JURNAL KOMUNIKASI HUKUM
Volume 8 Nomor 1, Februari 2022
P-ISSN: 2356-4164, E-ISSN: 2407-4276
Open Access at : https://ejournal.undiksha.ac.id/index.php/jkh
Program Studi Ilmu Hukum
Fakultas Hukum dan Ilmu Sosial
Universitas Pendidikan Ganesha Singaraja

PENCURIAN DATA PRIBADI DI INTERNET DALAM PERSPEKTIF KRIMINOLOGI

Fiqqih Anugerah, Tantimin

Fakultas Hukum, Universitas Internasional Batam
E-mail: 1951094.fiqqih@uib.edu

Info Artikel

Masuk: 1 Desember 2021
Diterima: 12 Januari 2022
Terbit: 1 Februari 2022

Keywords:
Personal Data, Legal Protection, Internet

Abstract

Advances in information and communication technology have led to social thinking, attitudes and lifestyles, including patterns of human behavior, not limited to law enforcement, cultural, economic and social relations. Confidentiality of personal data is important because it relates to self-respect and freedom of expression. So far, there is no specific regulation to combat the misuse of personal data which creates legal problems for personal data by the state. There are several factors that encourage the occurrence of criminal acts of data theft cases. Thus, this study aims to provide an understanding of how the legal protection policy is against the crime of theft of personal data on the internet and what are the factors that can lead to criminal acts of theft of personal data on the internet. This article uses a normative research method which is carried out by observing library materials such as legal materials, such as journals, concepts, theses, theories, principles, and legal norms currently in force in Indonesia.

Kata kunci:
Data Pribadi, Perlindungan Hukum, Internet

Abstrak

Perkembangan teknologi informasi dan komunikasi sudah membawa pada pemikiran sosial, sikap dan gaya hidup, termasuk pola perilaku manusia, tidak terbatas pada penegakan hukum, hubungan budaya,

Corresponding Author:
Fiqqih Anugerah

ekonomi dan sosial. Kerahasiaan data pribadi penting karena berkaitan dengan harga diri dan kebebasan berekspresi. Sejauh ini, belum ada regulasi khusus untuk memerangi penyalahgunaan data pribadi yang menimbulkan persoalan hukum atas data pribadi oleh negara. Terdapat beberapa faktor yang mendorong terjadinya tindak pidana kejahatan kasus pencurian data. Dengan demikian, penelitian bertujuan untuk memberikan pemahaman tentang kebijakan perlindungan hukum terhadap kejahatan pencurian data pribadi di internet dan apa saja faktor yang dapat menyebabkan tindak pidana kejahatan pencurian data pribadi di internet. Artikel ini memakai metode penelitian normatif yang dilakukan dengan cara mengamati bahan pustaka seperti bahan hukum, seperti jurnal, konsep, skripsi, teori, prinsip, serta norma hukum yang saat ini berlaku di Indonesia.

Pendahuluan

Seiring pada perkembangan zaman, kemajuan teknologi informasi semakin berkembang dengan pesat sehingga masyarakat di Indonesia dapat lebih mudah memperoleh informasi yang mereka inginkan. Hal ini membuat masyarakat menjadikan teknologi informasi sebagai kebutuhan sehari-hari 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 dalam masyarakat Indonesia.[2] Dengan perkembangan media elektronik dan komunikasi, waktu dan jarak bukan kembali menjadi permasalahan utama kepada semua individu, termasuk pemerintah. Setiap individu dapat berkomunikasi satu sama lain tanpa bertemu di ruang fisik.[3] Perusahaan dapat mengembangkan usahanya ke banyak negara hanya dengan pemasaran melalui internet dan komputer. Pemerintah hanya bisa menjalankan banyak kegiatan pemerintah melalui Internet dan komputer. Misalnya, dapat menjalin hubungan diplomatik antar negara di seluruh dunia tanpa harus pergi

[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.

[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.

ke negara yang bersangkutan. Jaringan telekomunikasi global telah menjadi bagian integral dari bisnis, pendidikan, dan pemerintahan modern.[4]

Kemajuan teknologi informasi sudah dianggap menjadi kekuatan yang bisa menentukan nasib seseorang.[5] Oleh karena itu dapat menyebabkan masyarakat Indonesia sangat bergantungan dengan teknologi informasi sehingga semakin banyak pula resiko timbulnya tindak kejahatan. Teknologi informasi dapat meningkatkan kemajuan dalam pandangan hidup manusia, namun juga bisa sebagai sarana melakukan tindak kriminal hukum yang dikenal sebagai "*cybercrime*".[6] *Cyber crime* merupakan tindak kejahatan atau kegiatan ilegal yang dilakukan melalui jaringan dunia elektronik. Kriminalitas dalam jaringan internet semakin berbahaya dikarenakan ruang lingkup tindakan tersebut sangat luas.[7] Tindakan kriminal dalam internet merupakan kejahatan yang berhubungan dengan dunia maya yang dapat membahayakan privasi seseorang. Kejahatan di dunia maya semakin banyak totalnya dan semakin banyak variasi karakteristik para pelaku. Para pelaku dengan mudah melakukan tindak kejahatan dengan memakai kemajuan teknologi informasi. Contoh dari kejahatannya seperti pornografi, perjudian *online*, terorisme, *hacking*, *carding*, ATM/EDC *Skimming*, *phishing*, dan masih banyak tindak kejahatan lainnya.[8]

Pencurian data dalam dunia internet bisa disebut sebagai *phising*, merupakan tindakan kejahatan mendapatkan informasi pribadi atau privasi seseorang dengan secara ilegal. Dari tindakan tersebut perlu mendapatkan nomor kartu kredit, PIN, *User ID*, nomor telepon, nomor rekening, dan informasi data pribadi lainnya.[9] Dari tindakan tersebut kemudian 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 adalah sebagai metode pendataan informasi atau data pribadi masyarakat oleh pemerintah yang pertama kali dijalankan saat awal tahun 2011, yakni pelaksanaan dari metode Nomor Induk Kependudukan (NIK). Dalam kebijakan tersebut menginginkan identitas setiap penduduk berlaku seumur hidup, dan setiap orang mempunyai 1 kartu yang dimana dalam kartu tersebut terdapat NIK. Seluruh informasi pribadi penduduk direkam yang didalamnya termasuk ciri-ciri fisik dan identitas. Dengan begitu data yang telah

---

[4] Tampubolon, K. E. A. (2019). Perbedaan Cyber Attack, Cybercrime, dan Cyber Warfare. *Jurist-Diction*, *2*(2), 539-554.

[5] Winarso, T., Disemadi, H. S., & Prananingtyas, P. (2020). Protection Of Private Data Consumers P2P Lending As Part Of E-Commerce Business In Indonesia. *Tadulako Law Review*, *5*(2), 206-221.

[6] Rumlus, M. H., & Hartadi, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik. *Jurnal HAM*, *11*(2), 285-299.

[7] Alhakim, A., & Sofia, S. (2021). Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia. *Jurnal Komunitas Yustisia*, *4*(2), 377-385.

[8] *Ibid*

[9] Elsinda, E. (2014). Aspek Hukum Perlindungan Data Pribadi di Dunia Maya. *Jurnal Gema Aktualita*, *3*(2).

ada di dalam e-KTP mudah disalahgunakan oleh para pelaku tindak kriminal, terlebih jika pengamanan dalam perlindungan data tersebut tidak kuat.[10]

Kasus kebocoran informasi pribadi sangat sering terjadi di Indonesia.[11] 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.[12]

Salah satu contoh kasus pencurian informasi atau data pribadi di Indonesia yang terjadi pada tanggal 12 Mei 2021, 279 juta informasi data pribadi warga Indonesia dibocorkan dan dijual di forum peretas oleh akun bernama Kotz. Data yang telah bocor tersebut yang berisikan nama lengkap Kartu Tanda Penduduk (KTP), nomor telepon, email, Nomor Identitas (NID), domisili serta pendapatan. 20 Juta diantara lainnya lengkap dengan foto pribadi penduduk Indonesia. Sebuah akun bernama kotz menyediakan 1 juta sampel data secara gratis dengan menyediakan 3 tautan dengan kata sandi yang diperlukan untuk tautan tersebut.[13]

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. 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

---

[10] *Ibid*

[11] Disemadi, H. S., & Prasetyo, D. (2021). Tanda Tangan Elektronik pada Transaksi Jual Beli Online: Suatu Kajian Hukum Keamanan Data Konsumen di Indonesia. *Wajah Hukum*, *5*(1), 13-20.

[12] Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences (BECOSS) Journal*, *1*(1), 147-154.

[13] 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.

mencuri data. Dapat diartikan bahwa korban pencurian data dapat mencakup tidak hanya individu tetapi juga komunitas dan rakyat Indonesia.[14] 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).[15]

Berdasarkan hal tersebut, artikel ini akan membahas pentingnya perlindungan hukum tindak kejahatan pencurian data pribadi dan apa saja faktor yang dapat menimbulkan pencurian data pribadi. Dikarenakan adanya regulasi berupa undang-undang yang berkaitan dengan data pribadi di Indonesia di kemudian hari sebelum adanya undang--undang perlindungan data pribadi yang baru. Bersumber pada paparan serta keterangan tersebut, maka rumusan masalah inti pada penelitian ini bisa diuraikan, yaitu: 1) Bagaimana pengaturan perlindungan hukum pencurian data pribadi di Indonesia?; dan 2) Apa faktor yang menyebabkan tindak kejahatan pencurian data pribadi di internet?.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif dengan teknik *library search* yang dimana adalah mencari bahan-bahan jurnal ataupun artikel yang berkaitan dengan judul serta tema yang penulis kaji untuk dijadikan sebagai referensi dalam pembuatan artikel ini.[16] Kemudian tentu dengan kata normatif ini akan mengkaji atau membandingkan dengan undang-undang serta peraturan yang berkaitan dengan tema yang penulis serta kelompok kaji tersebut, jadi dengan adanya metode istilah normatif tadi maka berarti dengan metode tersebut kita justru akan melalui tahap dengan mengamati serta mengkaji bahan-bahan pustaka yang sebagaimana tadi disebutkan dengan *library search* tersebut.

HASIL DAN PEMBAHASAN

Pengaturan Perlindungan Hukum Pencurian Data Pribadi di Indonesia

Sejalan dengan meningginya jumlah pemakai ponsel dan internet, pentingnya melindungi informasi atau data pribadi juga sangat meningkat.[17] Ini sering terjadi sehubungan dengan penyalahgunaan data pribadi dan tindak pidana, seperti jual beli informasi pribadi, penggelapan akun basah, berbagi informasi pribadi seseorang, penipuan dan kejahatan pornografi. Mengingat

[14] *Ibid*

[15] *Ibid*

[16] Tan, D. (2021). Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, *8*(8), 2463-2478.

[17] Disemadi, H. S. (2021). Legal Aspects Of 'Gali Lubang Tutup Lubang'in Fintech P2p Lending Business During Covid-19. *Tadulako Law Review*, *6*(2), 237-256.

kejadian kasus pencurian informasi atau data pribadi, diskusi tentang pentingnya undang-undang dan peraturan untuk perlindungan informasi pribadi semakin diperkuat. Perlindungan data pribadi terkait dengan konsep privasi. Konsep privasi adalah gagasan menjunjung tinggi integritas dan martabat individu. Privasi juga mencakup kemampuan individu untuk mengontrol siapa yang memiliki informasi tersebut dan dengan cara apa informasi itu digunakan.[18] Sebagai negara berkembang, negara Indonesia memiliki banyak konsumen teknologi serta sistem komunikasi modern. Tetapi sejauh ini, Indonesia tidak mempunyai undang-undang khusus yang mengatur tentang proteksi privasi dan data. Seiring karena bertambahnya penggunaan teknologi, begitu pula peraturan tentang menanggulangi masalah hukum berhubungan privasi dan perlindungan data. Peraturan perundang-undangan yang ada seringkali tidak dapat mengikuti perkembangan teknologi. Peraturan di Indonesia sering kali bergerak sangat daripada pembangunan sosial, termasuk perkembangan teknologi. Tentu saja, celah hukum ini mempengaruhi privasi dan perlindungan data pribadi. Indonesia membutuhkan regulasi tentang privasi dan perlindungan data pribadi, dan diharapkan regulasi tersebut dapat menyelesaikan permasalahan yang diakibatkan oleh penyalahgunaan pengelolaan informasi atau data pribadi.[19]

Informasi dan data pribadi adalah salah satu hal terpenting dalam kehidupan sosial. Apalagi sekarang kita berada di era digitalisasi. Di era digitalisasi, setiap aspek kehidupan kita bergantung pada teknologi, dan semua orang dapat terhubung tanpa terganggu oleh jarak atau waktu. Menurut ketentuan dalam Pasal 20, Pasal 1, Ayat 1 Peraturan Menteri Komunikasi dan Informatika Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik yang berbunyi "Data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya".[20] Ketika membahas pencurian informasi dan data pribadi yang marak terjadi di Indonesia, tidak bisa dilepaskan berasal pengkajian akan hal kemajuan teknologi komunikasi serta informasi yang mengakibatkan timbulnya tindak pidana baru yang mempunyai ciri yang berlainan dengan tindak pidana konvensional. Eksploitasi komputer merupakan salah satu akibat dari kemajuan teknologi yang tidak terlepas dari keunikannya dan menimbulkan masalah yang kompleks untuk dipecahkan dalam hal pemecahan masalah. Contoh tindak kriminal yang diakibatkan karena perkembangan teknologi informasi dan telekomunikasi yaitu tindak kriminal yang berhubungan melalui dunia internet atau biasa disebut *cybercrime.*[21]

---

[18] Sinaga, E. M. C., & Putri, M. C. (2020). Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *9*(2), 237.

[19] Dewi, S. (2016). Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia. *Yustisia Jurnal Hukum*, *5*(1), 35-53.

[20] Witasari, A., & Setiono, A. (2016). Perlindungan Hukum Pengguna Jasa Electronic Banking (E-Banking) di Tinjau dari Perspektif Hukum Pidana di Indonesia. *Jurnal Pembaharuan Hukum*, *2*(1), 126-137.

[21] 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.

Pada tahun 2017, setidaknya 3.885.567.819 orang di seluruh dunia menggunakan teknologi internet. Proporsinya telah mencapai 51,7 dalam populasi dunia, melebihi 7,5 miliar. Per 30 Juni 2017, berdasarkan data penggunaan Internet dan statistik penduduk dunia, Asia menempati posisi tertinggi dalam penggunaan Internet, dengan 50% dari 1.938.075.631 pengguna. Indonesia termasuk dalam 1.132.700.000 pengguna internet. Asosiasi Pengguna Jasa Internet Indonesia (APJII) menyatakan bahwa Indonesia berada di peringkat ke-4 di Asia dan ke-8 di dunia dalam hal penggunaan Internet. Jawa adalah pulau dengan penggunaan internet tertinggi di Indonesia.[22] Kemajuan teknologi informasi dan komunikasi telah membawa pada pemikiran sosial, sikap dan gaya hidup, termasuk pola perilaku manusia, tidak terbatas pada penegakan hukum, hubungan budaya, ekonomi dan sosial. Perlindungan data pribadi merupakan sistem hukum yang memiliki hak konstitusional di banyak negara atau disebut "data habeas" dan ada di negara tertentu, seperti data, rekening kartu kredit/debit, atau pembayaran lainnya. Informasi biometrik dari pelanggaran atau aktivitas kriminal yang mungkin disebabkan oleh informasi pengguna yang lebih rinci, kesehatan fisiologis dan mental pribadi, catatan medis, dan penyalahgunaan informasi pribadi.[23]

Secara khusus, tidak ada ketentuan hukum mengenai proteksi informasi atau data pribadi di Indonesia, tetapi memastikan proteksi hak privasi diatur pada Pasal 28G UUD 1945. Pada dalam pasal tersebut memang tidak dijelaskan secara spesifik tentang perlindungan data pribadi seseorang. Tetapi pasal tersebut mampu dipakai untuk membentuk peraturan terkait menggunakan perlindungan diri masyarakat negara Indonesia, menjadi keliru satunya adalah proteksi informasi atau data pribadi. Sejauh ini, pemerintah Indonesia telah mengambil tindakan upaya pencegahan untuk melindungi data pribadi, tetapi kebijakan ini masih diatur secara individual oleh beberapa peraturan yang diundang dan merupakan aspek umum dari perlindungan data pribadi.[24] Mengenai kebijakan tersebut diantaranya ada dalam UU ITE, Undang No. 36 Tahun 1999 tentang Telekomunikasi (UU Telekomunikasi), Undang-Undang No. 8 Tahun 1997 tentang Dokumen Perusahaan, Undang-Undang No. 7 Tahun 1971 tentang Ketentuan-Ketentuan pokok Kearsipan, Undang-Undang No. 36 Tahun 2009 tentang Kesehatan, Undang-Undang No. 10 Tahun 1998 tentang Perubahan atas Undang-Undang No. 7 Tahun 1992 tentang Perbankan, serta Undang-Undang No. 24 Tahun 2013 tentang Perubahan Atas Undang-Undang No. 23 Tahun 2006 perihal Administrasi Kependudukan (UU Adminduk). berdasarkan Peraturan Pemerintah No. 52 Tahun 2000 tentang Penyelenggaraan Telekomunikasi yang merupakan peraturan pelaksana berasal UU Telekomunikasi, Internet termasuk dalam jenis layanan multimedia yang diidentifikasi sebagai penyedia layanan telekomunikasi yang menyediakan layanan berlandas teknologi informasi. Dari sudut pandang peraturan,

---

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

[23] *Ibid*

[24] 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. In *Proceeding of Conference on Law and Social Studies*, 16-27.

memberikan bahwa peraturan Internet akan dimasukkan ke dalam UU Telekomunikasi. UU Telekomunikasi mengatur beberapa hal terkait kerahasiaan data pribadi.[25]

Diantaranya dalam Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi (UU Telekomunikasi) Pasal 22 dinyatakan bahwa setiap orang dilarang melakukan perbuatan tanpa hak, tidak legal, atau manipulasi: (a) akses ke jaringan telekomunikasi; dan /atau (b) akses ke jasa telekomunikasi; dan atau (c) akses ke jaringan telekomunikasi khusus. Bagi pelanggar ketentuan tersebut diancam pidana penjara maksimal enam tahun dan/atau denda maksimal Rp.600 juta. Selain itu, Pasal 40 menyatakan bahwa penyadapan atas segala bentuk informasi yang dikirimkan melalui jaringan telekomunikasi dilarang. Siapa pun yang melanggar ketentuan ini akan dihukum penjara dengan maksimal hingga 15 tahun. UU tersebut juga mengatur kewajiban penyelenggara jasa telekomunikasi untuk menyimpan pesan yang dikirim dan diterima oleh pelanggan jasa telekomunikasi melalui jaringan telekomunikasi dan/atau jasa telekomunikasi yang disediakan. (Pasal 42 ayat (1)). Bagi yang melanggar kewajiban tersebut diancam pidana penjara maksimal 2 tahun dan atau denda maksimal Rp.200 juta. Ketentuan lain mengenai perlindungan data pribadi pengguna internet diatur dalam UU ITE. Undang-undang ini tidak mencakup undang-undang perlindungan data langsung yang eksplisit. Namun, undang-undang tersebut secara implisit memperkenalkan pemahaman baru tentang perlindungan terhadap keberadaan data atau informasi elektronik publik dan privat.[26]

Klasifikasi perihal data pribadi diamanatkan lebih lanjut oleh UU ITE dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Perlindungan data pribadi pada sebuah sistem elektronik di UU ITE mencakup perlindungan dari penggunaan tanpa adanya izin, proteksi sang penyelenggara sistem elektronika, serta proteksi berasal akses serta interferensi ilegal. Berhubungan dengan menggunakan proteksi data pribadi berasal pemakaian tiadanya persetujuan, Pasal 26 UU ITE mengharuskan bahwa penerapan setiap data pribadi dalam sebuah media elektronik harus mempunyai izin dari seseorang yang mempunyai data berkaitan. Siapapun yang tidak mengikuti kebijakan ini dapat dituntut atas kerugian yang muncul. Isi pada pasal 26 UU ITE merupakan menjadi berikut: 1) Penggunaan setiap berita melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. 2) Setiap Orang yang dilanggar haknya sebagaimana dimaksud di ayat (1) bisa mengajukan gugatan atas kerugian yang ditimbulkan sesuai Undang-Undang ini pada penjelasannya, Pasal 26 UU ITE menyatakan bahwa data pribadi merupakan bagian dari hak individu atas privasi. Sementara itu, lihat Pasal 1 PP PSTE untuk definisi data langsung artinya, data pribadi seorang individu disimpan, dipelihara, disimpan dengan itikad baik dan dilindungi kerahasiaannya. Penjelasan pasal 26 ayat (1) UU ITE juga menjelaskan lebih

[25] *Ibid*

[26] *Ibid*

dalam seputar pengertian hak pribadi. Pernyataan terkait dengan penggunaan teknologi informasi dan perlindungan informasi atau data pribadi adalah bagian dari hak privasi *(privacy rights)*.[27]

Hak pribadi memiliki implikasi yakni hak pribadi adalah hak untuk memiliki kehidupan pribadi dan tidak boleh diganggu, hak pribadi adalah hak untuk bisa berkomunikasi menggunakan dengan orang lain tanpa dimata-matai, dan hak pribadi adalah hak untuk mengakses akses informasi tentang kehidupan langsung dan data seseorang. Interpretasi umum, maka proteksi data sesungguh nya sudah diatur oleh ketentuan UU ITE, yaitu di Pasal 30-33 dan pasal 35 yang masuk ke pada Bab VII tentang kegiatan yang tidak diperbolehkan. UU ITE dengan tegas melarang akses ilegal terhadap data orang lain melalui sistem elektronik dengan tujuan melanggar sistem keamanan dan memperoleh informasi. Selain itu, UU ITE dengan jelas menyatakan bahwa penyadapan adalah tindakan yang dilarang kecuali dilakukan oleh pihak yang berhak melakukannya dengan upaya hukum. Siapa pun yang merasa dirugikan oleh perilaku yang ditangguhkan dapat menuntut ganti rugi dan pelaku juga akan bertanggung jawab atas apa yang telah dikerjakannya.[28]

Jika dilihat dari penjelasan tersebut berhubungan dengan perlindungan data pribadi menjadi tanggung jawab bersama, baik antara individu, masyarakat bahkan badan hukum bahkan pemerintah. Hal itu karena pemerintah harus berperan dalam membentuk kebijakan hukum, tidak hanya bertumpu pada akal sehat, tetapi juga harus mampu memberikan perlindungan kepada masyarakat Indonesia. Dengan demikian, upaya preventif dan represif dapat dilakukan. Contoh upaya pencegahan adalah karena upaya pengungkapan dan pemantauan yang cermat atas informasi pribadi. Ada dua pihak yang dapat atau dapat melakukan pengawasan sektor swasta dan pemerintah. Pihak swasta dapat berasal dari penyedia konten dan layanan online, penyedia layanan internet, atau pemilik infrastruktur internet umumnya bersifat sectoral.[29]

Secara sosiologis, masyarakat Indonesia membutuhkan UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008 untuk mengatur berbagai aktivitas yang mereka lakukan ketika berinteraksi di dunia maya atau di internet. Dinamika globalisasi informasi menuntut adanya aturan untuk melindungi kepentingan penyelenggara jaringan dalam mengakses berbagai informasi. Peraturan dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sejalan dengan agama, nilai-nilai, dan prinsip moral yang berlaku umum untuk keberadaan *cyber law* untuk diakui, diterima, dan ditegakkan *information society*. Kepastian hukum adalah hal baru. Singkat kata, sudah positif dan publik sejak undang-undang itu diundangkan.[30]

Perlindungan data untuk elemen yang mendukung hak atas privasi (*the right of privacy*) wajib dimulai pada terciptanya kepastian hukum. Dengan demikian, ketentuan proteksi informasi atau data pribadi harus ditempatkan

---

[27] *Ibid*

[28] *Ibid*

[29] Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *SASI*, *27*(1), 38-52.

[30] 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.

dalam Konstitusi atau dokumen hukum dengan otoritas tertinggi, Konstitusi, sebagai instrumen hukum tertinggi di pada setiap negara. Kepastian hukum (asas legalitas) dibutuhkan serta tidak tersisihkan oleh semua negara pada bentuk penguatan peraturan kepastian hukum terletak pada pencantuman dan penjaminan hak-hak tersebut dalam konstitusi, yang melaluinya karakter negara memunculkan persoalan, metode hukum yang dipakai, serta cara pemerintah melakukannya, oleh karena itu, sudah saatnya pemerintah Indonesia mengeluarkan regulasi yang jelas tentang perlindungan informasi atau data pribadi.[31]

Faktor yang Menyebabkan Tindak Kejahatan Pencurian Data Pribadi di Internet

Tindak kejahatan dan perbuatan tercela merupakan perilaku yang melanggar hukum dan norma sosial, dan masyarakat tidak menerimanya. Tindak kejahatan sering kali disebabkan oleh berbagai banyak faktor. Faktor pemicu terjadinya tindak kejahatan adalah faktor biologis yang terdiri dari faktor ekonomi (tidak adanya lapangan pekerjaan), faktor mental atau fisik, dan faktor pribadi, faktor sosial, dan masih banyak faktor lainnya sebagai pemicu berbagai macam jenis tindak kejahatan. Tindak kejahatan dan perbuatan tercela merupakan perbuatan yang melanggar hukum dan melanggar norma sosial, dan masyarakat menentangnya. Tindakan pidana atau tindakan kriminal memiliki dampak yang sangat merugikan dalam kehidupan sosial di masyarakat Indonesia, sehingga dapat menimbulkan kecemasan, ketakutan, kecemasan, dan kepanikan di kalangan masyarakat Indonesia.[32]

Dengan meningkatnya kasus tindak kriminal dan revolusi dunia, khususnya peningkatan tindak kriminal di internet sangat tambah kekhawatiran, penegakan hukum merupakan inti utama dalam melawan tindakan kriminal di internet, sehingga penegakan hukum harus bekerja keras.[33] Terutama di negara Indonesia, penegakan hukum pada kasus *cybercrime* sangat didorong oleh 5 faktor yaitu undang-undang, budaya, institusi, perilaku masyarakat, dan pemikiran aparat penegak hukum. Hukum tidak dapat ditegakkan dengan sendirinya dan selalu menyertakan manusia dan perilaku manusia, juga tidak dapat dipaksakan tanpa permintaan. Selain bersikap profesional dan berhati-hati dalam penegakan hukum, aparat penegak hukum juga harus berhadapan dengan individu dan kelompok dalam masyarakat yang diduga melakukan tindak pidana.[34] Karena kemajuan teknologi, struktur masyarakat telah berubah dari masyarakat yang berbasis lokal menjadi masyarakat yang terstruktur secara global. Peralihan tersebut diakibatkan karena adanya adanya teknologi informasi. Kemajuan teknologi informasi yang

[31] Situmeang, S. M. T. (2021). *Op.Cit.*

[32] Lumenta, C. Y., Kekenusa, J. S., & Hatidja, D. (2012). Analisis jalur faktor-faktor penyebab kriminalitas di kota Manado. *Jurnal Ilmiah Sains*, *12*(2), 77-83.

[33] Haris, M. T. A. R., & Tantimin, T. (2022). Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan Artificial Intelligence Di Indonesia. *Jurnal Komunikasi Hukum (JKH)*, *8*(1), 307-316.

[34] Ketaren, E. (2016). Cybercrime, Cyber Space, dan Cyber Law. *Jurnal Times*, *5*(2), 35-42.

menggabungkan komputer dan media telah menciptakan alat baru yang disebut internet. Keberadaan internet sudah membawa sistem yang baru dalam aktivitas dalam masyarakat.[35] Hidup berubah dari realitas belaka ke realitas virtual baru. Realitas kedua biasanya terkait dengan internet dan dunia maya.[36]

Tindak pidana kejahatan pada teknologi informasi dapat diklasifikasikan sebagai *white crime* dikarenakan para pelaku kriminal di dunia maya merupakan seseorang yang memahami pemakaian aplikasi internet, atau mahir pada bagian tersebut. Karena tindak kriminal ini kerap dilakukan dengan cara transnasional atau secara melewati pemisah antar negara, tindak kriminal dunia maya ini disertai dengan dua kriteria kriminal, diantara lain *white crime* dan *transnational crime*. Terdapat beberapa kasus tindak kriminal di internet (*cyber crime*) yang kerap beraksi di kalangan masyarakat di Indonesia yakni penipuan, judi *online*, penyebaran berita *hoax*, *cracking*, hingga pencurian data pribadi melalui internet.[37] Bidang keamanan komputer terus berkembang pesat karena teknologi informasi semakin mempengaruhi pola kehidupan masyarakat di Indonesia seperti bekerja, berkomunikasi, berbelanja, dan lain-lainnya. Dengan perkembangan tersebut, ancaman terhadap keamanan komputer semakin meningkat, baik ancaman fisik maupun non fisik seperti kerentanan sistem operasi, serangan jaringan, dan virus. Aspek keamanan mutlak diperlukan dalam pengaturan sistem jaringan berbasis internet. Sistem tanpa sistem keamanan yang baik seperti mengundang pencuri ke rumah kita dan membiarkan mereka mengambil semua yang kita miliki. Saat membangun sebuah sistem, berbagai kerentanan sering ditemukan di dalam sistem. Namun, itu tidak dianggap sebagai kerentanan keamanan (*hole*), sehingga dianggap kecil. Celah keamanan sekecil itu tidak kita ketahui dan digunakan oleh para pelaku kriminal untuk melakukan aksi kejahatan.[38]

Data atau Informasi pribadi yang terkait dengan penduduk dan demografi di Indonesia seperti Kartu Keluarga (KK), Nomor Induk Kependudukan (NIK), serta Kartu Tanda Penduduk Elektronik (E-KTP) merupakan bagian terpenting untuk yang harus dilindungi agar terhindar dari eksploitasi. Dari beberapa kasus yang pencurian data pribadi di Indonesia, terdapat ada banyak bentuk eksploitasi data pribadi, misalnya jual beli data, pembuatan profil data, penelitian, tujuan pemasaran, dan kegiatan spionase. Yang lebih berbahaya lagi adalah penyalahgunaan informasi pribadi untuk kegiatan kriminal seperti transaksi illegal, penipuan, pembuatan akun palsu, serta pencucian uang. Sebaiknya data atau informasi disimpan dan dilindungi dengan baik,

---

[35] 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.

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

[37] Aryyaguna, A. D. (2017). Tinjauan Kriminologis Terhadap Kejahatan Penipuan Berbasis Online. *Tidak Dipublikasikan). Universitas Hasanuddin*.

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

dikarenakan para pelaku tindak kriminal menjual data pribadi seseorang di internet adalah sebagai pendapatan bagi para pelaku tindak kriminal.[39]

Data atau informasi pribadi adalah data tentang karakteristik individu, nama, usia, alamat, pekerjaan, pendidikan, status dalam keluarga, dam jenis kelamin. Jika dilihat secara yuridis, data pribadi yang dimana telah dijelaskan berdasarkan Peraturan Pemerintah Republik Indonesia No. 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik adalah data individu khusus yang dipelihara, disimpan, dan dijaga kerahasiaan dan kebenaran. Informasi atau pribadi penduduk yang dilindungi meliputi nomor kartu keluarga, nomor induk kependudukan, tanggal lahir, informasi kesehatan, NIK ayah, NIK ibu, NIK saudara kandung dan beberapa catatan kejadian penting. Informasi atau data pribadi terkait kependudukan NIK, e-KTP, KK, serta lainnya harus benar-benar dilindungi agar tidak mudah disalahgunakan oleh para pelaku tindak pencurian data pribadi.[40]

Data atau Informasi pribadi yang tidak memiliki bentuk fisik seringkali diabaikan, terutama jika menyangkut kehidupan sosial. Orang-orang berisiko karena mereka tidak harus mempublikasikannya di Internet untuk melindungi informasi pribadi mereka dan mencegah penghancuran informasi pribadi orang lain. Ketidaktahuan dan keramahan masyarakat menjadi budaya masyarakat Indonesia juga memberikan banyak celah dalam melakukan kejahatan terkait kepemilikan informasi data pribadi. Seperti diutarakan Deputi Direktur Riset Kementerian Perhubungan, kebiasaan pemaaf masyarakat Indonesia juga menjadi sumber kecurangan yang jarang dilaporkan. Sifat toleran ini mempengaruhi banyaknya penipuan yang terjadi terutama di dunia maya. Namun, sebagian besar korban penipuan *online* justru lebih memilih diam daripada melapor ke pihak berwajib. Jika kerugian melebihi Rp. 500.000, masyarakat umum akan melaporkannya.[41]

Faktor kelalaian pada seseorang merupakan celah terbesar dari penyebab terjadinya kasus tindak pidana kejahatan pencurian data, misalnya dengan tidak membuat *password* yang mudah ditebak atau mengganti password secara berkala. Atau biarkan orang lain mengakses ponsel kita dan memberi tahu orang asing nomor telepon kita. Kekhawatiran terbesar dalam keamanan informasi saat ini adalah apa yang umumnya dikenal sebagai serangan rekayasa sosial. Serangan yang memanfaatkan kelemahan manusia. Lagi pula, pekerja TI yang paling membutuhkan keamanan walaupun masih sering terdapat kejadian kelalaian dan berbagai bentuk serangan. Apalagi masyarakat umum adalah masyarakat umum dan khususnya kurang memiliki pengetahuan ini. Selama

[39] 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.

[40] 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.

[41] Ciptohartono, C. C., & Dermawan, M. K. (2019). Pencegahan Viktimisasi Pencurian Data Pribadi. *Deviance Jurnal kriminologi*, *3*(2), 157-169.

keterlibatan manusia terlibat, kejahatan bekerja di sana dan memanfaatkan kelemahan kecerobohan, keamanan, dan kepercayaan.[42]

Jika dilihat berdasarkan penjelasan fenomena yang sudah ada terjadi di kalangan masyarakat Indonesia, maka dapat diambil kesimpulan dari faktor kasus-kasus pencurian Informasi atau data pribadi yang telah terjadi sebagai berikut:[43] a) **Kurangnya kesadaran hukum dikalangan masyarakat**. Kesadaran hukum adalah pengetahuan yang berlandaskan persoalan apa yang harus atau larangan yang tidak boleh dilakukan dalam hubungannya dengan aturan dan undang-undang yang berlaku di masyarakat di Indonesia. Saat ini, kesadaran hukum masyarakat terhadap kejahatan dunia maya masih dianggap belum memadai karena kurangnya pemahaman tentang kejahatan dunia maya baik dari segi perilaku maupun dampaknya. Tingkat pengetahuan masyarakat terhadap teknologi dan aktivitas di dunia maya juga berpengaruh penting tentang apa saja aktivitas di dunia maya. Semakin seseorang sedikit pengetahuan tentang teknologi, semakin besar kemungkinannya untuk dieksploitasi oleh para tindak kriminal. Dengan mempelajari *cybercrime*, masyarakat bertindak dalam pencegahan *cybercrime.* Tanpa pengetahuan maraknya pelaku penjahat *cyber crime* dikarenakan masyarakat tidak mengetahui apa yang telah mereka lakukan sampai pada berbagai kerugian yang akan menimpa mereka; b) **Keamanan.** Sarana yang dipakai oleh penyerang *cybercrime* umumnya lain dengan beberapa penjahat lainnya. Para pelaku kejahatan di dunia maya khususnya pencurian informasi atau data pribadi memakai peluang internet yang dapat dipakai dimanapun, seperti di area tertutup maupun terbuka. Tetapi, karena sistem proteksi pada internet masih belum bagus, setiap orang memiliki kebebasan untuk melakukan aktivitas di dunia maya tanpa mengetahui batasan yang bisa berkontribusi pada penyebaran kriminal di dunia maya; c) **Aparat Penegak Hukum.** Tidak bisa disangkal bahwasanya beberapa aparat penegak hukum mungkin masih tidak mengetahui teknik yang digunakan penjahat untuk melakukan kejahatan dunia maya. Kejahatan dunia maya Penjahat jauh lebih kuat daripada aparat penegak hukum, dan kejahatan dunia maya menjadi lebih intens di Indonesia. Cara yang bisa diambil adalah mengoptimalkan peran petugas penegak hukum yang berkualitas dan terstruktur, dengan secara pribadi sekalipun di dalam organisasi, untuk mengkonsolidasikan komunitas yang berdedikasi untuk menangani semua jenis kejahatan dunia maya. Landasan hukum tindakan aparat penegak hukum sudah ada dan kinerja setiap individu dan organisasi harus dioptimalkan. Jika tidak ada penegakan hukum teknologi informasi telah terstruktur dan terorganisir, sulit untuk menangkap para pelaku kejahatan dunia maya, karena TKP kejahatan dunia maya ini dapat bersifat lintas negara; c) **Perundang-undangan yang tidak diperbaiki.** Sekarang ini Indonesia tidak mempunyai peraturan khusus yang mengendalikan tentang kejahatan dunia maya, tetapi UU pidana dan UU ITE yang semestinya berguna, tetapi peraturan yang ada tidak berlaku. Oleh aparat penegak hukum. Kondisi tersebut

[42] *Ibid*

[43] Fadhila, A. P. (2021). Tinjauan Kriminologi Dalam Tindakan Penipuan Ecommerce Berdasar Peraturan perundang-undangan Pada Masa Pandemi Covid19 di Indonesia. *Jurnal Suara Hukum*, *3*(2), 274-299.

disebabkan karena minimnya wawasan dan keterampilan di dunia maya. Pada faktanya, sudah banyak kasus pencurian informasi dan data pribadi yang sering terjadi di kalangan masyarakat, tetapi bagaimanapun juga, sudah banyak korban kasus pencurian data yang tidak khawatir atau mengabaikannya dan tetap tidak menyimpan data pribadinya dengan baik.[44]

KESIMPULAN

Bersumber pada analisis yang usai dibahas sebelumnya, dengan itu bisa disimpulkan, yaitu informasi atau data pribadi merupakan yaitu berwujud angka, huruf, identitas diri, simbol, atau kode. Istilah informasi pribadi atau perlindungan data juga digunakan di berbagai negara. Kebijakan hukum pidana yang mengatur tentang pencurian informasi pribadi sebagai penyalahgunaan teknologi komunikasi dan tindak pidana pencurian informasi atau data pribadi belum diatur oleh berbagai hukum di Indonesia. Implementasi dalam kebijakan undang-undang perlindungan data saat ini diyakini belum berhasil. Konsep pengaturan perlindungan data pribadi menginginkan aturan yang lebih ketat dan komprehensif yang membahas perkembangan sosial budaya, ekonomi dan politik serta mendukung nilai, norma, etika dan moral dan agama, dengan harapan hukum di Indonesia tidak ketinggalan dengan kemajuan teknologi dan informasi. Berbagai negara maju telah memiliki peraturan khusus mengenai perlindungan data pribadi, namun Indonesia saat ini belum memiliki peraturan tersebut. Permasalahan seperti ini hanya diatur dalam Pasal 26 UU ITE dan beberapa peraturan lainnya. Terdapat beberapa faktor yang mendorong terjadinya tindak pidana kejahatan kasus pencurian data, mulai dari faktor aparat penegakan hukum, keamanan, dan hukum yang resmi hingga kurangnya pengetahuan tentang hukum dari masyarakat di Indonesia, yang adalah penyebab terkuat kasus tindakan kriminal pencurian data pribadi. Faktor dapat dilihat masih sering terjadi seperti lalainya seseorang dalam menjaga data pribadinya dan lamanya proses penanganan kasus pencurian data yang secara tidak langsung sebagai faktor pendukung pagi para pelaku dalam melakukan tindak pidana kejahatan pencurian data.

Teruntuk pemerintah dan Dewan Perwakilan Rakyat (DPR) perlu mengadakan evaluasi tentang yurisdiksi perlindungan hukum tentang permasalahan terkait eksploitasi data pribadi khususnya pencurian informasi atau data pribadi di internet, dan peraturan tersebut secara otomatis menciptakan kepastian hukum bagi masyarakat. Penegak hukum harus memperkuat penegakkan hukum, memastikan koordinasi antar lembaga hukum, dan dapat berperan aktif agar dapat mencegah aktivitas tindak kriminal pencurian data pribadi, berkaitan dengan hal tersebut, peneliti telah mengusulkan penetapan standar sanksi pidana jera dalam penerapannya. Teruntuk pemerintah mengetahui kejadian kasus kejahatan di bidang perlindungan informasi atau data pribadi, kita dapat melihat bahwa ada beraneka ragam penyebab yang mempengaruhi perkara tersebut. Maka dari itu, pemerintah dituntut untuk mengoptimalkan peranan strategis atau pengutamaan nasionalnya, khususnya bagi para pelaku kejahatan pencurian data pribadi. Mengingat perkembangan teknologi transaksi elektronik, pemerintah

[44] *Ibid*

dituntut untuk mensosialisasikan perlindungan informasi pribadi kepada masyarakat dan agar masyarakat dapat lebih memahami bagaimana cara melindungi informasi pribadi secara tepat dan benar. Untuk penegakan hukum yang lebih cepat dan akurat, masyarakat perlu lebih memperhatikan aktivitas di dunia maya.

DAFTAR PUSTAKA

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.

Alhakim, A., & Sofia, S. (2021). Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia. *Jurnal Komunitas Yustisia*, *4*(2), 377-385.

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

Ciptohartono, C. C., & Dermawan, M. K. (2019). Pencegahan Viktimisasi Pencurian Data Pribadi. *Deviance Jurnal kriminologi*, *3*(2), 157-169.

Dewi, S. (2016). Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia. *Yustisia Jurnal Hukum*, *5*(1), 35-53.

Disemadi, H. S. (2021). Legal Aspects Of 'Gali Lubang Tutup Lubang'in Fintech P2p Lending Business During Covid-19. *Tadulako Law Review*, *6*(2), 237-256.

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.

Disemadi, H. S., & Prasetyo, D. (2021). Tanda Tangan Elektronik pada Transaksi Jual Beli Online: Suatu Kajian Hukum Keamanan Data Konsumen di Indonesia. *Wajah Hukum*, *5*(1), 13-20.

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.

Elsinda, E. (2014). Aspek Hukum Perlindungan Data Pribadi di Dunia Maya. *Jurnal Gema Aktualita*, *3*(2).

Fadhila, A. P. (2021). Tinjauan Kriminologi Dalam Tindakan Penipuan Ecommerce Berdasar Peraturan perundang-undangan Pada Masa Pandemi Covid19 di Indonesia. *Jurnal Suara Hukum*, *3*(2), 274-299.

Haris, M. T. A. R., & Tantimin, T. (2022). Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan Artificial Intelligence Di Indonesia. *Jurnal Komunikasi Hukum (JKH)*, *8*(1), 307-316.

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

Ketaren, E. (2016). Cybercrime, Cyber Space, dan Cyber Law. *Jurnal Times*, *5*(2), 35-42.

Lumenta, C. Y., Kekenusa, J. S., & Hatidja, D. (2012). Analisis jalur faktor-faktor penyebab kriminalitas di kota Manado. *Jurnal Ilmiah Sains*, *12*(2), 77-83.

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.

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.

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.

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

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

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik. *Jurnal HAM*, *11*(2), 285-299.

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. In *Proceeding of Conference on Law and Social Studies*, 16-27.

Sinaga, E. M. C., & Putri, M. C. (2020). Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *9*(2), 237.

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.

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *SASI*, *27*(1), 38-52.

Tampubolon, K. E. A. (2019). Perbedaan Cyber Attack, Cybercrime, dan Cyber Warfare. *Jurist-Diction*, *2*(2), 539-554.

Tan, D. (2021). Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, *8*(8), 2463-2478.

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.

Winarso, T., Disemadi, H. S., & Prananingtyas, P. (2020). Protection Of Private Data Consumers P2P Lending As Part Of E-Commerce Business In Indonesia. *Tadulako Law Review*, *5*(2), 206-221.

Witasari, A., & Setiono, A. (2016). Perlindungan Hukum Pengguna Jasa Electronic Banking (E-Banking) di Tinjau dari Perspektif Hukum Pidana di Indonesia. *Jurnal Pembaharuan Hukum*, *2*(1), 126-137.

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences (BECOSS) Journal*, *1*(1), 147-154.