SANISA
JURNAL KREATIVITAS MAHASISWA HUKUM
Volume 6 Nomor 1, April 2026: h. 46-62 E-ISSN: 2776-2289

Kebijakan Hukum Pidana Terhadap Tindak Pidana Peretasan Data Pribadi

Aulia Ridwan[1], Jacob Hattu [2]

[1,2] Fakultas Hukum Universitas Pattimura, Ambon, Indonesia.
: jacob.hattu@lecturer.unpatti.ac.id
: xxxxxxxxxxxxxxxx

Dikirim:	Direvisi:	Dipublikasi:

ABSTRACT

Introduction: *Personal data protection has been implemented in criminal law policies, but data breaches still occur. This demonstrates the weaknesses of Indonesian criminal law, which still require reform to protect public data security.*
Purposes of the Research: *This study aims to analyze criminal law policies regarding the crime of hacking personal data now and in the future.*
Methods of the Research: *The method used is a normative juridical method with a statutory, conceptual, and case-based approach. The legal sources consist of primary, secondary, and tertiary legal materials. The legal material collection procedure is carried out using a literature study method, and the processing and analysis of legal materials are carried out qualitatively.*
Results / Findings / Novelty of the Research: *The research findings show that current criminal law policy regarding personal data hacking lies in its substance or legal provisions, technology, and law enforcement. In terms of substance or legal provisions, the current Personal Data Protection Law (Law No. 27 of 2022) focuses more on individual personal data, such as identity data, financial data, and health data. In terms of technology, the current Personal Data Protection Law does not specifically regulate the use of personal data in the context of Artificial Intelligence (AI) technology, focusing on the analysis of data collected by IoT. In terms of law enforcement, the current Personal Data Protection Law still faces several challenges, such as a lack of detail in derivative regulations and the absence of a specific authority for data protection. Further research indicates that future criminal law policy regarding personal data hacking lies in its substance or legal provisions, technology, and law enforcement. The future Personal Data Protection Law will be more comprehensive. In terms of technology, the strengthening and expansion of the use of personal data in the context of AI technology focuses on the analysis of data collected by IoT, and its law enforcement will emphasize sanctions against perpetrators of personal data hacking.*

Keywords: Criminal Law Policy: Criminal Acts of Hacking Personal Data

ABSTRAK

Latar Belakang: Perlindungan data pribadi dalam kebijakan hukum pidana telah dilakukan namun tindak pidana peretasan data pribadi masih terjadi. Hal ini menunjukan kelemahan hukum pidana di Indonesia masih perlu dilakukan pembaharuan dalam melindungi keamanan data masyarakat.
Tujuan Penelitian: Penelitian ini bertujuan untuk menganalisa kebijakan hukum pidana terhadap tindak pidana peretasan data pribadi saat ini dan masa yang akan datang.
Metode Penelitian: Metode yang digunakan menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan kasus. Sumber bahan hukum terdiri dari bahan hukum primer, sekunder dan tersier. Prosedur pengumpulan bahan hukum dilakukan

dengan metode studi kepustakaan, dan Pengolahan dan Analisa Bahan hukum dilakukan secara kualitatif.

Hasil/Temuan/Penelitian: Hasil penelitian menunjukkan bahwa Kebijakan hukum pidan terhadap peretasan data pribadi saat ini terletak pada substansi atau aturan hukumnya, teknolog dan penegakan hukum. Pada substansi atau aturan hukumnya UU PDP saat ini (UU No. 27 Tahu 2022) lebih fokus pada data pribadi individu, seperti data identitas, data finansial dan dat kesehatan. Pada teknologinya, UU PDP saat ini belum secara spesifik mengatur penggunaan dat pribadi dalam konteks teknologi Artificial Intelligence **(**AI) berfokus pada analisis data yan dikumpulkan oleh IoT. Pada penegakan hukumnya UU PDP saat ini masih memiliki beberap tantangan dalam penegakan hukum, seperti kurangnya detail dalam aturan turunan dan belun adanya otoritas khusus untuk perlindungan data. Hasil penelitian lanjutan menunjukan bahw kebijakan hukum pidana terhadap peretasan data pribadi pada masa yang akan datang terleta peningkatan atau penguatan pada substansi atau aturan hukumnya, teknologi, dan penegaka hukum. Dimana UU PDP untuk masa yang akan datang akan lebih komprehensif, Pad teknologinya, pengutan dan perluasaan penggunaan data pribadi dalam konteks teknologi A berfokus pada analisis data yang dikumpulkan oleh IoT dan penegakan hukumnya lebi mempertegas sanksi terhadap pelaku peretasan data pribadi.

Kata Kunci: *Kebijakan Hukum Pidana; Tindak Pidana Peretasan Data Pribadi*

1. Pendahuluan

Revolusi Industri 4.0 atau *cyber physical system* muncul di abad ke-21 menjadi revolusi yang menitikberatkan pada otomatisasi serta kolaborasi antar teknologi siber. Ciri utamanya terletak pada integrasi informasi dan teknologi komunikasi dalam sektor industri.[1] Sejak tahun 2011, Indonesia telah memasuki era industry 4.0 yang ditandai dengan meningkatnya integrasi, interaksi, dan keterhubungan antara manusia, mesin, dan sumber daya lainnya melalui teknologi informasi dan komunikasi.[2] Sebagai salah satu negara terbesar di dunia, Indonesia memiliki potensi besar dalam menghasilkan dan memanfaatkan data. Pemanfaatan teknologi dan data dapat ditemukan secara masif, salah satunya melalui pesatnya pertumbungan layanan *e-commerce* dan layanan transportasi daring yang menjadi bukti nyata keberhasilan pemanfaatan teknologi di Indonesia.

Perkembangan Teknologi Informasi di Indonesia semakin hari semakin pesat. Dimana kemajuan dari Teknologi Informasi menyebabkan perubahan kehidupan manusia dari berbagai bidang yang secara langsung telah mempengaruhi lahirnya masalah-masalah yang timbul didalam masyarakat. Meskipun demikian, dibalik cahaya kemajuan ini terbentanglah bayangan kompleksitas hukum yang membuka jalan dan peluang bagi aktivitas *cybercrime.* Salah satu bentuk dari kompleksitas tersebut ialah peretasan data pribadi. Data pribadi merupakan privasi yang harus dilindungi oleh hukum, sebab privasi merupakan hak individu untuk menentukan data atau informasi apa saja tentang dirinya yang boleh diketahui dan tidak boleh diketahui orang lain dan termasuk Hak Asasi Manusia.[3]

Hal ini sejalan dengan amanat dalam Undang-Undang Dasar Negara Republik Indonesia

[1]Nabillah Purba, Mhd Yahya, dan Nurbaiti. "Revolusi Industri 4.0: Peran Teknologi dalam Eksistensi Penguasaan Bisnis dan Implementasinya". *JPSB* 9, No. 2, (2021): 91-98. https://doi.org/10.26486/jpsb.v9i2.2103

[2]Airlangga Hartarto, *Making Indonesia 4.0*, (Jakarta: Kementerian Perindustrian RI, 2018).

[3]Wahyudi Djafar. 'Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan, Tantangan Hukum dalam era Analisis Big Data.'(Kuliah Umum: Universitas Gadjah Mada, 2019).

tahun 1945, dalam Pasal 28G ayat (1) menyatakan bahwa:

> "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".

Pasal tersebut mengamanatkan bahwa hak asasi berhak untuk mendapatkan perlindungan dari ancaman yang dapat menimbulkan kerugian. Dalam konteks digital, data pribadi merupakan bagian dari hak asasi yang harus dilindungi sebab mempunyai nilai ekonomi dan bisa diperjual belikan. Lebih lanjut terkait perlindungan data pribadi dan peretasan sistem elektronik telah diatur di dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Selanjutnya disebut UU ITE), dalam Pasal 30 ayat (3) menyatakan bahwa :

> "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan"

Ketentuan ini menegaskan bahwa tindakan peretasan atau akses *illegal* terhadap sistem elektronik, termasuk yang memuat data pribadi merupakan pelanggaran hukum yang serius, selain itu telah diatur perlindungan data pribadi secara lebih lanjut dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Selanjutnya disebut UU PDP) dalam Pasal 65 ayat (1) jo. Pasal 67 ayat (1) pun menyatakan bahwa :

> "Setiap Orang yang dengan sengaja dan melawan hukum memproleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi, dipidana dengan pidana paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah)"

Pasal-pasal tersebut telah melarang perolehan, pengumpulan, pengungkapan, dan penggunaan data pribadi dengan sengaja, tanpa hak, dan secara melawan hukum. Hal ini menunjukan bahwa hukum memiliki peran penting dalam menyeimbangkan perkembangan teknologi dengan perlindungan hak individu yang mana merupakan wujud dalam menciptakan ketertiban dalam masyarakat.[4] Namun, dalam realitasnya, implemetasi hukum masih jauh dari ideal dan cukup memprihatinkan. Salah satu faktor utama yang menghambat penegakan prinsip tersebut adalah rendahnya kesadaran hukum di kalangan masyarakat, pemerintah, maupun penegak hukum.[5] Akibatnya, banyak pelanggaran yang terjadi diluar pengawasan ketat sehingga memperbesar resiko kebocoran dan penyalahgunaan data pribadi itu sendiri.

Rendahnya kesadaran dan lemahnya penegakan tersebut tercermin dalam meningkatnya kasus peretasan data pribadi di Indonesia. Salah satu contoh kasus yang mencuat adalah peretasan yang dialami oleh Badan Usaha Milik Negara (BUMN) yang bergerak di bidang perbankan syariah, yakni Bank Syariah Indonesia (Selanjutnya disebut BSI), pun tidak luput dari serangan siber. Dimana pada 8 Mei 2023 *hacker grup Lookbit* berhasil mencuri 1,5 *terabyte* data yang berisikan informasi pribadi dan keuangan, termasuk didalamnya terdapat nama, alamat, nomor kartu, nomor telepon, transaksi nasabah, serta dokumen keuangan dan kata sandi (*password)* untuk layanan internal dan eksternal yang digunakan oleh bank. Dampaknya, transaksi keuangan mengalami gangguan dan ekspos kondisi keuangan nasabah menampilkan saldo yang tidak wajar. Dalam menangani insiden ini, BSI mengambil berbagi langkah untuk memulihan sistem dan memberikan kompensasi kepada nasabah yang mengalami kerugian.

---

[4]Esmi Warassih, *Pemberdayaan Masyarakat Dalam Mewujudkan Tujuan Hukum (Proses Penegakan Hukum Dan Persoalan Keadilan)*, (Semarang: Diponegoro University Press, 2001), p. 31.

[5]Atang Hermawan Usman, "Kesadaran Hukum Masyarakat dan Pemerintah Sebagai Faktor Tegaknya Negara Hukum di Indonesia", *Jurnal Wawasan Yuridika* 30, No. 01 (2014): 26-53, https://doi.org/10.25072/jwy.v30i1.74

Upaya yang dilakukan mencakup pemulihan layanan perbankan, peningkatan keamanan siber, serta penyampaian permohonan maaf secara terbuka kepada nasabah.[6]

Namun, respon dan kompensasi yang diberikan BSI lebih bersifat administratif dan bertujuan untuk menjaga reputasi perusahaan, bukan bentuk pertanggungjawaban hukum sebagaimana telah diatur dalam regulasi yang ada. Kasus-kasus ini menegaskan bahwa lemahnya kesadaran hukum dan kurangnya perlindungan data pribadi telah memberikan celah bagi para pelaku kejahatan siber untuk melakukan pemerasan dan eksploitasi data secara bebas. Hal ini menunjukan kelemahan hukum pidana di Indonesia dalam melindungi keamanan data masyarakat. Meskipun telah ada regulasi, pendekatan penyelesaian kasus kebocoran data di Indonesia cenderung mengedepankan pemulihan sistem dibandingkan dengan penegakan hukum terhadap pelaku kejahatan siber. Ketertinggalan regulasi terhadap kejahatan siber yang semakin canggih membuat peretasan terus berulang, mengancam keamanan nasional dan kepercayaan publik. Diperlukan kebijakan hukum pidana yang lebih adaptif dan efektif terhadap perkembangan teknologi untuk perlindungan data di Indonesia.

2. Metode Penelitian

Metode yang digunakan menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan kasus. Sumber bahan hukum terdiri dari bahan hukum primer, sekunder dan tersier. Prosedur pengumpulan bahan hukum dilakukan dengan metode studi kepustakaan. Pengolahan dan Analisa Bahan hukum dilakukan secara kualitatif.

3. Hasil Dan Pembahasan

A. Kebijakan Hukum Pidana Terhadap Tindak Pidana Peretasan Data Pribadi Pada Saat Ini

Kebijakan hukum pidana dapat disimpulkan sebagai upaya atau tindakan yang diambil oleh penyelenggara negara (pemerintah) dalam memanfaatkan instrumen hukum pidana guna mencapai tujuan tertentu, khususnya dalam rangka penanggulangan kejahatan, dan perlu disadari bahwa terdapat berbagai pendekatan yang bisa ditempuh oleh setiap negara dalam menghadapi persoalan kriminalitas, dan salah satu pendekatan yang dapat dijadikan pilihan ialah melalui perumusan dan penerapan kebijakan hukum pidana, atau yang sering disebut sebagai politik hukum pidana.[7] Politik hukum juga dapat dimaknai sebagai kebijakan dalam menentukan kriminalisasi maupun dekriminalisasi atas suatu perbuatan. Melalui politik hukum pidana, negara memiliki kewenangan untuk menetapkan perbuatan mana yang dikualifikasikan sebagai tindak pidana, sehingga dapat menjadi dasar untuk menerapkan upaya represif terhadap pelanggarnya. Dengan demikian, hukum pidana menjalankan fungsi penting sebagai dasar legitimasi bagi tindakan pemidanaan yang dilakukan oleh negara terhadap seseorang atau kelompok yang melakukan pelanggaran hukum.[8] Tindak pidana peretasan data adalah suatu tindakan kejahatan yang berhubungan dengan dunia maya (*cyberspace)* dengan penggunaan komputer. beberapa ahli menyamakan tindak kejahatan siber (*cybercrime)* dengan kejahatan yang melibatkan komputer (*computer crime),* sementara ahli lain membedakan keduanya, meskipun hingga saat ini belum terdapat kepatenan mengenai defenisi kejahatan teknologi informasi, namun telah ada kesamaan pemahaman yang seragam terkait konsep kejahatan komputer.[9]

---

[6] Nicky Maulana, "Manajemen Krisis PT. BSI Tbk Pasca Peretasan Data Nasabah", *Innovative: Journal Of Social Science Research* 4, No. 1 (2024): 8244-58, https://doi.org/10.31004/innovative.v4i1.8620

[7] Aloysius Wisnubroto, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer,* (Yogyakarta: Penerbit Universitas Atmajaya, 1999) p. 10-11.

[8] Yesmil Anwar dan Adang, *Pembaharuan Hukum Pidana; Reformasi Hukum,* (Jakarta: PT. Gramedia Widiasarana Indonesia, 2008) p. 58-59.

[9] Dikdik Mansyur dan Elisatris Gultom, *Cyber Law: Aspel Hukum teknologi Informasi,* (Bandung: Refika Aditama, 2009) p. 8.

Pandangan ini disampaikan oleh Agus Raharjo, yang menyatakan bahwa istilah *cybercrime* masih belum memiliki kesatuan pendapat, bahkan belum diakui secara internasional sebagai istilah yang baku, meskipun terdapat sebagian pihak yang menggunakan istilah *cybercrime* dan *computer crime* secara sinonim.[10]

Cybercrime merupakan tindak pidana yang berkaitan erat dengan pemanfaatan dan penyalahgunaan informasi, sistem informasi (*information systems*), serta perangkat komunikasi digital yang berfungsi sebagai media untuk mentransmisikan informasi dari satu pihak ke pihak lain. Kejahatan siber tidak lagi semata-mata dipahami sebagai pelanggaran berbasis teknologi, melainkan telah menjadi ancaman serius terhadap sistem sosial, ekonomi, bahkan keamanan nasional di era digital. Termasuk di dalamnya adalah pengaksesan *illegal* terhadap sistem (*hacking*), perusakan situs atau *server (cracking*), pengubahan tampilan halaman web secara tidak sah (*defacing*) yang mengakibatkan pelanggaran hak kekayaan intelektual (pembajakan karya cipta), penyebaran konten pornografi, kejahatan finansial (*carding* dan *phising*), penipuan melalui surat elektronik (*email fraud*), pembobolan rekening bank, perjudian daring, propaganda radikal, hingga penyebaran ujaran kebencian yang memuat SARA.[11] Hal ini membuktikan pesatnya perkembangan teknologi digital yang semakin terintegrasi di kehidupan masyarakat dalam ekosistem berbasis data, dan memunculkan bentuk-bentuk *cybercrime* yang semakin kompleks dan mengkhawatirkan, yang salah satunya adalah peretasan data (*hacking*).

Peretasan atau *hacking,* merupakan salah satu bentuk kejahatan siber (*cybercrime)* yang berupa tindakan atau aktivitas memperoleh akses ke dalam sistem komputer, jaringan, atau perangkat elektronik secara tidak sah, dengan tujuan untuk memodifikasi, mencuri, merusak data, atau bahkan mengambil alih kendali atas sistem tersebut. Kegiatan ini umumnya melibatkan proses pengidentifikasian celah atau kelemahan dalam sistem keamanan komputer, serta eksplorasi dan memanipulasi data, baik dengan motif jahat maupun atas inisiatif pribadi. Peretasan biasanya dilakukan oleh individu yang memiliki kemampuan teknis tinggi serta pemahaman mendalam mengenai sistem keamanan siber. Sejalan dengan semakin kompleksnya kejahatan di ranah digital, bentuk tindak pidana peretasan data pun semakin beragam yang diantaranya :

1. Peretasan terhadap sistem komputer
2. Peretasan terhadap jaringan komputer
3. Peretasan terhadap situs *website*
4. Peretasan terhadap sandi (*Password hacking)*
5. Peretasan terhadap perangkat bergerak
6. Peretasan melalui rekayasa sosial

Kemudian, UU ITE juga mengkualifikasikan peretasan data atas beberapa jenis perbuatan pidana, yakni :

1. Akses Ilegal, diatur dalam Pasal 30 Ayat (3) UU ITE yang merujuk pada perbuatan seseorang yang dengan sengaja dan tanpa hak memasuki atau mengakses sistem elektronik milik pihak lain, baik dengan menerobos sistem keamanan maupun dengan cara lain yang bertentangan dengan hukum.
2. Pencurian Data, diatur dalam Pasal 32 UU ITE yang mencakup perbuatan mengambil, memindahkan, atau mentransfer data milik pihak lain tanpa izin dengan maksud untuk memperoleh keuntungan atau menyebarkannya kepada pihak ketiga.
3. Manipulasi Data, diatur dalam Pasal 35 UU ITE yakni tindakan secara sengaja mengubah, merusak, atau memalsukan data atau informasi elektronik, sehingga data tersebut seolah-olah memiliki keaslian yang sah di hadapan hukum atau pihak ketiga

Merujuk dari tujuan dilakukannya peretasan data maka tindak pidana peretasan data

[10] Agus Raharjo, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, (Bandung: Citra Aditya Bakti, 2002) p. 227.

[11] Hadion Wijoyo dkk, *Cyber Crime,* (Solok: Mafy Media Literasi Indonesia, 2024) p. 4.

terdiri dari :

1. *Phising*, metode peretasan yang dilakukan dengan cara menipu korban agar memberikan informasi pribadi, seperti *username, password*, atau data kartu kredit. Teknik ini sering kali dilakukan melalui *email*, pesan teks, atau situs *web* palsu yang menyerupai situs resmi dengan tujuan untuk memperoleh akses ke akun korban dan menyalahgunakan informasi yang didapatkan.
2. *Malware (malicious software*), adalah perangkat lunak berbahaya yang dirancang untuk merusak, mengakses, atau mencuri data dari sistem komputer tanpa sepengetahuan pemiliknya. Jenis malware yang umum digunakan dalam peretasan data adalah penyebaran virus, trojan, *spyware,* dan *ransomware* dan disebar melalui lampiran *email* yang tampak resmi, unduhan dari situs *web* atau melalui celah keamanan pada sistem yang belum diperbarui.
3. *Brute force attack,* yang merupakan metode peretasan yang dilakukan dengan cara mencoba berbagai kombinasi kata sandi hingga menemukan yang tepat. Teknik ini memanfaatkan kekuatan komputasi untuk menebak kata sandi secara otomatis walaupun memerlukan waktu yang lama, metode ini efektif jika kata sandi yang digunakan lemah atau mudah ditebak.
4. *SQL injection (Structured query language)*, ialah teknik peretasan yang memanfaatkan celah keamanan pada aplikasi *web* yang menggunakan basis data SQL. Metode ini memanfaatkan **kerentanan** dalam **aplikasi *web* yang menggunakan database SQL,** dengan cara menyisipkan perintah SQL berbahaya ke dalam *form* input (seperti kolom *login*, pencarian, atau pendaftaran).
5. *Man in the middle* (MitM) *attack*, merupakan bentuk serangan siber yang termasuk dalam kategori intersepsi komunikasi digital, dimana peretas menyusup di antara komunikasi dua pihak yang sedang berinteraksi tanpa sepengetahuan dua pihak tersebut. Dalam konteks peretasan data pribadi, MitM *attack* dilakukan dengan cara *spoofing* jaringan *wi-fi* publik, dimana para pengguna tidak menyadari bahwa mereka tersambung ke jaringan palsu.

Politik kriminal sebagai usaha rasional masyarakat untuk menanggulangi kejahatan, apabila ditinjau dari sarana yang dapat dipergunakan, dapat dibedakan menjadi, 2 (dua) yaitu usaha-usaha dengan menggunakan hukum pidana sebagai sarana geraknya; dan usaha-usaha dengan sarana dan hukum pidana. Usaha-usaha penanggulangan kejahatan dengan menggunakan sarana hukum pidana, lasim disebut pemidanaan terwujud melalui peradilan pidana. Sedangkan usaha-usaha non hukum pidana lebih berorientasi pada usaha-usaha pengcegahan kejahatan dengan cara menciptakan suasana lingkungan, sehingga kemungkinan terjadinya kejahatan diperkecil. Hubungan antara usaha-usaha melalui penerapan hukum pidana dengan usaha-usaha non hukum pidana bersifat saling menunjang dalam konteks penanggulangan kejahatan.[12]

Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menjadi tonggak penting dalam sistem hukum Indonesia, khususnya dalam menjawab kekosongan normatif yang sebelumnya tidak terakomodasi secara memadai dalam UU ITE dan Permenkominfo. Meski telah hadir lebih dulu, kedua regulasi tersebut, hanya memberikan perlindungan parsial terhadap data pribadi dan lebih menekankan pada aspek teknis maupun administratif. UU ITE, misalnya, tidak mengatur hak-hak subjek data secara eksplisit maupun prinsip dasar pengolahan data pribadi. Sementara itu, Permenkominfo tidak memiliki kedudukan hukum yang setara dengan undang-undang dan hanya mengatur sanksi kepada

[12] Jacob Hattu, "*Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan Anak*", *Jurnal Sasi* 20 No. 2 (2014): 47-52, https://doi.org/10.47268/sasi.v20i2.326

pengendali data hanya sebatas sanksi administratif, sehingga efektivitasnya terbatas dalam konteks perlindungan data sebagai hak konstitusional warga negara.

Secara konseptual dan normatif, UU PDP hadir dengan mengadopsi banyak prinsip dasar dari GDPR Uni Eropa, yang diakui secara luas sebagai kerangka hukum paling komprehensif dalam hal perlindungan data pribadi. Di dalamnya tercermin prinsip-prinsip fundamental seperti keabsahan pemrosesan, pembatasan tujuan, akuntabilitas, integritas dan kerahasiaan, serta hak-hak subjek data. Pengaruh GDPR dalam UU PDP bukan hanya sekadar adopsi prinsip, tetapi juga mencerminkan pergeseran paradigma perlindungan data pribadi di Indonesia dari pendekatan sektoral dan reaktif menuju pendekatan yang holistik, terstruktur, dan berbasis pada hak asasi manusia.

Harmonisasi ini menjadi sangat krusial dalam era digital saat ini yang ditandai oleh arus informasi dan data lintas batas negara. UU PDP memiliki 76 Pasal yang terbagi dalam 16 Bab yang mencakup berbagai aspek terkait perlindungan data pribadi. Dalam hal pemrosesan data pribadi telah disesuikan dengan prinsip-prinsip didalam GDPR yakni prinsip sesuai hukum, adil dan transparan, prinsip pembatasan tujuan, prinsip minimalisasi data, prinsip akurasi, prinsip retensi/batasan penyimpanan, prinsip kerahasiaan dan keamanan, serta prinsip akuntabilitas.

Kesamaan prinsip dalam GDPR dan UU PDP menunjukkan bahwa perlindungan data pribadi di Indonesia telah mengacu pada prinsip global, mengingat era perkembangan teknologi dan informasi yang pesat membuat batas-batas teritorial atau nasional tidak relevan lagi. Tidak hanya itu, pengakuan terhadap hak-hak subjek data yang menjadi kekurangan dalam UU ITE pun telah diatur dalam UU PDP, seperti hak atas akses, hak untuk menolak pemrosesan, dan hak atas portabilitas data, yang merupakan cerminan langsung dari norma-norma GDPR. Akan tetapi meskipun kerangka kebijakan hukum pidana di Indonesia saat ini telah mengakomodasi terkait perlindungan data pribadi melalui sejumlah peraturan perundang-undangan, terbentanglah bayangan kompleksitas hukum dimana dalam penegakan hukum hingga saat ini belum sepenuhnya sejalan dengan substansi peraturan perundang-undangan yang telah diatur.

Ketidakseimbangan ini tampak jelas dalam kasus peretasan data yang dialami BSI, tidak adanya proses hukum terhadap pelaku maupun upaya pemulihan hak korban yang diberikan oleh pihak BSI hanya bersifat administratif bukan pertanggungjawaban hukum sebagaimana telah diatur dalam peraturan perundang-undangan yang ada saat ini, menjadi contoh konkret lemahnya kapasitas negara dalam menindaklanjuti pelanggaran serius terhadap data pribadi, meskipun telah ada landasan hukum yang cukup komprehensif, kendala utama dalam proses penegakan hukum terhadap tindak pidana siber di Indonesia tidak semata-mata disebabkan oleh kelemahan dalam aspek peraturan perundang-undangan, tetapi juga dipengaruhi oleh keterbatasan kemampuan aparat penegak hukum serta rendahnya tingkat koordinasi antar lembaga terkait.[13]

UU PDP yang mengadopsi prinsip-prinsip GDPR, menuntut agar pengelola data, dalam hal ini BSI, bertanggung jawab penuh atas keamanan data pribadi yang mereka kelola, dan pelaku peretasan harus diusut serta diberi sanksi tegas. Namun, dalam praktiknya, penegakan hukum terhadap kasus ini masih sangat lemah. BSI sendiri lebih banyak melakukan penanganan secara administratif dan komunikasi publik yang kurang transparan, tanpa adanya proses hukum yang jelas terhadap pelaku peretasan maupun upaya pemulihan hak korban. Realitas ini memperlihatkan bahwa keberadaan regulasi saja belum mampu menangani masalah peretasan-peretasan data pribadi, karena tidak disertai dengan peningkatan kapasitas teknis aparat penegak hukum serta komitmen dalam membangun sistem perlindungan data pribadi yang menyeluruh. Efektivitas penegak hukum dalam menghadapi kejahatan digital membutuhkan pendekatan yang bersifat multidisipliner, yang tidak hanya bertumpu pada instrumen hukum

[13] Nur Afifah, 'Tantangan Penegakan Hukum Terhadap Kejahatan Siber di Indonesia' (Skripsi: Universitas Islam Indonesia, 2022)

formal, melainkan juga memerlukan kolaborasi antara lembaga hukum, industri teknologi, dan warga negara (masyarakat sipil).

Kebijakan hukum pidana terhadap peretasan data pribadi saat ini terletak pada substansi atau aturan hukumnya, teknologi, dan penegakan hukum. Pada substansi atau aturan hukumnya, UU PDP saat ini lebih fokus pada data pribadi individu, seperti data identitas, data finansial dan data kesehatan. Pada teknologinya UU PDP saat ini belum secara spesifik mengatur penggunaan data pribadi dalam konteks teknologi AI berfokus pada analisis data yang dikumpulkan oleh IoT dan membuat keputusan cerdas berdasarkan data tersebut. AI dapat digunakan untuk memprediksi, mengoptimalkan, atau bahkan mengontrol perangkat IoT secara otomatis dan *Internet of Things* (IoT) yang berkembang pesat dimana IoT berfokus pada koneksi antar perangkat dan pengumpulan data dari dunia fisik. Contohnya adalah perangkat pintar yang dapat memantau suhu, kelembaban, atau kondisi fisik lainnya dan mengirimkannya ke internet. Pada penegakan hukumnya UU PDP saat ini masih memiliki beberapa tantangan dalam penegakan hukum, seperti kurangnya detail dalam aturan turunan dan belum adanya otoritas khusus untuk perlindungan data.

Kebijakan hukum pidana terkait peretasan data pribadi pada saat ini berupaya untuk melindungi data pribadi dan mencegah akses illegal ke sistem komputer. UU ITE dan UU PDP memberikan dasar hukum untuk menindak peretasan data, namun tantangan tetap ada dalam penegakan hukum, meliputi keterbatasan regulasi (UU ITE dan UU PDP masih memiliki beberapa celah dan membutuhkan penyesuaian agar lebih efektif), kesulitan pengumpulan bukti (pengumpulan bukti diatur dalam kasus peretasan masih sulit dan membutuhkan keahlian khusus), kejahatan siber lintas negara (kejahatan siber dilakukan oleh pelaku yang berada di negara lain, sehingga menimbulkan tantangan dalam hal yuridiksi).

Meskipun secara normatif kebijakan hukum pidana terhadap tindak pidana peretasan data pribadi telah diatur namun dalam implementasinya masih terdapat sejumlah persoalan yang perlu dikritisi. Kebijakan yang telah dirancang dalam berbagai regulasi tersebut belum sepenuhnya menjawab kebutuhan dalam menghadapi kompleksitas kejahatan siber dan menyebabkan tumpang tindih regulasi, khususnya peretasan data pribadi. Oleh karena itu, insiden peretasan data pribadi yang dialami oleh BSI menjadi bukti nyata dari adanya ketimpangan antara norma hukum yang telah dirumuskan dalam peraturan perundang-undangan dan pelaksanaannya di lapangan. Ketimpangan ini tidak hanya menunjukkan lemahnya komitmen negara dalam menegakkan hukum, tetapi juga berdampak pada menurunnya tingkat kepercayaan masyarakat terhadap lembaga-lembaga negara yang seharusnya bertanggung jawab dalam menjamin hak atas perlindungan data pribadi. Salah satu pihak yang patut disoroti adalah Kementerian Komunikasi dan Informatika, yang berdasarkan ketentuan dalam UU ITE, memiliki wewenang untuk menjatuhkan sanksi administratif kepada pengendali atau prosesor data pribadi yang melanggar ketentuan. Namun, hingga saat ini fungsi tersebut belum dijalankan secara optimal.

Lebih lanjut, UU PDP secara tegas mengamanatkan pembentukan suatu lembaga independen yang bertugas melakukan pengawasan terhadap pelindungan data pribadi, termasuk menjatuhkan sanksi terhadap pelanggaran yang terjadi. Akan tetapi, hingga waktu transisi atau masa peralihan (*grace period*) yang ditentukan oleh UU PDP telah berakhir, lembaga pengawas yang dimaksud belum juga dibentuk. Ketidakhadiran lembaga tersebut menimbulkan kekosongan struktural dalam penegakan hukum perlindungan data pribadi, yang pada akhirnya menyebabkan hambatan dalam pelaksanaan sanksi serta ketiadaan mekanisme akuntabilitas yang efektif terhadap pelaku pelanggaran, baik dari sisi pengendali data maupun pihak ketiga lainnya.

Kelemahan yang perlu disoroti adalah minimnya evaluasi terhadap efektivitas regulasi yang ada. Misalnya, belum dilakukan analisis kritis apakah ancaman pidana yang diatur sudah cukup berat untuk memberikan efek jera bagi pelaku, atau apakah instrumen sanksi

administratif dalam UU PDP mampu mencegah terjadinya pelanggaran data pribadi secara efektif. Selain itu, belum terdapat pembahasan mendalam mengenai kapasitas aparat penegak hukum dalam menindak kasus-kasus peretasan data pribadi. Padahal, kesiapan teknis, sumber daya manusia, serta kemampuan forensik digital aparat penegak hukum sangat menentukan dalam efektivitas penegakan hukum terhadap kejahatan ini.

Kondisi ini menunjukkan bahwa Pemerintah belum sepenuhnya memaknai implementasi UU PDP sebagai suatu keniscayaan dalam pembangunan sistem hukum digital yang adil dan berkeadilan. Dalam konteks negara hukum yang menjunjung tinggi prinsip perlindungan hak asasi manusia, ketidaksesuaian antara norma hukum dan pelaksanaannya merupakan persoalan serius yang tidak dapat diabaikan. Apabila perlindungan data pribadi terus-menerus diperlakukan secara normatif tanpa adanya tindakan konkret dalam penegakan hukum, maka hal tersebut tidak hanya mencederai hak konstitusional warga negara, tetapi juga menghambat perkembangan tata kelola digital yang transparan dan bertanggung jawab. Oleh sebab itu, reformasi dalam tataran kelembagaan serta penguatan kapasitas penegakan hukum menjadi kebutuhan mendesak agar norma-norma dalam UU PDP dapat diimplementasikan secara efektif dan tidak berhenti pada tataran normatif semata.

B. Kebijakan Hukum Pidana Terhadap Tindak Pidana Peretasan Data Pribadi Pada Masa Yang Akan Datang

Tindak pidana peretasan data pribadi merupakan fenomena hukum yang tidak dapat dilepaskan dari dinamika kemajuan teknologi informasi dan komunikasi. Dalam era digital saat ini, keberadaan data pribadi yang tersimpan dalam sistem elektronik baik milik institusi pemerintah, korporasi swasta, maupun individu telah menjadi objek yang sangat bernilai dan rentan terhadap penyalahgunaan. Perkembangan teknologi digital telah menciptakan paradigma baru dalam ranah kejahatan, di mana muncul bentuk-bentuk tindak pidana non-konvensional yang memiliki karakteristik tersendiri, berbeda secara substansial dari tindak pidana tradisional. Hal ini menciptakan kompleksitas tersendiri dalam sistem penegakan hukum, baik dalam tahap penyelidikan, penyidikan, hingga proses peradilan, karena Tidak seperti tindak pidana konvensional yang dapat dilacak melalui bukti fisik dan saksi langsung, tindak pidana peretasan data memerlukan pendekatan digital forensik, di mana alat bukti berasal dari jejak digital seperti *log* akses, *metadata*, dan aktivitas jaringan.[14] Sifat kompleks dan multidimensi dari kejahatan siber ini juga diperparah oleh karakteristiknya yang tidak mengenal batas yurisdiksi nasional. Peretasan data sering kali melibatkan pelaku yang beroperasi lintas negara, sehingga penanggulangannya tidak dapat dilakukan secara parsial oleh satu negara saja. Dalam konteks ini, kerja sama internasional menjadi sangat penting, baik dalam bentuk *Mutual Legal Assistance* (MLA), kerja sama antar kepolisian lintas negara, maupun harmonisasi regulasi antarnegara. Kerja sama tersebut diperlukan agar proses investigasi, penindakan, dan ekstradisi pelaku kejahatan siber dapat berjalan efektif dan efisien, mengingat kejahatan siber sering kali melibatkan jaringan global yang rumit.[15]

Dalam menghadapi tantangan tersebut, aparat penegak hukum dituntut untuk memiliki kompetensi teknis yang memadai dalam mendeteksi, mengidentifikasi, dan mengungkap tindak pidana berbasis teknologi informasi. Kompetensi ini tidak hanya sebatas pada pemahaman hukum, tetapi juga mencakup kemampuan teknis forensik digital, analisis data, serta pemahaman terhadap modus operandi kejahatan siber yang terus berkembang. Namun,

---

[14] Edmon Makarim, *Pengantar Hukum Telematika Suatu Kajian Kompilasi,* (Jakarta: Raja Grafindo Persada, 2005) p. 42.

[15] Harjo Susmoro dan B. D. O. Siagian, *Dewan Keamanan Nasional: Solusi Mengatasi Ancaman Multidimensi,* (Bogor: Universitas Pertahanan RI Press, 2021) p. 56.

kenyataannya di Indonesia, keterbatasan sumber daya manusia dan teknologi menjadi hambatan utama dalam penegakan hukum di bidang ini. Selain itu, koordinasi antar lembaga penegak hukum dan instansi terkait juga masih belum optimal, sehingga proses penanganan kasus kejahatan siber sering kali terhambat dan kurang efektif.

Sebagai salah satu negara yang telah meratifikasi ICCPR melalui Undang-Undang Nomor 12 Tahun 2005 tentang kebebasan berpendapat, Indonesia memiliki kewajiban yuridis dan moral untuk menyesuaikan sistem hukum nasionalnya dengan prinsip-prinsip yang diamanatkan dalam konvenan tersebut. Hal ini termasuk di dalamnya adalah pengaturan mengenai perlindungan privasi dan data pribadi sebagai bentuk perlindungan terhadap HAM. Apalagi, di era digital yang semakin terintegrasi saat ini, ancaman terhadap privasi dan penyalahgunaan data pribadi semakin kompleks dan luas, oleh karena itu, Indonesia dituntut untuk tidak hanya memiliki kerangka hukum yang memadai, tetapi juga sistem perlindungan yang adaptif dan responsive terhadap perkembangan teknologi.

Sebagai negara anggota, Indonesia menunjukan konsistensi dalam menjungjung tinggi nilai-nilai HAM, melalui pembentukan regulasi dan kebijakan perlindungan data pribadi yang sejalan dengan standar Internasional, yang di antaranya :

1. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (Selanjutnya disebut UU PK). UU PK hanya mengatur perlindungan privasi dan data pribadi konsumen dalam Pasal 2 yang mana belum mengatur secara eksplisit dan komprehensif mengenai perlindungan data pribadi konsumen sebagai bagian integral dari hak-hak konsumen. Hal ini menjadi suatu kekurangan yang signifikan, mengingat dalam setiap transaksi antara pelaku usaha dan konsumen, hampir selalu terjadi pengumpulan, penyimpanan, dan pengolahan data pribadi sebagai bagian dari proses pelayanan, pemasaran, maupun pembukuan usaha.
2. Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan (selanjutnya disebut sebagai *UU Perbankan*). Dalam kerangka hukum pidana ekonomi, tindak pidana di bidang perbankan dikategorikan sebagai salah satu bentuk kejahatan kerah putih (*white collar crime)* yang umumnya dilakukan oleh individu atau korporasi dengan kedudukan dan kapasitas tertentu, serta memiliki motif ekonomi yang dapat merugikan masyarakat maupun negara.[16] Oleh karena itu, UU Perbankan secara tegas menekankan kewajiban bank dalam menjaga kerahasiaan data nasabah sebagaimana diatur dalam Pasal 40 Ayat (1).
3. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Selanjutnya disebut UU Telekomunikasi). Pada Pasal 42 Ayat (1) dan (2) mengatur penyelenggaraan telekomunikasi dan aspek perlindungan privasi dan data pribadi pengguna jasa telekomunikasi di Indonesia.
4. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (Selanjutnya disebut UU HAM), dalam Pasal 29 ayat (1) mencerminkan penghormatan negara terhadap nilai-nilai dasar kemanusiaan yang bersumber dari hak setiap warga negara. Dan dalam hal ini, negara mengakui dan menjamin hak privasi dan perlindungan data pribadi yang merupakan bagian inheren dari warga negara.
5. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Selanjutnya disebut UU KIP), dalam UU KIP, perlindungan privasi dan data pribadi tersirat dalam defenisi informasi publik dalam Pasal 1 angka (2) dan Pasal 6 Ayat (3) bahwa Informasi yang berkaitan dengan hak-hak pribadi, merupakan upaya atas perlindungan privasi dan data pribadi. Pun Informasi yang dimaksud berkaitan dengan diri seseorang/masyarakat/kelompok yang tercakup dalam kepentingan publik.

[16] Galang Djokdja, Sherly Adam, dan Margie Gladies Sopacua, *Pertanggungjawaban Pidana Pelaku Pembobolan Kartu Kredit dalam Tindak Pidana di Bidang Perbankan, Tatohi Jurnal Ilmu Hukum* 02 No. 02 (2022):178-192, https://doi.org/10.47268/tatohi.v2i2.909

6. Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan (Selanjutnya disebut UU Kesehatan), dalam Pasal 57 Ayat (1) secara eksplisit memberikan pengakuan terhadap pentingnya perlindungan privasi dan data pribadi dalam sektor kesehatan. Data kesehatan termasuk dalam kategori data pribadi yang bersifat *sensitive personal data* yang tidak hanya mencakup informasi administratif tetapi juga data yang berisikan hasil diagnosis, rekam medis, riwayat pengobatan, hasil pemeriksaan laboratorium, serta data biometrik. Penting untuk data-data tersebut dijaga kerahasiaannya, sebab dapat menimbulkan dampak serius bagi individu apabila terjadi peretasan atau kebocoran.
7. Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (Selanjutnya disebut UU AK), dalam Pasal 1 Angka 22 dan Pasal 84 Ayat (1) memuat perlindungan atas informasi perseorangan yang bersifat sensitif, serta menegaskan kewajiban negara untuk tidak hanya menyimpan dan memelihara data tersebut, tetapi juga menjamin kerahasiaannya.
8. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), merupakan salah satu tonggak awal regulasi di Indonesia yang secara eksplisit memberikan pengakuan hukum terhadap pentingnya perlindungan privasi dan data pribadi di ranah digital. Meskipun UU ini tidak secara komprehensif mengatur seluruh aspek perlindungan data pribadi, namun keberadaan Pasal 26 ayat (1) menjadi bukti awal hadirnya norma yang menempatkan hak atas kendali informasi pribadi sebagai bagian dari hak yang dilindungi secara hukum. Pasal ini menegaskan bahwa penggunaan data pribadi dalam bentuk apapun melalui media elektronik tidak dapat dilakukan secara sewenang-wenang, melainkan harus didasarkan pada persetujuan dari subjek data. Dalam hal ini, subjek data memiliki kontrol penuh atas informasi pribadinya, yang merupakan bentuk konkret dari hak individu untuk mengendalikan bagaimana data pribadinya dikumpulkan, digunakan, disimpan dan disebarluaskan. Norma ini sejalan dengan prinsip-prinsip perlindungan data dalam GDPR Uni Eropa, yakni prinsip Sesuai Hukum, Adil dan Transparan (*Lawfullness, Fairness, and Transparency)*. Selain Pasal 26, UU ITE juga memuat sejumlah ketentuan mengenai tindakan yang dilarang terkait penyalahgunaan informasi (privasi dan data pribadi) dan transaksi elektronik, sebagaimana diatur dalam Pasal 27 sampai dengan Pasal 37. Meskipun tidak secara spesifik menyebutkan data pribadi, namun norma-norma tersebut melarang berbagai tindakan yang dapat membuat kerugian melalui media elektronik, termasuk penghinaan, pencemaran nama baik, pemerasan, pengancaman, penyebaran informasi palsu, akses ilegal, hingga gangguan terhadap integritas sistem elektronik.
9. Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), UU ini merupakan pengaturan yang disahkan pemerintah dalam merespons tuntutan perlindungan privasi dan data pribadi di era digital, dengan mengatur perlindungan privasi dan data pribadi secara terpadu, dimulai dari ketentuan mengenai jenis data pribadi, hak subjek data pribadi, kewajiban pengendali data pribadi, serta sanksi administratif dan pidana bagi pelanggar. UU PDP memberikan perlindungan lebih lanjut terhadap data pribadi termasuk data yang dikumpulkan dan di proses dalam sistem elektronik. UU PDP memberikan kerangka hukum yang komprehensif, defenisi dan klasifikasi data pribadi (Pasal 1-Pasal 4), hak subjek data (Pasal 5-Pasal 13), pemrosesan data pribadi (Pasal 16-Pasal 18), kewajiban pengendali data pribadi (Pasal 19-Pasal 20), mekanisme persetujuan pemrosesan data pribadi (Pasal 21-Pasal 24), Pemrosesan data pribadi anak (Pasal 25), pemrosesan data pribadi penyandang disabilitas (Pasal 26), larangan penggunaan data pribadi (Pasal 65-Pasal 66) dan sanksi atas pelanggaran perlindungan data pribadi (Pasal 57, Pasal 67-Pasal 73). UU PDP menegaskan perlunya persetujuan pemilik data untuk pengumpulan dan pemrosesan data pribadi, serta penyelenggaran sistem elektronik untuk menjaga keamanan data. Hal ini mencerminkan

sikap negara yang mulai menyadari pentingnya mengatur tata kelola data secara menyeluruh, sebab sebelum adanya UU PDP standar perlindungan data pribadi di Indonesia diterapkan melalui berbagai undang-undang yang ada, banyaknya peraturan menyebabkan ketidaksinkronan satu sama lain, sehingga menciptakan kebingungan dalam implementasi dan kepatuhan terhadap perlindungan data pribadi. kehadiran UU PDP pun mengurangi tumpang tindih regulasi.[17]

Peraturan yang berlaku saat ini kerap kali belum mampu mengimbangi pesatnya kemajuan teknologi. Munculnya inovasi seperti kecerdasan buatan, *big data*, serta *Internet of Things (LoT)* menghadirkan berbagai tantangan baru dalam aspek perlindungan data pribadi, yang dalam banyak kasus belum sepenuhnya terakomodasi dalam kerangka regulasi yang ada. Kondisi ini menunjukan pentingnya pembaharuan dan penyesuaian regulasi secara berkelanjutan agar tetap selaras dan efektif dalam menjawab dinamika perlindungan data pribadi di era digital. Tanpa adanya regulasi yang bersifat adaptif dan menyeluruh, perlindungan terhadap data pribadi berisiko terus tertinggal dari laju perkambangan teknologi dan ancaman yang menyertainya.[18]

Diperlukan penguatan regulasi dan penegakan hukum yang efektif agar tidak hanya bersifat formalitas belaka, tetapi juga mencerminkan komitmen terhadap amanat DUHAM dan ICCPR. UU PDP hadir sebagai jawaban atas kekosongan hukum yang selama ini dirasakan dalam pengelolaan dan perlindungan data pribadi, tetapi juga sebagai bentuk aktualisasi nilai-nilai konstitusional yang berakar dari penghormatan terhadap martabat manusia, sebagaimana tercermin dalam Pasal 28G dan 28H UUD 1945 yang menjamin perlindungan atas diri pribadi dan rasa aman dari ancaman penyalahgunaan informasi.

Dalam menghadapi tantangan perlindungan data pribadi di tengah laju perkembangan teknologi informasi. UU PDP telah menandai pergeseran pendekatan hukum dari sekadar tindakan represif menjadi tindakan preventif dan struktural, di mana perlindungan terhadap data pribadi tidak hanya dimaknai sebagai isu teknis, tetapi sebagai hak asasi manusia yang fundamental dan dijamin oleh konstitusi. Untuk memastikan perlindungan data pribadi terlaksana secara efektif, maka dibutuhkan otoritas perlindungan data pribadi yang independent. Hal ini ditegaskan dalam Pasal 58 UU PDP yang menyatakan bahwa :

"(1) Untuk melaksanakan penyelenggaraan perlindungan data pribadi, dibentuk lembaga yang melaksanakan tugas dan wewenang secara independent.
(2) Lembaga sebagaimana dimaksud pada ayat (1) berada di bawah Presiden dan bertanggungjawab kepada Presiden"

Namun demikian, hingga saat ini lembaga independen yang bertugas khusus sebagai pengawas perlindungan data pribadi sebagaimana diamanatkan dalam UU PDP belum juga terbentuk. Keberadaan lembaga ini penting mengingat fungsinya yang strategis dalam merumuskan dan menetapkan kebijakan strategis perlindungan data pribadi, mengawasi penyelenggaraan terhadap perlindungan data pribadi, serta menegakkan hukum administratif terhadap pelanggar.

Ketiadaan lembaga pengawas yang independen menyebabkan upaya perlindungan data pribadi di Indonesia masih berjalan tidak optimal. Saat ini, fungsi pengawasan masih dijalankan secara sektoral oleh beberapa lembaga, seperti Kementerian Komunikasi dan Informatika (Selanjutnya disebut Kominfo), Otoritas Jasa Keuangan (Selanjutnya disebut OJK), Lembaga

[17] Fanisa Mayda Ayiliani dan Elfia Farida, Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Perlindungan Hukum Terhadap Transfer Data Pribadi Lintas Negara, *Jurnal Pembangunan Hukum Indonesia* 06 No. 03 (2024): 431-455. https://doi.org/10.14710/jphi.v6i3.%p

[18] Achmad Fachri Yamin dan Jonathan Kevin Wijaya, Perlindungan Data Pribadi dalam Era Digital: Tantangan dan Solusi, *Meroja Journal* 07 No. 02 (2024): 138-155. https://doi.org/10.33080/mrj.v7i2.352 https://doi.org/10.33080/mrj.v7i2.352

Perlindungan Konsumen, serta Kepolisian. Namun, masing-masing lembaga tersebut memiliki keterbatasan dalam hal kewenangan, cakupan pengawasan, dan efektivitas tindakan. Akibatnya, fungsi pengawasan yang seharusnya bersifat terintegrasi dan lintas sektor menjadi tidak efektif, karena lembaga-lembaga tersebut cenderung bekerja dalam kerangka sektoral yang kaku, parsial, dan rawan menimbulkan konflik kepentingan.

Kondisi ini memperlihatkan bahwa tanpa adanya satu lembaga pengawas independen yang memiliki otoritas penuh, upaya perlindungan data pribadi akan terus mengalami hambatan. Misalnya, Kominfo yang memainkan peran sentral dalam regulasi dan pengawasan di bidang ini, namun wewenangnya terbatas dan belum mencakup fungsi pengawasan yang independen, baik terhadap sektor publik maupun swasta. Kemampuan Kominfo dalam melakukan investigasi dan pengawasan juga dinilai belum maksimal, Oleh sebab itu, dibutuhkan pembaruan regulasi yang disertai dengan pembentukan ulang konsep kelembagaan pengawas perlindungan data pribadi yang lebih kuat dan independen, sebagai pilar utama dalam menjamin hak atas privasi di tengah tantangan era digital, sebagaimana diamanatkan oleh konstitusi.[19]

Kemudian, OJK memiliki peran dalam mengawasi lembaga keuangan yang juga mengelola data pribadi nasabah. Namun, pengawasan yang dilakukan masih bersifat sektoral dan tidak mencakup keseluruhan ekosistem data pribadi, serta dinilai kurang efektif, mengingat masih sering terjadinya kasus peretasan dan pencurian data nasabah di sektor perbankan.[20] Selain itu, lembaga Perlindungan Konsumen turut terlibat dalam masalah privasi dan perlindungan data, namun tidak memiliki kewenangan hukum yang cukup untuk menindaklanjuti pelanggaran secara langsung.[21]

Ketiadaan sistem pengawasan yang komprehensif terhadap perlindungan data pribadi di Indonesia semakin terlihat nyata melalui berbagai insiden peretasan data, Oleh karena itu, kebijakan hukum pidana terhadap tindak pidana peretasan data pribadi pada masa yang akan datang haruslah diarahkan pada pembentukan lembaga pengawas perlindungan data pribadi yang independen, sebagaimana diamaatkan dalam UU PDP Pasal 58. Langkah penataan kelembagaan pengawas perlindungan data pribadi harus independen dan berkaitan dengan struktur formal dan menyentuh dimensi fungsional serta substantif dari sebuah otoritas pengawasan.

Dalam hal ini, lembaga pengawas PDP idealnya memiliki kedudukan yang tidak bergantung pada otoritas sektoral tertentu, serta bebas dari intervensi politik dan kepentingan ekonomi. Hal ini penting agar proses pengawasan terhadap pelanggaran data, baik yang dilakukan oleh entitas pemerintah maupun swasta, dapat dilakukan secara objektif dan transparan. Merujuk pada prinsip *Independent Regulatory Agencies (*IRAs), lembaga ini harus memiliki kewenangan yang jelas, independensi pengambilan keputusan, serta mekanisme akuntabilitas publik yang kuat, agar dapat menjamin efektivitas dan akuntabilitas pengawasan.

Tanpa otoritas yang kuat dan legitimasi yang memadai, pengawasan terhadap praktik penyalahgunaan data pribadi akan terus terhambat oleh birokrasi dan tumpang tindih kewenangan. Lebih jauh, penguatan kelembagaan harus disertai dengan reformasi substansi hukum dan peningkatan kapasitas sumber daya manusia, termasuk aparat penegak hukum yang

---

[19] Juaningsih, Imas Novita, dan Rusli Dzakwan Nurirfan, Rekonsepsi Lembaga Pengawas Terkait Perindungan Data Pribadi oleh Korporasi Sebagai Penegakan Hak Privasi Berdasarkan Konstitusi, *Jurnal Sosial dan Budaya Syar-I* 08 No. 01 (2021): 467-484. 10.15408/sjsbs.v8i2.19904

[20] Sandi, Pengawasan Otoritas Jasa Keuangan (OJK) Terhadap Perbankan Sebagai Upaya Perlindungan Hukum Nasabah atas Penjualan Data Nasabah Bank, *Jurnal Idea Hukum* 05 No. 02 (2019): 1534. https://doi.org/10.20884/1.jih.2019.5.2.125

[21] Doly, Pembentukan Lembaga Pengawas Perlindungan Data Pribadi dalam Perspektif Pembentukan Lembaga Negara Baru, *Negara Hukum* 12 No. 02 (2021): 223-244. https://doi.org/10.22212/jnh.v12i2.2357

terlibat dalam proses investigasi dan adjudikasi. Seluruh elemen tersebut harus bergerak dalam kerangka kebijakan yang terintegrasi, tidak sektoral, serta mampu beradaptasi terhadap perkembangan teknologi digital yang terus berubah.

Arah politik hukum pidana di masa mendatang dalam isu perlindungan data pribadi harus menempatkan lembaga pengawas yang independen sebagai aktor utama dengan sistem kelembagaan yang kuat, akuntabel, dan independent. Hal ini bukan hanya untuk menjamin efektivitas pelaksanaan UU PDP, tetapi juga sebagai manifestasi dari komitmen negara terhadap perlindungan hak asasi manusia di ranah digital, sebagaimana tertuang dalam UUD 1945, Deklarasi Universal Hak Asasi Manusia (DUHAM), dan *International Covenant on Civil and Political Rights* (ICCPR) Uni Eropa. Tanpa mekanisme pembentukan lembaga pengawasan yang kredibel dan sistem penegakan hukum yang responsif, perlindungan data pribadi hanya akan menjadi retorika tanpa realisasi nyata di tengah ancaman kejahatan siber yang kian kompleks.

Kebijakan hukum pidana terhadap peretasan data pribadi pada masa yang akan datang harus terletak pada peningkatan atau penguatan substansi atau aturan hukumnya, teknologi, dan penegakan hukum. Dimana UU PDP untuk masa yang akan datang akan lebih komprehensif, termasuk data yang dihasilkan oleh teknologi canggih seperti AI. UU masa depan akan mencakup data yang dihasilkan oleh teknologi canggih seperti AI, IoT, dan data yang terkait dengan perilaku digital. Selain itu, masa depan akan melihat peningkatan penegakan hukum dan kemungkinan adanya otoritas khusus untuk perlindungan data. UU masa depan akan lebih detail dalam mengatur penggunaan data pribadi dalam konteks teknologi ini, termasuk transparansi algoritma AI dan perlindungan dari bias. UU masa depan diharapkan akan memiliki penegakan hukum yang lebih kuat, termasuk otoritas khusus yang bertanggung jawab untuk memantau kepatuhan dan menindak tindak pidana peretasan data pribadi.

Kebijakan hukum pidana dalam peretasan data pribadi pada masa yang akan datang dilakukan melalui pembaharuan hukum atau merevisi UU ITE dan UU PDP agar dapat menangani kasus peretasan data yang lebih canggih, mencakup peningkatan ancaman pidana untuk tindak pidana peretasan data pribadi, penyempurnaan defenisi dalam lingkup peretasan data pribadi yang lebih jelas, perluasan kewenangan penegak hukum untuk melakukan penyelidikan dan penangkapan pelaku peretasan data, serta pentingnya kebijakan hukum pidana yang kuat dalam mempertahankan keamanan data pribadi untuk menjaga kepercayaan publik dan mendorong inovasi teknologi.

UU masa depan akan menekankan pentingnya privasi berdasarkan desain, yaitu memastikan perlindungan data pribadi sejak awal dalam pengembangan sistem dan teknologi. UU masa depan akan mengharuskan organisasi untuk melakukan penilaian dampak privasi sebelum menerapkan teknologi baru yang melibatkan data pribadi, untuk mengidentifikasi dan mengurangi risiko privasi. UU masa depan akan lebih memperkuat hak-hak subjek data, seperti hak untuk mengakses, memperbaiki, dan menghapus data pribadi mereka. UU masa depan akan mengatur transfer data pribadi ke negara lain dengan lebih ketat, untuk memastikan bahwa data pribadi dilindungi di semua negara.

UU masa depan akan memiliki sanksi yang lebih tegas bagi pelanggaran data pribadi, untuk meningkatkan kepatuhan dan melindungi hak privasi individu. UU PDP mengatur bagaimana perusahaan dapat mengumpulkan dan menggunakan data pribadi, tetapi tidak secara spesifik mengatur bagaimana AI dapat menggunakan data pribadi, termasuk memastikan bahwa algoritma AI tidak diskriminatif dan bahwa individu memiliki hak untuk mengajukan keberatan atas keputusan yang dibuat oleh AI dapat menggunakan data pribadi untuk membuat keputusan atau rekomendasi.

Diharapkan UU PDP masa depan akan lebih komprehensif, teknologi-*savy*, dan memiliki penegakan hukum yang lebih kuat untuk melindungi data pribadi di era digital yang semakin kompleks. Perubahan ini akan membantu memastikan bahwa hak-hak individu atas privasi mereka dilindungi di era teknologi AI dan IoT.

Kesimpulan

Kebijakan hukum pidana terhadap peretasan data pribadi saat ini terletak pada substansi atau aturan hukumnya, teknologi, dan penegakan hukum. Pada substansi atau aturan hukumnya UU PDP saat ini (UU No. 27 Tahun 2022) lebih fokus pada data pribadi individu, seperti data identitas, data finansial dan data kesehatan. Pada teknologinya, UU PDP saat ini belum secara spesifik mengatur penggunaan data pribadi dalam konteks teknologi ***Artificial Intelligence*** **(**AI) berfokus pada analisis data yang dikumpulkan oleh IoT. Pada penegakan hukumnya UU PDP saat ini masih memiliki beberapa tantangan dalam penegakan hukum, seperti kurangnya detail dalam aturan turunan dan belum adanya otoritas khusus untuk perlindungan data.

Kebijakan Kebijakan hukum pidana terhadap peretasan data pribadi pada masa yang akan datang terletak peningkatan atau penguatan pada substansi atau aturan hukumnya, teknologi, dan penegakan hukum. Dimana UU PDP untuk masa yang akan datang akan lebih komprehensif, Pada teknologinya, pengutan dan perluasaan penggunaan data pribadi dalam konteks teknologi ***Artificial Intelligence*** **(**AI) berfokus pada analisis data yang dikumpulkan oleh IoT dan penegakan hukumnya lebih mempertegas sanksi terhadap pelaku peretasan data pribadi.

Referensi

Afifah, Nur. "Tantangan Penegakan Hukum Terhadap Kejahatan Siber di Indonesia". Skripsi: Universitas Islam Indonesia, 2022.

Anwar, Yesmil, dan Adang, *Pembaharuan Hukum Pidana; Reformasi Hukum,* Jakarta: PT. Gramedia Widiasarana Indonesia, 2008.

Ayiliani, Fanisa Mayda dan Elfia Farida. "Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Perlindungan Hukum Terhadap Transfer Data Pribadi Lintas Negara." *Jurnal Pembangunan Hukum Indonesia* 06 No. 03 (2024): 431-455. https://doi.org/10.14710/jphi.v6i3.%p

Djafar, Wahyudi. "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan, Tantangan Hukum dalam era Analisis Big Data". Kuliah Umum: Universitas Gadjah Mada, 2019.

Djokdja, Galang, Sherly Adam, dan Margie Gladies Sopacua. "Pertanggungjawaban Pidana Pelaku Pembobolan Kartu Kredit dalam Tindak Pidana di Bidang Perbankan." *Tatohi Jurnal Ilmu Hukum* 02 No. 02 (2022):178-192, https://doi.org/10.47268/tatohi.v2i2.909

Doly. "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi dalam Perspektif Pembentukan Lembaga Negara Baru." *Negara Hukum* 12 No. 02 (2021): 223-244. https://doi.org/10.22212/jnh.v12i2.2357

Hartanto, Airlangga, *Making Indonesia 4.0*, Jakarta: Kementerian Perindustrian RI, 2018.

Hattu, Jacob. "Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan Anak." *Jurnal Sasi* 20 No. 2 (2014): 47-52, https://doi.org/10.47268/sasi.v20i2.326

Juaningsih, Imas Novita, dan Rusli Dzakwan Nurirfan. "Rekonsepsi Lembaga Pengawas Terkait Perindungan Data Pribadi oleh Korporasi Sebagai Penegakan Hak Privasi Berdasarkan Konstitusi." *Jurnal Sosial dan Budaya Syar-I* 08 No. 01 (2021): 467-484. 10.15408/sjsbs.v8i2.19904

Makarim, Edmon. *Pengantar Hukum Telematika Suatu Kajian Kompilasi,* Jakarta: Raja Grafindo Persada, 2005.

Mansyur, Dikdik, dan Elisatris Gultom, *Cyber Law: Aspel Hukum teknologi Informasi,* Bandung: Refika Aditama, 2009.

Maulana, Nicky. "Manajemen Krisis PT. BSI Tbk Pasca Peretasan Data Nasabah." *Innovative: Journal Of Social Science Research* 4, No. 1 (2024): 8244-58,

https://doi.org/10.31004/innovative.v4i1.8620

Purba, Nabillah, Mhd Yahya, dan Nurbaiti. "Revolusi Industri 4.0: Peran Teknologi dalam Eksistensi Penguasaan Bisnis dan Implementasinya." *JPSB* 9, No. 2, (2021): 91-98. https://doi.org/10.26486/jpsb.v9i2.2103

Raharjo, Agus, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: Citra Aditya Bakti, 2002.

Sandi. "Pengawasan Otoritas Jasa Keuangan (OJK) Terhadap Perbankan Sebagai Upaya Perlindungan Hukum Nasabah atas Penjualan Data Nasabah Bank." *Jurnal Idea Hukum* 05 No. 02 (2019): 1534. https://doi.org/10.20884/1.jih.2019.5.2.125

Susmoro, Harjo dan B. D. O. Siagian, *Dewan Keamanan Nasional: Solusi Mengatasi Ancaman Multidimensi,* Bogor: Universitas Pertahanan RI Press, 2021.

Usman, Atang Hermawan. "Kesadaran Hukum Masyarakat dan Pemerintah Sebagai Faktor Tegaknya Negara Hukum di Indonesia." *Jurnal Wawasan Yuridika* 30, No. 01 (2014): 26-53, https://doi.org/10.25072/jwy.v30i1.74

Wijoyo, Hadion, dkk, *Cyber Crime,* Solok: Mafy Media Literasi Indonesia, 2024.

Warassih, Esmi, *Pemberdayaan Masyarakat Dalam Mewujudkan Tujuan Hukum (Proses Penegakan Hukum Dan Persoalan Keadilan)*, Semarang: Diponegoro University Press, 2001.

Wisnubroto, Aloysius, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer,* Yogyakarta: Penerbit Universitas Atmajaya, 1999.

Yamin, Achmad Fachri dan Jonathan Kevin Wijaya. "Perlindungan Data Pribadi dalam Era Digital: Tantangan dan Solusi." *Meroja Journal* 07 No. 02 (2024): 138-155. https://doi.org/10.33080/mrj.v7i2.352 https://doi.org/10.33080/mrj.v7i2.352