JURNAL MEDIA AKADEMIK (JMA)
Vol.3, No.2 Februari 2025
e-ISSN: 3031-5220; DOI: 10.62281, Hal XX-XX
PT. Media Akademik Publisher
AHU-084213.AH.01.30.Tahun 2023

ANALISIS KRIMINOLOGI DALAM TINDAK PIDANA PENCURIAN DATA PRIBDADI DI ERA DIGITAL

Oleh:

Komang Maysa Surya Aditya[1]
I Gusti Ngurah Nyoman Krisnadi Yudiantara[2]

Universitas Udayana
Alamat: JL. Pulau Bali No.1, Dauh Puri Klod, Kec. Denpasar Bar., Kota Denpasar, Bali (80114).
Korespondensi Penulis: Maysasurya12@gmail.com

Abstract. *Personal data theft has become a significant threat in today's digital era. This research aims to analyze the phenomenon of personal data theft from a criminological perspective in the context of the digital era. A criminological approach is used to understand the perpetrator's motivation, the modus operandi used, and the impact experienced by the victim. The research method used for analysis is qualitative by exploring data from primary and secondary sources that are relevant to the research topic. The research results show that the motivations of perpetrators of personal data theft in the digital era are very diverse, including financial goals, malicious intent, or the desire to damage the reputation of an individual or organization. Common modus operandi used include phishing attacks, malware, or identity theft. The impacts experienced by victims include financial losses, reputational losses, or even psychological losses. Criminological analysis of personal data theft in the digital era has important strengths in efforts to prevent and control cyber crime. Prevention efforts must include public education and awareness about the risks of personal data theft, improving cyber security, as well as implementing laws capable of protecting individuals and organizations from cybercrime attacks.*

Keywords: *Personal Data Theft, Digital Era, Criminology, Motivation, Modus Operandi, Impact.*

Received January 29, 2025; Revised February 11, 2025; February 17, 2025
*Corresponding author: *Maysasurya12@gmail.com*

ANALISIS KRIMINOLOGI DALAM TINDAK PIDANA PENCURIAN DATA PRIBDADI DI ERA DIGITAL

Abstrak. Pencurian data pribadi telah menjadi ancaman yang signifikan dalam era digital saat ini. Penelitian ini bertujuan untuk menganalisis fenomena pencurian data pribadi dari perspektif kriminologi dalam konteks era digital. Pendekatan kriminologi digunakan untuk memahami motivasi pelaku, modus operandi yang digunakan, serta dampak yang dialami oleh korban. Metode penelitian yang digunakan adalah analisis kualitatif dengan menggali data dari sumber primer dan sekunder yang relevan dengan topik penelitian. Hasil penelitian menunjukkan bahwa motivasi pelaku pencurian data pribadi dalam era digital sangat beragam, termasuk tujuan finansial, niat jahat, atau keinginan untuk merusak reputasi individu atau organisasi. Modus operandi yang umum digunakan meliputi serangan phishing, malware, atau pencurian identitas. Dampak yang dialami oleh korban mencakup kerugian finansial, kerugian reputasi, atau bahkan kerugian psikologis. Analisis kriminologi terhadap pencurian data pribadi dalam era digital memiliki implikasi penting dalam upaya pencegahan dan penanggulangan kejahatan siber. Upaya pencegahan harus mencakup pendidikan dan kesadaran publik tentang risiko pencurian data pribadi, peningkatan keamanan siber, serta pelaksanaan undang-undang yang memadai untuk melindungi individu dan organisasi dariserangan kejahatan siber.
Kata Kunci: Pencurian Data Pribadi, Era Digital, Kriminologi, Motivasi, Modus Operandi, Dampak.

LATAR BELAKANG

Dengan kemajuan teknologi informasi, masyarakat Indonesia kini memudahkan memperoleh informasi yang kita butuhkan. Hal ini membuat teknologi informasi menjadi bagian penting dalam kehidupan sehari-hari, mempermudah akses informasi secara cepat. Perkembangan teknologi dan informasi juga membawa perubahan dalam berbagai aspek kehidupan, seperti sosial, budaya, ekonomi, keamanan, dan penegakan hukum. Dengan adanya media dan komunikasi elektronik, kendala waktu dan jarak tidak lagi menjadi halangan, baik bagi individu maupun pemerintah. Orang bisa berkomunikasi tanpa perlu bertemu langsung, perusahaan dapat mengembangkan bisnisnya ke seluruh dunia melalui pemasaran di Internet dan komputer, serta pemerintah dapat menjalankan berbagai kegiatan administrasi menggunakan Internet dan komputer. Sebagai contoh, hubungan

diplomatik antar negara dapat dilakukan tanpa harus melakukan perjalanan fisik ke negara tersebut. [1]

Kemajuan teknologi informasi dianggap sebagai faktor yang dapat mempengaruhi kehidupan individu. Hal ini menyebabkan masyarakat Indonesia cenderung semakin bergantung pada teknologi informasi, yang juga meningkatkan potensi terjadinya tindak kejahatan. Teknologi informasi memiliki kemampuan untuk memperbaiki pola pikir masyarakat, namun di sisi lain, juga dapat disalahgunakan sebagai sarana untuk melakukan tindakan kriminal, yang dikenal dengan istilah "kejahatan dunia maya" atau "*cybercrime*". *Cybercrime* ialah merujuk kepada kejahatan atau tindakan ilegal yang dilakukan melalui jaringan elektronik global. Kejahatan di dunia maya semakin mengancam karena dampaknya yang luas. Kejahatan siber berhubungan dengan ruang digital yang dapat merusak privasi individu. Secara umum, kejahatan di dunia maya semakin meningkat, dengan karakteristik pelaku yang semakin beragam. Berkat kemajuan teknologi informasi, pelaku kejahatan dapat dengan mudah melakukan tindakan kriminal. Beberapa contoh kejahatan tersebut antara lain pornografi, perjudian online, terorisme, peretasan, judi kartu, skimming ATM/EDC, penipuan, dan masih banyak lagi.[2]

Pencurian data di dunia maya dikenal sebagai phishing, yaitu tindakan ilegal dimana bertujuan untuk memperoleh informasi yang bersifat pribadi atau data yang bersifat sensitif seseorang. Dalam aksi ini, pelaku berusaha mendapatkan data seperti nomor kartu kredit, PIN, ID pengguna, nomor telepon, nomor rekening, serta informasi pribadi lainnya. Setelah mendapatkan data tersebut, pelaku memanfaatkannya untuk merugikan korban melalui penipuan dan tindakan kriminal lainnya. Ancaman terhadap eksploitasi data pribadi di Indonesia semakin meningkat setelah pemerintah memperkenalkan kebijakan Kartu Tanda Penduduk Elektronik (e-KTP), yang bertujuan untuk mengumpulkan data kependudukan. Sejak kebijakan ini diterapkan pada tahun 2011, setiap individu diwajibkan memiliki kartu identitas yang memuat Nomor Induk

---

1. Disemadi, H. S. (2021). Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia. *Jurnal Wawasan Yuridika*,5(2), 177-199.
2. Afnesia, U., & Ayunda, R. (2022). Perlindungan Data Diri Peminjam Dalam Transaksi Pinjaman Online: Kajian Perspektif Perlindungan Konsumen Di Indonesia. *Jurnal Komunitas Yustisia*,4(3), 1035-1044

Kependudukan (NIK), yang berlaku seumur hidup.[3] Semua informasi pribadi penduduk, termasuk ciri-ciri fisik dan identitas lainnya, tercatat dalam e-KTP. Hal ini membuat data dalam e-KTP rentan terhadap penyalahgunaan jika tidak ada sistem keamanan dan perlindungan data yang memadai. Kasus kebocoran data pribadi sering terjadi di Indonesia, dan dalam sektor perbankan, pertukaran data pribadi melibatkan informasi nasabah yang dikirim antara pusat data kartu, pihak ketiga, serta transaksi antar bank atau yang melibatkan pemegang kartu kredit.

Proses ini bisa dilakukan melalui sistem terbuka atau melibatkan pihak ketiga, baik individu maupun perusahaan yang mengelola dan menukar informasi pribadi nasabah. Mengingat banyaknya kasus pencurian data yang terjadi, pemerintah harus mengambil langkah antisipasi untuk mengurangi kejadian ini, dengan menerapkan perlindungan hukum yang tegas terhadap pencurian data. Kejadian tersebut dapat menyebabkan kerugian baik material maupun immaterial bagi korban. Pencurian data pribadi tidak hanya berpengaruh pada individu, tetapi juga dapat memengaruhi perusahaan yang mengelola sistem elektronik serta lembaga keuangan yang terlibat dalam transaksi pembayaran. Dengan demikian, dampak dari pencurian data ini bisa meluas, melibatkan komunitas dan masyarakat Indonesia secara keseluruhan. Namun, di Indonesia, perlindungan data pribadi belum diatur secara rinci dalam perundang-undangan, sehingga peraturan yang ada masih bersifat parsial atau sektoral dan sering kali tumpang tindih. Beberapa undang-undang yang mengatur sistem elektronik, seperti Undang-Undang Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, hanya mencakup beberapa aspek perlindungan data pribadi secara umum. Artikel ini akan mengulas pentingnya perlindungan hukum terhadap kasus pencurian data pribadi serta berbagai faktor yang dapat menyebabkannya. Dengan diberlakukannya undang-undang perlindungan data pribadi yang baru, diharapkan regulasi di masa mendatang akan lebih tegas dan terperinci. [4]

3. Alhakim, A. (2022). Urgensi Perlindungan Hukum terhadap Jurnalis dari Risiko Kriminalisasi UU Informasi dan Transaksi Elektronik di Indonesia. *Jurnal Pembangunan Hukum Indonesia*,4(1), 89-106.
4. Disemadi, H. S., & Prasetyo, D. (2021). Tanda Tangan Elektronik pada Transaksi Jual Beli Online: Suatu Kajian Hukum Keamanan Data Konsumen di Indonesia. *Jurnal Wajah Hukum*, 5(1), 13-2

KAJIAN TEORITIS

Dalam tulisan ini, analisis terhadap tindak pidana pencurian data pribadi di era digital didasarkan pada teori penegakan hukum. Menurut Soerjono Soekanto, penegakan hukum merupakan upaya menyelaraskan hubungan antara nilai-nilai yang tertuang dalam aturan yang telah ditetapkan dengan perilaku masyarakat, sebagai bagian dari proses akhir dalam menjaga, menciptakan, dan mempertahankan ketertiban dalam kehidupan bermasyarakat. Berdasarkan pemahaman ini, penegakan hukum dalam kasus pencurian data pribadi dapat diartikan sebagai upaya untuk menyesuaikan nilai-nilai hukum dengan penerapan aturan yang mengatur perlindungan data pribadi. Hal ini mencakup langkah-langkah yang diambil oleh aparat penegak hukum untuk memastikan bahwa pelaku mendapatkan sanksi yang setimpal dengan perbuatannya. Dalam konteks kejahatan dunia maya, termasuk pencurian data pribadi, terdapat beberapa elemen penting yang harus diperhatikan, yaitu kepastian hukum, keadilan, dan kemanfaatan. Proses penegakan hukum tidak hanya bertujuan untuk memberikan sanksi, tetapi juga memastikan tercapainya keadilan substantif. Putusan pengadilan harus mencerminkan prinsip keadilan yang relevan dalam era digital, di mana perlindungan data pribadi menjadi krusial dalam masyarakat yang semakin bergantung pada teknologi informasi.[5]

Dalam kajian ini, penulis juga membandingkan dengan beberapa penelitian terdahulu yang membahas tentang pencurian data pribadi dan penerapan hukum dalam kejahatan dunia maya. Salah satu penelitian yang relevan adalah oleh Antonio B. Hernandez pada tahun 2022, yang fokus pada peran teknologi informasi dalam memperburuk tindak pidana pencurian data pribadi. Penelitian tersebut membahas bagaimana kemajuan teknologi, seperti perangkat lunak peretasan dan akses data secara daring, memperbesar potensi pencurian data.[6] Penelitian ini lebih menyoroti aspek teknis dan metode yang digunakan oleh pelaku kejahatan siber.Selain itu, penelitian oleh Michael T. Davis pada tahun 2023 mengangkat topik perlindungan hukum terhadap korban pencurian data pribadi. Penelitian tersebut lebih fokus pada hak-hak korban dan langkah-langkah hukum yang dapat diambil untuk melindungi data pribadi mereka. Meskipun penulisan ini juga mencakup perlindungan hukum bagi korban, penulis lebih

---

5. Soekanto, Soerjono**.** (2015). *Sosiologi Hukum: Suatu Pengantar*. Jakarta: RajaGrafindo Persada.
6. Hernandez, Antonio B. (2022). *The Role of Information Technology in the Escalation of Data Theft* Crimes. International Journal of Cybercrime Studies, 15(3), 220-237.

memfokuskan pada bagaimana hukum positif Indonesia mengatur tindak pidana pencurian data pribadi serta implementasinya dalam sistem peradilan pidana. Perbedaan dengan Penulisan Terdahulu Jika dibandingkan dengan penelitian-penelitian sebelumnya, penulisan jurnal ini berbeda dalam pendekatan dan analisis. Penelitian oleh Hernandez lebih berfokus pada aspek teknis dan kriminalitas siber, sementara Davis lebih membahas perlindungan hukum korban. Penulisan jurnal ini lebih mengarah pada analisis kriminologi terkait penegakan hukum dalam tindak pidana pencurian data pribadi. Penulis juga menyoroti bagaimana hukum positif Indonesia mengatur pencurian data pribadi dan peran teknologi dalam memperburuk tindak pidana ini, serta penerapan aturan tersebut dalam sistem peradilan pidana Indonesia, khususnya dalam konteks kasus-kasus pencurian data pribadi. [7]

Dalam penelitian ini, penulis mengangkat analisis kriminologi dalam tindak pidana pencurian data pribadi di era digital, dengan fokus pada penerapan hukum positif Indonesia dalam menangani kejahatan dunia maya ini. Penulis berusaha mengisi celah yang ada dalam penelitian terdahulu, dengan memberikan kajian lebih mendalam tentang proses penegakan hukum, faktor-faktor penyebab meningkatnya pencurian data pribadi, serta peran aparat penegak hukum dalam menanggulangi kejahatan digital yang merugikan masyarakat luas. Kajian ini akan sangat penting sebagai kontribusi terhadap pembaharuan hukum acara pidana di Indonesia yang lebih adaptif terhadap perkembangan teknologi dan kejahatan dunia maya.

METODE PENELITIAN

Penelitian ini tergolong dalam penelitian yuridis normatif dengan metode studi pustaka untuk mengumpulkan data sekunder. Pendekatan ini bertujuan menganalisis peraturan perundang-undangan dan doktrin hukum yang berkaitan dengan isu yang dibahas. Proses analisis mencakup telaah terhadap teori hukum, prinsip hukum, serta konsep hukum yang relevan, yang bersumber dari referensi hukum primer maupun sekunder. Penelitian hukum normatif bertujuan untuk memberikan pemahaman yang mendalam mengenai kerangka hukum yang mengatur suatu permasalahan atau fenomena

7. Davis, Michael T. (2023). *Legal Protection for Victims of Data Theft: A Global Perspective*. Journal of Cyber Law and Ethics, 20(4), 315-329.

hukum, serta menawarkan rekomendasi untuk pengembangan atau perbaikan regulasi yang sudah ada.

HASIL DAN PEMBAHASAN

Apa Saja Factor-Faktor Yang Dapat Memengaruhi Terjadinya Tindak Pidana Kejahatan Pencurian Data Pribadi Atau Kejahatan *Cybercrime* Di Era Digital Ini?

Kejahatan dan tindakan tercela merupakan pelanggaran terhadap hukum dan norma sosial yang tidak dapat diterima oleh masyarakat. Terjadinya kejahatan dipengaruhi oleh berbagai faktor, termasuk aspek ekonomi seperti keterbatasan lapangan kerja, faktor biologis yang mencakup aspek psikis dan fisik, serta faktor individu dan sosial yang berperan dalam mendorong perilaku kriminal. Kejahatan dan perilaku tidak terpuji merupakan pelanggaran hukum serta bertentangan dengan norma sosial, sehingga mendapat penolakan dari masyarakat. Tindakan kriminal memiliki dampak negatif yang signifikan terhadap kehidupan sosial di Indonesia, serta dapat menimbulkan rasa takut, cemas, khawatir, dan panik di kalangan warga negara.[8]

Seiring dengan meningkatnya kejahatan dan perkembangan dunia, terutama dalam ranah kejahatan siber, kekhawatiran terhadap efektivitas lembaga penegak hukum dalam memberantas kejahatan di internet semakin meningkat. Lembaga penegak hukum terus berupaya menghadapi tantangan ini. Di Indonesia, penegakan hukum terhadap kejahatan dunia maya sangat dipengaruhi oleh lima faktor utama yang saling berkaitan, yaitu hukum, budaya, kelembagaan, perilaku masyarakat, serta pola pikir aparat penegak hukum. Hukum tidak dapat ditegakkan secara terisolasi, karena selalu berkaitan dengan manusia dan tindakan mereka. Penegakan hukum membutuhkan motivasi dan dorongan yang kuat agar dapat berjalan efektif. Selain menerapkan hukum secara profesional dan konsisten, aparat penegak hukum juga harus menangani individu atau kelompok yang diduga terlibat dalam tindak kejahatan. Kejahatan yang berkaitan dengan teknologi informasi sering dikategorikan sebagai "kejahatan putih," karena pelakunya umumnya adalah individu yang memiliki pemahaman mendalam tentang aplikasi dan penggunaan internet. Karena sering dilakukan lintas batas negara, kejahatan dunia maya memenuhi dua kategori, yaitu kejahatan kerah putih dan kejahatan transnasional. Di Indonesia,

---

8. Ketaren, E. (2016). Cybercrime,(Cyber Space, dan Cyber Law. Jurnal Times,52), 35-42.

berbagai kasus kejahatan siber (*cybercrime*) kerap terjadi di tengah masyarakat. Beberapa di antaranya meliputi penipuan, perjudian online, penyebaran informasi hoaks, peretasan, serta pencurian data pribadi melalui internet. [9]

Keamanan komputer terus berkembang pesat seiring dengan meningkatnya pengaruh teknologi informasi dalam kehidupan masyarakat Indonesia, termasuk dalam bidang pekerjaan, komunikasi, dan transaksi belanja. Kemajuan ini juga membawa peningkatan ancaman terhadap keamanan komputer, baik dalam bentuk ancaman fisik maupun non-fisik, seperti kelemahan pada sistem operasi, serangan terhadap jaringan, dan penyebaran virus. Keamanan merupakan aspek krusial dalam pengembangan sistem jaringan berbasis internet. Tanpa perlindungan yang memadai, sistem menjadi rentan, layaknya rumah tanpa pengamanan yang memungkinkan pencuri masuk dan mengambil barang berharga. Dalam proses pembangunan sistem, sering kali ditemukan celah yang tampak sepele dan dianggap tidak berbahaya. Namun, celah keamanan kecil ini kerap luput dari perhatian dan dapat dimanfaatkan oleh pelaku kejahatan untuk melakukan tindakan kriminal.

Data dan informasi pribadi mengacu pada data berkarakteristik pribadi seseorang, nama, alamat, usia, pekerjaan, latar belakang, status, Pendidikan perkawinan dan jenis kelamin. Dari sudut pandang hukum, data pribadi dijelaskan berdasarkan Peraturan Pemerintah Republik Indonesia No. Data pribadi sebagaimana dimaksud dalam Undang-Undang Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik dapat dikumpulkan oleh badan publik atau badan privat yang berwenang atau pihak yang berkepentingan dalam rangka melaksanakan tugasnya sesuai dengan ketentuan peraturan perundang-undangan. data pribadi yang dikendalikan, disimpan, dan diproses oleh. Pencurian data pribadi melalui Internet merupakan bentuk umum kejahatan dunia maya. Penjahat dapat mencuri informasi pribadi Anda dengan berbagai cara, termasuk peretasan, phishing, dan malware. Mereka kemudian dapat menggunakan data tersebut untuk keuntungan pribadi, termasuk identitas palsu, penipuan, dan pemerasan. [10]

9. Disemadi, H. S., & Regent, R. (2021). Urgensi Suatu Regulasi yang Komprehensif Tentang Fintech Berbasis Pinjaman Online Sebagai Upaya Perlindungan Konsumen di Indonesia. *Jurnal Komunikasi Hukum* (JKH),7(2), 605-618.
10. Raodia, R. (2019). Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime). Jurisprudentie: Jurusan Ilmu Hukum Fakultas Syariah dan Hukum, 6(2), 230-239.

Ada beberapa langkah yang dapat Anda lakukan untuk melindungi diri Anda dari pencurian data pribadi :

1. Gunakan kata sandi yang kuat dan unik. Kata sandi sebaiknya terdiri dari kombinasi huruf besar dan kecil, angka, serta karakter khusus. Hindari penggunaan kata sandi yang mudah ditebak, seperti tanggal lahir atau nama lengkap. Selain itu, gunakan kata sandi yang berbeda untuk setiap akun daring Anda guna meningkatkan keamanan.
2. Selalu perbarui perangkat lunak secara berkala. Pastikan sistem operasi, program antivirus, dan aplikasi lainnya tetap diperbarui, karena pembaruan ini sering kali mencakup perbaikan keamanan yang melindungi pengguna dari serangan yang memanfaatkan celah atau kerentanan yang telah ditemukan.
3. Berhati-hatilah terhadap email dan tautan mencurigakan. Jangan mengklik tautan atau membuka lampiran dari email yang tidak dikenal atau mencurigakan. Pelaku kejahatan sering menggunakan teknik phishing dengan mengirimkan email palsu yang tampak resmi untuk mencuri informasi pribadi.
4. Gunakan koneksi internet yang aman. Hindari menggunakan jaringan Wi-Fi publik yang tidak terlindungi untuk mengakses akun pribadi atau melakukan transaksi sensitif. Jika perlu terhubung ke internet di tempat umum, gunakan koneksi yang lebih aman, seperti Jaringan Pribadi Virtual (VPN).
5. Berhati-hatilah terhadap identitas palsu dan penipuan daring. Jangan pernah membagikan informasi pribadi secara online kepada orang yang tidak dikenal. Waspadai tawaran yang terdengar terlalu bagus untuk menjadi kenyataan, dan hindari memberikan informasi pribadi atau keuangan kepada sumber yang tidak tepercaya.
6. Amankan perangkat seluler Anda. Aktifkan fitur keamanan seperti kunci layar, enkripsi, dan aplikasi keamanan untuk melindungi data pribadi. Jangan pernah meninggalkan perangkat tanpa pengawasan. Jika perangkat hilang atau dicuri, segera hapus data pribadi untuk mencegah penyalahgunaan.
7. Pantau riwayat aktivitas dan laporan kredit secara berkala. Periksa secara rutin aktivitas akun online serta laporan kredit Anda untuk mendeteksi adanya aktivitas mencurigakan atau transaksi yang berpotensi merupakan tindakan penipuan.

Selain langkah-langkah tersebut, penting untuk tetap waspada terhadap keamanan siber dan terus mengikuti perkembangan terbaru mengenai ancaman keamanan online. Dengan selalu memperbarui pengetahuan dan menerapkan praktik keamanan yang baik, risiko menjadi korban kejahatan siber dapat diminimalkan. Dengan mempraktikkan kebiasaan daring yang baik dan melindungi informasi pribadi Anda, Anda dapat mengurangi risiko menjadi korban kejahatan dunia maya. Jika Anda menjadi korban pencurian data pribadi, segera laporkan kejadian tersebut kepada pihak berwenang dan ikuti prosedur yang disarankan untuk menyelesaikan masalah.[11] Jika ditinjau dari penjelasan fenomena yang telah terjadi di masyarakat Indonesia, maka bisa disimpulkan beberapa faktor terkait kasus pencurian informasi atau data pribadi sebagai berikut :

A. Rendahnya kesadaran hukum di masyarakat. Kesadaran hukum mengacu pada pemahaman individu mengenai apa yang diperbolehkan dan dilarang berdasarkan peraturan dan hukum yang berlaku di Indonesia. Saat ini, kesadaran masyarakat terhadap kejahatan siber masih tergolong rendah, terutama karena kurangnya pemahaman mengenai perilaku yang termasuk dalam tindak kejahatan siber serta dampak yang ditimbulkannya. Tingkat pemahaman masyarakat terhadap teknologi dan aktivitas daring juga berkontribusi dalam mengenali serta memahami dinamika dunia maya. Semakin rendah tingkat pengetahuan seseorang mengenai teknologi, semakin rentan mereka menjadi sasaran eksploitasi oleh pelaku kejahatan siber. Dengan meningkatkan pemahaman tentang kejahatan siber, masyarakat dapat berperan aktif dalam upaya pencegahannya. Tanpa kesadaran akan modus operandi pelaku kejahatan siber, korban sering kali tidak menyadari telah menjadi target hingga mengalami kerugian.[12]
B. Keamanan. Alat yang digunakan oleh pelaku kejahatan siber biasanya berbeda dengan yang digunakan oleh penjahat konvensional. Pelaku kejahatan siber, terutama yang terlibat dalam pencurian data pribadi, memanfaatkan celah keamanan yang tersedia di dunia maya, baik pada platform terbuka maupun tertutup. Dengan akses internet yang luas dan tidak selalu memiliki sistem

11. Aryyaguna, A. D. (2017). Tinjauan Kriminologis Terhadap Kejahatan Penipuan Berbasis Online.Tidak Dipublikasikan). Universitas Hasanuddin.38Hasibuan, M. S. (2018). Keylogger pada Aspek Keamanan Komputer.Jurnal Teknovasi: *Jurnal Teknik dan Inovasi*,3(1), 8-15.
12. Wijayanto, H., Muhammad, A. H., & Hariyadi, D. (2020). Analisis Penyalahgunaan Data Pribadi Dalam Aplikasi Fintech Ilegal Dengan Metode Hibrid. *Jurnal Ilmiah Sinus*,18(1), 1-10.

perlindungan yang efektif, individu sering kali beraktivitas daring tanpa memahami batasan atau risiko yang dapat berkontribusi terhadap meningkatnya kejahatan siber.

C. Penegak Hukum. Beberapa aparat penegak hukum masih menghadapi tantangan dalam memahami teknik yang digunakan oleh pelaku kejahatan siber untuk menjalankan aksinya. Kejahatan di dunia maya sering kali berkembang lebih cepat dibandingkan dengan upaya penegakan hukum, sehingga kasus-kasus semacam ini terus meningkat di Indonesia. Solusi yang dapat diterapkan adalah memperkuat peran aparat penegak hukum yang memiliki kompetensi khusus dan sistem yang terstruktur, termasuk dalam organisasi yang berfokus pada pemberantasan kejahatan siber. Dasar hukum untuk tindakan aparat telah tersedia, namun perlu diiringi dengan peningkatan kinerja individu maupun organisasi. Tanpa strategi penegakan hukum yang terencana dan terkoordinasi dalam bidang teknologi informasi, upaya menangkap pelaku kejahatan siber akan sulit dilakukan, terutama karena kejahatan ini sering kali melintasi batas negara.

D. Tidak adanya perundang-undangan yang diperbaharui. meskipun Undang-Undang Pidana dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) seharusnya bermanfaat. Namun, peraturan yang ada tidak selalu dapat diterapkan secara efektif karena keterbatasan pemahaman dan keterampilan di bidang siber. Pada kenyataannya, kasus pencurian informasi dan data pribadi sudah sering terjadi di masyarakat. Sayangnya, banyak korban yang tidak menyadari risiko yang mereka hadapi atau cenderung mengabaikannya, sehingga tetap tidak menjaga keamanan data pribadi mereka dengan baik.[13]

Bagaimana Pengaturan Perlindungan Hukum Terhadap Pelaku Pencurian Data Pribadi Atau Kejahatan *Cybercrime* Di Indonesia ?

Dengan meningkatnya jumlah pengguna telepon seluler dan internet, kebutuhan akan perlindungan data pribadi semakin mendesak. Hal ini sering kali terkait dengan penyalahgunaan data pribadi serta tindak kejahatan seperti pencurian identitas, penipuan,

13. Mahira, D. F. F., Yofita, E., & Azizah, L. N. (2020). Consumer Protection System (CPS): Sistem Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept. *Jurnal Legislatif*, 287-302.

dan penyebaran konten pornografi. Mengingat banyaknya kasus pencurian data pribadi, perbincangan mengenai pentingnya undang-undang dan regulasi yang melindungi data pribadi semakin gencar. Perlindungan data pribadi sangat berkaitan dengan konsep privasi, yang meliputi perlindungan terhadap integritas dan martabat individu, serta memberikan kontrol kepada individu mengenai bagaimana data pribadi mereka digunakan. Privasi mencakup hak individu untuk menentukan siapa yang dapat mengakses informasi pribadi mereka serta bagaimana informasi tersebut digunakan. Sebagai negara berkembang dengan jumlah pengguna teknologi dan sistem komunikasi modern yang besar, Indonesia masih belum memiliki undang-undang khusus yang secara komprehensif mengatur privasi dan perlindungan data. Dengan pesatnya perkembangan teknologi, regulasi yang mengatur aspek hukum terkait privasi dan perlindungan data menjadi semakin mendesak, meskipun peraturan yang ada sering kali tidak mampu mengikuti kemajuan teknologi yang terjadi.[14]

Di Indonesia, regulasi sering kali tertinggal dari perkembangan sosial dan teknologi, sehingga celah hukum yang ada dapat berdampak pada perlindungan privasi serta data pribadi. Oleh karena itu, diperlukan peraturan yang tegas dan jelas mengenai privasi serta perlindungan data pribadi guna mengatasi permasalahan yang timbul akibat pengelolaan atau penyalahgunaan informasi pribadi. Data pribadi kini menjadi perhatian utama dalam kehidupan masyarakat, terutama di era digital saat ini. Kemajuan teknologi memungkinkan komunikasi tanpa batas ruang dan waktu. Namun, seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi, muncul pula berbagai bentuk kejahatan baru yang berkaitan dengan dunia digital, yang dikenal sebagai *cybercrime* atau kejahatan siber. Karena itu, perlindungan data pribadi menjadi hal yang sangat penting untuk menjaga integritas individu serta memastikan mereka memiliki kendali atas penggunaan informasi pribadinya. Hingga kini, Indonesia belum memiliki regulasi khusus yang mengatur secara rinci tentang privasi dan perlindungan data. Kekosongan hukum ini berdampak pada lemahnya perlindungan data pribadi, terutama karena peraturan yang ada sering kali tidak mampu mengikuti pesatnya perkembangan teknologi. Oleh sebab itu, diperlukan pembaruan dan penyesuaian regulasi agar lebih relevan dan efektif dalam menghadapi tantangan digital saat ini. Untuk mengatasi

14. Siregar, B. J. (2018). Problem dan Pengaturan Cybercrime Melalui Aktifitas Internet Dalam Kasus Sara Di Pilkada Serentak 2018.*Jurnal Penelitian Pendidikan Sosial Humaniora*,3(1), 330-336.

tantangan ini, Indonesia perlu menetapkan regulasi yang jelas dan komprehensif terkait privasi serta perlindungan data pribadi. Peraturan tersebut harus mampu mengatasi berbagai persoalan hukum yang muncul akibat pemanfaatan teknologi dan pertukaran informasi. Dengan adanya regulasi yang tepat, diharapkan tercipta lingkungan digital yang aman dan terpercaya bagi masyarakat. Saat ini, meskipun Indonesia belum memiliki aturan khusus mengenai perlindungan data pribadi, hak atas privasi telah diakui dalam Pasal 28G UUD 1945. Meskipun pasal tersebut tidak secara spesifik membahas perlindungan data pribadi, ia dapat menjadi dasar hukum dalam perumusan regulasi yang lebih rinci untuk melindungi privasi masyarakat, termasuk dalam aspek perlindungan data pribadi.[15]

Data pribadi merupakan isu penting dalam kehidupan bermasyarakat, khususnya di era digitalisasi. Teknologi memungkinkan kita terhubung tanpa hambatan jarak atau waktu. Namun seiring dengan kemajuan eiring dengan perkembangan teknologi informasi dan komunikasi, muncul pula kejahatan baru yang memanfaatkan teknologi tersebut. Kejahatan yang timbul akibat kemajuan di bidang teknologi informasi dan komunikasi antara lain adalah tindak kejahatan yang berkaitan dengan hal tersebut. internet atau biasa disebut dengan kejahatan siber. Perlindungan informasi pribadi penting untuk melindungi integritas individu dan memungkinkan individu mengontrol penggunaan informasi pribadi merekaSaat ini, Indonesia belum memiliki undang-undang yang secara khusus mengatur tentang privasi dan perlindungan data pribadi, sehingga kekosongan hukum ini mempengaruhi perlindungan data pribadi dan privasi. Peraturan yang ada sering kali tidak sejalan dengan kemajuan teknologi, oleh karena itu, peraturan perundang-undangan perlu diperbarui dan disesuaikan dengan perkembangan yang terjadi.

Mengingat tantangan-tantangan ini, penting bagi Indonesia untuk memiliki peraturan yang jelas dan komprehensif untuk melindungi privasi dan data pribadi. Pengaturan ini harus mempertimbangkan permasalahan hukum mengenai privasi dan perlindungan data yang timbul dari penggunaan teknologi dan pembagian informasi pribadi. Dengan adanya peraturan yang sesuai, kami berharap Dapat menciptakan suasana

---

15. Luthiya, A. N., Irawan, B., & Yulia, R. (2021). Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi.Jurnal Hukum Pidana dan Kriminologi,2(2), 14-29.

yang aman dan dapat dipercaya dalam pemanfaatan teknologi serta pengelolaan data pribadi. Meskipun di Indonesia belum ada undang-undang yang secara spesifik mengatur perlindungan informasi dan data pribadi, hak privasi telah diatur dalam Pasal 28G UUD 1945. [16]

Meskipun pasal ini tidak secara spesifik membahas perlindungan data pribadi, ia dapat menjadi dasar dalam merumuskan regulasi yang melindungi privasi warga negara Indonesia, termasuk perlindungan data pribadi dan informasi sensitif lainnya. Pemerintah Indonesia telah mengambil langkah-langkah untuk melindungi data pribadi, namun kebijakan yang ada masih tersebar dalam berbagai undang-undang yang terpisah dan hanya mencakup aspek umum dari perlindungan data pribadi. Oleh karena itu, diperlukan regulasi yang lebih terintegrasi dan komprehensif agar perlindungan data pribadi dapat diatur dengan lebih efektif.

Beberapa regulasi yang berkaitan dengan perlindungan data pribadi di Indonesia mencakup Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (UU Telekomunikasi), serta Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan. Selain itu, terdapat perubahan dalam Undang-Undang Nomor 7 Tahun 1971 tentang Ketentuan Pokok Kearsipan yang diatur dalam UU No. 3, serta Peraturan Pemerintah Nomor 52 Tahun 2000 yang membahas aspek perlindungan privasi dalam penyelenggaraan layanan telekomunikasi dan internet. Lebih lanjut, pemerintah juga telah menerbitkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang menjadi dasar hukum utama dalam mengatur perlindungan data pribadi secara lebih komprehensif. Undang-Undang ini mengatur berbagai aspek terkait perlindungan data pribadi, termasuk prinsip dasar, jenis data pribadi, serta hak individu yang datanya diproses. Selain itu, undang-undang ini mencakup ketentuan mengenai pemrosesan data pribadi, tanggung jawab pengendali dan pemroses data pribadi, serta mekanisme transfer data. Regulasi ini juga menetapkan sanksi administratif bagi pelanggaran, kerangka kerja sama antar lembaga, serta peran masyarakat dalam pengawasan perlindungan data. Penyelesaian sengketa dan proses litigasi hukum turut diatur, termasuk larangan tertentu dalam penggunaan data pribadi serta ketentuan dalam KUHP mengenai perlindungan data

16. Priscyllia, F. (2019). Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum.Jatiswara,34(3), 239-249.

pribadi. Perlindungan data pribadi sendiri merupakan upaya menyeluruh untuk menjaga keamanan informasi pribadi selama pemrosesan, guna menjamin hak konstitusional pemilik data.

Pasal 22 UU Telekomunikasi melarang akses tanpa izin, tindakan ilegal, atau manipulasi terhadap jaringan telekomunikasi, layanan telekomunikasi, atau jaringan telekomunikasi khusus. Pelanggaran terhadap ketentuan ini dapat dikenai hukuman penjara hingga enam tahun dan/atau denda maksimal Rp600 juta. Selain itu, Pasal 40 Undang-Undang Telekomunikasi melarang segala bentuk penyadapan atau intersepsi terhadap informasi yang dikirim melalui jaringan telekomunikasi, dengan ancaman hukuman hingga 15 tahun penjara bagi pelanggarnya. Undang-undang ini juga menetapkan kewajiban bagi penyelenggara layanan telekomunikasi untuk menyimpan pesan yang dikirim dan diterima oleh pengguna melalui jaringan atau layanan yang mereka sediakan. Jika kewajiban ini dilanggar, pelaku dapat dikenakan sanksi berupa pidana penjara maksimal dua tahun dan/atau denda hingga Rp200 juta. Selain Undang-Undang Telekomunikasi, perlindungan data pribadi pengguna internet juga diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Meskipun UU ITE tidak secara khusus mengatur perlindungan data pribadi, undang-undang ini secara implisit memberikan perlindungan terhadap data dan informasi elektronik, baik yang bersifat publik maupun pribadi, yang berhubungan dengan hak individu.[17]

Pernyataan ini menunjukkan bahwa perlindungan data pribadi merupakan tanggung jawab bersama baik individu maupun masyarakat, serta badan hukum dan pemerintah. Sebab, pemerintah tidak hanya harus mengandalkan akal sehat, tapi juga berperan dalam membentuk kebijakan hukum yang bisa memberikan perlindungan terhadap warga negara Indonesia. Dengan demikian, langkah-langkah preventif dan pengendalian dapat diterapkan. Salah satu contoh upaya pencegahan adalah dengan mengungkapkan dan memantau informasi pribadi secara hati-hati. Ada dua pihak yang berperan dalam mengawasi sektor swasta dan pemerintah, yaitu penyedia layanan internet, penyedia konten digital, serta pemilik infrastruktur di berbagai sektor. Dari

17. Sasongko, S., Dwipayana, D. P., Pratama, D. Y., Jumangin, J., & Roselawati, C. P. R. (2020, December). Konsep Perlindungan Hukum Data Pribadi dan Sanksi Hukum atas Penyalahgunaan Data Pribadi oleh Pihak Ketiga. InProceeding of Conference on Law and Social Studies, 16-27 Ibid

perspektif sosiologis, masyarakat Indonesia memerlukan Undang-Undang Nomor 1 Tahun 2024 yang merupakan perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, guna memperkuat regulasi terkait pengawasan dan perlindungan data pribadi.

Perkembangan globalisasi informasi menuntut adanya regulasi yang dapat melindungi kepentingan penyelenggara jaringan dalam mengakses berbagai informasi. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dirancang untuk mendukung tujuan tersebut dengan tetap berlandaskan pada prinsip moral yang berlaku secara umum, termasuk nilai-nilai agama, norma sosial, serta hukum siber. Regulasi ini juga harus diakui, diterima, dan ditegakkan oleh masyarakat dalam ekosistem informasi digital. Kepastian hukum merupakan hal baru. Artinya, undang-undang tersebut bersifat proaktif dan bersifat publik sejak diberlakukan. Perlindungan data, salah satu elemen yang mendukung hak privasi, harus diawali dengan terciptanya kepastian hukum. Oleh karena itu, ketentuan mengenai perlindungan informasi dan data pribadi harus dituangkan dalam konstitusi atau dokumen hukum, yang merupakan dokumen hukum tertinggi dan otoritas final di negara mana pun. Stabilitas hukum (asas legalitas) merupakan elemen penting yang harus dijaga oleh setiap negara. Salah satu upaya untuk memperkuat stabilitas hukum adalah dengan menetapkan serta menjamin hak-hak tersebut dalam konstitusi, yang pada akhirnya memunculkan diskusi mengenai esensi dari suatu negara. Dalam konteks ini, pemerintah Indonesia berupaya memperjelas regulasi terkait perlindungan informasi dan data pribadi guna memastikan kepastian hukum bagi masyarakat.[18]

KESIMPULAN DAN SARAN

Berdasarkan analisis yang telah dikemukakan sebelumnya, dapat disimpulkan bahwa data pribadi mencakup berbagai elemen seperti angka, huruf, identitas individu, simbol, atau kode. Konsep perlindungan data pribadi juga telah diadopsi di berbagai negara. Namun, di Indonesia, regulasi hukum pidana yang secara khusus mengatur

18. Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber.SASI,27(1), 38-52.30Siregar, B. J. (2018). Problem dan Pengaturan Cybercrime Melalui Aktifitas Internet Dalam Kasus Sara Di Pilkada Serentak 2018.Jurnal Penelitian Pendidikan Sosial Humaniora,3(1), 330-336

pencurian data pribadi sebagai bentuk penyalahgunaan teknologi komunikasi serta tindak pidana terkait masih belum diatur secara rinci. Saat ini, penerapan undang-undang perlindungan data masih dianggap belum optimal. Perlindungan data pribadi memerlukan regulasi yang lebih ketat dan menyeluruh agar dapat menyesuaikan dengan dinamika sosial, budaya, ekonomi, dan politik. Selain itu, regulasi tersebut harus selaras dengan nilai-nilai, norma, etika, moral, dan aspek keagamaan, sehingga hukum di Indonesia dapat mengikuti perkembangan teknologi dan informasi. Sementara banyak negara maju telah memiliki regulasi khusus terkait perlindungan data pribadi, Indonesia masih menghadapi keterbatasan dalam hal tersebut. Isu-isu terkait perlindungan data pribadi saat ini hanya diatur dalam Pasal 26 UU ITE dan beberapa regulasi lainnya. Peningkatan kasus pencurian data disebabkan oleh berbagai faktor, termasuk lemahnya penegakan hukum, sistem keamanan yang belum memadai, serta kurangnya pemahaman masyarakat terhadap aspek hukum yang melindungi data pribadi. Selain itu, kelalaian individu dalam menjaga informasi pribadi mereka dan lambatnya proses penanganan kasus pencurian data turut memberikan celah bagi pelaku untuk terus melakukan kejahatan tersebut.

Pemerintah dan Dewan Perwakilan Rakyat (DPR) perlu mengevaluasi yurisdiksi terkait perlindungan hukum terhadap eksploitasi data pribadi, terutama kasus pencurian informasi di internet. Regulasi yang ada harus mampu memberikan kepastian hukum bagi masyarakat. Selain itu, aparat penegak hukum harus memperkuat upaya penegakan hukum, meningkatkan koordinasi antar lembaga terkait, serta berperan aktif dalam mencegah tindak kejahatan pencurian data pribadi. Dalam konteks ini, penyelidik telah mengusulkan penerapan sanksi pidana yang bersifat memberikan efek jera. Pemerintah perlu memahami berbagai faktor yang memengaruhi kasus kejahatan terkait perlindungan data pribadi. Oleh karena itu, peran strategis pemerintah harus dioptimalkan, terutama dalam menindak pelaku pencurian data pribadi. Seiring dengan pesatnya perkembangan teknologi transaksi elektronik, pemerintah juga harus mengedukasi masyarakat tentang perlindungan data pribadi agar mereka lebih memahami cara menjaga keamanan informasi pribadi secara efektif. Untuk meningkatkan efektivitas penegakan hukum, masyarakat diimbau untuk lebih berhati-hati dan waspada dalam beraktivitas di dunia digital. Kesadaran akan pentingnya perlindungan data pribadi perlu ditingkatkan agar individu dapat mengantisipasi potensi risiko dan menghindari tindakan yang dapat membahayakan informasi pribadi mereka.

DAFTAR REFERENSI

Buku

Maskun., Maskun. 2017. *Kejahatan Siber (Cyber Crime) Suatu Pengantar*. Jakarta : Prenada Media

Yurizal., Yurizal. 2018. Penegak Hukum Tindak Pidana *Cybercrime*. Malang : Media Nusa Creative

Widiatno.,Andi, 2024. Tindak Pidana Siber (Cyber Crime) Pasca Terbitnya UU ITE No. 1 Tahun 2024. Jakarta. Genta Publishing

Soekanto, Soerjono. (2015). *Sosiologi Hukum: Suatu Pengantar*. Jakarta: RajaGrafindo Persada.

Hernandez, Antonio B. (2022). *The Role of Information Technology in the Escalation of Data Theft Crimes*. International Journal of *Cybercrime* Studies, 15(3), 220-237.

Davis, Michael T. (2023). *Legal Protection for Victims of Data Theft: A Global Perspective*. Journal of Cyber Law and Ethics, 20(4), 315-329.

Jurnal

Disemadi, H. S. (2021). Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia. *Jurnal Wawasan Yuridika*,5 (2), 177-199.

Afnesia, U., & Ayunda, R. (2022). Perlindungan Data Diri Peminjam Dalam Transaksi Pinjaman Online: Kajian Perspektif Perlindungan Konsumen Di Indonesia. *Jurnal Komunitas Yustisia*,4(3), 1035-1044

Alhakim, A. (2022). Urgensi Perlindungan Hukum terhadap Jurnalis dari Risiko Kriminalisasi UU Informasi dan Transaksi Elektronik di Indonesia. *Jurnal Pembangunan Hukum Indonesia*, 4(1), 89-106.

Ketaren, E. (2016). *Cybercrime*,(Cyber Space, dan Cyber Law. *Jurnal Times*, 52), 35-42. Disemadi, H. S., & Regent, R. (2021). Urgensi Suatu Regulasi yang Komprehensif

Tentang Fintech Berbasis Pinjaman Online Sebagai Upaya Perlindungan Konsumen di Indonesia. *Jurnal Komunikasi Hukum* (JKH),7(2), 605-618.

Raodia, R. (2019). Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (*Cybercrime*).Jurisprudentie: Jurusan Ilmu Hukum Fakultas Syariah dan Hukum,6(2), 230-239.

Aryyaguna, A. D. (2017). Tinjauan Kriminologis Terhadap Kejahatan Penipuan Berbasis Online.Tidak Dipublikasikan). Universitas Hasanuddin.38Hasibuan,

M. S. (2018). Keylogger pada Aspek Keamanan Komputer.Jurnal Teknovasi: *Jurnal Teknik dan Inovasi*,3(1), 8-15.

Wijayanto, H., Muhammad, A. H., & Hariyadi, D. (2020). Analisis Penyalahgunaan Data Pribadi Dalam Aplikasi Fintech Ilegal Dengan Metode Hibrid. *Jurnal Ilmiah Sinus*,18(1), 1-10.

Mahira, D. F. F., Yofita, E., & Azizah, L. N. (2020). Consumer Protection System (CPS): Sistem Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept. *Jurnal Legislatif*, 287-302.

Siregar, B. J. (2018). Problem dan Pengaturan *Cybercrime* Melalui Aktifitas Internet Dalam Kasus Sara Di Pilkada Serentak 2018.Jurnal Penelitian Pendidikan Sosial Humaniora,3(1), 330-336.

Luthiya, A. N., Irawan, B., & Yulia, R. (2021). Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi. *Jurnal Hukum Pidana dan Kriminologi*,2(2), 14-29.

Priscyllia, F. (2019). Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum. *Jurnal Jatiswara*,34(3), 239-249.

Sasongko, S., Dwipayana, D. P., Pratama, D. Y., Jumangin, J., & Roselawati, C. P. R. (2020, December). Konsep Perlindungan Hukum Data Pribadi dan Sanksi Hukum atas Penyalahgunaan Data Pribadi oleh Pihak Ketiga. InProceeding of Conference on Law and Social Studies, 16-27 Ibid

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber.SASI,27(1), 38-52.30Siregar, B. J. (2018). Problem dan Pengaturan *Cybercrime* Melalui Aktifitas Internet Dalam Kasus Sara Di Pilkada Serentak 2018.*Jurnal Penelitian Pendidikan Sosial Humaniora*,3(1), 330-336

Peraturan Perundang-Undangan

Undang-Undang Dasar Negara Republik Indonesia

Undang Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang

Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi (UU Telekomunikasi), Dan Undang-Undang Nomor 8 Tahun 1997 Tentang Dokumen Perusahaan.

UU No. 3. Perubahan Atas Undang-Undang Nomor 7 Tahun 1971 Tentang Ketentuan-Ketentuan Pokok Kearsipan,

Undang-Undang Nomor 36 Tahun 2009 Tentang Kesehatan,

Peraturan Pemerintah Nomor 52 Tahun 2000 Tentang Penyelenggaraan Telekomunikasi Mengatur Tentang Perlindungan Privasi Dalam Penyelenggaraan Layanan Internet, Selain Itu Baru