Jurnal Legal Dialogica
Volume I Issue 2 Tahun 2026

Melawan Tindak Pidana Pencurian Identitas Di Era Digital

Muhammad Abid Athallah[1], Hardianto Djanggi [2], Mustamin Mustamin[3]

[123]Fakultas Hukum Universitas Muslim Indonesia, Indonesia

Email Koresponden : hardianto.djanggih@umi.ac.id

Abstrak: Penelitian ini bertujuan untuk mengetahui dan memahami bagaimana pengaturan sanksi hukum terkait tindak pidana siber pencurian data berupa identitas, serta untuk mengetahui dan memahami bagaimana bentuk perlindungan hukum bagi korban tindak pidana siber pencurian data berupa identitas di Indonesia. Perkembangan teknologi informasi dan komunikasi yang semakin pesat telah memberikan kemudahan dalam berbagai aspek kehidupan masyarakat, namun di sisi lain juga menimbulkan berbagai bentuk kejahatan baru di ruang digital, salah satunya adalah pencurian data pribadi berupa identitas. Tindak pidana ini dapat menimbulkan kerugian yang besar bagi korban, baik secara materiil maupun immateriil, seperti penyalahgunaan identitas untuk tindakan penipuan, akses ilegal terhadap rekening keuangan, pencemaran nama baik, hingga pelanggaran hak privasi.

Metode penelitian yang digunakan dalam penelitian ini adalah penelitian hukum normatif dengan pendekatan perundang-undangan (statute approach) dan analisis kualitatif-deskriptif. Penelitian dilakukan dengan mengkaji berbagai peraturan perundang-undangan yang berkaitan dengan perlindungan data pribadi, tindak pidana siber, dan perlindungan korban, serta didukung oleh bahan hukum sekunder berupa literatur, jurnal ilmiah, dan dokumen hukum lainnya.

Kebaruan penelitian ini terletak pada analisis yuridis pasca pengesahan Undang-Undang Perlindungan Data Pribadi (UU PDP) sebagai tonggak penting dalam penguatan hak privasi dan perlindungan data pribadi di Indonesia.

Kata Kunci: Tindak Pidana Siber, Pencurian Data, Identitas

Abstract*:* This study aims to identify and understand the regulation of legal sanctions related to cybercrime involving identity data theft, as well as to examine and understand the forms of legal protection available for victims of cybercrime involving identity data theft in Indonesia. The rapid development of information and communication technology has provided convenience in various aspects of social life; however, on the other hand, it has also given rise to various new forms of crime in the digital sphere, one of which is the theft of personal identity data. This criminal act can cause significant losses to victims, both materially and immaterially, such as the misuse of identity for fraudulent activities, illegal access to financial accounts, defamation, and violations of privacy rights.

The research method used in this study is normative legal research employing a statutory approach and qualitative-descriptive analysis. The research was conducted by examining various laws and regulations related to personal data protection, cybercrime, and victim

protection, supported by secondary legal materials in the form of literature, scientific journals, and other legal documents.

The novelty of this research lies in its juridical analysis following the enactment of the Personal Data Protection Law (PDP Law), which serves as an important milestone in strengthening privacy rights and personal data protection in Indonesia.

Keywords: Cyber Crime, Data Theft, Identity

PENDAHULUAN

Cybercrime (Tindak Pidana Siber) adalah kejahatan yang memanfaatkan teknologi computer dan jaringan internet, salah satunya adalah *Data Theft* (Pencurian Data).[1] Pencurian Data merupakan tindakan memperoleh data orang lain secara ilegal baik untuk digunakan sendiri ataupun diberikan kepada pihak lain.[2] Pencurian Data merupakan masalah nyata yang dihadapi oleh masyarakat di era modern saat ini, diperlukan keseriusan dalam menyikapi fenomena ini karena data yang telah dicuri dapat disalah gunakan pihak – pihak yang tidak bertanggung jawab yang bisa berdampak kerugian bagi korban maupun organisasi. Salah satu bentuk dari penyalahgunaan atas data yang telah dicuri umumnya digunakan untuk melakukan tindakan penipuan berskala besar seperti Pencurian Identitas (Identity Theft).[3] Identity Theft (Pencurian Identitas) atau penyalahgunaan identitas adalah fenomena dimana seseorang menggunakan informasi pengenal pribadi orang lain, seperti nama, nomor pengenal, atau nomor kartu kredit, tanpa izin untuk melakukan penipuan atau kejahatan lainnya. Kejahatan ini dilakukan dengan cara mencuri informasi pribadi milik korban terlebih dahulu untuk kemudian disalahgunakan dalam berbagai aktivitas ilegal seperti penipuan (fraud), pemerasan, pembobolan akun, hingga pencucian uang. Pencurian data identitas tidak hanya merugikan korban secara finansial, tetapi juga mengancam privasi, keamanan, dan kepercayaan publik terhadap keamanan sistem digital.[4]

Insiden ini bukan lagi menjadi hal baru di Indonesia. Mengutip artikel pemberitaan yang dibawakan oleh media Liputan 6 berdasarkan informasi yang diperoleh dari *National Cyber Security Index* (NCSI) menyatakan bahwa indeks terkait keamanan siber Indonesia di masa tahun 2022 memperoleh angka 38,96 dari 100. Dimana Indonesia menempati

posisi ke tiga di antara seluruh negara-negara yang tergabung dalam G20. Dan jika di amati secara Global Indonesia di masa tahun 2022 menempati posisi ke 83 dari total 160 negara yang turut masuk dalam laporan tersebut. Dalam data yang telah disajikan dapat kita nilai bahwa pentingnya peran pemerintah dalam menangani tindak pidana siber di Indonesia dalam aspek cyberSecurity.[5] Identitas adalah Informasi pribadi dan merupakan ranah vital yang tidak boleh sembarangan untuk di publikasiakan, dan maka dari itu menjadikannya memiliki nilai yang sangat penting bukan hanya bagi pemiliknya tetapi juga bagi pelaku – pelaku kejahatan yang bisa merasakan manfaat dari tindakan kejahatannya menggunakan data dan infromasi orang lain. Mengingat akibat yang di timbulkan dari pencurian identitas bisa sangat buruk, yang mana tidak sebatas berdampak pada kerugian secara finansial, tetapi juga mampu merusak reputasi dan berdampak pada psikologis yang kemudian berujung terganggunya ketenangan mental dan kesejahteraan korban. Maka dari itu, perlu adanya kesadaran mengenai pentingnya perlindungan atas identitas dan informasi pribadi.[6]

METODE PENELITIAN

Tipe penelitian yang digunakan adalah tipe penelitian normatif. Pendekatan ini bertujuan untuk mendeskripsikan dan menganalisis peraturan hukum yang ada. Bahan hukum dalam penelitian hukum normatif meliputi bahan hukum primer mencakup Undang-undang nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik. Dan bahan hukum sekunder yang terdiri dari kajian pustaka yang mencakup buku, jurnal, artikel, dan dokumen hukum yang relevan dengan topik penelitian.

PEMBAHASAN

Pengaturan Sanksi Hukum Terhadap Tindak Pidana Siber Pencurian Data Berupa Identitas

1. **Undang-undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi**

Undang – Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (UU PDP) mulai berlaku di Indonesia sejak bulan Oktober Tahun 2022. Undang – undang ini berlaku untuk semua pihak termasuk lembaga publik dan organisasi internasional yang melakukan tindakan hukum di wilayah hukum Negara Kesatuan Republik Indonesia.[7] Undang – undang ini dibentuk dengan tujuan melindungi hak privasi masyarakat dan memastikan bahwa nilai perlindungan data pribadi diakui dan dihormati. Selain itu dengan dibentuknya aturan ini juga diharapkan dapat meningkatkan kemampuan negara dalam melindungi data pribadi. serta membangun kesadaran masyarakat akan pentingnya perlindungan data pribadi mengingat banyaknya perubahan dan masalah yang kian timbul terkait permasalahan data pribadi.[8]

Menurut Undang – Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, terdapat beberapa tindakan yang tidak diperbolehkan untuk dilakukan, seperti memperoleh, mengungkapkan, menggunakan data pribadi yang bukan miliknya dan membuat data palsu. Bagi pihak yang melanggar aturan tersebut dapat dijerat dengan sanksi pidana, berupa penjara atau denda.[7] Undang - Undang Perlindungan Data Pribadi (UU PDP) secara jelas menyatakan adanya sanksi hukum yang dapat menjerat bagi pihak manapun yang melakukan pelanggaran terkait Data Pribadi.[9] Adapun sanksi tersebut termuat dalam Pasal 67 dan Pasal 68 berikuta:

a. Pasal 67 Ayat (1), (2) dan (3)
   (1) Pasal 67 Ayat 1 berbunyi: “Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah)”.
   (2) Demikian juga diatur dalam Pasal 67 Ayat 2 berbunyi: “Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara

paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah)".

(3) Pasal 67 Ayat 3: "Setiap Orang yang dengan senqaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp 5.000.000.000,00 (lima miliar rupiah)".

b. Pasal 68

Pasal 68 Undang – Undang Perlindungan Data Pribadi berbunyi "setiap orang yang dengan sengaja membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain sebagaimana yang dimaksud dalam pasal 66 dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau pidana denda paling banyak Rp6.000.000.000,00 (enam miliar rupiah)".

Selain dikenakan sanksi pidana sebagaimana yang diatur dalam ketentuan Pasal 67 dan Pasal 68, para pelanggar atau pelaku juga kemungkinan dapat dikenakan pidana tambahan sebagaimana yang tercantum dalam Pasal 69 Undang – Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022 yang berbunyi: "selain dijatuhi pidana sebagaimana dimaksud dalam pasal 67 dan pasal 68 juga dapat dijatuhi pidana tambahan berupa perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian".[5] Dalam pasal ini secara jelas tertulis bahwa pidana tambahan yang dimaksud berupa perampasan keuntungan dan/atau harta kekayaan yang diperoleh pelaku dari hasil tindakan ilegal serta pembayaran ganti kerugian. Jika pelaku tindakan ini bukan perorangan yang dalam artian dilakukan oleh suatu perusahaan maka sanksi dapat dikenakan kepada manajer, pemegang kontrol, pihak yang memberi instruksi. pemilik manfaat, dari perusahaan yang bersangkutan. Selain itu sanksi administratif juga diterapkan dalam Undang – Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (UU PDP). Diterapkannya Sanksi administratif ini dalam UU PDP adalah sebagai bentuk peringatan terhadap pemrosesan data pribadi yang tidak memiliki dasar, dan sanksi

ini juga diterapkan untuk pelanggaran yang berkaitan dengan kesesuaian tujuan pengolahan data pribadi, serta pelanggaran dalam memperoleh persetujuan dari subjek data pribadi. Sanksi administratif yang diberikan bisa berbentuk peringatan tertulis, penghentian sementara aktivitas pemrosesan data, hingga denda administratif yang signifikan. Sanksi ini secara jelas diatur dalam Undang – Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Bentuk – bentuk sanksi administratif sesuai Pasal 57 meliputi:

a. Peringatan lisan atau tertulis, kepada pengelola data pribadi yang telah melakukan pelanggaran
b. Penghentian sementara kegiatan pemrosesn data pribadi, yang tidak sesuai dengan aturan yang telah ditetapkan
c. Penghapusan atau pemusnahan Data Pribadi yang telah diproses secara ilegal dan/atau
d. Denda administratif paling tinggi 2 (dua) persen dari pendapatan tahunan atau penerimaan tahunan terhadap variable pelanggaran.

Pemberian sanksi administratif bermaksud untuk memberi efek jera kepada pelanggar dan memastikan bahwa pengelola data pribadi lebih serius dan berhati – hati dalam menjalankan tugasnya dengan penuh tanggungjawab di dalam mengelola data pribadi. Adanya penerapan sanksi administratif ini juga dimaksudkan dengan harapan membuat pengelolaan data pribadi dapat berjalan dengan lebih aman serta dapat dipercaya. Agar masyarakat lebih merasa aman dan nyaman ketika melakukan aktivitas diruang digital.[7]

2. **Undang-undang Nomor 1 Tahun 2024 perubahan kedua atas undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik**

Selain diatur dalam undang-undang perlindungan data pribadi (UU PDP) pengaturan sanksi hukum terkait tindak pidana siber pencurian data berupa identitas juga diatur didalam Undang – Undang Nomor 1 Tahun 2024 yang merupakan perubahan kedua atas Undang – Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi

Elektronik (UU ITE). UU ITE ini mengatur terkait "perbuatan yang dilarang untuk dilakukan melalui media/system elektronik", serta membebankan sanksi hukum kepada individu yang terbukti melakukan tindak pidana. UU ITE secara jelas menyatakan adanya sanksi hukum yang dapat menjerat bagi pihak manapun yang melakukan pelanggaran terkait Data Pribadi.[10] Menurut UU ITE sebagaimana yang tercantum dalam Bab 7 terdapat beberapa perbuatan yang dilarang salah satu diantaranya adalah, larangan bagi setiap orang yang secara sengaja dan tanpa hak mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun. Sebagaimana yang telah diatur dalam pasal 30 Ayat (1), Yang mana dalam hal ini Pasal 46 Ayat (1) UU ITE mengancam pelaku dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (eman ratu juta rupiah).Selain itu dalam UU ITE korban juga berhak dalam mengajukan gugatan secara perdata atau ganti rugi terhadap pelaku sesuai dengan ketentuan Undang - Undang Nomor 1 Tahun 2024 perubahan kedua atas Undang - Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, pada Pasal 26 Ayat 2 yang berbunyi “setiap orang yang yang mengakses data pribadi orang lain tanpa persetujuan pihak yang mempunyai data pribadi, maka pihak yang di rugikan dapat melakukan gugatan atas kerugian yang di timbulkan berdasarkan hukum yang berlaku positif”. Gugatan yang diajukan terhadap pelaku termasuk kategori PMH atau disebut Perbuatan melawan hukum, Sesuai dengan pasal 1365 KUHPerdata.[11]

Dengan adanya sanksi hukum dalam pengaturan terkait perlindungan data pribadi dan UU ITE diharapkan mampu menjadi pelindung dalam menjaga hak privasi warga negara dan menjerat siapapun pihak – pihak yang melanggar hak privasi individu – individu yang lain. Hal tersebut merupakan wujud nyata hadirnya negara dalam memberikan keadilan bagi warga negara. Dengan memberikan sanksi pidana dengan bentuk pidana penjara dan pidana denda dengan nominal yang banyak bertujuan memberikan dampak jera kepada pelanggar yang melakukan tindakan penyalahgunaan data pribadi untuk tidak mengulangi perbuatan yang sama. Hadirnya peraturan ini juga bertujuan untuk menunjang serta menjamin keamanan aktivitas

digital masyarakat Indonesia yang rentan akan penyebarluasan data pribadi serta menjamin adanya perlindungan hukum.[5]

Perlindungan Hukum Terhadap Korban Tindak Pidana Siber Pencurian Data Berupa Identitas

Di dalam konstitusi negara Indonesia, negara melindungi data pribadi dan privasi individu sesuai dengan apa yang tertuang dalam Undang – Undang Dasar Negara Indonesia Tahun 1945 pada Pasal 28G ayat 1 yang berbunyi "semua warga negara Indonesia berhak mendapatkan perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang di bawah kekuasaannya, serta memiliki hak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi manusia". Selain itu di dalam Pasal 1 Ayat 2 Undang – Undang Nomor 27 Tahun 2022 juga menjelaskan bahwa data pribadi wajib untuk dilindungi guna menjamin keamanan hak – hak konsistensi subjek data pribadi. Artinya dapat kita ketahui bahwa hal yang terkait data pribadi merupakan hal krusial yang wajib mendapat perhatian berbentuk perlindungan dari negara serta mempunyai kepastian hukum untuk memperoleh hak dan kewajiban yang diatur oleh peraturan perundang – undangan.[11]

Indonesia sebagai negara hukum tentunya mempunyai kewajiban dalam melindungi warga negaranya secara menyeluruh dari tindakan kejahatan yang merugikan, sebagai bentuk respon atas apa yang telah diamanatkan dalam konstitusi negara yang menyatakan "setiap warga negara berhak mendapatkan perlindungan hukum". Perlindungan hukum dapat diartikan sebagai perlindungan oleh hukum atau perlindungan dengan menggunakan pranata dan sarana hukum.[9]

Menurut R. La porte dalam Journal of Financial Economics, bentuk-bentuk perlindungan hukum yang menggunakan pranata dan sarana penegakan hukum yang diberikan oleh negara memiliki dua karakteristik, yaitu perlindungan hukum yang bersifat represif dan perlindungan hukum bersifat preventif. Perlindungan hukum yang bersifat Represif adalah bentuk perlindungan hukum yang diwujudkan melalui

sanksi dan aturan, dengan tujuan menyelesaikan permasalahan yang telah terjadi, melalui lembaga-lembaga negara berwenang dalam penegakan hukum seperti polisi, jaksa, pengadilan. Sementara itu, Perlindungan yang bersifat Preventif adalah bentuk perlindungan hukum dengan tujuan mencegah sebelum terjadinya pelanggaran. Hal ini terdapat dalam peraturan perundang - undangan dengan maksud untuk mencegah agar pelanggaran tidak terjadi serta berfungsi sebagai rambu – rambu atau batasan dalam melakukan suatu kewajiban.[5]

Di negara Indonesia perlindungan hukum terkait data atau informasi pribadi dapat dilakukan dengan berbagai bentuk baik represif maupun preventif. Adapun cara – cara yang diberikan oleh negara dalam memberi perlindungan hukum untuk mengatasi permasalahan terkait data dan informasi pribadi di Indonesia sebagai berikut:

1. Perlindungan *Represif*

   Perlindungan hukum represif adalah salah satu bentuk perlindungan hukum yang diberikan kepada korban apabila tindakan pelanggaran telah terjadi. Bentuk perlindungan ini bersifat reaktif, yang mana bertujuan memberikan rasa keadilan bagi korban, dan memberi sanksi terhadap pelaku sebagai bentuk pertanggungjawaban hukum. Adapun teori Dalam kerangka pemikiran teori keadilan retributif yang dikemukakan oleh John Rawls, 1971 dalam (Rosel Denis, et al. 2025), perlindungan represif berfungsi sebagai upaya menegakkan keseimbangan moral dan hukum di masyarakat dengan memastikan bahwa setiap pelaku kejahatan mendapatkan ganjaran yang setimpal atas perbuatannya, sementara korban memperoleh pemulihan atas kerugiannya. Perlindungan represif ini penting mengingat tidak semua upaya pencegahan (preventif) dapat mengatasi kejahatan pencurian data pribadi. Maka dari itu mekanisme hukum yang efektif diperlukan guna memberikan rasa keadilan dan kepastian hukum.[12]

   Bentuk perlindungan hukum secara represif terkait data pribadi di Indonesia diberikan oleh negara dalam bentuk aturan dan sanksi pidana sebagaimana diatur dalam peraturan perundang – undangan yang relevan dengan fenomena terkait

keamanan data dan informasi pribadi. Adapun hukum yang mengatur data pribadi di Indonesia tertuang dalam Undang - Undang No.27 tahun 2022 Tentang Perlindungan Data pribadi (UU PDP), dan Undang – undang Nomor 1 Tahun 2024 perubahan kedua atas Undang – undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE).[13]

Melalui regulasi tersebut korban tindak pidana pencurian data pribadi dapat melaporkan tindakan tersebut sebagai perbuatan tindak pidana atau menggugat secara perdata dengan cara melaporkan tindakan tersebut kepada pihak yang berwajib atau bisa dengan meminta bantuan kepada lembaga bantuan hukum atau advokat. Pelaku tindakan tersebut dapat dijerat dengan sanksi pidana sebagaimana dengan ketentuan yang diatur dalam pasal 67 Undang - Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi berbunyi "Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah)". Dalam pasal ini secara eksplisit menjelaskan bahwa larangan keras terhadap pencurian, dan pengumpulan data pribadi yang bukan hak nya di larang dan akan terkena pidana. Selain itu pasal, pasal 67 ayat 3 Undang-undang Nomor 27 Tahun 2022 Perlindungan Data Pribadi berbunyi "Setiap Orang yang dengan senqaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp 5.000.000.000,00 (lima miliar rupiah). Dalam pasal ini menjelaskan juga bahwa tindakan dari hasil pengumpulan data pribadi lalu dipergunakan untuk keuntungan diri sendiri dan orang lain dilarang dan bisa dikenakan pidana penjara serta denda.[14]

Selain dengan menempuh jalur pidana, korban juga dapat menuntut ganti rugi dengan mengajukan gugatan perdata. Pada penjelasan Undang - Undang Nomor 1

Tahun 2024 perubahan kedua atas Undang – Undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik, pada Pasal 26 Ayat 2 menyatakan ”Setiap orang yang yang mengakses data pribadi orang lain tanpa persetujuan pihak yang mempunyai data pribadi, maka pihak yang di rugikan dapat melakukan gugatan atas kerugian yang di tumbulkan berdasarkan hukum yang berlaku positif. Perlindungan ini diberikan didasarkan oleh asas tanggung jawab perdata yang diatur dalam Pasal 1365 KUHPerdata mengenai perbuatan melawan hukum (onrechtmatige daad). Dalam konteks ini korban bisa melayangkan gugatan perdata kepada pelaku dengan tuntutan agar pelaku melakukan pembayaran ganti rugi atas kerugian materiil dan/atau immateriil yang muncul di akibatkan tindakan pencurian data pribadi. Gugatan perdata ini dikatakan perlu mengingat akibat yang ditimbulkan dari tindakan pencurian data pribadi tidak hanya merugikan korban secara finansial, tetapi juga bisa berakibat pada rusaknya reputasi, kerugian psikologis, hingga hilangnya peluang kerja atau bisnis di masa depan. Adapun teori ganti rugi yang mendukung perlindungan represif ini yang dikemukakan oleh Salim HS, 2011 dalam (Rosel Denis, et al. 2025) yang mana menekankan bahwa korban yang mengalami kerugian akibat perbuatan melawan hukum berhak mendapatkan pemulihan penuh agar berada dalam posisi yang sama seperti sebelum peristiwa tersebut terjadi. Oleh karena itu, mekanisme gugatan perdata menjadi salah satu instrumen penting dalam memberikan keadilan bagi korban tindak pidana pencurian data pribadi.[5]

2. Perlindungan *Preventif*

Perlindungan hukum Preventif adalah salah satu bentuk perlindungan hukum yang diberikan sebelum terjadinya tindakan pelanggaran. Tujuan utama dari bentuk perlindungan ini yaitu mencegah agar insiden pelanggaran atau penyalahgunaan terkait data pribadi tidak terjadi. Menurut Sudikno Mertokusumo, 2013 dalam (Rosel Denis, et al. 2025). perlindungan preventif memiliki tugas penting dalam menjamin keamanan kepada individu dengan menekankan kewajiban penyedia

layanan atau pengendali data untuk bertanggung jawab secara proaktif terhadap kemungkinan terjadinya tindakan yang dapat merugikan pihak lain.[14]

Bentuk perlindungan hukum secara preventif terkait data pribadi di Indonesia diberikan oleh negara dalam wujud pengambilan langkah – langkah pencegahan, seperti melakukan Sosialisasi, edukasi, pencegahan terjadi nya pencurian data pribadi dan Penyuluhan Hukum mengenai pencurian data pribadi. Pengambilan langkah edukasi, dan sosialisasi kepada masyarakat adalah salah satu tindakan penting dalam hal pencegahan. Edukasi menjadi hal penting mengingat tingkat literasi digital mayoritas masyarakat Indonesia tergolong rendah, yang mana membuat masyarakat tidak sepenuhnya memahami akan potensi ancaman yang muncul akibat pencurian data pribadi. Rendahnya tingkat literasi digital mayoritas masyarakat Indonesia dapat membuat ruang besar bagi tindak pidana yang berkaitan dengan pencurian data pribadi dalam mengelabui masyarakat melalui berbagai modus yang tidak disadari seperti phising, malware, atau teknik social engineering lainnya. Maka dari itu, pemerintah, melalui kementerian terkait seperti Kementerian Komunikasi dan Informatika (KOMINFO), bersama lembaga non-pemerintah dan sektor swasta, memiliki peran strategis dalam melakukan kampanye edukasi publik secara masif dan berkesinambungan. Kampanye edukasi ini meliputi penyuluhan tentang pentingnya menjaga kerahasiaan data pribadi, mengenali potensi ancaman, memahami hak – hak individu sebagai subjek data, serta rangkaian cara dalam mengamankan data pribadi pada platform digital. Prayoga dan Suharnoko (2022) dalam penelitiannya menunjukkan peningkatan literasi digital masyarakat secara signifikan dapat mengurangi risiko terjadinya kejahatan siber, termasuk pencurian data pribadi.[5]

Selanjutnya pengambilan langkah Penetapan regulasi, dan standar keamanan. Perlindungan preventif dalam konteks ini direalisasikan dengan membebankan kewajiban hukum kepada penyelenggara sistem elektronik dan pengendali data pribadi untuk menerapkan standar keamanan tertentu dalam pengelolaan data. UU PDP (2022) secara jelas mengatur bahwa setiap pengendali data perlu mengambil

tindakan – tindakan teknis dan organisasi yang diperlukan untuk menjaga data pribadi dari ancaman penyalahgunaan, akses ilegal, dan kebocoran data. Standar keamanan ini meliputi penerapan enkripsi data, penggunaan sistem autentikasi ganda, pembatasan akses berdasarkan prinsip least privilege, hingga penerapan firewall dan sistem deteksi intrusi (IDS/IPS). Menurut Nurul Qamar (2023), penguatan standar keamanan teknis melalui regulasi yang ketat dapat menjadi compliance driver bagi para pengendali data untuk meningkatkan tata kelola keamanan data mereka secara lebih serius. Langkah audit, merupakan salah satu langkah preventif yang tidak kalah penting dalam mencegah tindak pidana ini. Audit dilakukan guna memastikan bahwa penyelenggara sistem elektronik sudah menerapkan standar keamanan sesuai dengan ketentuan yang berlaku. Pelaksanaan audit wajib dilaksanaan secara berulang dan independen agar hasil audit yang diperoleh bersifat objektif, sehingga kemudian dapat digunakan sebagai dasar untuk melakukan pembenahaan terkait kebijakan keamanan data. Selain audit, pengawasan aktif dari otoritas perlindungan data, yaitu Lembaga Pengawas Perlindungan Data Pribadi sebagaimana yang sudah diamanatkan oleh UU PDP, menjadi instrumen penting untuk mencegah pelanggaran data. Pengawasan ini bisa dilakukan lewat pemeriksaan rutin pemantauan aktivitas pemrosesan data, serta mekanisme pelaporan insiden kebocoran data secara transparan. Sebagaimana yang dikemukakan oleh Warren dan Brandeis dalam teori The Right to Privacy, perlindungan privasi diperlukan adanya intervensi negara lewat regulasi dan pengawasan yang efektif untuk mencegah dominasi penyalahgunaan kekuasaan oleh pengendali data terhadap individu sebagai subjek data.[14] prtlindungan hukum secara *represif* dan *preventif* pada dasarnya memiliki tujuan yang sama yaitu melindungi korban dari tindaka kejahatan terkait data pribadi aan tetapi efektivitas dari perlindungan tersebut ditentukan dari seberapa baik kerjasama dan koordinasi dari berbaigai pihak. Baik itu aparat penegek hukum, dan penyedia layanan. Agar memastikan tindakan pelanggaran terkait kejahatan ini dapat degera di tindak lanjuti. [15]

KESIMPULAN

Pengaturan sanksi hukum terhadap Tindak Pidana Siber Pencurian Data Berupa Identitas diatur dalam UU No 27 Tahun 2022 (UU PDP) dan UU No 1 Tahun 2024 (UU ITE). Perlindungan hukum bagi korban Tindak Pidana Siber Pencurian Data Berupa Identitas diberikan oleh negara dengan bentuk *represif* atau sebagai upaya menyelesaikan konflik, dan bentuk *preventif* sebagai upaya mencegah.

REFERENSI

[1] A. V. Maramis, M. Doodoh, and M. L. Lambonan, "Maramis et al. (2025)_Daffa Nasywan Islamy," *Lex Privatum*, vol. 14, no. 5, 2025.

[2] R. Fiddiyansyah, Izra Noor Zahara Aliya, and Moh Azzam Priyanto, "Dampak Identity Theft Berdasarkan Artikel Berita Dan Crawling Data Sentimen Twitter," *Prosiding Seminar Nasional Teknologi dan Sistem Informasi*, vol. 3, no. 1, pp. 629–638, 2023, doi: 10.33005/sitasi.v3i1.399.

[3] Y. Otniel Purba and A. Mauluddin, "Kejahatan Siber dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi Tentang Potensi Pencurian Data Online," *JCIC : Jurnal CIC Lembaga Riset dan Konsultan Sosial*, vol. 5, no. 2, pp. 55–66, 2023, doi: 10.51486/jbo.v5i2.113.

[4] D. Wira Pramudya and H. Yusuf, "Pencurian Data Identitas Sebagai Kejahatan Cyber Related Crime: Tinjauan Kriminologis Atas Kasus Pencurian Data Pada Akun Marketplace Identity Data Theft as a Cyber Crime Related Crime: A Criminological Review of Marketplace Account Data Theft Cases," *Jurnal Intelek Insan Cendikia*, pp. 13469–13478, 2025.

[5] Diyu Sulaeman and Anyelir Puspa Kemala, "Analisis Hukum terhadap Tindak Pidana Pencurian Identitas di Indonesia," *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora*, vol. 3, no. 2, pp. 133–148, 2025, doi: 10.59246/aladalah.v3i2.1258.

[6] H. H. Rifai and A. U. I. Hosnah, "Tinjauan Yuridis terhadap Tindak Pidana Pencurian Identitas di Bawah Ketentuan KUHP," vol. 8, pp. 17000–17004, 2024.

[7] Shafa Salsabila and Sidi Ahyar Wiraguna, "Pertanggungjawaban Hukum atas Pelanggaran Data Pribadi dalam Perspektif Undang-Undang Pelindungan Data Pribadi Indonesia," *Konsensus : Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi*, vol. 2, no. 2, pp. 145–157, 2025, doi: 10.62383/konsensus.v2i2.736.

[8] D. E. Mahameru, A. Nurhalizah, A. Wildan, M. Haikal, and M. H. Rahmadia, "Implementasi Uu Perlindungan Data," *Jurnal Esensi Hukum*, vol. 5, no. 20, pp. 115–131, 2023.

[9] Evelyn Angelita Pinondang Manurung, "TINJAUAN YURIDIS PERLINDUNGAN DATA PRIBADI BERDASARKAN UU NOMOR 27 TAHUN 2022," *Jurnal Hukum Saraswati*, vol. Volume. 04, pp. 139–148, 2022.

[10] N. Faisal, A. Aswari, and M. A. Ilham, "Penegakan Hukum Terhadap Eksistensi Tindak Pidana Pemalsuan Identitas di Era Digital," *Legal Dialogica*, vol. 1, no. 1, pp. 1–19, 2025.

[11] A. Nur Luthiya, B. Irawan, and R. Yulia, "Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi," *Jurnal Hukum Pidana dan Kriminologi*, vol. 2, no. 2, pp. 14–29, 2021, doi: 10.51370/jhpk.v2i2.43.

[12] S. Setiawan and N. Fatmawati O, "Urgensi Perlindungan Identitas Anak Melalui Media Sosial," *AKADEMIK: Jurnal Mahasiswa Humanis*, vol. 4, no. 3, pp. 700–712, 2024, doi: 10.37481/jmh.v4i3.977.

[13] A. D. Akmal and S. Royal, "URGENSI PERLINDUNGAN HUKUM BAGI KORBAN TINDAK PIDANA KEJAHATAN TEKNOLOGI INFORMASI," *Journal of Science and Social Research*, vol. 4307, no. August, pp. 39–46, 2019.

[14] I. Salsabila kiasatina, O., Wulandari, L., & Amin, "Perlindungan Hukum terhadap Korban Tindak Pidana Pencurian Data Pribadi," *Journal Parhesia*, vol. 03 No.1, M, no. 1, pp. 1–15, 2025.

[15] A. S. Idriansyah1 and N. Afifah2, "Perlindungan Hukum Terhadap Korban Cyber Crime di Indonesia dalam Aliran Hukum Pada Kasus Pencurian Data Pribadi," vol. 2, no. 4, pp. 463–469, 2024.