Legal Dialogica
Volume 1 Issue 1

Penegakan Hukum Terhadap Eksistensi Tindak Pidana Pemalsuan Identitas di Era Digital

Nurhalisa Faisal[1], Aan Aswari[2], Muhammad Azham Ilham[3]
[1]*Fakultas Hukum, Universitas Muslim Indonesia*
[2]*Fakultas Hukum, Universitas Muslim Indonesia*
[3]*Fakultas Hukum, Universitas Muslim Indonesia*
[Ω]*Surel Koresponden: nurhalisafsl@gmail.com*

***Abstract**:*
This research aims to determine and analyze the application of material criminal law to criminal acts of identity fraud in the digital era and criminal law enforcement in protecting individual personal data based on the Criminal Code (KUHP). This research uses Normative Empirical legal research methods. The results of this research show that (1) The application of material criminal law to criminal acts of identity fraud in the digital era has shown an unpreparedness in dealing with crimes that are developing along with the rapid progress of information and communication technology. Factors such as the public's lack of legal awareness, as well as the incompatibility between existing regulations and technological developments, influence the effectiveness of the application of material criminal law to the crime of digital identity fraud. (2) the effectiveness of criminal law enforcement in protecting individual personal data based on the Criminal Code (KUHP) is still considered less than optimal. The regulations regarding personal data protection in the Criminal Code are not specific enough considering the rapid development of information technology which affects the way personal data is collected, processed and distributed.

***Keywords:** identity fraud, Criminal Code, Law Enforcement*

***Abstrak**:*
Penelitian ini bertujuan untuk mengetahui dan menganalisis penerapan hukum pidana materil terhadap tindak pidana pemalsuan identitas di era digital dan penegakan hukum pidana dalam melindungi data pribadi individu berdasarkan Kitab Undang-Undang Hukum Pidana (KUHP). Penelitian ini menggunakan metode penelitian hukum Normatif Empiris. Hasil penelitian ini menunjukan bahwa (1) Penerapan hukum pidana materil terhadap tindak pidana pemalsuan identitas di era digital telah menunjukkan adanya ketidaksiapan dalam mengatasi kejahatan yang berkembang seiring dengan pesatnya kemajuan teknologi informasi dan komunikasi. Faktor seperti kurangnya kesadaran hukum masyarakat, serta ketidaksesuaian antara regulasi yang ada dan perkembangan teknologi, mempengaruhi efektivitas penerapan hukum pidana materil terhadap kejahatan pemalsuan identitas digital. (2) efektivitas penegakan hukum pidana dalam melindungi data pribadi individu berdasarkan Kitab Undang-Undang Hukum Pidana (KUHP) masih terbilang kurang optimal. Pengaturan tentang perlindungan data pribadi dalam KUHP tidak cukup spesifik mengingat pesatnya perkembangan teknologi informasi yang mempengaruhi cara data pribadi dikumpulkan, diproses, dan disebarkan.

***Kata Kunci**: pemalsuan identitas, KUHP, Penegak Hukum.*

PENDAHULUAN

Di era digital teknologi informasi telah membawa perubahan besar dalam berbagai aspek kehidupan, termasuk kemudahan akses data dan transaksi. Era digitalisasi ini setiap orang memiliki kesempatan yang sama untuk menampilkan versi media teks merek kepada

publik. Keuntungan lain yang ditawarkan oleh progress digitalisasi berkaitan dengan kreatifitas. Ketika teks media menjadi lebih terbuka dan jenis medium menjadi lebih beraneka ragam, maka ada lebih banyak kesempatan bagi kreatifitas dan spesialisasi atas produk media itu. Namun, disisi lain kemajuan ini juga menghadirkan berbagai tantangan terutama terkait dengan keamanan dan perlindungan data pribadi. Salah satu tantangan terbesar adalah tindak pidana pemalsuan identitas yang kian marak seiring dengan meningkatnya penggunaan platform digital.[1]

Pemalsuan identitas di era digital dapat dilakukan melalui berbagai metode, mulai dari pencurian data pribadi di media sosial hingga peretasan basis data yang menyimpan informasi sensitif. Menurut beberapa penelitian sebelumnya, pemalsuan identitas bukan hanya berdampak pada individu yang menjadi korban, tetapi juga merugikan institusi atau perusahaan yang terkait. Pemalsuan identitas di era digital saat ini menunjukkan bahwa kejahatan ini semakin marak seiring dengan meningkatnya penggunaan teknologi informasi. Pemalsuan identitas sering terjadi dalam konteks online, seperti dalam pengajuan pinjaman atau transaksi digital, di mana pelaku menggunakan identitas palsu untuk mendapatkan keuntungan finansial. Dengan meningkatnya penggunaan internet dan media sosial, individu semakin rentan terhadap kejahatan seperti pemalsuan identitas. Data menunjukkan bahwa kerentanan terhadap penipuan digital di Indonesia mencapai 98,3%, dengan banyak individu yang pernah menjadi korban penipuan identitas. Fenomena ini menciptakan kerugian bagi individu dan institusi, serta menimbulkan kekhwatiran terkait keamanan data pribadi.

Salah satu contoh nyata dari fenomena ini adalah kasus pemalsuan identitas yang terjadi di platform media sosial, di mana individu dapat dengan mudah menciptakan akun palsu untuk menipu orang lain. Pelaku membuat akun dengan nama dan foto profil seseorang yang dikenal, kemudian menghubungi teman-teman korban dengan menawarkan investasi atau produk yang tidak ada. Dalam beberapa kasus, pelaku juga meminta uang dengan dalih mendesak. Banyak korban mengalami kerugian finansial dan kehilangan kepercayaan terhadap platform media sosial. Beberapa korban juga mengalami dampak psikologis akibat penipuan tersebut.

Perbuatan tersebut sebagaimana diatur dalam Pasal 45 Ayat (3) UU ITE ssmengatur tentang sanksi pidana bagi pelaku yang menyebarkan identitas orang lain tanpa izin. Sanksi ini mencakup pidana penjara paling lama 4 tahun dan/atau denda paling banyak Rp750.000.000,00. Ini menunjukkan bahwa tindakan pemalsuan identitas digital, seperti pembuatan akun palsu di media sosial, dapat dikenakan sanksi yang tegas.

Berbagai penelitian telah menunjukkan bahwa regulasi hukum yang ada meskipun sudah mengatur pemalsuan identitas masih mengalami tantangan dalam implementasinya di era digital. Salah satu penyebabnya adalah perkembangan teknologi yang jauh lebih cepat dibandingkan dengan kemampuan penegak hukum untuk beradaptasi. Fenomena pemalsuan identitas di era digital melibatkan berbagai teknik, seperti penggunaan nama palsu atau data palsu untuk melakukan penipuan. Dalam konteks ini, pentingnya memahami bahwa tindakan ini sering kali dilakukan dengan modus operandi yang canggih

[1] Agus Hiplunudin. (2019). *Politik Era Digital.* Yogyakarta: Suluh Media, hlm. 29.

dan memanfaatkan kelemahan dalam sistem verifikasi identitas digital. Pemalsuan identitas tidak hanya berdampak finansial tetapi juga dapat mengakibatkan kerugian reputasi dan dampak psikologis yang signifikan bagi korban. Korban sering mengalami stres, kecemasan, dan kehilangan kepercayaan diri akibat tindakan penipuan ini.

Selain itu, batasan yurisdiksi internasional kerap kali menjadi hambatan dalam penegakan hukum terhadap pelaku yang beroperasi lintas negara. Alasan yang mendasari dilakukan penelitian pemalsuan identitas ini merupakan salah satu tindak pidana yang semakin marak terjadi seiring dengan perkembangan teknologi di era digital. Kemajuan teknologi informasi telah mempermudah akses terhadap data pribadi yang kemudian disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab untuk tujuan kejahatan. Pemalsuan identitas tidak hanya merugikan individu, tetapi juga perusahaan, lembaga, negara, dan terutama dalam sektor keuangan, perdagangan, dan layanan publik.

Dalam era digital yang semakin maju, teknologi telah membuka peluang baru dalam berbagai aspek kehidupan, termasuk komunikasi, transaksi bisnis, dan penyebaran informasi. Namun, kemajuan ini juga membawa tantangan baru, terutama dalam hal keamanan dan perlindungan identitas. Tindak pidana pemalsuan identitas kini menjadi ancaman serius di dunia digital, di mana pelaku kejahatan dapat dengan mudah mengakses, mengubah, atau menyalahgunakan identitas individu untuk kepentingan tertentu. Meskipun Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) mengatur beberapa aspek kejahatan digital, termasuk penyalahgunaan data, namun regulasi yang secara spesifik mengatur tentang pemalsuan identitas masih minim. UU ITE dan peraturan terkait cenderung bersifat umum dan belum mengakomodasi modus-modus baru dalam pemalsuan identitas digital, seperti penggunaan akun palsu untuk pencucian uang, penipuan keuangan, atau manipulasi data pribadi secara langsung untuk kepentingan kriminal. Tanpa pengaturan yang jelas, penegakan hukum menjadi lemah karena sulit untuk menentukan batasan pelanggaran dan jenis sanksi yang tepat.

Segala sesuatu yang telah diketahui berkaitan dengan masalah yang diteliti:

1. Beberapa penelitian terdahulu menunjukkan bahwa pemalsuan identitas sering kali terjadi karena lemahnya proteksi data pribadi di dunia maya serta rendahnya kesadaran masyarakat akan pentingnya menjaga keamanan data.
2. Pentingnya penelitian Ini dilakukan dilakukan karena maraknya pemalsuan identitas digital saat ini dapat menimbulkan dampak yang luas terhadap masyarakat mulai dari kerugian materiil hingga pelanggaran hak privasi. Jika pemalsuan identitas dibiarkan tanpa penanganan yang efektif maka akan berpotensi mengganggu stabilitas ekonomi, sosial, dan keamanan nasional. Selain itu, dengan meningkatnya tren transformasi digital saat di berbagai sektor, keberadaan regulasi yang kuat dan penegakan hukum yang tegas sangat diperlukan untuk melindungi masyarakat dari tindak pidana ini.
3. Dalil Aqli (Al-Qur’an dan Hadist) dan Analisis Keterkaitannya
   Dalam perspektif Islam, menjaga kehormatan dan identitas pribadi merupakan bagian dari menjaga harta dan hak-hak seseorang. Al-Qur'an mengingatkan umat Islam untuk tidak melakukan penipuan dan kezaliman. Ayat ini menegaskan bahwa setiap bentuk kezaliman termasuk pemalsuan identitas untuk mengambil keuntungan secara tidak sah adalah tindakan yang dilarang dalam Islam. Pemalsuan identitas dapat merampas hak-

hak individu dan menimbulkan kerugian materil maupun non-materil, yang pada dasarnya bertentangan dengan prinsip keadilan dalam Islam. Penegakan hukum terhadap tindak pidana pemalsuan identitas di era digital menjadi bentuk nyata dari usaha menjaga keadilan dan melindungi hak-hak setiap individu sebagaimana diajarkan dalam syariat Islam.[2]

Dalam sebuah hadis, Rasulullah SAW bersabda tentang pentingnya kejujuran: "Tanda munafik itu ada tiga: jika berbicara, ia berdusta; jika berjanji, ia ingkar; dan jika diberi amanah, ia khianat." Ini menunjukkan bahwa pemalsuan identitas merupakan tindakan yang sangat dilarang dalam Islam.

METODE

Tipe penelitian yang akan digunakan adalah Penelitian hukum Normatif Empiris yaitu penelititian ini bertujuan untuk mengevaluasi dan memahami bagaimana hukum yang ada diterapkan serta bagaimana hukum tersebut mengatur tindakan pemalsuan identitas, dan adanya data-data lapangan sebagai sumber data utama seperti wawancara yang berhubungan dengan judul skripsi penulis.

HASIL DAN PEMBAHASAN

A. Penerapan Hukum Pidana Materil terhadap Tindak Pidan Pemalsuan Identitas di Era Digital

Penerapan hukum berarti bahwa tindak pidana merupakan tindakan yang dilarang oleh peraturan hukum, yang mana larangan tersebut disertai dengan ancaman sanksi pidana. Penerapan hukum berperan dalam memastikan kepastian hukum serta memberikan perlindungan hukum di tengah era modernisasi dan globalisasi saat ini, agar nilai-nilai moral dalam masyarakat tetap terjaga dengan baik, selaras, seimbang, dan harmonis.

Soerjono Soekanto dalam bukunya yang berjudul “Pendekatan Sosiologi terhadap Hukum” menyatakan bahwa penerapan hukum *(law enforcement)* memerlukan empat syarat, yaitu: pertama, adanya aturan hukum yang jelas; kedua, adanya lembaga yang bertanggung jawab untuk menerapkan aturan tersebut; ketiga, adanya fasilitas yang mendukung pelaksanaan aturan itu; dan keempat, adanya kesadaran hukum dari masyarakat yang terpengaruh oleh aturan tersebut.

Penerapan hukum pidana terdiri dari tiga tahap, yaitu:

1. Tahap Formulasi: Pada tahap ini, penegakan hukum pidana dimulai dengan badan pembentuk undang-undang. Dalam tahap ini, pembuat undang-undang memilih nilai-nilai yang relevan dengan kondisi dan situasi saat ini serta yang akan datang. Nilai-nilai tersebut kemudian dirumuskan dalam bentuk peraturan perundang-undangan pidana dengan tujuan mencapai hasil yang baik dalam sistem perundang-undangan pidana. Tahap ini juga dikenal sebagai tahap kebijakan legislasi.
2. Tahap Aplikasi: Pada tahap ini, penegakan hukum pidana dilakukan oleh aparat penegak hukum, mulai dari Kepolisian, Kejaksaan, hingga Pengadilan. Aparat penegak hukum bertugas untuk menegakkan dan menerapkan peraturan perundang-undangan

[2] QS. Al-Baqarah (2:188)

pidana yang telah dibuat oleh badan pembentuk undang-undang. Dalam menjalankan tugasnya, aparat penegak hukum harus tetap berpegang pada nilai-nilai keadilan dan kemanfaatan. Tahap ini disebut juga sebagai tahap kebijakan yudikatif.

3. Tahap Eksekusi: Tahap ini adalah penegakan hukum pidana secara konkret oleh aparat pelaksana pidana, yang bertugas untuk menegakkan aturan yang telah ditetapkan oleh pembentuk undang-undang melalui penerapan pidana yang diputuskan oleh pengadilan.

Pengaruh teknologi dan globalisasi terhadap hukum pidana materil merupakan fenomena yang signifikan dalam perkembangan sistem hukum saat ini. Perubahan teknologi yang pesat dan globalisasi telah memberikan dampak mendalam terhadap jenis-jenis kejahatan yang muncul serta cara penegakan hukum dan penanganannya. Berikut adalah beberapa aspek utama dari pengaruh teknologi dan globalisasi dalam hukum pidana materil:

1. **Perkembangan Kejahatan Teknologi**: Teknologi informasi dan internet memudahkan pelaku kejahatan dalam melakukan tindak pidana seperti kejahatan dunia maya *(cybercrime),* pencurian identitas, penipuan online, dan penyebaran konten ilegal atau merugikan.
2. **Perlindungan Data Pribadi**: Dengan meningkatnya penggunaan teknologi digital, perlindungan terhadap data pribadi dan keamanan informasi menjadi isu penting. Hukum pidana materiel harus dapat mengadaptasi perlindungan terhadap privasi dan keamanan dalam konteks perkembangan teknologi yang terus berubah.
3. **Penyelundupan dan Perdagangan Global**: Globalisasi mempermudah pergerakan barang dan orang lintas batas negara, yang juga membawa tantangan baru dalam penanganan kejahatan seperti penyelundupan narkotika, senjata ilegal, dan perdagangan manusia.
4. **Pembuktian Elektronik**: Perkembangan teknologi mempengaruhi cara pembuktian dalam proses hukum pidana, di mana bukti elektronik dan digital menjadi semakin penting. Hal ini memerlukan keahlian khusus untuk analisis dan verifikasi bukti tersebut.
5. **Hukum Internasional dan Kerjasama Antarnegara**: Globalisasi mendorong perlunya kerjasama internasional dalam penegakan hukum, terutama dalam hal pengejaran pelaku kejahatan lintas batas serta harmonisasi hukum pidana materil antar negara.[3]

Penerapan hukum sangat berhubungan dengan tindak pidana pemalsuan identitas di era digital, karena kemajuan teknologi informasi dan komunikasi telah menciptakan ruang baru bagi munculnya kejahatan tersebut. Pemalsuan identitas di dunia digital bisa terjadi melali berbagai cara, seperti penyalahgunaan data pribadi, pencurian identitas, atau manipulasi informasi yang dapat merugikan korban secara finansial maupun reputasi.

Kejahatan pemalsuan mengandung unsur ketidakbenaran atau kepalsuan terhadap suatu objek yang seolah-olah tampak benar dari luar, padahal sesungguhnya bertentangan dengan kenyataan. Perbuatan pemalsuan merupakan jenis pelanggaran terhadap dua norma dasar, yaitu:

[3] Henny Saida Flora et al., (2024). *Hukum Pidana di Era Digital*. Batam: CV. Rey Media Grafika, hlm. 38-39.

1. Kebenaran (kepercayaan), yang pelanggarannya termasuk dalam kelompok kejahatan penipuan.
2. Ketertiban masyarakat, yang pelanggarannya dapat digolongkan dalam kelompok kejahatan terhadap negara atau ketertiban masyarakat.[4]

Perlindungan yang memadai sangat diperlukan untuk penyebaran gagasan dalam bentuk publikasi, baik itu melalui surat kabar, majalah, buku, pamflet, film, televisi, atau, yang terbaru, internet, agar suatu masyarakat dapat dianggap benar-benar demokratis. Pemerintah perlu menetapkan regulasi yang mendukung pengembangan teknologi informasi untuk mendorong perdagangan dan pertumbuhan ekonomi negara, sekaligus mencegah penyalahgunaannya.

Sebuah sistem hukum baru, yang dikenal sebagai "hukum siber" atau "hukum telematika", telah muncul. Istilah "hukum siber" dan *"cyber law"* digunakan secara internasional untuk merujuk pada hukum yang mengatur penggunaan teknologi informasi dan komunikasi. Ini bertujuan untuk menyeimbangkan pembangunan nasional Indonesia yang tengah berlangsung. Dalam bidang teknologi informasi dan transaksi elektronik, diperlukan globalisasi informasi yang berdampak pada perubahan sosial dan perilaku masyarakat.[5]

Mengingat Indonesia adalah bagian dari masyarakat informasi global, maka perlu ada peraturan mengenai pengelolaan informasi di tingkat nasional. Untuk memastikan perkembangan teknologi informasi dapat berjalan secara optimal dan seragam, serta dapat diakses oleh seluruh lapisan masyarakat guna meningkatkan kualitas hidup, hal ini memerlukan undang-undang yang jelas untuk melindungi informasi dari penyalahgunaan, dengan tetap memperhatikan peraturan hukum yang ada dan menghormati nilai-nilai keagamaan dan sosial budaya masyarakat Indonesia.

1. Pertanggungjawaban Tindak Pidana pada Kasus Pemalsuan Identitas di Era Digital

Pertanggungjawaban tindak pidana terhadap seseorang yang melakukan pelanggaran atau perbuatan pidana memerlukan asas-asas hukum pidana. Salah satu asas hukum pidana yang penting adalah asas *nullum delictum nulla poena sine previa lege*, yang sering disebut asas legalitas. Asas ini menjadi dasar utama yang tidak tertulis dalam menjatuhkan pidana kepada seseorang yang telah melakukan perbuatan pidana. Seseorang tidak dapat dijatuhi pidana jika tidak ada kesalahan yang dapat dipertanggungjawabkan. Dengan kata lain, seseorang hanya dapat diminta pertanggungjawaban apabila orang tersebut melakukan kesalahan atau perbuatan yang melanggar peraturan perundang-undangan. Adapun pertanggungjawaban dalam tindak pidana terdiri atas dua yaitu, Undang-undang Perlindungan Data Pribadi (PDP) dan Undang-Undang Informasi dan Transaksi Elektronik (ITE) yang dimana merupakan dua

---

4 Romli Armasasmita (1989). *Asas-Asas Perbandingan Hukum Pidana*. Jakarta: Yayasan LBH Cet. Pertama), hlm. 79.

5 Muhammad Rafi Mahendar Nasution & Marlina (2021). Implementasi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik Terkait Dengan Kebebasan Berpendapat Dalam Perspektif Hak Asasi Manusia. *Jurnal Ilmiah Metadata*, hlm. 719-743.

undang-undang yang mengatur perlindungan data pribadi dan keamanan internet di Indonesia.

1). Undang-Undang Perlindungan Data Pribadi (PDP)

Ada 3 pihak yang diatur oleh UU PDP terkait dengan data pribadi, yaitu pemilik data (juga dikenal sebagai subjek data pribadi), pengontrol atau pengumpul data (yang meliputi setiap orang, lembaga hukum atau organisasi internasional) dan data prosesor (pihak yang memproses data setelah dikumpulkan). Pengontrol dan pengolah data bisa merupakan pihak yang sama, tetapi bisa juga berbeda. Pengumpul data dapat merupakan entitas di luar Indonesia tetapi harus berada di negara yang memiliki Peraturan Khusu tentang perlindungan data. Undang-Undang PDP masih mengizinkan transfer data dari instansi A ke instansi B berdasarkan aturan tertentu. Misalnya, prosesor harus menjaga kerahasiaan data.

UU PDP juga mengatur mengenai lembaga yang mengawasi data pribadi. Pasal 58 UU PDP menyatakan bahwa pengelolaan data pribadi diatur dan bertanggung jawab kepada presiden. Instansi yang ditugaskan untuk melaksanakan perlindungan data pribadi akan merumuskan dan menetapkan kebijakan yang menjadi pedoman bagi semua pihak. Selain itu, lembaga ini juga memiliki tugas untuk mengawasi tindakan administratif terkait pelanggaran terhadap UU PDP. Pasal 65 UU PDP menyatakan bahwa setiap orang atau pihak dilarang melanggar hukum dengan memperoleh informasi pribadi yang bukan miliknya untuk kepentingan pribadi. Larangan ini juga berlaku terhadap pengungkapan data pribadi yang bukan milik Anda. Pelanggaran terhadap larangan ini dapat dikenakan pidana penjara paling lama 5 tahun atau denda paling banyak Rp 5 Miliar. Sementara itu, pihak yang dengan sengaja memalsukan data pribadi untuk keuntungan pribadi dapat dipidana dengan hukuman maksimal 6 tahun penjara atau denda maksimal Rp 6 Miliar. Larangan dan pidana terkait penggunaan data pribadi diatur dalam beberapa pasal, salah satunya adalah Pasal 65 yang berbunyi:

a. Setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain, yang dapat mengakibatkan kerugian bagi subjek data pribadi.
b. Setiap orang dilarang secara melawan hukum mengungkapkan data pribadi yang bukan miliknya.
c. Setiap orang dilarang secara melawan hukum menggunakan data pribadi yang bukan miliknya.

Pengaturan dalam Pasal 66 ini bertujuan agar seseorang tidak menggunakan data pribadi yang bukan miliknya, yang dapat merugikan pemilik data tersebut. Selain itu, terdapat ketentuan pidana dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang termaktub dalam Pasal 67, sebagai berikut:

a. Setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan tujuan untuk menguntungkan diri sendiri atau orang lain, yang mengakibatkan kerugian bagi subjek data pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1), dapat

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. Setiap orang yang dengan sengaja dan melawan hukum mengungkapkan data pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2), dapat dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp 4.000.000.000,00 (empat miliar rupiah).
c. Setiap orang yang dengan sengaja dan melawan hukum menggunakan data pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3), dapat dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp 5.000.000.000,00 (lima miliar rupiah).[6]

Pasal 68 menjelaskan tentang pemalsuan data pribadi yang menyebabkan kerugian bagi korban dan keuntungan bagi pelaku, dengan menyatakan bahwa "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 terhadap orang lain sebagaimana dimaksud dalam Pasal 66, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau pidana denda paling banyak Rp 6.000.000.000,00 (enam miliar rupiah)." Selain dijatuhi pidana sesuai Pasal 67 dan Pasal 68, pelaku juga dapat dikenakan pidana tambahan sesuai dengan Pasal 69, yang mencakup perampasan keuntungan dan/atau harta benda yang diperoleh melalui tindak pidana serta pembayaran ganti rugi.

Jika korporasi terbukti melakukan tindak pidana, sanksi lebih lanjut dapat dijatuhkan sesuai dengan Pasal 70, yang mengatur hal-hal berikut:

a. Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 67 dan Pasal 68 dilakukan oleh korporasi, pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/atau korporasi itu sendiri.
b. Pidana yang dapat dijatuhkan kepada korporasi hanya pidana denda.
c. Pidana denda yang dijatuhkan kepada korporasi paling banyak 10 (sepuluh) kali dari maksimal pidana denda yang diancamkan.
d. Selain pidana denda, korporasi dapat dijatuhi pidana tambahan berupa:
    1. Perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil tindak pidana;
    2. Pembekuan seluruh atau sebagian usaha korporasi;
    3. Pelarangan permanen untuk melakukan perbuatan tertentu;
    4. Penutupan seluruh atau sebagian tempat usaha dan/atau kegiatan korporasi;
    5. Pelaksanaan kewajiban yang telah dilalaikan;
    6. Pembayaran ganti kerugian;
    7. Pencabutan izin;
    8. Pembubaran korporasi.

Dalam proses penerapan hukum materil, hukum formil atau hukum acara juga berperan penting dalam proses peradilan. Hukum acara yang baik akan berdampak positif terhadap keadilan. Mengenai kasus peretasan data pribadi atau

---

6 Febyola Indah et al., (2023). Peran cyber security terhadap keamanan data penduduk negara Indonesia (Studi kasus: Hacker Bjorka)*. Jurnal Bidang Penelitian Informatika*, hlm. 57-64.

kejahatan hacking data pribadi, hal ini diatur dalam Pasal 71 dan Pasal 72 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 71 berbunyi:

a. Dalam hal pengadilan menjatuhkan keputusan pidana denda, terpidana diberikan waktu 1 (satu) bulan sejak putusan memperoleh kekuatan hukum tetap untuk membayar denda tersebut.
b. Jika ada alasan kuat, jangka waktu tersebut dapat diperpanjang paling lama 1 (satu) bulan.
c. Jika terpidana tidak membayar pidana denda dalam jangka waktu yang ditentukan, harta kekayaan atau pendapatan terpidana dapat disita dan dilelang oleh jaksa untuk melunasi pidana denda yang belum dibayar.
d. Jika penyitaan dan pelelangan harta kekayaan atau pendapatan tidak cukup atau tidak memungkinkan, pidana denda yang tidak dibayar akan diganti dengan pidana penjara paling lama yang diancamkan untuk tindak pidana yang bersangkutan.
e. Lamanya pidana penjara sebagaimana dimaksud pada ayat (4) ditentukan oleh hakim dan dicantumkan dalam putusan pengadilan.[7]

Peraturan dan lembaga penyelenggara perlindungan data pribadi yang disebutkan di atas menunjukkan keseriusan pemerintah dalam melindungi informasi data pribadi warga negara Indonesia dari ancaman yang ditimbulkan oleh pihak-pihak yang tidak bertanggung jawab.

Dilihat dari perspektif kepentingan atau perlindungan umum, suatu tindak pidana dianggap efektif jika pemidanaannya dapat mencegah dan menanggulangi kejahatan tersebut seefektif mungkin. Oleh karena itu, efektivitas dapat diukur dari sejauh mana frekuensi tindak pidana dapat berkurang. Dengan kata lain, ujiannya adalah sejauh mana efek preventif dari hukuman penjara secara keseluruhan dapat membuat masyarakat merasa jera untuk melakukan kejahatan. Dari sudut pandang rehabilitasi pelaku, tingkat keefektifannya terletak pada aspek pencegahan kejahatan secara khusus. Jadi, ukuran efektivitasnya bergantung pada seberapa besar pengaruh pemidanaan (penjara) terhadap pelaku terpidana.[8]

Aparat penegak hukum (APH) harus menerapkan prinsip ini secara konsisten. Undang-undang Perlindungan Data Pribadi (PDP) bertujuan untuk mengisi kekosongan standar dan kriteria perlindungan data pribadi yang belum ada sebelumnya. Undang-undang ini juga merespons kekhawatiran komunitas bisnis dan investasi yang melibatkan data pribadi dalam operasional mereka. Dengan kata lain, UU PDP hadir sebagai solusi atas ketidakpastian hukum yang ada. Kepastian hukum adalah unsur krusial dalam negara hukum, karena baik secara filosofis maupun pragmatis, salah satu tujuan hukum adalah menciptakan kepastian hukum.

---

7 Miptahul (2020). Analisis Yuridis Hak Kebebasan Berpendapat Bagi Pengguna Media Sosial Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Studi Putusan No. 3168/PID. SUS/2018/PN. MDN). S*OSEK: Jurnal Sosial dan Ekonomi*, hlm. 76-87.

8 Meyse Stevely Sisilia Wuwungan (2024). Perlindungan Hukum terhadap Pemilik Data Pribadi Pengguna Teknologi Informasi Akibat Tindak Pidana Peretasan. *LEX PRIVATUM*.

Kepastian hukum dalam bentuk aturan tentang PDP menjadi semakin penting, khususnya di negara-negara yang menganut sistem hukum Eropa Kontinental, seperti Indonesia, yang menekankan pentingnya hukum tertulis. Sebelumnya, pelaku ekonomi khawatir bahwa aktivitas bisnis mereka dapat melanggar perlindungan data pribadi meski belum ada aturan yang jelas. Oleh karena itu, UU PDP memberikan jawaban atas semua keraguan tersebut. Inilah yang dimaksud dengan kepastian hukum, di mana selama seseorang memenuhi kewajibannya, menghindari pelarangan, dan mengikuti mekanisme serta standar yang diatur dalam UU PDP, dia tidak akan terjerat pelanggaran PDP.

2). Undang-Undang Informasi dan Transaksi Elektronik (ITE)

Hukum dibuat dan diberlakukan untuk melindungi setiap individu, memberikan rasa aman dari segala perbuatan yang dapat mengancam dan merugikan mereka. Adanya sanksi dalam hukum diharapkan dapat memberikan perlindungan terhadap setiap orang dari berbagai gangguan tersebut. Tindak pidana pemalsuan data adalah salah satu perbuatan yang dapat mengganggu dan merugikan, sehingga ketentuan dan sanksinya harus ditegakkan dengan tegas. Begitu pula dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, terdapat ketentuan sanksi pidana bagi siapa saja yang melakukan pemalsuan data yang dapat menimbulkan hak atau perikatan palsu sebagai bukti suatu hal, atau melakukan pemalsuan terhadap akta-akta otentik.

UU ini mengatur "perbuatan terlarang yang dilakukan melalui media/sistem elektronik" serta memberikan sanksi hukum terhadap individu yang terbukti melakukan tindak pidana, sekaligus menetapkan prosedur arbitrase untuk menyelesaikan sengketa perdata atau pidana. Perbuatan yang dilarang dalam UU ITE tercantum dalam Bab 7, yang mencakup larangan menyebarkan informasi atau dokumen elektronik yang mengandung unsur "penghinaan dan/atau pencemaran nama baik", sebagaimana diatur dalam Pasal 27 ayat (3). Dalam hal ini, Pasal 45 ayat (3) UU ITE mengancam pelaku dengan pidana penjara maksimal enam tahun dan/atau denda hingga Rp1.000.000.000,00 (satu miliar rupiah). Hukum pidana dalam UU ITE bertujuan untuk mengatur hubungan antara warga negara dengan negara, dengan fokus pada kepentingan umum dan kebaikan bersama. Sesuai dengan pandangan Budianto, hukuman yang diberikan berorientasi pada rehabilitasi atau reintegrasi narapidana ke dalam masyarakat.

Berikut poin-poin yang direvisi dari UU ITE 2008 yang menurunkan ancaman pidana dengan dua ketentuan, yakni:

1. Pengurangan ancaman pidana penghinaan atau pencemaran nama baik dari pidana penjara paling lama enam tahun menjadi empat tahun. Sementara penurunan denda dari paling banyak Rp1 miliar menjadi Rp750 juta.
2. Pengurangan ancaman pidana pengiriman informasi elektronik berisi ancaman kekerasan atau menakut-nakuti dari pidana penjara paling lama 12 tahun menjadi empat tahun. Pun begitu dengan denda yang dibayarkan, dari paling banyak Rp 2 miliar menjadi Rp 750 juta.

Lalu, dalam Undang-Undang Nomor 1 Tahun 2024, tidak mencantumkan aturan yang sebelumnya ada di pasal 27 ayat (3) tentang pidana penghinaan atau pencemaran nama baik melalui saluran elektronik. Namun, UU tersebut mencantumkan dua pasal baru, yakni 27A dan 27B. Pasal 27A berbunyi *"Setiap orang dengan sengaja menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal dengan maksud supaya hal tersebut diketahui umum dalam bentuk informasi elektronik dan/atau dokumen elektronik yang dilakukan melalui sistem elektronik"*. Kemudian, pasal 27B berbunyi "Setiap orang dengan sengaja atau tanpa hak mendistribusikan dan/atau mentransmisikan informasi elektronik dan/atau dokumen elektronik, dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa orang dengan ancaman kekerasan untuk:

1. Memberikan suatu barang, yang sebagian atau seluruhnya milik orang tersebut atau milik orang lain, atau
2. Memberi utang, membuat pengakuan utang atau menghapuskan piutang.[9]

Ada empat perubahan pada Pasal 27 ayat (3) UU ITE yang mengatur penghinaan dan pencemaran nama baik. Pertama, diberikan penjelasan tentang istilah "mendistribusikan, mentransmisikan, dan membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik". Kemudian, ditegaskan bahwa UU ITE didasarkan pada delik aduan, bukan delik umum. Terakhir, ditegaskan bahwa ketentuan tersebut mengacu pada ketentuan KUHP tentang pencemaran nama baik dan fitnah. Terakhir, ancaman kriminal dihapus. Karena revisi hanya mengurangi ancaman pidana, bukan menghapus kebebasan ekspresi, UU ITE tetap berpotensi mengancam kebebasan ekspresi. Selanjutnya, masalah duplikasi tindak pidana muncul karena ketentuan-ketentuan yang sama dalam KUHP masih dapat mengakomodasi perbuatan yang dilakukan melalui media internet.

2. Keterkaitan antara UU PDP dan UU ITE

Struktur hukum *(legal structure)* merujuk pada susunan atau tingkatan hukum, termasuk pelaksana hukum, lembaga-lembaga hukum, sistem peradilan, dan pembuat hukum. Sementara itu, budaya hukum *(legal culture)* menggambarkan perilaku dan sikap masyarakat terhadap hukum, serta faktor-faktor yang mempengaruhi bagaimana sistem hukum diterima dan diterapkan dalam masyarakat, sejalan dengan budaya sosial yang ada. Budaya hukum mencakup cara-cara masyarakat berinteraksi dengan hukum dan sejauh mana hukum dipahami serta dihormati oleh warga negara.[10]

Dalam konteks Perlindungan Data Pribadi (PDP) dan keamanan siber, sistem hukum yang ada mencakup beberapa aspek, dimulai dari:

---

9 Lalujan (2020). Implementasi Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Ite Terhadap Kebebasan Berpendapat Di Indonesia. *Lex Et Societatis*.

10 Friedman & Lawrence (2001). *Hukum Amerika Sebuah Pengantar*. *Terjemahan dari American Law An Introduction, 2nd Edition, Alih Bahasa: Wisnu Basuki.* Jakarta: Tatanusa, hlm. 6-9.

1. substansi hukum, yang melibatkan materi hukum yang tercantum dalam peraturan perundang-undangan. Saat ini, baik landasan hukum untuk PDP maupun keamanan siber belum diatur secara komprehensif. Pengaturannya masih bersifat sektoral dan tersebar dalam beberapa peraturan yang berbeda. Untuk keamanan siber, dasar hukum yang digunakan merujuk pada UU ITE yang mencakup pengaturan tentang siber, namun sifatnya masih terbatas dan bersifat umum. Jika dibandingkan dengan negara-negara ASEAN lainnya, seperti Malaysia, Singapura, Thailand, Vietnam, dan Filipina, Indonesia merupakan satu-satunya negara yang belum memiliki undang-undang khusus tentang Keamanan Siber dan Kejahatan Siber. Sementara itu, terkait dengan PDP, Indonesia dan Thailand juga belum memiliki undang-undang yang mengatur perlindungan data pribadi secara khusus. Pengaturan data pribadi di Indonesia masih tersebar dalam berbagai UU dengan sifat pengaturan yang general, sehingga dapat menimbulkan ketidakpastian hukum. Merespons kondisi ini, dalam daftar Program Legislasi Nasional (Prolegnas) 2019- 2024, baik PDP maupun keamanan dan ketahanan siber tercatat sebagai prioritas RUU yang diusulkan oleh DPR RI. Namun, hanya RUU PDP yang menjadi prioritas pembahasan tahun 2021, sedangkan RUU Keamanan dan Ketahanan Siber yang sempat dibahas di Badan Legislasi mengalami penundaan pembahasan.

2. Dalam aspek struktur hukum, hal ini berkaitan dengan kelembagaan pelaksana hukum, kewenangan lembaga, dan aparat penegak hukum. Saat ini, kewenangan pengaturan dan pengawasan terkait Perlindungan Data Pribadi (PDP) berada di bawah Kementerian Komunikasi dan Informasi. Untuk meningkatkan efektivitas penegakan hukum terkait PDP, dalam pembahasan RUU PDP, terdapat wacana untuk membentuk lembaga khusus yang independen untuk menangani masalah PDP. Sementara itu, di bidang penyelenggaraan keamanan siber, telah dilakukan penguatan kelembagaan dengan diterbitkannya Peraturan Presiden No. 53 Tahun 2017 mengenai Badan Siber dan Sandi Negara (BSSN). BSSN, yang berada di bawah dan bertanggung jawab langsung kepada Presiden, memiliki tugas untuk melaksanakan keamanan siber secara efektif dan efisien, serta memanfaatkan, mengembangkan, dan mengonsolidasikan berbagai unsur yang terkait dengan keamanan siber dari berbagai organisasi.

3. Kultur atau budaya hukum yang berkaitan dengan perilaku hukum masyarakat Indonesia menunjukkan bahwa banyak orang masih belum memandang data pribadi sebagai suatu properti yang perlu dilindungi. Hal ini terlihat dari cara masyarakat memanfaatkan ruang siber yang mengandung konten data pribadi, baik di platform media sosial maupun di grup jejaring sosial. Selain itu, saat menggunakan berbagai platform sistem elektronik seperti *e-commerce*, transportasi online, *fintech*, dan sebagainya, banyak pengguna yang belum sepenuhnya memahami kebijakan privasi, syarat-syarat, dan ketentuan layanan dari setiap aplikasi, khususnya yang berkaitan dengan penggunaan data pribadi. Minimnya kesadaran masyarakat ini menjadi masalah yang perlu mendapat perhatian dari pemerintah dan pihak-pihak terkait lainnya.

PDP (Perlindungan Data Pribadi) dan keamanan siber memiliki keterkaitan dan sinergitas yang erat, karena keduanya merupakan bagian dari Hak Asasi Manusia (HAM) yang dijamin oleh konstitusi. Namun, pengaturannya saat ini masih belum memadai, terutama disebabkan oleh adanya pengaturan yang bersifat sektoral. Pengaturan yang terfragmentasi ini berpotensi menyebabkan tumpang tindih dalam regulasi dan menimbulkan ketidakpastian hukum, yang pada gilirannya menghambat upaya perlindungan terhadap data pribadi serta meningkatkan risiko terhadap keamanan siber.

Dalam konteks penegakan hukumnya, sistem hukum yang ada untuk PDP dan keamanan siber belum berfungsi dengan baik. Setiap subsistem hukum yang mempengaruhi penyelenggaraan kedua hal tersebut masih memiliki kelemahan, antara lain karena regulasi yang tersebar dalam berbagai Undang-Undang (UU) sektoral dan pengaturannya yang belum komprehensif. Selain itu, lembaga-lembaga yang menangani masalah ini belum berfungsi secara optimal, dan minimnya kesadaran masyarakat mengenai pentingnya perlindungan data pribadi semakin memperburuk situasi ini.

Hubungannya dengan UU ITE adalah bahwa UU ITE mencakup aspek penting dari keamanan siber dan perlindungan data pribadi. UU ini mengatur berbagai tindak pidana yang berkaitan dengan penyalahgunaan data pribadi melalui sistem elektronik, termasuk pemalsuan data, penipuan, dan pencemaran nama baik melalui internet. UU ITE memiliki peran penting dalam memberikan landasan hukum terhadap tindakan yang melanggar hukum di dunia maya, meskipun pengaturannya masih terbatas dan bersifat umum. Keterkaitan antara PDP dan keamanan siber dalam konteks ini adalah bahwa keduanya berfokus pada perlindungan terhadap data pribadi dan mengatur cara agar data yang beredar di dunia maya tetap aman dan tidak disalahgunakan. Namun, karena pengaturannya belum terintegrasi dengan baik, perlu adanya perbaikan dalam regulasi dan penguatan lembaga terkait agar perlindungan data pribadi dan keamanan siber dapat lebih optimal.

B. Efektivitas Penegakan Hukum Pidana dalam Melindungi Data Pribadi Individu Berdasarkan Kitab Undang-Undang Hukum Pidana (KUHP)

Perkembangan teknologi saat ini telah menyebabkan maraknya kejahatan di dunia maya yang dikenal dengan sebutan *cybercrime*. Kejahatan ini dilakukan oleh pelaku untuk memperoleh informasi secara ilegal dan menyalahgunakan data demi keuntungan pribadi. *Cybercrime* merujuk pada tindakan kejahatan yang terjadi di dunia maya dengan memanfaatkan komputer dan jejaring sosial sebagai sarana untuk melakukan tindak kejahatan. *Cybercrime* merupakan ancaman baru yang belum pernah ada sebelumnya di masyarakat global. Beberapa bentuk kejahatan internet yang berisiko tinggi dan sering menimbulkan kerugian besar meliputi *hacking, cracking, defacing, sniffing, carding, phishing, spamming,* dan *scam*. Tindak pidana *cybercrime* jauh lebih kompleks daripada yang terlihat, terutama dalam hal penegakan hukumnya, mulai dari undang-undang yang

mengatur kejahatan ini hingga pengadilan mana yang memiliki kewenangan untuk mengadili kasus tersebut.[11]

Dibalik kelebihan dan kemudahan yang ditawarkan oleh kemajuan teknologi ini, ternyata memberikan juga dampak negatif yang dapat menghancurkan kehidupan dan budaya manusia itu sendiri. Salah satu nya terhadap kebocoran data pengguna teknologi termasuk penggguna sosial media. Dengan maraknya para pengguna media sosial Indonesia tidak bisa dipungkiri bahwa banyaknya kasus kebocoran data pribadi para pengguna. Data pribadi adalah informasi yang melekat pada setiap individu dan bersifat sensitif. Data ini harus dilindungi karena merupakan hak privasi setiap orang. Hak privasi itu sendiri merupakan hak konstitusional yang diatur dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Sebagai hak konstitusional, negara memiliki kewajiban untuk melindungi hak-hak warganya. Namun, di Indonesia saat ini, banyak terjadi masalah hukum terkait penyalahgunaan data pribadi seseorang untuk kepentingan pribadi.[12]

Alasan utama terjadinya *cybercrime* adalah tingginya ketergantungan masyarakat pada teknologi digital dan internet dalam berbagai aspek kehidupan, seperti transaksi keuangan, media sosial, dan komunikasi online. Banyak individu yang kurang menyadari pentingnya melindungi data pribadi mereka atau tidak memiliki pengamanan yang memadai, sehingga membuka celah bagi pelaku kejahatan untuk memanfaatkan kelemahan ini. Selain itu, adanya pasar gelap untuk data pribadi yang dicuri juga menjadi faktor pendorong bagi pelaku untuk terus melakukan kejahatan ini, karena dapat menghasilkan keuntungan besar melalui penjualan atau penyalahgunaan data tersebut.

Menurut Bapak Iptu H. Nursaleh Muslimin, S.Psi., M.H dalam wawancara yang dilakukan bersama peneliti menyatakan bahwa:[13]

> "Penyebab terjadinya pemalsuan identitas ini mungkin yang pertama yaitu soal materi seperti salah satunya kejadian baru-baru ini ada seseorang yang memakai foto saya kemudian meminta uang, salah satu contohnya adalah love scamming yang mengaku sebagai polisi atau pejabat kemudian menghubungi korban lewat media sosial kemudian meminta untuk keperluan pribadi".

Selain itu, menurut Bapak Briptu Riswandi Ashar menyatakan bahwa:[14]

> "Kebanyakan *cybercrime* memang salah satu faktor utamanya yaitu soal ekonomi, pelaku menggunakan identitas palsu untuk melakukan penipuan, seperti mengelabui korban dalam transaksi online mungkin dengan tujuan untuk memperoleh keuntungan finansial tanpa terdeteksi".

---

11 Nopit Ernasari (2024). Perlindungan Data Pribadi Dalam Penegakan Hukum Pidana di Era Digital Ditinjau dari Perspektif Implementasi Prinsip Right to be Forgotten di Indonesia. *Jurnal Surya Kencana Satu: Dinamika Masalah Hukum dan Keadilan*, hlm. 163-174.

12 Endah Pertiwi et al., (2021). Analisis yuridis terhadap penyalahgunaan data pribadi pengguna media sosial. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, hlm. 18-24.

13 Nursaleh Muslimin, PAMIN 5 SUBBAGRENMIN DITRESKRIMSUS POLSA SULSEL, *wawancara*. Makassar. 5 Februari 2025.

14 Riswandi Ashar, BA DITRESKRIMSUS POLDA SULSEL, *wawancara*. Makassar. 5 Februari 2025.

Berdasarkan pernyataan di atas, faktor ekonomi menjadi salah satu penyebab utama terjadinya pemalsuan identitas dalam kejahatan siber. Pelaku sering menggunakan identitas palsu atau mencuri data pribadi untuk melakukan penipuan, terutama dalam transaksi online, dengan tujuan memperoleh keuntungan finansial secara ilegal tanpa terdeteksi. Pemalsuan identitas ini dapat terjadi dengan cara menggunakan foto atau informasi pribadi seseorang untuk menipu korban dan meminta uang, yang menggambarkan besarnya ancaman *cybercrime* dalam dunia digital saat ini.

Problematika tentang pentingnya pelindungan data pribadi mulai menguat seiring dengan meningkatnya jumlah pengguna telepon seluler dan internet. Banyak kasus terjadi yang berkaitan dengan kasus penyalahgunaan dan kejahatan data pribadi. Oleh karena itu, haruslah setiap individu atau kelompok melakukan upaya perlindungan diri baik itu secara fisik ataupun data-data pribadi yang dapat menjerumuskan kepada hal-hal yang tidak diinginkan.

Konsep pelindungan diri pribadi juga memungkinkan seseorang untuk mengontrol sejumlah elemen kehidupan pribadinya, diantaranya mengenai informasi tentang diri pribadinya, kerahasiaan identitas pribadi, akses terhadap data pribadi yang dimiliki oleh pihak tertentu, intersepsi komunikasi, pilihan atau perubahan nama, kehidupan seksual, profesi atau domisili, pelindungan terhadap gangguan lingkungan, serta hak untuk membangun dan mengembangkan hubungan dengan orang lain. Perlindungan data pribadi dilakukan untuk menghindari:

1. Ancaman pelecehan seksual, perundungan online, hingga Kekerasan Berbasis Gender Online (KBGO)

   Ancaman pelecehan seksual, perundungan online, dan Kekerasan Berbasis Gender Online (KBGO) merupakan bentuk kekerasan yang terjadi di dunia maya, yang dapat menimpa siapa saja, terutama perempuan dan anak-anak. Pelecehan seksual online sering melibatkan eksploitasi gambar atau video pribadi tanpa izin, sementara perundungan online melibatkan pelecehan, penghinaan, atau ancaman secara terus-menerus di media sosial. KBGO merujuk pada segala bentuk kekerasan yang berhubungan dengan jenis kelamin yang dilakukan melalui platform digital, seperti intimidasi atau penganiayaan berbasis gender.
2. Mencegah penyalahgunaan data pribadi oleh oknum atau pihak tidak bertanggung jawab dan menghindari potensi pencemaran nama baik.

   Menghindari penyalahgunaan data pribadi dan pencemaran nama baik sangat penting untuk melindungi diri dari kerugian yang dapat merusak kehidupan pribadi dan profesional. Penyalahgunaan data pribadi dapat mengakibatkan identitas seseorang dicuri, disalahgunakan untuk penipuan, atau dimanfaatkan untuk kepentingan ilegal, yang berpotensi menimbulkan kerugian finansial dan psikologis. Sementara itu, pencemaran nama baik dapat merusak reputasi seseorang, mengakibatkan dampak sosial dan emosional yang besar, serta berpotensi menurunkan kualitas hidup dan hubungan

sosial. Oleh karena itu, menjaga privasi dan reputasi secara online adalah langkah penting untuk menghindari dampak negatif yang bisa berlangsung lama.[15]

Perlindungan data pribadi masih diatur secara terpisah dalam beberapa peraturan perundang-undangan, sehingga diperlukan adanya satu undang-undang yang mengatur secara jelas dan tegas terkait penyalahgunaan data pribadi. Saat ini, perlindungan data pribadi tercakup dalam beberapa peraturan perundang-undangan, di antaranya Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). KUHP masih digunakan sebagai dasar hukum untuk menjerat tindak pidana siber, khususnya jenis-jenis tindak pidana siber yang memenuhi unsur-unsur dalam pasal-pasal KUHP. Namun, ketika produk hukum ini dirasa belum cukup untuk menjangkau beberapa jenis tindak pidana siber, maka selain mencoba menggunakan dasar hukum di luar KUHP, juga digunakan penafsiran hukum. Salah satu dasar hukum dalam KUHP yang digunakan oleh aparat penegak hukum dalam menangani pencurian data adalah Pasal 362 KUHP yang menyebutkan bahwa: "Barang siapa mengambil sesuatu yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak sembilan ratus rupiah (Rp. 900.000)."

Keseluruhan uraian kebijakan yang diambil oleh pembuat undang-undang mengenai penanggulangan masalah pencurian data pribadi dengan menggunakan Pasal 362 KUHP dapat disimpulkan bahwa apabila melihat unsur-unsurnya, maka pasal tersebut tidak lagi dapat dikenakan atau dapat menjerat pelaku dengan hukuman pidana, karena pencurian data pribadi merupakan kejahatan yang relatif baru. Oleh karena itu, penerapan Pasal-Pasal KUHP saat ini sudah tidak relevan untuk menangani tindak pidana teknologi informasi, karena pasal tersebut lebih berlaku untuk pencurian secara umum dan tidak secara khusus mengatur tindak pidana pencurian data pribadi. Kebijakan pengaturan tindak pidana siber dalam KUHP dapat dilakukan dengan merumuskan tindak pidana baru apabila rumusan yang ada saat ini tidak cukup memadai untuk mengatur tindak pidana siber, atau dapat juga dengan memodifikasi rumusan tindak pidana yang sudah ada agar dapat mencakup berbagai perkembangan baru di bidang teknologi informasi.

Di Indonesia, perlindungan hukum terhadap data pribadi masih dianggap kurang optimal dikarenakan penegak hukum kesulitan dalam menanggapi kejahatan digital ini dengan perangkat hukum yang ada, karena hukum yang ada belum memadai untuk menjangkau seluruh aspek kejahatan yang berkaitan dengan data pribadi dan teknologi informasi, selain itu penegak hukum juga kesulitan dalam mengidentifikasi pelaku, karena kejahatan siber sering kali dilakukan secara anonim melalui platform digital yang sulit dilacak. Hal ini mempersulit aparat penegak hukum untuk menemukan bukti yang cukup dan menentukan siapa yang bertanggung jawab. Hakim yang tidak terbiasa dengan teknologi digital juga menjadi kendala, karena mereka kesulitan dalam memahami dan menilai bukti yang berkaitan dengan kejahatan siber.

---

[15] Syaifuddin (2020). Perlindungan Hukum Terhadap Para Pihak Di Dalam Layanan Financial Technology Berbasis Peer To Peer (P2P) Lending (Studi Kasus di PT. Pasar Dana Pinjaman Jakarta). *Dinamika*, hlm. 408-421.

Hal ini sesuai dengan yang diungkapkan oleh Bapak Iptu Riswandi Ashar yang menyatakan bahwa:[16]

> "Tantangannya adalah belum bisa mengetahui siapa yang menggunakan data karena masih anonim, bukti digital yang digunakan dalam kasus pelanggaran data pribadi seringkali sulit diverifikasi dipengadilan, mengingat belum semua hakim terbiasa dengan aspek teknik forensik digital".

Berdasarkan hasil wawancara di atas, maka dapat disimpulkan bahwa tantangan yang dihadapi oleh aparat penegak hukum dan hakim harus di atasi dengan cara diadakan pelatihan dan peningkatan pemahaman bagi aparat penegak hukum, termasuk hakim, mengenai teknik forensik digital dan bukti-bukti yang relevan dengan kejahatan dunia maya, agar proses hukum dapat berjalan lebih efektif dan akurat dalam menangani pelanggaran data pribadi.

Meskipun begitu, menurut Bapak Iptu H. Nursaleh Muslimin, S.Psi., M.H, cara mengatasi tantangan tersebut adalah:[17]

> "Diperlukan langkah strategi yang terstruktur, kolaboratif, dan komprehensif. Edukasi terhadap masyarakat juga penting untuk melindungi data pribadi, misalnya melalui kampanye keamanan digital".

Untuk mengatasi tantangan yang dihadapi oleh aparat penegak hukum dan hakim dalam menangani kejahatan dunia maya, terutama yang berkaitan dengan pelanggaran data pribadi, diperlukan strategi yang terstruktur, kolaboratif, dan komprehensif. Strategi terstruktur melibatkan pelatihan berkelanjutan bagi aparat penegak hukum dan hakim mengenai teknik forensik digital dan cara mengidentifikasi bukti-bukti relevan dalam kasus dunia maya. Pelatihan ini harus disusun dengan kurikulum yang jelas dan up-to-date, serta dilakukan secara berkelanjutan untuk mengikuti perkembangan teknologi. Selain itu, penting untuk mengintegrasikan topik ini dalam pendidikan formal agar aparat penegak hukum siap menghadapi tantangan ini sejak awal. Strategi kolaboratif mencakup kerjasama antara aparat penegak hukum, hakim, dan ahli forensik digital yang dapat memberikan keahlian dalam menganalisis bukti digital secara akurat. Kolaborasi antara lembaga penegak hukum, lembaga peradilan, serta instansi terkait lainnya juga perlu dilakukan untuk mempercepat penanganan kasus dan memperkaya pengetahuan semua pihak. Sementara itu, strategi komprehensif mencakup pengembangan kebijakan dan regulasi yang jelas mengenai perlindungan data pribadi dan pengelolaan bukti digital, sehingga proses hukum dapat berjalan dengan lebih efektif dan sesuai dengan standar yang ada. Dengan pendekatan yang terstruktur, kolaboratif, dan komprehensif, aparat penegak hukum dan hakim akan lebih siap menghadapi tantangan dalam menanggulangi kejahatan dunia maya dan melindungi data pribadi masyarakat.

KESIMPULAN DAN SARAN

[16] Riswandi Ashar, BA DITRESKRIMSUS POLDA SULSEL, *wawancara*. Makassar. 5 Februari 2025.
[17] Nursaleh Muslimin, PAMIN 5 SUBBAGRENMIN DITRESKRIMSUS POLSA SULSEL, *wawancara*. Makassar. 5 Februari 2025.

Penerapan hukum pidana materil terhadap tindak pidana pemalsuan identitas di era digital telah menunjukkan adanya ketidaksiapan dalam mengatasi kejahatan yang berkembang seiring dengan pesatnya kemajuan teknologi informasi dan komunikasi. Meskipun terdapat regulasi seperti Undang-Undang Perlindungan Data Pribadi (PDP) dan Undang-Undang Informasi dan Transaksi Elektronik (ITE), implementasi hukum di lapangan masih menghadapi kendala dalam hal penegakan yang konsisten dan efektif. Faktor seperti kurangnya kesadaran hukum masyarakat, serta ketidaksesuaian antara regulasi yang ada dan perkembangan teknologi, mempengaruhi efektivitas penerapan hukum pidana materil terhadap kejahatan pemalsuan identitas digital. Dalam penelitian ini, terlihat bahwa aparat penegak hukum masih perlu meningkatkan pemahaman dan keterampilan mereka dalam mengatasi kejahatan dunia maya, terutama terkait dengan pemalsuan data dan identitas. Selain itu, pentingnya kolaborasi antara lembaga-lembaga terkait, seperti Kepolisian, Kejaksaan, dan pengadilan, dalam menangani tindak pidana ini perlu diperkuat agar hukum dapat berjalan secara lebih efektif, memberikan perlindungan terhadap korban, dan menciptakan kepastian hukum di tengah tantangan era digital. Berdasarkan hasil penelitian, efektivitas penegakan hukum pidana dalam melindungi data pribadi individu berdasarkan Kitab Undang-Undang Hukum Pidana (KUHP) masih terbilang kurang optimal. Meskipun KUHP menyediakan dasar hukum untuk beberapa kejahatan yang terkait dengan penyalahgunaan data pribadi, seperti penipuan dan pencemaran nama baik, regulasi yang ada belum sepenuhnya menjawab tantangan yang timbul di era digital. Pengaturan tentang perlindungan data pribadi dalam KUHP tidak cukup spesifik mengingat pesatnya perkembangan teknologi informasi yang mempengaruhi cara data pribadi dikumpulkan, diproses, dan disebarkan. Penegakan hukum pidana terkait perlindungan data pribadi masih menghadapi kendala dalam hal pemahaman aparat penegak hukum tentang isu-isu siber, serta kurangnya kesadaran hukum dari masyarakat terkait pentingnya melindungi data pribadi mereka. Selain itu, meskipun ada upaya untuk mengintegrasikan peraturan terkait perlindungan data pribadi, seperti yang diatur dalam Undang-Undang Perlindungan Data Pribadi (PDP) dan Undang-Undang Informasi dan Transaksi Elektronik (ITE), implementasi hukum pidana dalam konteks ini masih terbatas dan sering kali terhambat oleh ketidaksempurnaan regulasi dan koordinasi antar lembaga yang menangani kasus tersebut.

Penyuluhan Hukum dan Sosialisasi kepada Masyarakat. Untuk mengurangi tingginya angka kejahatan pemalsuan identitas digital, perlu dilakukan penyuluhan hukum kepada masyarakat, khususnya mengenai pentingnya menjaga dan melindungi data pribadi. Hal ini dapat dilakukan melalui kampanye kesadaran hukum yang melibatkan media sosial dan media massa. Peningkatan Kolaborasi Antar Lembaga. Koordinasi antara berbagai lembaga yang terlibat dalam penanganan tindak pidana pemalsuan identitas perlu diperkuat. Kepolisian, Kejaksaan, Pengadilan, dan lembaga lainnya harus bekerja sama dengan lebih efektif dalam menangani kasus pemalsuan identitas digital, mulai dari penyidikan hingga proses pengadilan.

REFERENSI

1) Agus Hiplunudin. (2019). *Politik Era Digital.* Yogyakarta: Suluh Media, hlm. 29.
2) QS. Al-Baqarah (2:188)

3) Henny Saida Flora et al., (2024). *Hukum Pidana di Era Digital*. Batam: CV. Rey Media Grafika, hlm. 38-39.
4) Romli Armasasmita (1989). *Asas-Asas Perbandingan Hukum Pidana*. Jakarta: Yayasan LBH Cet. Pertama), hlm. 79.
5) Muhammad Rafi Mahendar Nasution & Marlina (2021). Implementasi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik Terkait Dengan Kebebasan Berpendapat Dalam Perspektif Hak Asasi Manusia. *Jurnal Ilmiah Metadata*, hlm. 719-743.
6) Febyola Indah et al., (2023). Peran cyber security terhadap keamanan data penduduk negara Indonesia (Studi kasus: Hacker Bjorka). *Jurnal Bidang Penelitian Informatika*, hlm. 57-64.
7) Miptahul (2020). Analisis Yuridis Hak Kebebasan Berpendapat Bagi Pengguna Media Sosial Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Studi Putusan No. 3168/PID. SUS/2018/PN. MDN). S*OSEK: Jurnal Sosial dan Ekonomi*, hlm. 76-87.
8) Meyse Stevely Sisilia Wuwungan (2024). Perlindungan Hukum terhadap Pemilik Data Pribadi Pengguna Teknologi Informasi Akibat Tindak Pidana Peretasan. *LEX PRIVATUM*.
9) Lalujan (2020). Implementasi Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Ite Terhadap Kebebasan Berpendapat Di Indonesia. *Lex Et Societatis*.
10) Friedman & Lawrence (2001). *Hukum Amerika Sebuah Pengantar*. *Terjemahan dari American Law An Introduction, 2nd Edition, Alih Bahasa: Wisnu Basuki.* Jakarta: Tatanusa, hlm. 6-9.
11) Nopit Ernasari (2024). Perlindungan Data Pribadi Dalam Penegakan Hukum Pidana di Era Digital Ditinjau dari Perspektif Implementasi Prinsip Right to be Forgotten di Indonesia. *Jurnal Surya Kencana Satu: Dinamika Masalah Hukum dan Keadilan*, hlm. 163-174.
12) Endah Pertiwi et al., (2021). Analisis yuridis terhadap penyalahgunaan data pribadi pengguna media sosial. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, hlm. 18-24.
13) Syaifuddin (2020). Perlindungan Hukum Terhadap Para Pihak Di Dalam Layanan Financial Technology Berbasis Peer To Peer (P2P) Lending (Studi Kasus di PT. Pasar Dana Pinjaman Jakarta). *Dinamika*, hlm. 408-421.