

## Analisis Hukum terhadap Tindak Pidana Pencurian Identitas di Indonesia

Diyu Sulaeman<sup>1\*</sup>, Anyelir Puspa Kemala<sup>2</sup>

<sup>1,2</sup> Sekolah Tinggi Ilmu Hukum IBLAM, Indonesia

[\\*vdiyus22@gmail.com](mailto:*vdiyus22@gmail.com)<sup>1</sup>

[\\*Ladieslawyer99@gmail.com](mailto:*Ladieslawyer99@gmail.com)<sup>2</sup>

Alamat: Jl. Poltangan Raya No.6, RT.3/RW.5 Tanjung. Barat., Kec. Jagakarsa, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12530

**Abstract** *The rapid development of technology has led to the emergence of new crimes, one of which is the theft of personal data. Crimes of personal data theft in Indonesia often occur every year, this is due to weak supervision and lack of public education regarding personal data protection, especially according to data from the Ministry of Communication and Information, there are still many regional communities who still do not fully understand digitalization regarding data protection. In the PDP regulation, there are derivative regulations that have not been made by the government, which makes the effectiveness of handling personal data theft still not optimal. From this, problems are obtained, namely how the mode of crime of personal data theft and the extent to which the government prepares to educate the digital community and how legal protection for victims applies in Indonesia. With these two problems, the research method used is juridical normative research. The results of this method show that the perpetrators without asking permission can obtain the personal data of the victims through social media, illegal online loans and lottery scams. In Indonesia itself there is legal protection that regulates, namely in Law. No. 27 of 2022 concerning personal data protection, although the PDP regulation itself creates a new task for the government to make its regulatory delegation..*

**Keywords** *Fraud mode, Legal protection, Theft of personal data.*

**Abstrak.** Perkembangan teknologi yang begitu pesat membuat tindakan kejahatan baru bermunculan, salah satu kejahatan yang masif ialah pencurian data pribadi. Tindak kejahatan pencurian data pribadi di Indonesia sering terjadi setiap tahun nya, hal ini disebabkan lemahnya pengawasan dan masyarakat kurang edukasi mengenai perlindungan data pribadi, terlebih menurut data dari kominfo masih banyak masyarakat daerah yang masih belum mengerti sepenuhnya digitalisasi mengenai perlindungan data nya. Dalam regulasi PDP terdapat peraturan turunan yang belum dibuat pemerintah yang mana keefektifan penanganan pencurian data pribadi masih belum maksimal. Dari hal tersebut didapatkan permasalahan yakni bagaimana modus kejahatan pencurian data pribadi serta sejauh mana persiapan pemerintah mengedukasi masyarakat digital dan bagaimana perlindungan hukum bagi korban yang berlaku di Indonesia. Dengan adanya dua permasalahan tersebut, adapun metode penelitian yang digunakan yakni penelitian normative yuridis. Didapatkan hasil dari metode tersebut bahwa pelaku tanpa meminta izin dapat mendapatkan data pribadi para korban melalui media sosial, pinjaman online ilegal dan undian penipuan. Di Indonesia sendiri terdapat perlindungan hukum yang mengatur yaitu dalam UU. No. 27 tahun 2022 tentang perlindungan data pribadi, walaupun Dalam regulasi PDP sendiri membuat tugas baru bagi pemerintah untuk membuat delegasi peraturannya.

**Kata kunci:** Modus Penipuan, Pencurian Data Pribadi, Perlindungan Hukum

### 1. LATAR BELAKANG

Perkembangan teknologi informasi yang begitu masif diyakini telah sampai dimana tahap yang dapat mempengaruhi nasib kehidupan umat manusia di masa depan. Hampir setiap kegiatan masyarakat akan selalu melibatkan inovasi teknologi, seperti jual beli, transaksi elektronik, dan komunikasi, perkembangan pengguna teknologi informasi juga berkaitan dengan perkembangan kejahatan. (Fadli et al., n.d.)

Fenomena kejahatan siber menjadi perhatian khusus masyarakat era modern ini karena dunia siber telah mengambil alih berbagai aspek kehidupan yang beberapa di antaranya termuat ketentuan data pribadi. Beberapa layanan publik yang disediakan oleh negara juga mengarah pada modernisasi dengan menggunakan teknologi informasi karena pada beberapa kasus, layanan pemerintah dapat diakses dengan memasukkan data pribadi tertentu seperti nomor induk kependudukan. Data pribadi ini dapat menjadi target kejahatan siber jika tidak dikelola dengan baik.

Dampak dari kejahatan siber merupakan masalah yang sangat penting bagi pemerintah karena dapat mempengaruhi kerugian di masyarakat secara keseluruhan. Perlu disadari bahwa kejahatan siber dapat menyebabkan kerugian kolektif bagi masyarakat Indonesia. Setidaknya terdapat dua faktor yang menyebabkan terjadinya kejahatan siber, yaitu faktor teknis dan faktor sosial ekonomi. Pencurian data melalui teknologi informasi di era modern disebut sebagai phishing yaitu sebuah aktivitas secara melawan hukum untuk menguasai dan mendapatkan informasi pribadi seseorang atau sekelompok tertentu. Tindakan pencurian data pribadi memiliki tujuan, yaitu dengan memperoleh data pribadi maka selanjutnya dengan kejahatan terhadap harta, dengan meretas akun rekening keuangan atau hal berharga yang bisa di akses melalui data pribadi atau mengumpulkan semua data pribadi lalu dijual dalam situs gelap.

Insiden atau peristiwa yang berhubungan dengan kebocoran data pribadi bukanlah fenomena baru di Indonesia, peristiwa ini sering sekali terjadi pada rentang tahun 2023-2024. Salah satunya adalah situs yang menunjukkan bahwa informasi pribadi masyarakat Indonesia telah diperjual belikan di dunia internasional. Data pribadi yang telah disebarluaskan dapat mengakibatkan kerugian bagi masyarakat karena dapat digunakan untuk mengakses segala informasi baik keuangan maupun aktivitas lainnya (Citrazalabilla & Yusuf, 2024). Berdasarkan hal tersebut, maka dapat kita nilai peranan dari pemerintah dalam memerangi kejahatan siber di Indonesia dalam ranah *cyberSecurity* sangatlah minim.

Mengutip dari artikel pemberitaan yang disampaikan oleh media Liputan 6, Laporan *National Cyber Security Index (NCSI)* menyatakan indeks keamanan siber Indonesia pada tahun 2022 adalah 38,96 dari 100. Indonesia berada di peringkat ke-3 di antara negara-negara G20 dalam indeks tersebut. Jika dinilai secara global, Indonesia berada di peringkat 83 dari 160 negara yang termasuk dalam laporan tersebut (Gideon, 2023). Pada tahun 2024 di Indonesia sendiri terjadi 40 kasus dugaan pencurian data pribadi, salah satu kasus yaitu kebocoran data PDNS yang menyebabkan gangguan sistem layanan pemerintah, dan terjadi kasus pembobolan data NPWP sebanyak 6,6 juta yang diperjual belikan di situs gelap.

Berdasarkan data yang disajikan, maka masih terdapat titik lemah bagi pemerintah Indonesia dalam implementasi perlindungan data pribadi masyarakat serta aturan hukum yang belum dapat dieksekusi dengan baik dari ancaman tindak pidana kejahatan siber, Yang seharusnya hukum tampil untuk mengatur (aspek *regulative*), agar kepentingan utama umat manusia untuk mencapai kesejahteraan dan perlindungan hak-haknya tercapai. Penggunaan hukum secara sadar untuk dipakai sebagai instrumen merupakan salah satu ciri yang menonjol dari hukum modern (*law as a tool of social engineering*), di samping ada fungsi lain dan hukum yaitu sebagai alat kontrol. (*law as a tool of social control*) (Rahmat Dwi Putranto, 2023).

Indonesia sendiri mengenai Peraturan PDP (hukum positif) telah hadirnya UU No. 27 tahun 2022 tentang perlindungan data pribadi. Namun melihat fakta yang ada masih terdapat kebocoran data pribadi yang terjadi di kalangan masyarakat Indonesia, hal ini ditambah setelah terbitnya UU PDP pada tahun 2022 belum adanya suatu lembaga atau komisi perlindungan data pribadi. UU PDP sendiri mengamanatkan regulasi turunan yaitu 9 peraturan pemerintah dan 1 peraturan presiden yang saat ini tahun 2024 belum di buat 10 peraturan tersebut oleh pemerintah sebagai lembaga eksekutif, hal ini membuat suatu pertanyaan tentang keefektifan dalam pasal UU PDP sendiri dalam menangani pencurian data pribadi di Indonesia.

## 2. METODE PENELITIAN

Penelitian ini akan dilandaskan pada penelitian normative yuridis. Penelitian normative yuridis adalah pendekatan pada teori, konsep, dan mempelajari peraturan perundang-undang yang berkaitan dengan penelitian (Pujiati, 2024). Pada penelitian jurnal mengacu pada ketentuan hukum positif yang berlaku atau perundang-undangan yang sah. Pendekatan ini mengarah pada pendekatan hukum positif dengan cara meneliti semua hukum positif dan regulasi. Pendekatan kasus dilakukan dengan cara melakukan telaah terhadap kasus-kasus yang berkaitan dengan isu yang dihadapi yang telah terjadi di Indonesia.

## 3. HASIL DAN PEMBAHASAN

### ***A. Analisis Bentuk-bentuk Perlindungan Hukum terkait tindak pidana pencurian data pribadi serta persiapan pemerintah dalam mengedukasi masyarakat digital.***

Perkembangan era teknologi dan digitalisasi telah memberikan dampak yang sangat signifikan terhadap perubahan sosial, gaya hidup dan perilaku masyarakat modern. Penggunaan teknologi dan informasi dapat kita rasakan baik dalam bidang hiburan, pendidikan maupun hal-hal yang berkaitan dengan kemajuan ilmu pengetahuan. Dengan menggunakan teknologi kita dapat dengan mudah mengakses informasi apapun bahkan mendapatkan jutaan

informasi dalam sehari, dengan banyaknya informasi yang kita terima tentunya memudahkan kita untuk melakukan pekerjaan kita secara efisien, akurat dan minim kesalahan informasi. inovasi dimaksudkan untuk membawa manfaat positif bagi kehidupan manusia, karena kemajuan teknologi akan selalu berjalan seiring dengan kemajuan ilmu pengetahuan.

Perkembangan era teknologi dengan segala kelebihanannya tidak hanya memberikan dampak positif tetapi juga dampak negatif atau masalah yang akan dihadapi masyarakat, seperti adanya wadah bagi kejahatan-kejahatan baru seperti phising dan lain sebagainya, Adanya kejahatan tersebut menandakan bahwa tidak adanya sistem pengawasan atau sistem keamanan yang sederhana, sehingga dengan mudah diretas oleh para pelaku kejahatan siber. Pencurian identitas sendiri merupakan salah satu pelanggaran hukum di bidang teknologi informasi, dimana data pribadi merupakan data yang dilindungi oleh negara dan merupakan bagian dari hak asasi manusia seperti yang dicantumkan pada pasal 29 ayat (1) UU No. 39 tahun 1999 tentang Hak Asasi Manusia menyatakan bahwa setiap warga Indonesia berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan hak miliknya.

Mengetahui bahwa hak data pribadi kita perlu dilindungi oleh negara. Masyarakat Indonesia perlu mengerti dan mengetahui kegiatan penyalahgunaan data pribadi dan bentuk modus pelaku pencurian data pribadi. Terdapat beberapa contoh dari kegiatan penyalahgunaan data pribadi antara lain:

1. Mengcopy data informasi tanpa adanya izin dan data kartu akun bank nasabah (Skimming), saat pelaku melakukan aksinya di tempat penarikan uang.
2. Para pelaku biasanya memanfaatkan pinjaman online ilegal, dimana mekanisme transaksi pengisian data secara online. Jika penerima pinjaman mengalami gagal bayar maupun keterlambatan maka penerima nasabah akan mengalami peneroran disertakan data pribadi penerima hutang akan di kumpulan serta mengakses tanpa sepengetahuan korban.
3. Pengumpulan data yang telah dilakukan pelaku biasanya pelaku melakukan pelecehan seksual melalui nomor WhatsApp. Serta mengirimkan foto senonoh. (Maulida et al., n.d.)

Terdapat modus pidana pencurian data pribadi yang selalu dilakukan oleh pelaku pencurian data pribadi antara lain:

Pertama yaitu dengan cara Social Engineering, modus dalam tindakan ini berupa manipulasi psikologis target pencurian data untuk mengungkapkan informasi sensitif, Biasanya selalu terjadi melalui telepon atau internet dan pelaku mencoba mendapatkan data informasi korban dengan berpura-pura menjadi pekerja pemberi layanan atau bisnis tertentu. Manipulasi dilakukan agar korban percaya bahwa pelaku adalah seorang pekerja Bantuan atau sejenisnya,

Ketika sudah mendapatkan kepercayaan data pribadi akan diminta, Target yang percaya bahwa mereka memberikan data pribadi kepada pihak yang berwenang akan memberikannya secara sukarela, dengan harapan bahwa masalah akan segera terselesaikan atau mendapatkan semacam undian hadiah.

Kedua, modus berikut dengan lebih canggih yaitu penggunaan Malware, Malware adalah program yang dirancang untuk menyebabkan kerusakan dan kesalahan sistem pada perangkat lunak (Software) komputer. Malware sendiri terdiri dari beberapa jenis dan semuanya memiliki tujuan yang sama yaitu merusak sistem komputer. Jenis malware yang umum adalah spyware, yang dapat mengumpulkan data informasi dari perangkat yang dimasukinya, dan mengirimkannya ke pihak lain atau pelaku tanpa persetujuan. Sesuai dengan namanya, perangkat lunak ini bertindak sebagai mata-mata perangkat yang memberikan informasi kepada pihak lain tanpa izin.

Ketiga yaitu modus dengan aplikasi pinjaman online yang tidak di bawah OJK, modus ketiga ini bisa dikatakan modus terbaru dan terpopuler, pelaku akan mencoba menawarkan pinjaman online atau pinjol secara mudah dan cepat cair, dalam jumlah yang sangat besar. Sasaran hanya perlu mengunggah foto KTP, beserta pas foto selfie yang dimiliki sebagai syarat. Namun, sudah jelas bahwa pinjaman semacam itu memiliki bunga yang tinggi dan merugikan korbannya serta biasanya pinjol ini tidak terdaftar oleh OJK. Data diri yang telah dimiliki oleh pelaku kemudian digunakan untuk melakukan intimidasi, ancaman dan tindakan lainnya yang dapat merugikan korban. (Verihubs, 2022)

Menurut data yang telah dikeluarkan oleh Kominfo, jumlah kasus dugaan pelanggaran perlindungan data pribadi pada tahun 2024 sebanyak 40 kasus, mirisnya jumlah pada tahun ini melebihi dari jumlah pada tahun sebelumnya pada tahun 2022 dengan jumlah 35 kasus (Ibnu Naufal, 2024), serta setiap tahun banyaknya pelaporan polisi pencurian data pribadi individu, yang mana data yang diambil digunakan sebagai tindak pidana penipuan dll. Berdasarkan data yang dijelaskan, kita dapat menilai dan menyimpulkan bahwa pemerintah telah gagal menjamin keamanan data pribadi warga serta negara tidak secara jelas dalam pengawasan dan mengontrol terhadap pihak swasta mengenai perlindungan data pribadi.

Dari 40 kasus pencurian data pribadi terbesar di Indonesia, terdapat satu kasus yang dapat penulis jelaskan lebih lanjut berikut salah satu kasus-kasus terbesar yang terjadi di 2024. Serangan awal dilakukan pada tanggal 20 Juni 2024 ketika Pusat Data Nasional Sementara (PDNS 2) mendapat gangguan sistem layanan publik, termasuk data imigrasi, yang mengalami serangan pertama insiden gangguan PDNS 2 ini terjadi di Surabaya. Serangan ini berdampak sangat signifikan yang mengganggu terhadap layanan publik penting di Indonesia. Gangguan

ini mengakibatkan terjadinya antrian yang sangat Panjang dan keterlambatan proses imigrasi yang dampaknya mengganggu layanan fasilitas publik. Serangan yang dilakukan terhadap server PDNS mengalami dampak eror sistem dengan total 210 Instansi yang terkena dampak. Sistem perlintasan untuk pemeriksaan ke imigrasian seperti autogate, aplikasi Visa, izin tinggal aplikasi M- Paspur mengalami masalah down yang sama. Kerugian selanjutya terdapat 47 layanan Kemendikbud mengalami down server, seperti layanan Sistem Pengadaan Secara Elektronik (SPSE), dan gangguan layanan informasi data Beasiswa Pendidikan Indonesia. (Andika Dwi, 2024)

Badan Siber dan Sandi Negara atau yang disingkat (BSSN) serangan gangguan layanan PDNS tersebut menggunakan ransomware terbaru yaitu Lockbit 3.0 atau disebut Brain Chipher 3.0. Para pelaku pembobolan ini meminta kepada pemerintah Surabaya untuk menebus Rp 131 Miliar rupiah atau sebesar US\$ 8 juta agar layanan PDNS dapat dijalankan seperti normal, dikarenakan serangan ini ada 210 pemerintah pusat dan daerah terdampak serangan ransomware PDNS. (tim CNN Indonesia, 2024)

Berdasarkan salah satu kasus terbesar yang terjadi di instansi negara terkait bentuk kasus pencurian data pribadi, saya menilai bahwa tindakan para pelaku sangat bervariasi dan dalam penyerangan pencurian identitas juga memiliki teknologi terbaru seiring dengan perkembangan zaman, Bahkan tindakan dapat berubah-ubah atau tindakan baru yang sebelumnya tidak pernah diketahui oleh korban yang dapat dilakukan oleh pelaku, maka dari itu kita perlu mengetahui seberapa jauh peranan pemerintah dalam mengedukasi masyarakat untuk mengerti tentang teknologi atau tujuan pemerintah yang disebut dengan Masyarakat Indonesia Digital. Berikut data survey secara menyeluruh dari berbagai Provinsi di Indonesia yang dilakukan oleh KOMINFO.

## Hasil Perhitungan Indeks Masyarakat Digital Indonesia 2023



**Sumber:** Indeks Masyarakat Digital Indonesia tahun 2023 KOMINFO

Berdasarkan hasil perhitungan indeks masyarakat digital di Indonesia terdapat 20 daerah kota yang nilai IMDI di atas IMDI nasional atau tercapainya minimal target pemerintah, dan terdapat 18 daerah kota yang nilai IMDI nya masih dibawah IMDI nasional, yang artinya masyarakat Indonesia dalam memahami dunia teknologi internet masih belum sepenuhnya mengerti dan dari data tersebut masih belum memenuhi target ideal pemerintah. Penulis nilai bahwa tugas pemerintah melalui KOMINFO masih banyak nya pekerjaan rumah untuk meningkatkan kesadaran atau meleknya masyarakat terhadap teknologi agar tidak menjadi korban dalam pencurian data pribadi. Pembangunan infrastruktur perlu juga lagi ditingkatkan walaupun dalam indeksnya sudah melebihi 57,09 karena infrastruktur adalah menjadi salah satu instrumen penting dalam meningkatkannya pendalaman teknologi informasi masyarakat serta untuk pencegahan terhadap pencurian data pribadi.

### B. Perlindungan Hukum Bagi Korban Tindak Pidana pencurian data Pribadi

Dalam konstitusi negara Indonesia, negara melindungi data pribadi dan privasi individu seperti yang tercantum dalam UU Dasar Negara Indonesia Tahun 1945 pada pasal 28G ayat 1

“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”. Dan juga dalam pasal 1 ayat 2 UU dan juga dalam Pasal 1 ayat 2 UU N0. 27 Tahun 2022 menjelaskan bahwa data pribadi harus dilindungi untuk menjamin hak-hak konsistensi subjek data pribadi. Artinya dapat kita pahami bahwa data pribadi merupakan bagian yang harus dilindungi oleh negara dan memiliki kepastian hukum untuk memiliki hak dan kewajiban yang diatur oleh peraturan perundang-undangan.

Sebagai negara yang menganut hukum, Indonesia memiliki kewajiban untuk melindungi seluruh warga negaranya dari berbagai bentuk kejahatan. Hal yang sejalan dengan tujuan hukum itu sendiri adalah upaya para penegak hukum (Rani Purwaningsih & Rahmat Dwi Putranto, 2023). Tujuan dari perlindungan hukum pencurian data pribadi dapat dilihat dari beberapa sudut pandang, yang meliputi aspek subjek (korban), objek (pelaku), dan kejadian yang sifatnya merugikan secara progresif antara pelaku dan korban. Secara harfiah perlindungan hukum yang menggunakan pranata dan sarana penegakan hukum dapat diberikan oleh negara yaitu *by giving regulation* yaitu pada pelaku dan memberikan hak subjek yang dilindungi dan *by law enforcement* yaitu memberikan aturan tegas seperti pidana, perdata dan pencegahan kejahatan. (Sasongko, 2007)

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 preventif dan hukuman atau repressif. Tindakan represif diimplementasikan dalam bentuk aturan dan sanksi, salah satu konsep perlindungan hukum yang paling menjamin adalah adanya lembaga-lembaga negara penegakan hukum seperti polisi, jaksa, pengadilan, yang dirancang untuk menghukum para pelanggar melalui aturan-aturan yang ada yang dilaksanakan oleh lembaga-lembaga penegak hukum, Namun pula dapat diselesaikan kepada lembaga penyelesaian sengketa non litigasi diluar pengadilan (Sasongko, 2007). Langkah Preventif ialah Langkah untuk mencegah timbulnya kejadian konflik, serta subjek hukum diberikan kesempatan untuk mengajukan keberatan atau pendapat sebelum keputusan pemerintah menjadi final. Karena dengan adanya perlindungan preventif, pemerintah dapat lebih berhati-hati dan dapat mendengar suara masyarakat dalam keputusan pengambilan peraturan maupun diskresi (Andika Hidayatullah & Mulyati, 2023).

Di Indonesia Perlindungan Hukum mengenai data Pribadi dapat kita lakukan bisa berbagai bentuk seperti Sosialisasi Modus tindak pencurian data pribadi, Sosialisasi Perlindungan hukum perdata, Sosialisasi Perlindungan Hukum pidana mengenai pencurian data pribadi dan



lain sebagainya. Maka dari itu perlindungan hukum mengenai tindak pidana pencurian data pribadi dapat dilakukan dengan bentuk Preventif maupun Repreventif. Ada berbagai cara bentuk perlindungan hukum pencurian data pribadi di Indonesia, Berikut beberapa contoh nya:

1. Perlindungan Repreventif. Perlindungan ini memiliki fungsi untuk menghukum atau membuat rasa jera terhadap pelaku karena telah melakukan kejahatan. Dalam hal ini penulis berpendapat aturan yang memadai serta adanya *by giving regulation*. penegakan hukum seperti Polisi, Jaksa dan Hakim berperan sangat penting. Upaya Litigasi dalam repreventif di utamakan demi 3 Tujuan hukum yaitu kepastian hukum, Kemanfaatan Hukum dan keadilan hukum. Bentuk repreventif ialah perlindungan terakhir yang dapat dilakukan oleh korban dan pemerintah.

2. Perlindungan Preventif. Perlindungan ini berfungsi untuk pencegahan kejadian permasalahan sejak awal, dalam hal ini, Pemerintah dapat melakukan Sosialisasi, edukasi, pencegahan terjadi nya pencurian data pribadi dan Penyuluhan Hukum mengenai pencurian data pribadi. Lembaga Pemerintah yang mempunyai kewenangan dalam melakukan perlindungan preventif ialah Kementerian Komunikasi Dan Informatika dan Otoritas Jasa Keuangan atau disebut OJK, dan Civitas akademika seperti Perguruan tinggi.

3. Kerja Sama antara Lembaga Pemerintah dan Pihak Internasional: Kerja sama adalah salah satu bentuk perlindungan Repreventif berkelanjutan. Kejahatan dunia Internet tidak hanya terjadi di Indonesia, kejahatan ini terkoneksi di berbagai negara. *Conventionzon Cybercrime* misalnya, Pertemuan tersebut menyebutkan bahwa negara perlunya kerjasama internasional dalam memerangi cybercrime yang bersifat global dan tanpa batas wilayah. Permasalahan yang selalu kita alami dalam penegakan hukum pencurian data pribadi ialah kurangnya bukti tindak kejahatan serta penegak sulit menemukan pelaku dalam tindak kejahatan ini, maka dari itu pemerintah perlu berkerja sama dengan pihak luar.

Perlindungan hukum mengenai data pribadi dengan bentuk repreventif dan Preventif ialah bertujuan untuk mencegah terjadinya kerugian, mencegah tindakan pidana maupun perdata, menghukum pelaku, dan dapat memberikan dasar hukum untuk menangani masalah yang berkaitan dengan perlindungan data pribadi di Indonesia.

Hukum yang mengatur data pribadi di Indonesia atau disebut dalam teori perlindungan hukum Repreventif yaitu *by giving regulation* tertuang dalam UU No.27 tahun 2022 tentang Perlindungan Data pribadi, dan secara perdata diatur UU No. 1 tahun 2024 yang telah diubah ketiga kali nya Undang-undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Menteri Komunikasi dan Informatika No. 20 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (PDPSE) tahun 2016. Selain itu, ada UU No. 31/2014 tentang perlindungan saksi dan korban. UU No. 31/2014 untuk memberikan keuntungan dan

perlindungan bagi saksi dan korban, tetapi tidak secara khusus dan ilmiah membahas korban pencurian identitas.

Perlindungan Hukum pencurian data pribadi dapat dilaporkan sebagai tindak pidana atau gugatan secara perdata, dengan cara melaporkan ke pihak yang berwajib, atau dengan menguasai penguat untuk meminta Bantuan kepada Lembaga Bantuan Hukum atau advokat. Sanksi hukuman bagi pelaku diatur dalam pasal 67 UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi berbunyi “Setiap Orang yang dengan sengaja dan melawan hukum mendapatkan atau mengumpulkannya Data Pribadi yang bukan miliknya bertujuan untuk menguntungkan diri sendiri atau orang lain yang berakibat 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 (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. Lalu dalam pasal, pasal 67 ayat 3 Undang-undang No. 27 tahun 2022 Perlindungan data pribadi berbunyi “Setiap Orang yang dengan sengaja 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 5 Miliar. Dalam pasal ini menjelaskan juga bahwa tindakan dari hasil pengumpulan data pribadi lalu dipergunakan untuk keuntungan diri sendiri dan orang lain dilarah dana kan terkena pidana penjara serta denda.

Pelaku tindak pidana pencurian identitas dapat berupa perorangan, institusi, perusahaan, dan komunitas. Jika pelaku adalah orang banyak dan menguasai suatu lembaga atau perusahaan, pertanggungjawaban hukum dibebankan kepada pengurus, pengendali atau penerima manfaat dari lembaga atau perusahaan yang bersangkutan. Sanksi tambahan yang berlaku jika pelakunya adalah lembaga atau perusahaan antara lain perampasan keuntungan dan/atau aset yang berasal dari tindak pidana dan pembayaran ganti rugi, sanksi tambahan ini tercantum dalam Pasal 69 UU Perlindungan Data Pribadi No. 27 Tahun 2022.

Selain pidana, para korban dapat juga mengajukan gugatan perdata atau ganti rugi. Pada penjelasan UU No. 1 tahun 2024 perubahan kedua atas UU Nomor 11 tahun 2008 tentang informasi dan Transaksi Elektronik, Pada pasal 26 ayat 2 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. Gugatan yang diajukan termasuk kategori PMH atau disebut Perbuatan melawan hukum, Sesuai dengan pasal 1365 KUHPperdata.

Pembahasan mengenai peraturan UU No. 27 Tahun 2022, penulis menilai bahwa penerapan dalam undang-undang ini belum dapat dikatakan selaras dengan baik dalam implementasinya, dikarenakan dalam UU PDP ini mengamanatkan 10 peraturan turunan, yang artinya menjadi 10 pekerjaan rumah bagi pemerintah. UU yang belum adanya Peraturan Pemerintah sebagai peraturan pelaksana biasanya menghadapi Persoalan. Persoalan yang sering timbul dengan keefektivitasan suatu UU muncul karena penerapannya memungkinkan terjadinya penafsiran-penafsiran bebas atau liar, jika tidak ada nya peraturan yang secara teknis dan rinci dalam penerapannya (Yusuf, n.d.).

Apabila penafsiran dari suatu UU terus berlanjut atau terus dibiarkan maka tujuan kebijakan dari suatu Undang-undang dapat menjadi tidak sejalan dengan tujuan politik hukum dari UU yang di atas nya atau yang mendelegasikannya, atau bahkan dapat digunakan oleh badan dan pejabat pemerintah untuk bertindak sewenang-wenangnya dengan menggunakan atau memanfaatkan UU yang masih belum jelas. Dengan demikian, akan timbul pertanyaan mengenai keabsahan dari suatu UU yang yang belum atau tidaknya diterbitkan turunan peraturan nya atau PP sebagai peraturan pelaksana nya. Baik dari tataran suatu normatif maupun teoritis.

Secara Konstitusi UUD 1945 negara Indonesia pembentukan peraturan Pemerintah (PP) mengacu pada pasal 5 ayat (2) yaitu. “Presiden menetapkan PP yang berfungsi untuk menjalankan UU sebagaimana mestinya”. Termuat juga dalam UU 12 tahun 2011 tentang pembentukan peraturan perundang-undangan. Dapat dipahami sesuai amanat UUD bahwa fungsinya adalah untuk melaksanakan sebuah UU. Baik UU secara eksplisit menyatakan bahwa PP diperlukan sebagai peraturan tambahan maupun tidak mencantumkan secara tegas di dalam UU.

Menurut guru besar Prof. Dr. Moh. Fadli, S.H., M.Hum dari Fakultas Hukum Universitas Brawijaya beliau mengatakan dalam acara legislataalk Pada Channel Youtube. Prof. Dr. moh Fadli mengungkapkan Bahwa pasal dalam UU yang mendelegasikan pelaksanaan PP maka pasal tersebut tidak dapat dilaksanakan sebelum PP tersebut dibentuk. Penulis mengerti bahwa untuk menjalankan UU secara efektifitas serta dapat memenuhi kebutuhan masyarakat Indonesia secara optimal maka harus memenuhi unsur dari asas yang terdapat pada UU no. 12 tahun 2011 pada pasal 5 yaitu:

- a. Kejelasan tujuan
- b. Lembaga dan pejabat yang mumpuni
- c. Kesamaan antara jenis hierarki
- d. Mudah diterapkan

- e. Kedayagunaan dan kegunaan
- f. Kejelasan rumusan
- g. Keterbukaan

Sesuai asas yang diperlukan maka penulis menilai bahwa UU PDP belum bisa se efektifitas yang kita harapkan, karena UU PDP belum adanya lembaga atau komisi yang dibuat oleh pemerintah serta belum adanya kejelasan pada rumusan terkait pelaksanaannya, karena belum terbitnya suatu PP yg dibutuhkan.

Dalam UU PDP mengamankan 10 peraturan yaitu berupa 9 peraturan pemerintah serta 1 peraturan presiden Dari 10 aturan tersebut berikut yang dapat penulis Jelaskan antara lain:

1. Pengaturan mengenai pelanggaran terhadap pemrosesan data pribadi dan tata cara pengenaan ganti kerugian terhadap penggugat atas pelanggaran data pribadi yang dilakukan oleh oknum yang tidak bertanggung jawab. Ketentuan ini dijelaskan pada pasal 12 ayat 1 UU PDP. Yang menyebutkan. “subjek data pribadi mempunyai hak penuh menggugat dan menerima ganti rugi pelanggaran yaitu pemrosesan data pribadi.
2. Mengenai ketentuan kepada hak subjek data dalam menggunakan, mengirim dan menyimpan data pribadi tentang dirinya ke pengendali data pribadi lainnya, selama sistem yang ditawarkan dan digunakan dapat saling berkomunikasi secara aman dan terlindungi dengan sesuai prinsip” perlindungan data pribadi. Ketentuan ini terdapat pada pasal 13 ayat 2 UU PDP.
3. Pemrosesan data pribadi yang penjelasannya antara lain: a. pengumpulan dan pengelolaan, b. penganalisis, c, penyimpanan, d. perbaikan dan pembaharuan, e. pempublikasian dan f. pemusnahan. Semua ketentuan ini tertera pada pasal 16 ayat 1.
4. Mengenai ketentuan terkait dengan penilain dampak perlindungan data pribadi akan diatur melalui peraturan Pemerintah. Pengaturan mengenai pengendali data pribadi yang mempunyai kewajiban dalam menilai dampak terhadap perlindungan data pribadi dalam hal pemrosesan yang memiliki potensi resiko kepada subjek atau pemilik data pribadi. Ketentuan ini diatur pada pasal 34 ayat 1.
5. Amanat selanjutnya mengenai turunan yaitu persoalan mengenai pengendali data pribadi berbentuk badan hukum yang telah melakukan penggabungan, pengambilalihan, pemisahan, peleburan atau pembubaran suatu badan hukum wajib memberitahukan suatu penyampaian kepada pengalihan data pribadi kepada subjek data pribadi. Serta penyimpanan, transfer dan pemusnahan wajib memberi tahu kepada subjek. Ketentuan tersebut tertera pada pasal 48 ayat (1), (2), dan (4).

6. Peraturan mengenai fungsi atau kewajiban pejabat dan petugas yang melaksanakan fungsi perlindungan data pribadi akan diberi peraturan lebih rinci melalui Peraturan Pemerintah. Peraturan pemerintah mengenai fungsi pejabat ini akan menjabarkan fungsional secara terperinci dan terjabar, pejabat dan petugas wajib melaksanakan fungsi perlindungan data pribadi yang mempunyai tugas. Tugas ini secara singkat seperti menginformasikan dan memberikan saran terkait pengendali data pribadi agar selalu mengikuti ketentuan UU PDP kemudian mengawasi dan memastikan kepatuhannya terhadap UU PDP, hal ini juga termasuk memberikan saran mengenai penilaian dampak perlindungan data pribadi dan memantau kinerja dan pemroses data pribadi, serta mengkoordinasi dan bertindak sebagai memberi saran terhadap isu perlindungan data pribadi fungsi lebih jelasnya dicantumkan pada pasal 54 ayat (1). Ketentuan turunan peraturan ini terdapat pada pasal 54.
7. Ketentuan peraturan turunan mengenai transfer data pribadi kepada pengendali data pribadi atau prosesor yang di luar wilayah Indonesia harus sesuai dengan yang diatur dalam UU PDP. Untuk melakukan transfer data pribadi, pengendali data pribadi memiliki kewajiban memastikan suatu negara tempat kedudukan pengendali data pribadi dan atau prosesor yang telah menerima transfer data pribadi. ketentuan mengenai transfer data pribadi ini terdapat pada pasal 56 yang akan di buat lebih rinci dalam berupa PP.
8. Pengaturan tentang tata cara pengenaan berupa Sanksi administratif dalam pelanggaran terkait UU PDP. Sanksi administratif yaitu denda administratif dimaksud pada pasal 57 ayat (2) huruf d yaitu paling tinggi 2 persen dari pendapatan pertahunan atau penerimaan tahunan. Ketentuan saksi administratif ini akan dijelaskan dalam aturan PP.
9. Pengaturan tentang pelaksanaannya terhadap wewenang lembaga yang akan menyelenggarakan perlindungan data pribadi yang mana kewenangan lengkapnya pada pasal 60. Ketentuan mengenai tata cara pelaksanaan kewenangan lembaga perlindungan data pribadi diatur dalam PP.
10. Terakhir UU PDP amanatkan Peraturan Presiden, dalam PP ini pemerintah wajib berperan dalam mewujudkan suatu penyelenggaraan perlindungan data pribadi yang sesuai dengan UU PDP dengan suatu lembaga yang ditetapkan dan bertanggung jawab kepada presiden. Ketentuan ini pada pasal 58 ayat (2).

#### **4. KESIMPULAN DAN SARAN**

##### **A. KESIMPULAN**

Berdasarkan penelitian diatas dapat kita beri kesimpulan bahwa banyak jenis untuk melakukan modus kejahatan pencurian data pribadi, pencurian data pribadi yang sering dilakukan pelaku yakni dengan mencari informasi data pribadi korban yang mudah di akses tanpa melalui perizinan korban lalu pelaku melakukan pengumpulan data tersebut. Pada 3 tahun terakhir meningkatnya kasus tindak pencurian negara data pribadi yang paling sering dialami oleh instansi negara, ini membuktikan bahwa pemerintah tidak dapat menjaga serta mengawasi data pribadi warga negara Indonesia. perlu melindungi data pribadi karena data pribadi karena data pribadi menjadi suatu hal yang dilindungi oleh negara karena tercantum dalam konstitusi negara Indonesia.

Dengan meningkatnya jumlah kasus dalam 3 tahun terakhir, perlu adanya regulasi peraturan undang-undang yang melindungi para korban. Menurut penulis, pemerintah dapat memberikan perlindungan secara preventif dan hukuman (reprentif) perlindungan preventif di bertujuan untuk pencegahan awal tindak kejahatan pencurian data pribadi, dengan cara lembaga pemerintah seperti OJK dan Kominfo melakukan edukasi kepada masyarakat bertujuan agar masyarakat mengerti tentang menjaga data pribadi dan tidak mudah menjadi sasaran pelaku tindak kejahatan pencurian data pribadi. Lalu perlindungan reprentif memiliki fungsi untuk menghukum dan membuat jera terhadap pelaku kejahatan, yang mana dalam menjalankan reprentif ini penegak hukum seperti kepolisian, Jaksa dan hakim memegang peranan penting. Regulasi yang mengatur yaitu UU no. 27 tahun 2022 yang mengacu pada perlindungan data pribadi, dimana korban dapat menuntut hak-hak mereka. Perlindungan secara perdata juga dapat di lakukan yang di atur dalam perubahan kedua UU ITE No. 1 tahun 2024, yang termasuk juga kategori PMH sesuai pada pasal 1365 KUH Perdata. UU PDP sendiri perlu adanya delegasi peraturan turunan yaitu terdapat 9 peraturan pemerintah serta 1 peraturan pemerintah, UU PDP sendiri memerlukan peraturan turunan agar adanya prosedur sesuai amanat UU itu sendiri. di kerjakan oleh pemerintah secepat mungkin agar keefektifan UU PDP berjalan maksimal yang diharapkan.

##### **B. SARAN**

Mempercepat pembentukan komisi perlindungan data pribadi, dikarenakan dalam pasal 58 hingga 60 UU PDP telah diatur tegas dan wewenang lembaga perlindungan data pribadi. Pembentukan Hal ini dilakukan agar memperkuat mekanisme pengawasan, Menyusun pedoman operasional yang jelas, serta meningkatkan kapasitas sumber daya manusia yang ikut

terlibat dalam pengelolaan dan penegakan regulasi perlindungan data pribadi dalam menjalankan fungsinya secara efisien dan efektif. Selain itu, penting untuk memastikan adanya transparansi dan akuntabilitas dalam mekanisme operasional Lembaga ini guna menjamin perlindungan hak-hak pribadi warga negara.

Pemerintah dan sektor swasta harus memberikan perhatian khusus untuk mengembangkan dan meningkatkan jumlah personil yang berkompeten di bidang cybercrime. Hal ini dapat dilakukan melalui pelatihan berkelanjutan, seperti sertifikasi profesi, dan kerja sama dengan lembaga pendidikan dan universitas untuk mempersiapkan tenaga profesional yang siap menjawab tantangan perlindungan data pribadi. Penguatan SDM diharapkan dapat meningkatkan mekanisme pengawasan dan penegakan hukum terkait kejahatan siber.

Pemerintah perlu meningkatkan Standar kompetensi SDM Pengelolaan Data Pribadi yaitu pengembangan SDM Administrator database. Pengembangan SDM dalam profesi administrator database sangat diperlukan karena peran ini lah yang akan mengawasi, menyimpan, Menyusun dan mengontrol data pribadi masyarakat.

Kominfo dan OJK menjalankan suatu program pelatihan dan forum diskusi tentang pengelolaan data pribadi yang terstruktur kepada masyarakat maupun Instansi swasta dan negeri. Perkembangan teknologi begitu maka diperlukan forum yang sering dilaksanakan diskusi perkembangan teknologi serta cara melindungi data pribadi yang benar. Kominfo perlu melakukan konten sosialisasi di media sosial ditunjukkan untuk meningkatkan kesadaran atau awareness masyarakat dan mensosialisasi terkait pengelolaan data pribadi.

## 5. DAFTAR REFERENSI

- Andika Hidayatullah, T., & Mulyati, N. (2023). Perlindungan Hukum terhadap Korban Tindak Pidana Peretasan (Hacking) Berkaitan dengan Pencurian Data. 6(1). <https://doi.org/10.31933/unesrev.v6i1>
- Citrazalabilla, R., & Yusuf, H. (2024). JICN: Jurnal Intelek dan Cendekiawan Nusantara Pencurian Data Pribadi Di Internet Dari Sudut Pandang Kriminologi Theft of Personal Data on the Internet from a Criminological Point of View. <https://jicnusantara.com/index.php/jicn>
- Dr. Rahmat Dwi Putranto, S. H. , M. H. (2023). Teknologi Hukum Paradigma Baru Hukum di Dunia Digital (Irfan Hakim, Ed.). KENCANA.
- Fadli, M., Widijowati, D., & Andayani, D. (n.d.). Pencurian Data Pribadi di Dunia Maya (Phising Cybercrime) yang ditinjau dalam Perspektif Kriminologi. <https://journal.ikopin.ac.id>
- Gideon. (2023, March 26). Keamanan siber Indonesia peringkat 3 terbawah di negara G20. Liputan 6. <https://www.liputan6.com/bisnis/read/5243523/keamanan-siber-indonesia-peringkat-3-terbawah-di-g20-ego-sektoral-kronis-jadi-biang-keladinya?page=2>

- Ibnu Naufal. (2024, August 18). Ketoprak Kebocoran Data Pribadi di Era Jokowi. Inilah.Com. <https://www.inilah.com/ketoprak-kebocoran-data-pribadi-di-era-jokowi>
- Maulida, D. N., Kaimuddin, A., & Andriyansyah, M. F. (n.d.). TINDAK PIDANA PENCURIAN DATA PRIBADI DI INTERNET.
- Pujiati. (2024, October 21). Metode Penelitian Yuridis Normatif di Bidang Hukum. Deepublish. <https://penerbitdeepublish.com/metode-penelitian-yuridis-normatif/>
- Rani Purwaningsih, & Rahmat Dwi Putranto. (2023). 8021-Article Text-27645-1-10-20230225. 16 no 1.
- Sasongko, W. (2007). KETENTUAN-KE TENTUAI{ POKOK HT]KT]MPEMKONST]MEN.
- tim CNN Indonesia. (2024, June 25). Fakta-fakta Kebocoran data PDNS, dalang hingga jumlah tebusan . CNN Indonesia . <https://www.cnnindonesia.com/teknologi/20240624122531-185-1113359/fakta-fakta-kebocoran-data-pdns-dalang-hingga-jumlah-tebusan>
- Verihubs. (2022, November 14). 3 Modus Pencurian Data Pribadi yang Paling Sering Dilakukan. Verihubs. <https://verihubs.com/blog/pencurian-data-pribadi>
- Andika Dwi. (2024, July 1). 6 Dampak Serangan Ransomware ke Server PDNS. TEMPO. <https://www.tempo.co/digital/6-dampak-serangan-ransomware-ke-server-pdns-44346>
- Yusuf, M. (n.d.). Keberlakuan Peraturan dalam Undang-Undang Yang Tidak Kunjung Diterbitkan Peraturan Pemerintah sebagai Peraturan Pelaksananya.