

[8] Ineu Rahmawati, 2017, *Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense,* Jurnal Pertahanan dan Bela Negara, Vol. 7 No. 2, Alumni Universitas Pertanahan Indonesia, Yogyakarta, hlm. 54-56.

DOI: https://doi.org/10.62017/syariah

3. Kejahatan terkait identitas adalah kejahatan yang dilakukan oleh seorang individu identitasnya dicuri atau disalahgunakan oleh orang lain untuk hal yang jahat atau tidak sah tujuan tertentu seperti penipuan.
4. Kejahatan peretasan, adalah kegiatan dimana seseorang mengekploitasi kelemahan dan kerentanan dalam suatu sistem untuk keuntungan atau kepuasan dirinya sendiri.
5. Penolakan mengakomodasi informasi merupakan tren baru *ransomware* yang serupa dengan menolak akases individu ke informasi mereka sendiri.[9]

Seiring dengan lajunya perkembangan zaman, teknologi yang semakin berkembang dan digunakan oleh berbagai kalangan baik anak muda, orang tua dan sebagainya. Berkembangnya zaman semakin meningkat pula kejahatan siber apalagi mengenai pencurian data dan informasi pribadi seseorang. Penyalahgunaan data pribadi tanpa disadari dapat terjadi karena merupakan kelalaian dari calon korban (masyarakat) itu sendiri dalam melaksanakan kegiatan sehari-hari.

Data pribadi ini disebutkan dalam Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, mendefinisikan bahwa dara pribadi sebagai data perseorangan tertentu yang disimpan dan dijaga kebenaran serta dilindungi kerahasiaannya.[10]

Salah satu dampak negatif dari kemajuan teknologi adalah kejahatan pencurian data. Pencurian data pribadi merupakan kejahatan yang sangat berbahaya dimana kejahatan ini merupakan awal dari kejahatan lainnya didalam dunia *cyber.* Kejahatan *cyber* juga merupakan sebuah kejahatan yang susah diungkap dikarenakan media digital bersifat global atau luas. Pengaturan data pribadi dalam sistem perundang-undangan di Indonesia diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang ITE dan Peraturan Menteri Komunikasi dan Informasi Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sitem Elektronik (PDSE).[11]

Faktor yang melatarbelakangi adanya kejahatan pencurian data dan informasi pribadi terjadi karena beberapa sebab, diantaranya yaitu sebagai berikut :

a. *Human error,* fitrah manusia yang hobi mempraktekkan kebiasaan ekonomis diantaranya dengan mencari *free software* atau aplikasi bajakan (yang biasanya memberikan iming-iming *free trial* atau bonus-bonus lainnya) memaksa penggunanya untuk secara suka rela memasukkan data pribadi berupa nomor telepon di situs atau aplikasi yang tidak terjamin keamanannya.
b. Serangan *malware,* manusia lalai dan tidak teliti dalam menerima maupun mengirim email, yang berpotensi menjadi pintu masuk *malware. Malware* pada dasarnya adalah program yang dirancang untuk merusak dengan menyusup ke sistem komputer, salah satu jenis *malware* yang berbahaya yaitu *spyware.* Menurut salah satu vendor antivirus yang sudah mendunia Karsperky, *spyware* merupakan *software* yang didesain untuk masuk ke dalam perangkat komputer yang mempunyai kemampuan mengumpulkan data-data pribadi user dan mengirimnya kepada pihak ketiga tanpa persetujuan user.
c. *Social engineering,* yaitu penggunaan manipulasi psikologis untuk mengumpulkan data sensitive seperti nama lengkap, *username, password,* dan sebagainya melalui media elektronik dengan menyamar sebagai pihak yang dapat dipercaya. Biasanya *phishing* memanfaatkan email untuk mengelabui korbannya. Email yang dikirimkan pelaku dapat berisi sesuatu yang mengatasnamakan pihak tertentu dan memancing korban untuk meng-klik tautan yang tercantum didalamnya.[12]

Pencurian data pribadi terbagi menjadi 5 (lima) kategori yaitu sebagai berikut :

[9] Russel Butarbutar, 2023, *Kejahatan Siber Terhadap Individu : Jenis, Analisis Dan Perkembangannya,* Jurnal Teknologi dan Ekonomi, Vol. 2 No. 2, Universitas Bung Karno, Jakarta Pusat, hlm. 302-303.

[10] Sahat Maruli Tua Situmeang, 2021, Peny*alahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber,* Jurnal SASI, Vol. 27 No. 1, Fakultas Hukum, Universitas Komputer, Bandung, hlm. 41.

[11] Muhammad Triadi, Sumiadi, and Yusrizal, 2023, *Perlindungan Tehadap Korban Pencurian Data Pribadi Melalui Media Digital,* Jurnal Ilmu Hukum Reusam, Vol. 11 No. 1, Fakultas Hukum, Universitas Malikussaleh, Aceh Utara, hlm. 1.

[12] https://www.djkn.kemenkeu.go.id/artikel/baca/14838/Belajar-Dari-Kebocoran-Data-Kredensial-Data-Yang-Paling-Berharga-adalah-Data-Pribadi.html#:~:text=Dari%20beberapa%20literatur%2C%20penulis%20mengelompokkan,manipulasi%20psikologis%20melalui%20social%20engineering, diakses Pada Jumat 22 November 2024 Pukul 21.00.

DOI: https://doi.org/10.62017/syariah

1) *Businnes/Commercial Identity Theft*, tipe ini menggunakan nama bisnis dari orang lain untuk mengambil kredit. Pelaku jenis ini menggunakan metode *pretexting* dalam menjalankan aksinya yakni menggunakan identitas atau dengan alasan palsu untuk memperoleh informasi dari korban.
2) *Criminal Identity Theft,* tipe ini beraksi sebagai orang lain ketika akan melakukan tindakan kejahatan.
3) *Financial Identity Theft,* tipe ini menggunakan identitas orang lain untuk memperoleh kredit, barang serta layanan yang dimiliki oleh orang tersebut. Pelaku jenis ini menggunakan metode *skimming.*
4) *Identity Clonning,* tipe ini menggunakan identitas serta informasi yang dimiliki orang lain dalam kehidupannya sehari-hari. Pelaku jenis ini biasanya menggunakan metode *system exploit* jenis *password cracking,* yakni melakukan tindakan penebakan password degan berbagai metode, yang paling banyak dilakukandengan metode *bruteforce* atau menebak dengan menggunakan daftar kata.
5) *Medical Identity Theft,* tipe ini menggunakan identintas orang lain untuk memperoleh layanan kesehatan dan obat-obatan. Pelaku jenis ini menggunakan metode hamper sama dengan jenis nomor 4 yakni mencuri identitas pribadi seseorang untuk kepentingan mendapatka layanan kesehatan dan obat-obatan denga memanfaatkan data pribadi korban.[13]

Dampak Pencurian Data dan Informasi Pribadi Terhadap Korban Kejahatan Siber di Indonesia.

Kebocoran data pribadi di era digital menjadi salah satu ancaman besar yang mengancam keamanan keuangan dan integritas informasi pribadi. Ancaman ini mencakup pencurian identitas dan informasi pribadi, yang dapat mencakup data seperti data Kesehatan, data biometric, data genetik, catatan kejahatan, dan data keuangan pribadi.

Pencurian identitas adalah masalah serius yang berdampak pada privasi dan keamanan data pribadi. Beberapa aspek yang terkait dengan pencurian identitas dan privasi data pribadi mencakup kesulitan dalam pendeteksian dan penanganannya, kerentanan dalam keamanan data di organisasi, platform online atau aplikasi, kurangnya kesadaran dan pemahaman akan risiko pencurian identitas dalam penggunaan teknologi digital, serangan yang cepat dan melibatkan banyak korban, serta tantangan hukum dan penegakan hukum terkait pencurian identitas di era digital. Terlebih lagi, di era digital, privasi menjadi semakin kompleks dengan penggunaan media social, analisis data, dan praktik pengumpulan data yang meluas, yang dapat mengorbankan privasi individu dan meningkatkan risiko penyalahgunaan identitas.

Perlindungan terhadap data pribadi menjadi isu yang sangat penting, terutama mengingat insiden kebocoran data nasabah yang sering terjadi karena kelalaian dan kurangnya pemahaman Masyarakat terhadap risiko keamanan data. Untuk menghindari pencurian identitas, seseorang harus berhati-hati dalam membagikan informasi pribadi mereka secara online, menggunakan kata sandi yang kuat, dan terus memonitor laporan kredit mereka untuk mendeteksi aktivitas yang mencurigakan. Di Indonesia, pemerintah telah mengesahkan Undang-Undang Perlindungan Data Pribadi sebagai landasan hukum untuk melindungi data pribadi dan memastikan keamanan informasi pribadi warga negara.

Pencurian identitas memiliki potensi dampak serius pada keuangan individu yang menjadi korban. Salah satu konsekuensinya adalah penipuan keuangan, dimana pelaku pencurian identitas dapat memanfaatkan informasi pribadi yang mereka curi unruk mencuri uang melalui tindakan penipuan dalam ranah finansial. Selain itu, korban pencurian identitas juga dapat menghadapi pembobolan rekening bank yang tidak sah. Ada juga risiko kerugiam finansial tambahan yang dapat timbul, seperti biaya yang harus dikeluarkan untuk memperbaiki catatan

[13] Mia Puspita Sari, Damrah Mamang, and Moh Zakky, 2021, *Penegakkan Hukum Terhadap Tindak Pidana Pencurian Data Pribadi Melalui Internet Ditinjau Dari UU Nomor 19 Tahun 2016 Tentang Perubahan Atas UU No 11 Tahun 2008 Tentang ITE (Informasi Dan Transaksi Elektronik),* Jurnal Jurisdictie, Vol. 3 No. 2, Program Sarjana Ilmu Hukum, Universitas Islam As-Syafi'iyah, Bekasi, hlm. 6-7.

DOI: https://doi.org/10.62017/syariah

kredit yang terpengaruh dan dampak negatif pada reputasi pribadi, yang pada akhirnya dapat mempengaruhi aspek finansial dan pribadi korban.

Pencurian identitas memiliki potensi untuk merusak catatan kredit seseorang jika pelaku menggunakan informasi tersebut untuk melakukan tindakan seperti membuka akun baru atau melakukan transaksi kredit yang merugikan korban. Selain itu, pencurian identitas juga dapat berdampak pada keuangan korban, termasuk kemungkinan pembobolan rekening bank dan kerugian finansial lainnya.[14]

Korban pencurian identitas sering mengalami tekanan psikologis dan dampak emosional negatif lainnya, termasuk kecemasan dan keraguan terhadap keamanan informasi pribadi mereka. Pencurian identitas dapat mengakibatkan kerusakan emosional yang substansial pada korban, seperti perasaan takut, kemarahan, serta hilangnya kepercayaan terhadap individu lain. Korban juga mungkin menghadapi kesulitan dalam memulihkan reputasi mereka setelah mengalami pencurian identitas.

Penyalahgunaan data pribadi dalam skala besar juga dapat mengancam keamanan nasional. Informasi sensitif yang jatuh ke tangan yang salah dapat digunakan untuk tujuan spionase, sabotase, atau serangan siber terhadap infrastruktur kritis.[15]

Dengan adanya penyalahgunaan data pribadi, maka dapat terlihat adanya kelemahan sistem, kurangnya pengawasan, sehingga data pribadi dapat disalahgunakan dan mengakibatkan kerugian bagi pemilik data tersebut. Penyalahgunaan, pencurian, penjualan data pribadi merupakan suatu pelanggaran hukum dalam bidang teknologi informasi dan juga dapat dikategorikan sebagai pelanggaran atas hak asasi manusia, karena data pribadi merupakan bagian dari hak asasi manusia yang harus dilindungi.[16]

Upaya Pemerintah Dalam Melakukan Perlindungan Hukum Bagi Korban Pencurian Data dan Informasi Pribadi di Era Kejahatan Siber.

Pencurian data dan informasi pribadi adalah kejahatan yang sangat serius, yang sering kali menjadi pemicu bagi kejahatan lain di media digital. Kejahatan siber ini sulit untuk diungkap karena sifat media digital yang berskala global. Akibatnya, banyak korban mengalami kesulitan dalam melaporkan kejadian tersebut dan mendapatkan kembali hak-hak mereka. Kerugian yang dialami oleh korban tidak hanya berupa uang atau harta, tetapi juga mencakup pelanggaran terhadap privasi.

Pencurian data dan informasi pribadi di Indonesia masih dianggap sebagai masalah yang kurang mendapat perhatian serius. Hal ini disebabkan oleh belum jelasnya beberapa peraturan perundang-undangan yang mengaturnya, serta sikap masyarakat yang cenderung meremehkan dan tidak menganggap serius ancaman kejahatan tersebut. Padahal, kasus pencurian data dan informasi pribadi sering kali terjadi di Indonesia.

Kewajiban Pemerintah Negara Indonesia dalam memberikan perlindungan data pribadi didasarkan pada ketentuan pada Pasal 28G ayat (1) UUD NRI Tahun 1945 menyebut bahwa:

"Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, harta benda yang di bawah kekuasaannya serta berhak atas rasa aman serta berhak atas perlindungan dari ancaman rasa ketakutan untuk berbuat sesuatu atau tidak berbuat sesuatu yang merupakan hak asasi."

Meskipun tidak secara langsung menyebutkan tentang privasi dan perlindungan data pribadi, ketentuan tersebut secara implisit menunjukkan bahwa perlindungan terhadap hak pribadi adalah bagian dari tujuan negara yang harus diwujudkan oleh Indonesia. Hal ini mencakup

[14] Putri Nurhaliza, 2023, *Pengaruh Pencurian Identitas Terhadap Keamanan Keuangan dan Data Pribadi*, Thesis: Sekolah Tinggi Ilmu Hukum IBLAM, Jakarta.

[15] Muhammad Fadli, Dijan Widijowati, dan Dewi Andayani, 2024, *Pencurian Data Pribadi di Dunia Maya (Phising Cybercrime) yang ditinjau dalam Perspektif Kriminologi,* Jurnal Ekonomi, Koperasi dan Kewirausahaan, Vol. 14 No. 12, Universitas Bhayangkara, Jakarta.

[16] Sahat Maruli Tua, 2021, *Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber,* Jurnal SASI Vol. 27 No. 1, Fakultas Hukum Universitas Komputer, Bandung, Jawa Barat.

DOI: https://doi.org/10.62017/syariah

perlindungan hak individu dalam masyarakat terkait dengan pengumpulan, pengolahan, pengelolaan, dan penyebaran data pribadi.[17]

Perlindungan data pribadi di Indonesia saat ini telah diatur dalam beberapa peraturan perundang-undangan seperti halnya : Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia, Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 24 Tahun 2013 Tentang Administrasi Kependudukan, Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan, Undang-Undang Nomor 36 Tahun 2009 Tentang Kesehatan, Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik, dan Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi. Namun, dari peraturan yang telah berlaku, masih belum ada pengaturan yang lebih spesifik dan komprehensif mengatur tentang perlindungan data pribadi.[18]

Penyelenggara sistem elektronik diatur oleh seperangkat peraturan perundang-undangan. Diantaranya adalah UU No. 11 Tahun 2008, UU juncto UU 19 Tahun 2016, dan peraturan pelaksanaan lainnya. Misalnya saja Peraturan Pemerintah No. 71 Tahun 2019 mengatur tentang penyelenggaraan sistem dan transaksi elektronik, dan Peraturan Menteri PDP Nomor 20 Tahun 2016 mengatur tentang perlindungan data pribadi. Penyelenggara sistem elektronik diwajibkan oleh UU ITE untuk mengambil tindakan pencegahan terhadap potensi ancaman dan menghapus data atau dokumen yang tidak perlu yang disimpan secara elektronik.[19]

Dalam upaya melindungi data dan informasi pribadi setiap masyarakat oleh pemerintah untuk mencegah pencurian identitas dan penipuan di dunia cyber. Di Indonesia, aturan perlindungan data pribadi diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Sanksi administratif dapat dikenakan atas pelanggaran perlindungan data pribadi, seperti pemberitahuan tertulis kepada lembaga pemerintah yang lalai melindungi informasi pribadi. Pemerintah juga dapat memerintahkan pelanggar untuk mengungkapkan pelanggaran kepada publik atau pihak terkait. Gugatan perdata terhadap pemerintah dapat diajukan jika terjadi kelalaian dalam melindungi informasi pribadi, dan jika gugatan tersebut dimenangkan, pengadilan dapat memerintahkan pemerintah untuk membayar ganti rugi atau tindakan lain yang diperlukan.

Penyelesaian masalah perlindungan data pribadi dilakukan melalui beberapa cara yaitu "arbitrase, pengadilan, atau lembaga penyelesaian sengketa alternatif sesuai dengan ketentuan peraturan perundangan-undangan dengan alat bukti sah undang-undang yang meliputi alat bukti sebagaimana yang ada dalam hukum acara dan alat bukti lain berupa informasi elektronik, dokumen elektronik sesuai dengan peraturan perundang-undangan". UU PDP memiliki empat jenis pelanggaran yang tertulis pada Pasal 67, Pasal 68, dan Pasal 70. Pada Pasal 67 yang menyebutkan "dengan memperoleh data pribadi yang bukan miliknya untuk menguntungkan diri sendiri dan dapat merugikan subjek data pribadi serta setiap orang yang sengaja dan melawan hukum menggunakan data pribadi yang bukan miliknya, akan dipidana penjara lima tahun dan pidana denda paling banyak 5 miliar, dan jenis pelanggaran dengan menggunakan data pribadi yang bukan miliknya akan dikenai penjara paling lama empat tahun dengan denda pidana 4 miliar." Pada Pasal 68 UU PDP yang menyebutkan "setiap orang yang sengaja membuat data pribadi palsu atau memalsukan data pribadi untuk menguntungkan diri sendiri maka akan dikenakan denda penjara paling lama enam tahun dan denda pidana sebanyak 6 miliar. Sedangkan dalam Pasal 70 terkhusus untuk korporasi yang mana dimaksud dalam Pasal 67 dan

[17] A A Ngurah Oka, Yudistira Darmadi, dan Nyoman Satyayudha Dananjaya, 2023, *PERLINDUNGAN HUKUM TERHADAP KORBAN KEBOCORAN DATA PRIBADI (STUDI KASUS DI KOTA DENPASAR),* Jurnal Kertha Semaya, Vol. 11, No. 5, Fakultas Hukum Universitas Udayana, Denpasar Bali.

[18] Ni Made Dwi Gayatri Putri, Ni Luh Made Mahendrawati, dan Ni Made Puspasutari Ujianti, 2024, *Perlindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022,* Jurnal Preferensi Hukum, Vol. 5, No. 2, Fakultas Hukum Universitas Warmadewa, Denpasar Bali, hlm. 2

[19] Galang Surya Mahendra, 2024*, Perlindungan Hukum Terhadap Korban Yang Data Pribadi Passportnya Tersebar Akibat Kelalaian Pemerintah*, Terang : Jurnal Kajian Ilmu Sosial, Politik dan Hukum, Vol. 1, No. 3, Ilmu Hukum, Universitas 17 Agustus 1945 Surabaya.

DOI: https://doi.org/10.62017/syariah

68 jika korporasi melakukan pelanggaran maka hukum akan dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat dan/atau korporasi dengan pidana banyak 10 kali dari maksimal denda yang diancamkan, yang mana pidana korporasi hanya dijatuhkan pidana denda seperti perampasan keuntungan, pembekuan usaha korporasi, pembayaran ganti rugi, pencabutan izin, penutupan korporasi dan pembubaran korporasi."

Upaya perlindungan preventif (pencegahan) untuk melindungi data pribadi dapat dilakukan dengan cara menghindari "sharing data" secara sembarangan serta menghindari penggunaan platform yang tidak sah, karena aplikasi ilegal dapat berisiko menimbulkan tindak kejahatan siber. Selain itu, kesadaran masyarakat dalam menjaga data pribadi sangat penting. Sementara itu, pemerintah akan melakukan uji kepatuhan "compliance" untuk memastikan kesesuaian antara peraturan Undang-Undang dan kewajiban yang harus dipenuhi oleh Sistem Elektronik. Upaya perlindungan represif (pemaksaan) diterapkan jika terjadi kebocoran data pribadi, dengan sanksi yang tercantum dalam Undang-Undang PDP, seperti yang diatur dalam Pasal 67 dan Pasal 68 yang mencakup hukuman denda dan pidana penjara. Selain itu, Pasal 70 mengatur sanksi bagi pelanggaran yang dilakukan oleh korporasi. Jika terjadi kebocoran data pribadi akibat ketidakpatuhan terhadap Undang-Undang PDP, sanksi yang diatur dalam Undang-Undang tersebut akan diberlakukan.[20]

KESIMPULAN

1. Faktor yang Melatarbelakangi Terjadinya Kejahatan Pencurian Data dan Informasi Pribadi di Indonesia Pencurian data dan informasi pribadi di Indonesia dipengaruhi oleh berbagai faktor, terutama perkembangan teknologi informasi dan komunikasi yang pesat. Dalam konteks ini, beberapa faktor kunci yang melatarbelakangi terjadinya kejahatan tersebut adalah:
   a. Perkembangan Teknologi Kemajuan teknologi, khususnya dalam penggunaan perangkat mobile dan internet, telah memudahkan individu untuk bertransaksi dan berbagi informasi secara online. Namun, hal ini juga membuka peluang bagi pelaku kejahatan untuk melakukan pencurian data.
   b. Human Error
      Banyak individu yang tidak berhati-hati dalam menjaga informasi pribadi mereka. Misalnya, penggunaan aplikasi bajakan atau perangkat lunak yang tidak terjamin keamanannya dapat menyebabkan pengguna secara tidak sadar memberikan data pribadi kepada pihak yang tidak bertanggung jawab.
   c. Serangan Malware
      Ketidakwaspadaan dalam menerima atau mengirim email dapat menjadi pintu masuk bagi malware yang dirancang untuk mencuri data pribadi. Spyware, sebagai salah satu jenis malware, dapat mengumpulkan informasi sensitif tanpa sepengetahuan pengguna.
   d. Social Engineering
      Metode manipulasi psikologis yang digunakan oleh pelaku untuk mendapatkan informasi sensitif. Phishing adalah contoh umum di mana pelaku menyamar sebagai pihak tepercaya untuk mengelabui korban agar memberikan data pribadi.
   e. Kurangnya Kesadaran
      Banyak orang yang tidak menyadari risiko yang terkait dengan penggunaan teknologi digital, sehingga mereka cenderung mengabaikan langkah-langkah keamanan yang diperlukan.
2. Dampak Pencurian Data dan Informasi Pribadi Terhadap Korban Kejahatan Siber di Indonesia Pencurian data pribadi dapat memberikan dampak yang signifikan bagi korban, baik secara finansial maupun psikologis. Beberapa dampak tersebut meliputi:

[20] Ni Made Dwi Gayatri Putri, Ni Luh Made Mahendrawati, dan Ni Made Puspasutari Ujianti, 2024, *Perlindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022,* Jurnal Preferensi Hukum, Vol. 5, No. 2, Fakultas Hukum Universitas Warmadewa, Denpasar Bali, hlm. 4

DOI: https://doi.org/10.62017/syariah

a. Kerugian Finansial
   Korban dapat mengalami penipuan keuangan, pembobolan rekening bank, dan kerugian terkait lainnya. Biaya untuk memperbaiki catatan kredit yang terpengaruh juga dapat menjadi beban tambahan.
b. Kerusakan Reputasi
   Pencurian identitas dapat merusak reputasi individu, yang dapat mempengaruhi kehidupan pribadi dan profesional mereka.
c. Dampak Emosional
   Korban sering kali mengalami kecemasan, ketidakpercayaan, dan stres akibat pelanggaran privasi yang mereka alami. Perasaan takut dan kemarahan juga dapat muncul, serta kesulitan dalam memulihkan reputasi yang telah rusak.
d. Ancaman Keamanan Nasional
   Penyalahgunaan data pribadi dalam skala besar dapat berpotensi mengancam keamanan nasional, terutama jika informasi sensitif jatuh ke tangan yang salah.

3. Upaya Pemerintah Dalam Melakukan Perlindungan Hukum Bagi Korban Pencurian Data dan Informasi Pribadi di Era Kejahatan Siber Pemerintah Indonesia telah mengambil langkah-langkah untuk melindungi data pribadi warganya melalui berbagai peraturan dan undang-undang. Beberapa upaya tersebut meliputi:
   a. Peraturan Perundang-Undangan
      Pengaturan mengenai perlindungan data pribadi di Indonesia diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan peraturan terkait lainnya. UU PDP memberikan landasan hukum bagi individu untuk melindungi data pribadi mereka dan menetapkan sanksi bagi pelanggaran.
   b. Pencegahan dan Penegakan Hukum
      Pemerintah melakukan uji kepatuhan untuk memastikan bahwa penyelenggara sistem elektronik mematuhi peraturan yang ada. Jika terjadi pelanggaran, sanksi administratif dan pidana dapat dikenakan kepada pelanggar.
   c. Kesadaran Masyarakat
      Pemerintah juga berupaya meningkatkan kesadaran masyarakat mengenai pentingnya menjaga data pribadi dan risiko yang terkait dengan penggunaan teknologi.
   d. Sistem Penyelesaian Sengketa
      UU PDP menyediakan mekanisme penyelesaian sengketa, termasuk arbitrase dan pengadilan, untuk menangani pelanggaran terhadap perlindungan data pribadi. Dengan langkah-langkah tersebut, diharapkan perlindungan data pribadi di Indonesia dapat ditingkatkan, serta korban pencurian data dapat memperoleh keadilan dan perlindungan yang layak.

DAFTAR PUSTAKA

Alhakim and Sofia, 2021, *Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia,* Jurnal Komunitas Yustisia, Vol. 4 No. 2, Fakultas Hukum, Universitas Internasional Batam, Batam.

Alhakim, 2022, *Urgensi Perlindungan Hukum Terhadap Jurnalis Dari Risiko Kriminalisasi UU Informasi Dan Transaksi Elektronik Di Indonesia*, Jurnal Pembangunan Hukum Indonesia, Vol. 4 No. 1, Fakultas Hukum, Universitas Internasional Batam, Batam.

A A Ngurah Oka, Yudistira Darmadi, dan Nyoman Satyayudha Dananjaya, 2023, *PERLINDUNGAN HUKUM TERHADAP KORBAN KEBOCORAN DATA PRIBADI (STUDI KASUS DI KOTA DENPASAR),* Jurnal Kertha Semaya, Vol. 11, No. 5, Fakultas Hukum Universitas Udayana, Denpasar Bali.

Disemadi, 2021, *Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia,* Jurnal Wawasan Yuridika, Vol. 5 No. 2, Fakultas Hukum, Universitas Internasional Batam, Batam, Indonesia.

Fiqqih Anugerah and Tantimin, 2022, *Pencurian Data Pribadi Di Internet Dalam Perspektif Kriminologi,* Jurnal Komunikasi Hukum, Vol. 8 No. 1, Fakultas Hukum, Universitas Internasional Batam, Indonesia.

Galang Surya Mahendra, 2024*, Perlindungan Hukum Terhadap Korban Yang Data Pribadi Passportnya Tersebar Akibat Kelalaian Pemerintah*, Terang : Jurnal Kajian Ilmu Sosial, Politik dan Hukum, Vol. 1, No. 3, Ilmu Hukum, Universitas 17 Agustus 1945 Surabaya.

Ineu Rahmawati, 2017, *Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense,* Jurnal Pertahanan dan Bela Negara, Vol. 7 No. 2, Alumni Universitas Pertanahan Indonesia, Yogyakarta.

Miftakhur Rokhman, 2020, *Kejahatan Teknologi Informasi (Cyberr Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia,* Jurnal Al-Qanun : Jurnal Pemikiran dan Pembaharua Hukum Islam, Vol. 23 No. 2, UIN Sunan Ampel, Surabaya.

Mia Puspita Sari, Damrah Mamang, and Moh Zakky, 2021, *Penegakkan Hukum Terhadap Tindak Pidana Pencurian Data Pribadi Melalui Internet Ditinjau Dari UU Nomor 19 Tahun 2016 Tentang Perubahan Atas UU No 11 Tahun 2008 Tentang ITE (Informasi Dan Transaksi Elektronik),* Jurnal Jurisdictie, Vol. 3 No. 2, Program Sarjana Ilmu Hukum, Universitas Islam As-Syafi'iyah, Bekasi.

Muhammad Anthony Aldrino and Mas Agus Priyambodo, 2022, *Cyber Crime Dalam Sudut Pandang Hukum Pidana, Jurnal Kewarganegaraan,* Vol. 6 No. 1, Sekolah Tinggi Ilmu Hukum IBLAM, Jakarta Pusat.

Muhammad Triadi, Sumiadi, and Yusrizal, 2023, *Perlindungan Tehadap Korban Pencurian Data Pribadi Melalui Media Digital,* Jurnal Ilmu Hukum Reusam, Vol. 11 No. 1, Fakultas Hukum, Universitas Malikussaleh, Aceh Utara.

Muhammad Fadli, Dijan Widijowati, dan Dewi Andayani, 2024, *Pencurian Data Pribadi di Dunia Maya (Phising Cybercrime) yang ditinjau dalam Perspektif Kriminologi,* Jurnal Ekonomi, Koperasi dan Kewirausahaan, Vol. 14 No. 12, Universitas Bhayangkara, Jakarta.

Ni Made Dwi Gayatri Putri, Ni Luh Made Mahendrawati, dan Ni Made Puspasutari Ujianti, 2024, *Perlindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022,* Jurnal Preferensi Hukum, Vol. 5, No. 2, Fakultas Hukum Universitas Warmadewa, Denpasar, Bali.

Putri Nurhaliza, 2023, *Pengaruh Pencurian Identitas Terhadap Keamanan Keuangan dan Data Pribadi*, Thesis: Sekolah Tinggi Ilmu Hukum IBLAM, Jakarta.

Russel Butarbutar, 2023, *Kejahatan Siber Terhadap Individu : Jenis, Analisis Dan Perkembangannya,* Jurnal Teknologi dan Ekonomi, Vol. 2 No. 2, Universitas Bung Karno, Jakarta Pusat.

Sahat Maruli Tua Situmeang, 2021, Peny*alahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber,* Jurnal SASI, Vol. 27 No. 1, Fakultas Hukum, Universitas Komputer, Bandung.

Direktorat Jendral Keuangan Negara, 2024, *Belajar Dari Kebocoran Data Kredensial : Data yang Paling Berharga adalah Data Pribadi,* https://www.djkn.kemenkeu.go.id/artikel/baca/14838/Belajar-Dari-Kebocoran-Data-Kredensial-Data-Yang-Paling-Berharga-adalah-Data-Pribadi.html#:~:text=Dari%20beberapa%20literatur%2C%20penulis%20mengelompokkan,manipulasi%20psikologis%20melalui%20social%20engineering, diakses Pada Jumat 22 November 2024 Pukul 21.00.