

## Upaya Perlindungan Hukum Bagi Korban Tindak Pidana Pencurian Secara Digital

**Reisha Resmalah Febrianti**

Universitas 17 Agustus 1945 Surabaya, reisha.resmala@gmail.com

**Dr. Otto Yudianto, SH., M.Hum.**

Universitas 17 Agustus 1945 Surabaya, otto@untag-sby.ac.id

### **Abstract**

*nowdays namely the modern era where everything is digital, it does not rule out the possibility of digital theft and the need for protection for victims of digital theft. This research aims to learn about legal protection for victims of digital theft and how to advocate for the rights of these victims. Digital tools are also known as cyber or online tools. In general, all activities in modern times are digital and this research discusses forms of legal protection in the context of electronic transaction information law using normative legal research methods, especially approaches based on statutory regulations. legislative invitation and legal doctrine. Electronic transaction laws protect victims of digital theft of personal data. The use of any information regarding a person's personal data through electronic media must be carried out with the consent of the person concerned, in accordance with Article 26 paragraph (1) of the law on electronic transaction information, unless otherwise provided by laws and regulations. To determine criminal and material sanctions against perpetrators of personal data theft originating from outside Indonesia, the government must have an effective legal umbrella to protect consumers and users of digital technology. However, if the victim of personal data theft is from Indonesia, then the victim can get legal protection in the form of compensation submitted to the Witness and Victim Protection Agency (LPSK). Restitution is compensation for losses suffered by victims as a result of illegal activities, including digital theft of personal data.*

*Keywords: Victims, Theft, Digital*

### **Abstrak**

Pada masa sekarang yakni masa modern yang mana semua serba digital tidak menutup kemungkinan akan terjadi pencurian secara digital dan perlu adanya perlindungan bagi korban pencurian secara digital. Penelitian ini bertujuan untuk mempelajari tentang perlindungan hukum bagi korban pencurian digital dan bagaimana mengadvokasi hak-hak korban tersebut. Alat digital juga dikenal sebagai alat siber atau online. Pada umumnya segala aktivitas di zaman modern yang mana secara digital dan penelitian ini membahas tentang bentuk perlindungan hukum dalam konteks hukum informasi transaksi elektronik dengan menggunakan metode penelitian hukum normatif, khususnya pendekatan berdasarkan peraturan perundang-undangan. undang legislatif dan doktrin hukum. Undang-undang transaksi elektronik melindungi korban pencurian digital atas data pribadi. Penggunaan setiap informasi mengenai data pribadi seseorang melalui media elektronik harus dilakukan dengan persetujuan yang bersangkutan, sesuai dengan Pasal 26 ayat (1) undang-undang tentang informasi transaksi elektronik, kecuali ditentukan lain oleh peraturan perundang-undangan. Untuk menetapkan sanksi pidana dan materiil terhadap pelaku pencurian data pribadi yang berasal dari luar Indonesia, pemerintah harus memiliki payung hukum yang efektif untuk melindungi konsumen dan pengguna teknologi digital. Namun, jika korban pencurian data pribadi tersebut berasal dari Indonesia, maka korban dapat memperoleh perlindungan hukum berupa ganti rugi yang diserahkan kepada Lembaga Perlindungan Saksi dan Korban (LPSK). Restitusi adalah penggantian kerugian yang diderita oleh korban sebagai akibat dari aktivitas ilegal, termasuk pencurian data pribadi secara digital.

Kata kunci: korban, pencurian, digital

## Pendahuluan

Kasus pencurian di Indonesia terus melanda masyarakat sehingga perlu ditindaklanjuti dan diantisipasi. Motivasi pelaku tindak pidana pencurian umumnya untuk memenuhi kebutuhan ekonomi. Salah satunya adalah kurangnya ketersediaan lapangan kerja. Banyak orang telah menjadi korban pencurian dan tidak mengetahui proses pelaporan kejahatan kepada pihak berwenang.

Percepatan informasi itu sendiri juga harus diperhatikan dalam bidang informasi dan layanan. Setiap individu di era modern ini memiliki akses mudah ke banyak hal melalui internet. Laptop, tablet, ponsel pintar, dan perangkat lainnya dapat digunakan untuk mengakses internet. Kemudahan akses meningkatkan jumlah pengguna internet di Indonesia. Saat ini kemajuan teknologi sangat pesat. Dengan munculnya berbagai bentuk media digital, setiap individu kini memiliki banyak kemungkinan untuk mendapatkan informasi apapun yang mereka inginkan.

Memanfaatkan pesatnya perkembangan teknologi informasi dan komunikasi elektronik di era digital ini, pembatasan informasi ini dapat memudahkan masyarakat untuk melaporkan pencurian melalui aplikasi mobile smartphone di era digital ini. Semakin banyak institusi publik dan swasta yang mampu memanfaatkan teknologi informasi modern untuk meningkatkan kehidupan manusia, efisiensi, dan produksi. Namun, teknologi informasi di Internet berdampak serius dan berbahaya bagi keamanan data pribadi, karena dapat diretas dan semua perangkat yang terhubung ke Internet dapat digunakan oleh seseorang/orang-orang yang tidak bertanggung jawab atas apa yang disebut peretas (*hacker*). Menyiapkan sistem perlindungan data dan anti pencurian digital saat ini merupakan cara paling umum untuk memisahkan aliran pendapatan data berdasarkan jenis proyek uji tuntas.

Penting untuk dapat menciptakan dan mengesahkan undang-undang secara khusus/ditujukan untuk perlindungan data pribadi yang terkait dengan publik dan yang terkait dengan pencegahan pencurian data pribadi melalui sarana elektronik di Indonesia. Isu ini dikenal dengan perkembangan teknologi informasi modern yang menjadi tantangan hukum, terutama terkait dengan perlindungan data pribadi yang dikirimkan secara elektronik. Banyak pihak menggunakan email untuk berkomunikasi dan bernegosiasi, yang berujung pada pencurian identitas. Namun, saat ini belum ada undang-undang khusus yang melindungi masyarakat dari berbagai masalah terkait pencurian digital yang muncul saat menggunakan data pribadi dalam proses penggunaan teknologi informasi.

Peraturan tentang perlindungan sumber daya alam selama transit ke dan melalui Indonesia. Termasuk UU Perbankan No. 10 Tahun 1998 yang mengatur tentang data deposit/perbankan dan simpanan, serta UU No. 19 Tahun 2016 mengubah UU No. 11 Tahun 2008 tentang Informasi transaksi dan elektronik (UU ITE). Diperlukan konvergensi, yang memerlukan penggabungan beberapa peraturan ini menjadi satu undang-undang yang membahas perlindungan hukum atas data pribadi. Di Indonesia, kebijakan anti maling digital saat ini berbasis pada e-law. Kebijakan anti-pencurian digital berdasarkan e-law, mis. dengan penghapusan. Penghapusan di sini berdasarkan permintaan pemilik data seperti KTP/Kartu Keluarga/barang berharga lainnya yang tersimpan di handphone, guna meminimalisir terulangnya pencurian digital sekali klik. Pemberhentian berdasarkan perintah pengadilan.

Saat file ditautkan atau diklik, ponsel dan produk digital seperti laptop dan iPad secara otomatis dibajak, dan data disalahgunakan jika tidak dihapus.

Sementara itu, Kebijakan Penyalahgunaan Data Pribadi tertuang pada Pasal 15, 16, dan 17 Peraturan Pemerintah Nomor 71 Tahun 2019 “Tentang Penyelenggaraan Sistem dan Transaksi Elektronik”. Kebijakan pencurian identitas dilandasi oleh Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan khususnya terkait dengan pengucapan, pelapukan bisa juga dibagi dengan menjadi dua, yaitu delisting (hak delisting) dan delisting dari *search engine*. (Hak atas pengecualian). menghapus). Dijalankan oleh keputusan pengadilan sehubungan dengan dokumen elektronik dan / atau informasi tentang pencurian data. Pencurian digital sebanding dengan phishing ketika Anda mencoba mendapatkan informasi rahasia seseorang secara ilegal. Serangan phishing menargetkan informasi pribadi (nama, umur, alamat), informasi akun (nama pengguna dan kata sandi), dan informasi keuangan (nomor kartu kredit, akun). Seperti yang telah disebutkan pada kalimat sebelumnya, tindakan pencurian digital termasuk dalam kategori aturan nol. Karena kekosongan normatif bisa juga diartikan sebagai “keadaan masyarakat yang kosong, atau ketiadaan perundang-undangan (hukum) yang mengatur masyarakat (tatanan)”, maka kekosongan hukum/kekosongan norma yang berada didalam hukum positif lebih tepat diartikan yakni sebagai “kekosongan”.

Penulis menemukan beberapa poin perbedaan pada penelitian sebelumnya dengan topik pembahasan yang serupa dengan penelitian ini, yang mana penelitian ini memiliki kebaharuan yang membahas mengenai urgensi pembentukan peraturan perundang-undangan terkait pelaksanaan perlindungan hukum bagi korban pencurian digital yang perlu mendapatkan penyesuaian dalam penerapannya. agar tidak terjadi kekosongan norma yang dapat mengakibatkan tidak adanya upaya perlindungan hukum bagi korban pencurian digital dan pembahasan tersebut tidak ditemukan dalam beberapa penelitian berikut :

1. Jurnal tahun 2020 karya Muhammad Ramadhan, Dwi Oktafia Ariyanti dan Nita Ariyani yang berjudul “Pencurian *e-money* pada *e-commerce* dalam Tindak Pidana Ekonomi” dimana fokus penelitiannya menekankan pada bentuk konsep hukum pidana dalam memandang kejahatan *cybercrime* sebagai kejahatan ekonomi [1].
2. Jurnal tahun 2022 karya Putri Wahyu Widayanti yang berjudul “Tindak Pidana Pencurian Data Nasabah dalam bidang Perbankan sebagai *cybercrime*” yang dimana fokus penelitiannya menekankan pada bentuk modus operandi yang sering digunakan dalam tindak pidana pencurian data pribadi nasabah secara *cybercrime* [2].
3. Jurnal tahun 2020 karya Muhamad Hasan Rumlus dan Hanif Hartadi yang berjudul “Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik (*Policy the Discontinuation of Personal Data Storage In Electronic Media*)” yang dimana fokus penelitiannya mengenai keamanan atas data pribadi yang berlangsung melalui media elektronik [3].

Berdasarkan interpretasi diatas, maka penelitian di jurnal ini akan memberikan fokus tumpuan kepada “Bagaimanakah perlindungan hukum bagi korban pencurian secara digital menurut undang-undang Informasi Transaksi Elektronik?”.

### **Metode**

Penelitian ini menggunakan metode penelitian hukum normatif. Penelitian hukum yang menempatkan hukum sebagai sistem bangunan norma mengenai asas, norma, kaidah

hukum, putusan pengadilan, perjanjian, dan doktrin dikenal dengan penelitian yuridis normatif. Dilakukan dengan cara meneliti kepustakaan dan berperan dalam menyelesaikan dan mengklarifikasi persoalan-persoalan hukum yang sedang diselidiki. Pendekatan masalah menggunakan pendekatan undang-undang (*statute approach*), yaitu dilakukan dengan menelaah semua peraturan perundang-undangan yang terkait dengan masalah (*legal issues*) yang sedang dihadapi, dan pendekatan konseptual (*conceptual approach*), yang didasarkan pada pandangan dan doktrin yang berkembang dalam ilmu hukum. Menggunakan bahan hukum sekunder, primer, dan juga tersier digunakan dalam penelitian ini. Teknik ini penting karena dengan mengetahui pandangan-pandangan/doktrin-doktrin yang muncul dalam ilmu hukum dapat menjadi landasan untuk mengembangkan argumentasi-argumen hukum untuk menyelesaikan kesulitan-kesulitan hukum.

## **Hasil Dan Pembahasan**

### **Perlindungan Hukum**

Untuk memberi rasa aman kepada korban perlu adanya perlindungan hukum bagi korban. Yang dimaksud dengan perlindungan hukum adalah upaya untuk melindungi hak asasi manusia yang telah dilanggar ataupun dirampas oleh orang lain. Perlindungan hukum dapat dilakukan dalam beberapa bentuk, antara lain peraturan perundang-undangan, pemberian pertolongan kepada saksi dan/atau korban, dan pemberian jaminan kepastian hukum. Perlindungan hukum juga dapat dipandang sebagai jaminan yang diberikan oleh negara kepada semua pihak untuk dapat memperjuangkan hak dan kepentingan hukumnya dalam kedudukannya sebagai subjek hukum yang adil dan perlakuan yang sama di depan hukum. Pegawai Negeri Sipil (ASN) juga dapat diberikan perlindungan hukum berdasarkan asumsi tidak bersalah.

Cara untuk memperoleh perlindungan hukum bisa dilakukan juga dengan cara mengajukan gugatannya kepada pengadilan, melaporkan kejadian ke pihak berwajib, atau meminta bantuan dari lembaga perlindungan hukum seperti advokat atau lembaga bantuan hukum. Selain itu, masyarakat juga dapat memperoleh perlindungan hukum melalui kebijakan pemerintah yang memberikan perlindungan terhadap hak-hak warga negaranya. Dalam praktiknya, perlindungan hukum dapat diberikan dalam berbagai bentuk, seperti perlindungan hukum perdata, perlindungan anak, perlindungan konsumen, dan lain sebagainya. Perlindungan hukum juga dapat diberikan dalam bentuk preventif maupun represif [4].

Ada berbagai bentuk perlindungan hukum dalam konteks transaksi dan aktivitas digital di Indonesia. Berikut beberapa contohnya:

- a) Perlindungan Preventif: Perlindungan preventif ditujukan untuk mencegah terjadinya bahaya sejak awal. Dalam konteks transaksi digital, perlindungan preventif dapat dilakukan melalui edukasi dan sosialisasi, maupun melalui pembentukan badan pengatur seperti Otoritas Jasa Keuangan (OJK) yang memiliki tugas untuk memberi rasa aman terhadap konsumen juga masyarakat.
- b) Perlindungan Represif: Perlindungan represif ditujukan untuk menghukum mereka yang telah melakukan kejahatan. Dalam konteks transaksi digital, perlindungan represif dapat diberikan melalui upaya litigasi dan penegakan hukum oleh otoritas seperti kepolisian.

- c) Kerangka Hukum: Kerangka hukum seperti UU ITE memberikan dasar perlindungan hukum dalam konteks transaksi digital. UU ITE memuat ketentuan terkait kontrak elektronik, *cybercrime*, dan perlindungan konsumen.
- d) Bukti Elektronik: Penggunaan bukti elektronik dalam proses hukum adalah bidang lain di mana perlindungan hukum penting. UU ITE yaitu memberikan penggunaan alat-alat bukti/*proof* elektronik dipengadilan, namun masih terdapat tantangan terkait pembuktian dan keabsahan alat bukti tersebut.
- e) Kerjasama Internasional: Kerjasama internasional juga merupakan bentuk perlindungan hukum yang penting dalam konteks transaksi digital. Kejahatan dunia maya semakin menjadi perhatian di Indonesia, dan perlindungan hukum terhadap kejahatan dunia maya merupakan aspek penting dari keamanan digital. *Convention on Cybercrime* misalnya, menekankan perlunya kerjasama internasional dalam memerangi *cybercrime* yang bersifat global dan tanpa batas wilayah.
- f) Bitcoin dan Mata Uang Virtual: Dengan uang tersebut maupun lainnya dapat menghadirkan tantangan unik untuk perlindungan hukum. Meskipun ada upaya yang sedang berlangsung untuk mengatur mata uang virtual di Indonesia, masih terdapat ketidakjelasan mengenai status hukumnya dan perlindungan yang diberikan kepada investor [5].

Secara keseluruhan, perlindungan hukum dalam konteks transaksi digital di Indonesia dapat dilakukan dalam berbagai bentuk, antara lain tindakan preventif dan represif, kerangka hukum, dan kerjasama internasional. Bentuk-bentuk perlindungan ini bertujuan untuk mencegah terjadinya kerugian, menghukum mereka yang telah melakukan kerugian, dan memberikan dasar hukum untuk menangani masalah yang berkaitan dengan transaksi digital.

#### **Perlindungan Hukum Bagi Korban Pencurian secara Digital**

Dalam era modern seperti saat ini tentunya sudah memasuki era digital/online yang dimana semua hal berbasis online namun masih kurang adanya perlindungan hukum dan perlu adanya peraturan perundang-undangan yang membahas mengenai ini. Pencurian secara digital dapat memiliki dampak yang merugikan bagi korban. Korban pencurian data pribadi dapat mengalami kerugian finansial, seperti kehilangan uang dari rekening bank atau kartu kredit yang digunakan oleh pelaku. Selain itu, korban juga dapat mengalami kerugian non-finansial, seperti pencemaran nama baik atau identitas palsu yang digunakan oleh pelaku untuk melakukan tindakan kriminal lainnya. Korban juga dapat mengalami kerugian emosional, seperti kehilangan privasi dan rasa aman karena data pribadi mereka telah dicuri. Dalam hal ini, perlindungan hukum bagi ciptaan-ciptaan didalam era digital dan perlindungan data pribadi menjadi penting untuk mencegah terjadinya pencurian secara digital dan melindungi korban dari dampak yang merugikan.

Hak asasi manusia digital didefinisikan sebagai seperangkat hak masyarakat untuk mengakses, memanfaatkan, membuat, mentransmisikan, dan memperdagangkan informasi dan teknologi digital serta menyadari hak asasi manusia dalam ranah digital yang terikat pada pengguna tersebut sebagai subjek hukum [6]. Selain itu, perlindungan hukum di era digital juga mencakup perlindungan hak privasi atas data diri, hak cipta karya, dan hak konsumen

dalam transaksi digital. Pemerintah dan regulator perlu memperkuat sistem hukum di era teknologi digital untuk melindungi hak-hak tersebut.

Perlindungan hukum bisa diberikan terhadap korban pencurian secara digital dengan berlandaskan oleh UU No. 11 tahun 2008 tentang informasi dan transaksi elektronik. Pembajakan online dapat dilakukan berdasarkan ketentuan UU ITE [7]. UU ITE mengatur mengenai tindak pidana meliputi permasalahan tentang penggunaan teknologi informasi dan transaksi elektronik, termasuk tindakan pidana yang terkait dengan pencurian data atau informasi secara digital. Pasal 26 ayat (1) UU ITE yang menyatakan bahwa penggunaan suatu informasi melalui media elektronik mengenai data pribadi seseorang harus dilakukan atas persetujuan yang bersangkutan, kecuali ditentukan lain oleh peraturan perundang-undangan, merupakan salah satu pasal-pasal yang berkaitan dengan tindak pidana pencurian dalam UU ITE. Selain itu, privasi data pribadi yang diatur didalam Undang-Undang Perlindungan Data Pribadi (UU PDP), yang memberikan hak kepada pemilik data untuk menuntut kerugian yang timbul akibat penggunaan data pribadi yang tidak sah [8].

Penguatan sistem hukum di era teknologi digital juga menjadi suatu hal yang harus dapat dilakukan oleh setiap negara termasuk Indonesia, untuk menjaga keseimbangan antara efektivitas dan efisiensi dengan moralitas etika dan Pasal 30 yang mengatur tentang tindakan pidana yang terkait dengan akses ilegal. Dilain hal, pada pasal 31 UU ITE mengatur kejahatan atau yang disebut dengan tindak pidana yang berhubungan dengan penggunaan data atau informasi yang tidak sah, misalnya KUHP mengatur kejahatan pencurian identitas "di tangan orang yang terlibat". Tindakan hukum bisa dilakukan. Bagaimana sistem hukum di Indonesia terhadap orang yang melakukan pencurian data online dan kejahatan pencurian identitas. Pelaku kejahatan ini dapat dipenjara dan/atau didenda [9]. Terjadinya pencurian merupakan akibat buruk dari kemajuan negara kita. Misalnya, pencurian sebagian besar dilakukan oleh individu sebagai akibat dari struktur ekonomi yang rusak akibat seringnya kenaikan harga dan inflasi yang tinggi, serta distribusi pendapatan yang tidak merata dalam masyarakat dan tingkat pertumbuhan penduduk yang disebabkan oleh sulitnya mencari pekerjaan. Kesempatan untuk melakukan kejahatan, pengaruh lingkungan, kurangnya kesadaran hukum pelaku, dan unsur sosial lainnya adalah beberapa hal lain yang mendorong melakukan kejahatan pencurian [10].

Menurut perspektif didalam UU ITE, Korban pencurian digital yakni dilindungi undang-undang. Berikut beberapa poin penting terkait perlindungan korban pencurian digital di Indonesia:

- a) Cybercrime: Cybercrime menjadi perhatian yang berkembang di Indonesia, seperti di banyak negara lain. UU ITE memuat ketentuan terkait kejahatan dunia maya, seperti peretasan, penipuan kartu kredit, dan bentuk kejahatan dunia maya lainnya yang tidak dibatasi oleh batas wilayah.
- b) Perlindungan Hukum: UU ITE memberikan perlindungan hukum bagi korban pencurian digital. Undang-undang tersebut memuat ketentuan terkait transaksi elektronik, antara lain kontrak elektronik, kejahatan siber, dan perlindungan konsumen
- c) Litigasi: Korban pencurian digital dapat mencari jalan hukum melalui litigasi. UU ITE memungkinkan sanksi perdata dan pidana bagi mereka yang melakukan pencurian digital

Secara keseluruhan, korban pencurian digital dilindungi oleh UU ITE. Undang-undang tersebut memuat ketentuan terkait kejahatan dunia maya dan memberikan perlindungan hukum bagi korban pencurian digital. Korban dapat mencari jalan hukum melalui litigasi, yang memungkinkan hukuman perdata dan pidana bagi mereka yang terlibat dalam pencurian digital [11].

Selain itu, korban pencurian secara online juga dapat memperoleh perlindungan hukum dengan melaporkan kejadian ke pihak berwajib, mengajukan gugatan ke pengadilan, atau meminta bantuan dari lembaga perlindungan hukum seperti advokat atau lembaga bantuan hukum. Dalam praktiknya, korban pencurian secara digital dapat memperoleh perlindungan hukum dengan mengajukan laporan ke pihak berwajib yang memiliki kewenangan untuk menangani kasus pencurian secara online. Selain itu, korban juga dapat meminta bantuan dari lembaga perlindungan hukum seperti advokat atau lembaga bantuan hukum untuk mendapatkan bantuan hukum dalam menyelesaikan kasusnya .

Upaya mempertahankan hak korban pencurian secara digital bisa juga melakukan dengan beberapa cara. Yang mana salah satunya yaitu bisa memperkuat sistem hukum di era teknologi digital untuk melindungi hak privasi dan data pribadi korban. Selain itu, korban juga dapat melakukan tindakan preventif untuk melindungi data pribadi mereka, seperti memastikan data terenkripsi, menghindari *access point* (akses poin) yang berpotensi akan meminta username, password, dan informasi pribadi lainnya, dan waspada terhadap tautan phishing. Jika terjadi pencurian data, korban dapat melaporkan kejadian tersebut ke pihak berwenang dan meminta bantuan untuk mengembalikan data yang dicuri serta memperoleh restitusi. Selain itu, penting juga untuk meningkatkan kesadaran masyarakat tentang pentingnya melindungi data pribadi dan hak privasi mereka di era digital [12].

Untuk memberikan sanksi pidana dan materiil terhadap pelaku pencurian data pribadi yang berasal dari luar Indonesia, pemerintah perlu memiliki payung hukum yang memadai untuk melindungi konsumen dan pengguna teknologi digital. Selain itu, perlindungan hukum terhadap hak cipta karya dalam era digital juga perlu diperhatikan [13]. Dalam kasus pencurian identitas, pelaku pertama-tama mendapatkan akses secara tidak sah ke sistem komputer orang lain dan dapat dikenakan hukuman pidana. Namun, jika menjadi korban pencurian identitas di Indonesia, korban dapat berhak mendapatkan perlindungan hukum dengan mengajukan surat pernyataan kepada Lembaga Perlindungan Korban dan Saksi (LPSK). Restitusi adalah pengembalian kerugian yang diderita oleh korban akibat tindak pidana, termasuk pencurian data pribadi secara digital.

Perbedaan pencurian di Kitab Undang-Undang Hukum Pidana (KUHP) lama dan KUHP 2023 belum dapat dijelaskan secara rinci karena pencurian merupakan tindak pidana yang diatur dalam KUHP baik yang lama maupun yang baru. Namun, pada KUHP lama diatur dua jenis hukuman pidana, yaitu pidana pokok dan pidana tambahan, sedangkan pada UU Nomor 1 Tahun 2023, diatur tiga jenis sanksi pidana, yaitu pidana pokok, pidana tambahan, dan pidana khusus. Ancaman hukuman bagi pelaku tindak pidana pencurian diatur dalam Pasal 362-365 KUHP, yang mengatur tentang pencurian biasa, pencurian dengan pemberatan, dan pencurian ringan. Tujuan pembaruan dalam UU ITE di Indonesia adalah untuk memberikan perlindungan yang lebih baik bagi kreator, pemegang hak cipta, dan kreator konten yang telah menciptakan ide kreatif berupa konten video di platform seperti YouTube [14]. Pembatasan yang ada tidak cukup untuk melindungi dari pelanggaran hak

cipta dan kejahatan dunia maya lainnya. Selain itu, undang-undang teknologi informasi bertujuan untuk mengatur penggunaan teknologi informasi, khususnya di bidang transaksi elektronik, agar dilakukan secara benar, menghormati keamanan, dan kepentingan orang. Namun, penggunaan UU ITE berpotensi menimbulkan tindak pidana jika melanggar undang-undang. Pemutakhiran UU ITE juga dapat membantu mengatasi masalah yang berkaitan dengan kejahatan dunia maya, termasuk pencurian dunia maya dan penipuan dunia maya. Selanjutnya, pemutakhiran UU ITE dapat mendorong literasi digital dan kemandirian belajar di kalangan siswa dengan memanfaatkan bahan ajar berbasis internet [15].

Kerja sama internasional sangat penting dalam memerangi kejahatan dunia maya, termasuk pencurian dunia maya. Sifat global kejahatan dunia maya mempersulit masing-masing negara untuk mengatasi masalah ini sendirian. Oleh karena itu, kerja sama hukum internasional diperlukan untuk membangun landasan yang kuat dalam memerangi kejahatan dunia maya. Beberapa organisasi internasional dan masing-masing negara memiliki pengalaman dan praktik yang luas di bidang ini yaitu Organisasi dan negara ini telah membentuk kerangka peraturan untuk memerangi kejahatan dunia maya. Beberapa organisasi internasional yang menangani kejahatan dunia maya termasuk *United Nations Office on Drugs and Crime* dan Dewan Eropa (UNODC). UNODC telah mengembangkan rancangan studi komprehensif tentang kejahatan dunia maya, sementara Dewan Eropa telah membentuk Konvensi Kejahatan Dunia Maya, yang melibatkan pelaksanaan kerja sama internasional. Selain itu, studi perbandingan strategi keamanan siber nasional sepuluh negara menemukan bahwa perang melawan kejahatan dunia maya merupakan upaya bersama antara berbagai pemangku kepentingan, dikarenakan demikian maka dari itu diperlukan kerja sama internasional yang kuat.

Namun, penting untuk dicatat bahwa ini bukan satu-satunya organisasi atau negara yang berurusan dengan kejahatan dunia maya, dan mereka telah menetapkan kerangka peraturan untuk memerangi kejahatan dunia maya. Namun, masih ada tantangan yang dihadapi oleh pemerintah yang mengadopsi undang-undang dan konvensi internasional melawan kejahatan dunia maya. Kerangka hukum yang ada untuk kerja sama internasional dalam melawan kejahatan dunia maya bersifat regional, terfragmentasi, dan tidak efisien. Singkatnya, kerja sama internasional sangat penting dalam mengatasi pencurian dunia maya dan bentuk kejahatan dunia maya lainnya yang memengaruhi banyak negara.

### **Kesimpulan**

UU ITE memberikan perlindungan bagi korban pencurian data pribadi secara digital. Beberapa pendekatan dapat diambil untuk melindungi hak-hak korban pencurian digital. Untuk melindungi hak privasi dan informasi pribadi korban dengan lebih baik di era teknologi digital, salah satu solusinya adalah dengan meningkatkan sistem hukum. Selain itu, korban dapat mengambil tindakan pencegahan untuk melindungi informasi sensitif mereka. Pemerintah membutuhkan kerangka hukum yang efektif untuk melindungi konsumen dan pengguna teknologi digital guna memberikan hukuman pidana dan materiil terhadap pelaku pencurian data pribadi yang berasal dari luar Indonesia. Pasal 26 ayat (1) UU ITE memberikan perlindungan bagi korban pencurian data pribadi secara digital. Upaya perlindungan hak korban pencurian digital dapat dilakukan dengan berbagai cara. Untuk melindungi hak privasi dan informasi pribadi korban dengan lebih baik di era teknologi digital, salah satu



solusinya adalah dengan meningkatkan sistem hukum. Selain itu, korban dapat mengambil tindakan pencegahan untuk melindungi informasi sensitif mereka. Untuk menetapkan hukuman pidana dan materiil terhadap pelaku pencurian data pribadi yang berasal dari luar Indonesia, pemerintah harus memiliki kerangka hukum yang memadai untuk melindungi pengguna dan pelanggan teknologi digital.

### Ucapan Terima Kasih

Penulis mengucapkan terima kasih dan juga rasa syukur karena telah menyelesaikan penulisan jurnal sebagai syarat mengerjakan tugas akhir yaitu skripsi yang berjudul “Perlindungan Hukum Bagi Korban Tindak Pidana Pencurian secara Digital” kepada:

1. Tuhan Yang Maha Esa
2. Prof. Dr. Slamet Suhartono, S.H., M.H., CMC. Selaku dekan fakultas hukum Universitas 17 Agustus 1945 Surabaya.
3. Dr. Otto Yudianto, SH., M.Hum. selaku dosen pembimbing yang senantiasa membimbing dalam penulisan jurnal ini.

### Daftar Pustaka

- [1] Muhammad Ramadhan, D. O. Ariyanti, and Nita Ariyani, “Pencurian e-money pada e-commerce dalam Tindak Pidana Cybercrime sebagai Tindak Pidana Ekonomi,” *Reformasi Hukum*, vol. 24, no. 2, pp. 169–188, Dec. 2020, doi: 10.46257/jrh.v24i2.179.
- [2] Putri Wahyu Widayanti, “TINDAK PIDANA PENCURIAN DATA NASABAH DALAM BIDANG PERBANKAN SEBAGAI CYBER CRIME,” vol. 2, no. 2, Jul. 2022.
- [3] Muhamad Hasan Rumlus and Hanif Hartadi, “Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik,” vol. 1, no. 2, 2020.
- [4] S. Yuniarti, “PERLINDUNGAN HUKUM DATA PRIBADI DI INDONESIA,” *Business Economic, Communication, and Social Sciences (BECOSS) Journal*, vol. 1, no. 1, pp. 147–154, Sep. 2019, doi: 10.21512/becossjournal.v1i1.6030.
- [5] M. Minarosa, “Legal Protection of Personal Data Owners as Cybercrime Victims Based on regulations regarding Electronic Information and Transactions,” in *Proceedings of the First Multidiscipline International Conference, MIC 2021, October 30 2021, Jakarta, Indonesia*, EAI, 2022. doi: 10.4108/eai.30-10-2021.2315833.
- [6] S. A. Kusnadi, “PERLINDUNGAN HUKUM DATA PRIBADI SEBAGAI HAK PRIVASI,” *AL WASATH Jurnal Ilmu Hukum*, vol. 2, no. 1, 2021, doi: 10.47776/alwasath.v2i1.127.
- [7] M. P. Sari, D. Mamang, and M. Zakky, “Penegakkan Hukum terhadap Tindak Pidana Pencurian Data Pribadi melalui Internet Ditinjau dari Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE (Informasi dan Transaksi Elektronik),” *Jurnal Hukum Jurisdictie*, vol. 3, no. 2, 2021, doi: 10.34005/jhj.v3i2.44.
- [8] M. R. Hertianto, “Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia,” *Kertha Patrika*, vol. 43, no. 1, p. 93, Apr. 2021, doi: 10.24843/KP.2021.v43.i01.p07.
- [9] 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, 2021, doi: 10.51370/jhpk.v2i2.43.
- [10] A. Dermawan, “Urgensi Perlindungan Hukum Bagi Korban Tindak Pidana Kejahatan Teknologi Informasi,” vol. 2, no. 2, p. 44, 2019.
- [11] R. Oktana, S. Akub, and M. Maskun, “Social Media in the Process of Evidence of Electronic Information and Transaction Crimes,” *SIGn Jurnal Hukum*, vol. 4, no. 2, pp. 320–331, Mar. 2023, doi: 10.37276/sjh.v4i2.252.

- [12] L. K. Saragih, D. Budhijanto, and S. Somawijaya, "PERLINDUNGAN HUKUM DATA PRIBADI TERHADAP PENYALAHGUNAAN DATA PRIBADI PADA PLATFORM MEDIA SOSIAL BERDASARKAN UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEK," *DE'RECHTSSTAAT*, vol. 6, no. 2, pp. 125–142, Oct. 2020, doi: 10.30997/jhd.v6i2.2676.
- [13] I. Anggraeny, C. Monique, Y. Puspitasari Wardoyo, and A. Bhirini Slamet, "The Urgency of Establishing Guidelines for Handling Cybercrime Cases in the Indonesian National Police Department," *KnE Social Sciences*, Oct. 2022, doi: 10.18502/kss.v7i15.12107.
- [14] K. M. Simatupang, "Tinjauan Yuridis Perlindungan Hak Cipta dalam Ranah Digital," *Jurnal Ilmiah Kebijakan Hukum*, vol. 15, no. 1, p. 67, Mar. 2021, doi: 10.30641/kebijakan.2021.V15.67-80.
- [15] M. Prasetyo, "Legal Protection as a Form of State Responsibility for Victims of Cyber Crime in Indonesia," in *Proceedings of The International Conference on Environmental and Technology of Law, Business and Education on Post Covid 19, ICETLAWBE 2020, 26 September 2020, Bandar Lampung, Indonesia*, EAI, 2020. doi: 10.4108/eai.26-9-2020.2302588.