UNES Journal of Swara Justisia
e-ISSN: 2579-4914 | p-ISSN: 2579-4701
https://swarajustisia.unespadang.ac.id/index.php/UJSJ/index
DOI: https://doi.org/10.31933/ujsj.v7i2

PERLINDUNGAN HUKUM POSITIF INDONESIA TERHADAP KEJAHATAN PENYALAHGUNAAN DATA PRIBADI

Beni Kharisma Arrasuli[1*], Khairul Fahmi[2]
[1,2]Fakultas Hukum, Universitas Andalas, Indonesia

**Corresponding Author:* beniarrasuli.fhua@gmail.com

Info Artikel
Diterima, 11/05/2023
Direvisi, 12/06/2023
Dipublikasi, 01/07/2023

Kata Kunci:
Perlindungan Hukum; Perlindungan Data Pribadi

Abstrak

Artikel ini membahas mengenai eksistensi dan kemampuan hukum positif di Indonesia dalam melindungi pengguna dari kejahatan terkait penyalahgunaan terhadap data pribadi dan melihat pelaksanaan penegakan hukum serta pertanggungjawaban hukum pengendali dan prosesor data pribadi jika terjadi penyalahgunaan terhadap data pribadi pengguna. Hal ini terkait dengan semakin meningkatnya kejahatan dengan menggunakan data pribadi seseorang tanpa izin dari pemilik data, bahkan pemilik data dapat mengalami kerugian secara materiil dan mendapat intimidasi atau pengancaman. Sebelum disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, pengaturan hukum positif di Indonesia selama ini yang mengatur terkait data pribadi masih tersebut dalam beberapa peraturan perundang-undangan dengan bersifat sektoral. Artikel ini membahas setiap peraturan tersebut yang berfungsi melindungi data pribadi pengguna selama ini, serta mendalami sejauh mana pengaturan tersebut berfungsi. Pendekatan yang digunakan dalam penulisan artikel ini adalah pendekatan normatif-empiris, yaitu metode penelitian hukum yang mengkaji hukum tertulis dan kepustakaan atau penelitian hukum dari beragam perspektif, serta menghubungkannya dengan realitas yang terjadi di masyarakat. Analisis dilakukan secara deskriptif yaitu mengumpulkan semua data dan menghubungkan permasalahan dengan analisis berdasarkan teori hukum yang disusun sistematis. Sehingga dalam artikel ini dapat dilihat dan disimpulkan bahwa pengaturan mengenai penyalahgunaan data pribadi yang bersifat sektoral di Indonesia selama ini belum efektif dan tidak mampu menanggulangi kejahatan yang terjadi, serta upaya hukum yang dapat ditempuh dengan peraturan yang ada selama ini juga sangat minim. Hadirnya Undang-Undang Perlindungan Data Pribadi yang secara fokus mengatur masalah data pribadi, diharapkan mampu kedepannya menjadi solusi dalam mencegah terjadinya kejahatan menggunakan data pribadi dan menjadi payung hukum yang kuat dalam melakukan upaya penegakan hukum.

Keywords: *Legal Protection, Personal Data Protection*

Abstract

This article discusses the existence and ability of positive law in Indonesia to protect users from crimes related to misuse of personal data and looks at the implementation of law enforcement and the legal responsibilities of controllers and processors of personal data in the event of misuse of users' personal data. This is related to the increasing crime by using someone's personal data without the permission of the data owner, even the data owner can suffer material losses and receive intimidation or threats. Prior to the enactment of Law Number 27 of 2022 concerning Protection of Personal Data, positive legal arrangements in Indonesia so far that regulated personal data were still mentioned in several statutory regulations with a sectoral nature. This article looks at each of these rules that have served to protect users' personal data so far, and explores how far these settings work. The approach used in writing this article is a normative-empirical approach, namely a legal research method that examines written law

and literature or legal research from various perspectives, and relates it to the reality that occurs in society. The analysis was carried out descriptively, namely collecting all data and linking the problems with analysis based on legal theory arranged systematically. So that in this article it can be seen and concluded that regulations regarding sectoral misuse of personal data in Indonesia have so far been ineffective and unable to deal with crimes that have occurred, as well as legal remedies that can be taken with existing regulations so far are also very minimal. The presence of the Personal Data Protection Act which focuses on regulating personal data issues, is expected to be able to become a solution in the future in preventing crimes using personal data and become a strong legal umbrella in carrying out law enforcement efforts

PENDAHULUAN

Perkembangan teknologi informasi telah mengubah banyak hal tentang kehidupan manusia. Teknologi bukan hanya saja memoles gaya hidup, tetapi juga telah menempatkan pola interaksi antar-manusia. Berbagai aktifitas dan interaksi yang sebelumnya dilaksanakan dalam ruang dan waktu yang nyata, kini dilaksanakan secara digital. Ruang dan waktu nyata digantikan oleh tempat elektronik (telepon, *whatsapp*, televisi) atau ruang virtual (internet).[1]

Teknologi semakin terus dikembangkan untuk semakin mempermudah manusia dalam melakukan suatu aktivitas dalam kehidupan sehari-hari. Internet menjadi salah satu produk teknologi informasi dan komunikasi yang perkembangan kecanggihannya sangat cepat dan pesat sehingga sudah menguasai hampir diseluruh aspek kehidupan manusia. Saat ini dunia sudah masuk pada suatu zona dan peradaban baru, dimana kehidupan manusia sudah berada dalam basis lingkungan yang serba digital.[2] Akses terhadap media digital telah menjadi salah satu kebutuhan primer setiap orang. Hal itu disebabkan adanya kebutuhan akan informasi, hiburan, pendidikan, dan akses pengetahuan dari belahan bumi yang berbeda. Kemajuan teknologi dan informasi serta semakin canggihnya perangkat-perangkat yang diproduksi oleh industri seperti menghadirkan dunia dalam genggaman.[3] Istilah ini sejajar dengan apa yang diutarakan oleh Thomas L. Friedman sebagai the *world is flat* bahwa dunia semakin rata dan setiap orang bisa mengakses apapun dari sumber manapun.

Indonesia dengan jumlah populasi penduduk yang sangat besar menjadikannya sebagai tempat perkembangan dunia digital yang sangat pesat. Pada Tahun 2021 Wearesosial Hootsuite merilis hasil risetnya, bahwa pengguna internet di indonesia mencapai 202,6 juta atau sebesar 73,7% dari total populasi masyarakat Indonesia yang berjumlah 274,9 juta orang.[4] Jumlah tersebut terus naik dari tahun-tahun sebelumnya. Sedangkan 170 juta orang merupakan pengguna yang aktif berselancar di sosial media di Indonesia.[5] Dengan tinggi jumlah pengguna, media digital akhirnya memegang peranan penting dalam komunikasi antar-manusia, sehingga media digital dan internet pun telah menjadi entitas baru dalam kehidupan manusia, termasuk dalam dunia kejahatan.

Media digital dapat berpotensi menjadi alternatif sarana kejahatan. Kemajuan ilmu pengetahuan dan teknologi informasi yang didasari serba digital dengan mudah akan

[1] Yasraf Amir Piliang, *Dunia yang Dilipat, Tamasya Melampaui Batas-batas Kebudayaan*, (Bandung: Jalasutra, 2004), hlm. 475
[2] Edmon Makarim, *Pengantar Hukum Telematika* (Jakarta: Raja Grafindo Persada, 2005), hlm. 31
[3] Rulli Nasrullah, *Media Sosial Perspektif Komunikasi, Budaya, dan Sosioteknologi*, (Bandung: Simbiosa Rekatama Media, 2017), hlm. 1
[4] Hootsuite WeareSocial, Indonesian Digital Report 2021
[5] *Ibid*

menimbulkan dan menciptakan suatu perubahan yang mendasar dan sangat luas dalam suatu arus informasi. Media digital menjadi suatu ruang publik, menjadi ruang terbuka, dan ruang alternatif.[6] Salah satunya tindak kejahatan siber atau kejahatan dalam dunia digital.

Pembicaraan mengenai teknologi informasi dan ruang siber (*cyberspace)* selama ini banyak melihat kepada pemanfataan teknologi digital tersebut dalam konteks yang memudahkan, seperti perdagangan online dan komunikasi jarak jauh, dan sering juga pada sisi penyalahgunaanya dalam bentuk kejahatan siber (*cybercrime*).[7] Pembicaraan yang ada belum kepada isu yang tentang bagaimana pertanggungjawaban hukum terhadap sistem. Oleh karenanya juga diperlukan suatu aturan hukum untuk memperkecil kemungkinan jahat itu terjadi. Salah satu kejahatan yang sering terjadi dalam dunia digital saat ini adalah penyalahgunaan data pribadi.

Data privasi merupakan salah satu topik bahasan yang saat ini sedang menjadi perhatian, hal ini juga disebabkan karena kita sedang menuju "*web of the world*" pada saat komunikasi antar manusia menggunakan komunikasi bergerak khususnya pengguna *smartphone*, komputer tablet yang terkoneksi dengan internet yang dapat menghubungkan dunia fisik ke dalam satu jaringan.[8] Kemajuan tersebut memiliki dampak lain yang lebih besar juga, yaitu berupa ancaman terhadap privasi dengan memberikan peluang besar bagi pihak yang memiliki akses terhadap data pribadi seseorang.

Modus operandi yang menyerang data pribadi tersebut dapat dilakukan dengan suatu akses yang tidak sah. Akses tidak sah atau *illegal access* tersebut dalam bentuk memasuki sistem komputer, seperti data penyimpanan rahasia tanpa seizin pemilik atau adanya upaya menggunakan akses komputer tersebut untuk melakukan perbuatan yang melanggar hukum. Beberapa jenis kejahatan ini antara lain:[9]

1. Penyadapan tidak sah, yaitu aktifitas memasang alat bantu teknis, baik perangkat keras maupun perangkat lunak untuk menyalin informasi atau identitas yang ada di internet.
2. Penipuan melalui bank, yaitu tindakan mengambil uang dengan cara yang tidak sah, dan didapat dengan cara yang illegal maupun meretas program.
3. Pencucian uang, merupakan upaya menggunakan dunia siber untuk memindahkan uang atau melakukan transfer melalui atau antar akun rekening bank.
4. Penggunaan jaringan milik pihak lain secara ilegal.

Melihat kepada kasus dan modus yang ada, perlindungan hukum mengenai terhadap upaya penyalahgunaan data pribadi untuk melakukan suatu kejahatan ini mutlak diperlukan. Data pribadi merupakan suatu elemen dan bagian kunci bagi suatu kebebasan dan harga diri individu. Perlindungan data menjadi dorongan kuat untuk terciptanya kebebasan politik, spritual, keagamaan, bahkan kegiatan seksual. Hak untuk menentukan nasib sendiri, kebebasan berekspresi, dan privasi adalah hak-hak yang penting untuk menjadikan kita sebagai manusia.[10]

Di Indonesia, kebocoran data pribadi dan dipergunakan untuk melakukan kejahatan sudah banyak terjadi. Maraknya *skimming* atau penyalinan data dan informasi kartu ATM,

[6] Gomgom T.P Siregar, Suatu analisis mengenai tindak pidana pencemaran nama baik melalui media elektronik, (Bandung: Refika Aditama, 2020), hlm. 3

[7] Edmon Makarim, "Tanggungjawab Penyelenggara Terhadap Tata Kelola Yang Baik Dalam Penyelenggaraan Sistem Elektronik (Good Electronic Governance)", (Disertasi Doktor Universitas Indonesia, Depok, 2009), hlm.9

[8] Sinta Dewi Rosadi, Cyber Law, (Bandung: Refika Aditama, 2015), hlm. 1

[9] Rulli Nasrullah, *Media Sosial Perspektif Komunikasi, Budaya, dan Sosioteknologi*, hlm. 192

[10] Sinta Dewi Rosadi, Cyber Law, hlm. 9

pinjaman *online* dengan menggunakan identitas pribadi orang lain yang sering berakhir dengan ancaman atau intimidasi, bahkan penyebarluasan informasi pribadi kepada publik atau yang dikenal dengan *doxing*, merupakan contoh kejahatan dan pelanggaran terhadap hak privasi seseorang.

Pengaturan tentang data pribadi sangat diperlukan karena mengatur mengenai mekanisme pengumpulan, penggunaan, pengungkapan, pengiriman, dan keamanan data privasi, serta secara umum pengaturan data privasi adalah untuk mencari keseimbangan antara kebutuhan terhadap perlindungan data pribadi individu dengan kebutuhan pemerintah dan pelaku bisnis untuk memperoleh dan memproses data privasi untuk keperluan yang wajar dan sah.[11]

Ketiadaan hukum yang melindungi data pribadi di Indonesia selama ini juga merupakan suatu kelemahan. Padahal, perkembangan pengaturan data privasi akan mendukung pembangunan masa depan Indonesia sebagai pusat data global.[12] Hingga akhirnya pada Oktober 2022, DPR menyepakati RUU Perlindungan Data Pribadi menjadi undang-undang, yang kemudian ditandatangani oleh Presiden menjadi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU PDP ini setidaknya mengatur mengenai bermacam jenis data pribadi, subjek data pribadi, pengendali dan prosesor data pribadi, sampai mengenai sanksi yang dapat dikenakan. Namun, masih terdapat banyak tantangan yang akan dihadapi dalam menjalankan undang-undang ini kedepannya, salah satunya yang menjadi persoalan adalah mengenai kelembagaannya. Dalam undang-undang ini disebutkan bahwa penyelenggara perlindungan data pribadi dilaksanakan oleh lembaga yang ditetapkan oleh dan bertanggungjawab kepada presiden, meskipun sampai saat ini belum ada pengaturan tentang kedudukan dan struktur kelembagaan serta otoritas yang diberikan kepada lembaga ini.

Diundangankannya RUU PDP menjadi angin segar dalam ketidakkaruannya proses perlindungan terhadap data pribadi di Indonesia. Namun, selain dengan adanya UU PDP yang beru diundangkan, perlu juga untuk melihat lebihb dalam beberapa pengaturan lain yang berkaitan dengan perlindungan data pribadi ini. Maka dalam artikel ini, difokuskan kepada pembahasan isu hukum yang dapat digambarkan dalam pertanyaan, bagaimana hukum positif Indonesia saat ini melindungi pengguna media digital terhadap penyalahgunaan data pribadi? Bagaimana penegakan hukum dan pertanggungjawaban pihak penyelenggara sistem data pribadi yang disalahgunakan?

Maka untuk menjawab itu semua, sangat penting untuk membahas dan mendalami UU PDP ini termasuk juga undang-undang lain yang berkaitan dengan perlindungan data pribadi di Indonesia, agar dapat ditemukan suatu kesimpulan yang komprehensif perihal perlindungan terhadap data pribadi masyarakat di dunia digital, serta dapat ditemui suatu konsep yang tepat dalam menyelesaikan setiap persoalan yang berkaitan dengan kejahatan penyalahgunaan data pribadi kedepannya.

KERANGKA TEORI

1. Teori Perlindungan Hukum

Negara Indonesia telah mendeklarasikan diri sebagai negara hukum, sebagaimana yang termaktub di dalam rumusan Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik

[11]Sinta Dewi Rosadi, Cyber Law, hlm. 15
[12]*Ibid*

Indonesia, yang menyatakan bahwa "Negara Indonesia adalah negara hukum". Negara hukum sebagaimana dipahami dengan r*echstaat* menurut Eropa Kontinental dan *rule of law* menurut Anglo Saxon, mempunyai beberapa ciri utama yang dikemukakan oleh Frederich Julius Stahl (ditinjau ulang oleh *International Commision of Jurist*), diantaranya:[13]

a) Perlindungan konstitusional, artinya selain menjamin hak-hak individu konstitusi harus pula menentukan cara prosedural untuk memperoleh perlindungan atas hak-hak yang dijamin;
b) Badan kehakiman yang bebas dan tidak memihak;
c) Pemilihan umum yang bebas;
d) Kebebasan menyatakan pendapat;
e) Kebebasan berserikat;
f) Pendidikan kewarganegaraan.

Dari uraian tersebut, secara implisit dapat disimpulkan bahwasanya perlindungan hukum adalah hal yang mutlak diperlukan dalam konsep negara hukum. Hal ini dikarenakan lahirnya konsep negara hukum memiliki tujuan utama dalam pengakuan dan perlindungan hak-hak asasi manusia. Dengan demikian, konsep negara hukum akan terlaksana secara utuh dan konsekuen apabila diikuti oleh upaya-upaya yang dilakukan negara dalam memberikan perlindungan kepada warga negaranya. Di dalam suatu negara akan terjadi hubungan timbal balik antara warga negaranya, kemudian hubungan ini yang akan melahirkan suatu hak dan kewajiban satu sama lain. Perlindungan hukum akan menjadi hak bagi warga negara, sedangkan disisi lain perlindungan hukum merupakan kewajiban bagi negara terhadap warga negaranya.

Satjipto Rahardjo menyatakan perlindungan hukum adalah upaya untuk mengorganisasikan berbagai kepentingan dalam masyarakat supaya tidak terjadi tubrukan antar-kepentingan dan dapat menikmati semua hak-hak yang diberikan oleh hukum.[14] Pengorganisasian dilakukan dengan cara membatasi suatu kepentingan tertentu dan memberikan kekuasaan pada yang lainnya secara terukur dan terstruktur.

Teori perlindungan hukum yang dikemukakan oleh Satjipto Rahardjo ini terinspirasi oleh pendapat Fitzgerald tentang tujuan hukum, yaitu untuk mengintegrasikan dan mengkoordinasikan berbagai kepentingan dalam masyarakat dengan cara mengatur perlindungan dan pembatasan terhadap berbagai kepentingan tersebut. Artinya, perlindungan hukum adalah hukum itu sendiri dalam mewujudkan kepastian, kemanfaatan, dan keadilan bagi masyarakat secara luas.

Prinsip perlindungan hukum terhadap tindakan pemerintah bertumpu dan bersumber dari konsep tentang pengakuan dan perlindungan terhadap hak-hak asasi manusia. Lahirnya konsep-konsep tentang pengakuan dan perlindungan terhadap hak-hak asasi manusia di arahkan kepada pembatasan dan peletakan kewajiban masyarakat dan pemerintah. Prinsip kedua yang mendasari perlindungan hukum terhadap tindakan pemerintah adalah prinsip negara hukum. Apabila dikaitkan dengan pengakuan dan perlindungan terhadap hak-hak asasi manusia, pengakuan dan perlindungan terhadap hak asasi manusia mendapat tempat utama yang dikaitkan dengan tujuan dari negara hukum.[15]

[13]Fakhurohman, *Memahami Keberadaan Mahkamah Konstitusi di Indonesia,* (Bandung: Citra Aditya Bakti, 2004) hlm.1
[14]Satjipto Rahardjo, 2000, *Ilmu Hukum*, PT Citra Aditya Bakti: Bandung, hlm, 53-54
[15]Philipus M Hadjon, 1987, *Perlindungan Bagi Rakyat Indonesia,* (Surabaya: PT Bina Ilmu, 1987) hlm. 30

2. Konsep Mengenai Data Pribadi

Data pribadi sering disamakan dengan istilah *personal data* (berkembang di Eropa) atau *personal information* (Amerika Serikat). Malaysia menggunakan Istilah *data peribadi*, Singapura menggunakan istilah *personal data*, sementara Philipina menggunakan istilah *Personal Information*, seperti halnya Jepang dan Korea Selatan. Berbagai istilah yang digunakan tersebut secara substansial bermakna sama. Sementara menurut Kamus Besar Bahasa Indonesia, Data pribadi berarti data yang berkenaan dengan ciri seseorang, misalnya nama, umur, jenis kelamin, pendidikan, pekerjaan, alamat, dan kedudukan dalam keluarga.[16]

Sedangkan negara-negara Uni Eropa dalam *EU General Personal Data Regulation (EU GDPR)* mendefinisikan personal data adalah berkaitan erat dengan berbagai informasi yang berkaitan dengan orang individu yang 'diidentifikasi' atau dapat diidentifikasi. Gagasan tentang 'data pribadi' memang sengaja didefinisikan secara luas, sehingga memungkinkan badan legislatif negara-negara Eropa dapat memasukkan semua data yang mungkin terkait dengan seorang individu.[17]

Pada akhirnya, seseorang dapat membatasi ruang lingkup informasi pribadi hanya untuk yang berhubungan dengan individu. Richard Murphy mendefinisikan ruang lingkup informasi pribadi sebagai terdiri dari setiap data tentang seorang individu yang dapat diidentifikasi oleh individu tersebut. Namun demikian, definisi Murphy terlalu luas karena ada sejumlah besar informasi yang dapat diidentifikasi kepada kita dan yang kita lakukan.[18] Perlindungan Data pribadi merupakan hak asasi manusia sebagai bagian dari *hak privacy* yang mendapatkan jaminan perlindungan baik instrument hukum internasional dan konstitusi negara.

Perlindungan akan hak privasi ini sejalan dengan konstitusi Indonesia yang tercantum pada Pasal 28G ayat (1) UUD NRI 1945 yang mengatakan 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."

Sementara itu dalam instrumen internasional lainnya, hak privasi juga diatur di dalam *Universal Declaration of Human Rights* (1948) Pasal 12 dan *International Covenant on Civil and Political Rights (ICCPR)* 1966 yaitu dalam Pasal 17.

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum. Penelitian ini akan menggunakan penelitian normatif-empiris. Penelitian normatif mengkaji hukum tertulis dari beragam perspektif, dan *library research* atau penelitian hukum kepustakaan untuk mendekati pokok masalah atau isu hukum berdasarkan berbagai kajian yang dapat ditelusuri,[19] karena penelitian ini mendiskripsikan mengenai eksistensi hukum pidana Indonesia saat ini terhadap kejahatan siber yang berkaitan dengan kejahatan penyalahgunaan data pribadi. Sedangkan penelitian empiris melihat gejala-gejala sosial yang berkaitan dengan hukum dalam praktek legislasi di Indonesia.

[16] Wahyudi Djafar dan M. Jodi Santoso, 2019, *Perlidnungan Data Pribadi Konsep, Instrumen, dan Prinsipnya,* Lembaga Studi dan Advokasi Masyarakat (ELSAM), hlm. 7

[17] Orla Lynskey, "*Deconstructing Data Protection: the 'Added-Value' of a Right to Data Protection in the EU Legal Order"*. International and Comparative Law Quarterly, (2014) 63 (3). pp. 569-597

[18] Wahyudi Djafar dan M. Jodi Santoso, *Perlidnungan Data Pribadi Konsep, Instrumen, dan Prinsipny,* hlm. 7

[19] Muladi, Kapita Selekta Sistem Peradilan Pidana, (Semarang: Badan Penerbit Undip, 2004), hlm 7.

Pendekatan empiris dilakukan untuk melihat dan mengkaji bagaimana ketentuan normatif diwujudkan dalam kenyataannya pada masyarakat.[20]

Maka dalam penelitian ini merupakan penelitian yang akan mengkaji kemampuan hukum positif di Indonesia dalam melindungi masyarakat dari kejahatan penyalahgunaan data pribadi, serta melihat penegakan hukum dan pertanggungjawaban pengendali dan prosesor data pribadi dalam kasus penyalahgunaan data pribadi di Indonesia.

PEMBAHASAN

Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi

Data pribadi adalah data yang berupa identitas, kode, simbol, huruf atau angka penanda personal seseorang yang bersifat pribadi dan rahasia.[21] Pengertian lain menyebutkan data pribadi merupakan data yang berkenaan dengan ciri seseorang, nama, umur, jenis kelamin, pendidikan, pekerjaan, alamat, dan kedudukan dalam keluarga.[22]

Perlindungan data atau informasi secara khusus dijelaskan oleh Alan Wastin yang mendefiniskan pertama kali data privasi atau "*information privacy"* sebagai hak individu, keluarga ataupun kelompok sejauh mana mereka dapat menentukan hal-hal yang dibatasi atas data privasinya. Kemudian dikembangkan oleh pakar hukum lainnya, salah satunya Arthur Miller yang menjelaskan data privasi sebagai kemampuan seseorang dapat mengontrol informasi yang berkaitan pada dirinya dapat diketahui. Begitu juga dalam hal perkembangan teknologi tentang informasi seseorang yang dapat diakses, diproses, dikumpulkan dan dimanupulasi secara umum. Pandangan Westen juga atas hak privasi tidaklah absolut, sebab memiliki konseksuensi sosial sebagai tanggungjawab yang perlu diperhatikan atas informasi privasi individu.[23]

Dalam sejarahnya, istilah privasi dan data pribadi sebenarnya bukanlah hal yang baru. Meskipun *International Covenant on Civil and Political Rights* (ICCPR) tidak secara tegas menyebutkan istilah dengan penggunaan kalimat data pribadi, akan tetapi secara substansial pelindungan atas data pribadi adalah bagian dari privasi atau kehidupan pribadi setiap orang. Pelindungan atas data pribadi tidak hanya diatur di konvensi regional Uni Eropa (*General Data Protection Regulation*/GDPR), melainkan juga regional lainnya seperti Afrika (*African Union Convention on Cyber Security and Personal Data Protection*) dan juga Asia. Di dalam *ASEAN Declaration of Human Rights* (2012) secara tegas dinyatakan bahwa data pribadi adalah bagian dari privasi meski tidak diuraikan lebih detail.[24]

Beberapa negara mengatur privasi dalam konstitusinya, seperti Afrika Selatan dan Hungaria termasuk hak khusus untuk mengakses dan mengontrol data privasi seseorang. Di banyak negara juga perjanjian internasional yang mengakui hak-hak privasi seperti Konvenan Internasional Tentang Hak Sipil Dan Politik atau Konvensi Eropa Tentang Hak Asasi Manusia

[20]Soerjono soekanto dan Sri Mamudji, Penelitian Hukum Normatif: Suatu Tinjauan Singkat, (Jakarta: PT Rajagrafindo Persada, 2001), hlm. 13

[21]Rosalinda Elsina Latumahina, "Aspek Hukum Perlindungan Data Pribadi di Dunia Maya", sebagaimana dikutip oleh Lia Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia; Studi Perbandingan Hukum Inggris Dan Malaysia", Kanun Jurnal Ilmu Hukum 2, (Agustus, 2018), hlm. 372

[22]https://kbbi.kemdikbud.go.id/

[23]Wahyudi Djafar, Bernhard Ruben Fritz, dan Blandina Lintang, "Perlindungan Data Pribadi; Usulan Pelembagaan Kebijakan dari Perspektif HAM", (Jakarta: ELSAM, 2016), hlm 5.

[24]Edmon Makarim, Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi, Kolom Hukumonline.com

diadopsi kedalam hukum nasionalnya, termasuk Indonesia, yaitu ratifikasi ICCPR ke dalam UU No. 12 Tahun 2009.[25]

Pada awal 1970-an negara-negara mulai mengadopsi undang-undang yang luas yang dimaksudkan untuk melindungi privasi individu. Diberbagai belahan dunia telah berkembang kecendrungan untuk mengadopsi undang-undang data privasi yang komprehensif yang mengatur baik sektor publik maupun sektor privat yang dipengaruhi oleh model pengaturan Uni Eropa.[26]

Konsep hak privasi dalam Pasal 12 Deklarasi Umum Hak Asasi Manusia berbunyi:

"Tidak seorangpun dapat diganggu dengan sewenang-wenang urusan pribadi, keluarga, rumah tangga atau hubungan suratmenyurat, juga tak diperkenankan pelanggaran atas kehormatan dan nama baiknya. Setiap orang berhak mendapatkan perlindungan hukum terhadap gangguan atau pelanggaran seperti itu"

Kemudian dipertegas dipertegas dengan adanya Pasal 17 ICCPR yang diuraikan ke dalam beberapa ayat:

1) *Tidak boleh seorangpun yang dapat secara sewewangwenang atau secara tidak sah mencampuri masalah-masalah pribadinya, kelaurganya, rumah atau hubungan surat-menyurat, atau secara tidak sah diserang kehormatan dan nama baiknya*
2) *Setiap orang berhak atas perlindungan hukum terhadap campur tangan atau serangan sepertu tersebut diatas.*

Tujuan adanya perlindungan hak privasi hanyalah untuk melindungi individu atas gangguan yang dianggap melanggar hukum dan tindakan lainnya yang sewenang-wenang terhadap informasi privasi, tetapi gambaran yang diberikan juga tidaklah cukup detail mengenai pengertian gangguan yang sewenang-wenang atau melawan hukum (*unlawfull interference)* terhadap privasi. Unsur-usnur yang dapat dilakukan tentunya telah ditetapkan oleh Undang-Undang sebagai gangguan yang telah memenuhi prasyarat yang ditentukan.[27]

Data pribadi sebagai bagian dari privasi individu meupakan hak asasi manusia yang fundamental. Sebelum disahkannya undang-undang tentang perlindungan data pribadi, Indonesia telah membuat beberapa peraturan perundang-undangan yang didalamnya mengatur mengenai privasi dalam berbagai bidang. Untuk dapat mengetahui bagaimana Indonesia mengatur mengenai perlindungan data pribadi ini, lebih lanjut akan dibahas dan dilihat pengaturan data pribadi di Indonesia, mulai dari yang terbaru yaitu disahkannya undang-undang tentang perlindungan data pribadi dan juga undang-undang lainnya sebelum undang-undang perlindungan data pribadi ini disahkan dan diundangkan.

1) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Kegiatan telekomunikasi erat kaitannya dengan proses transmisi, interkoneksi, perpindahan data dan informasi dengan cepat. Perpindahan data dan informasi ini dapat terjadi dengan sangat cepat, oleh karenanya, untuk menjaga lalu lintas informasi dari penyelenggara telekomunikasi, pada Pasal 18 ayat (1) dan (2) diatur mengenai kewajiban penyelenggara

[25] David Banisar and Simon Davis, 1999 sebagaimana dikutip Sinta Dewi Rosadi, Cyber Law, hlm. 3
[26] *Ibid*
[27] Wahyudi Djafar dan Asep Komarudin, Perlindungan Hak Atas Privasi Di Internet: Beberapa Penjelasan Kunci, (Jakarta: ELSAM, 2014), hlm. 6

telekomunikasi untuk mencatat atau merekam secara rinci pemakaian dari jasa telekomunikasi.[28] Pasal 18 ayat (1) dan (2) tersebut berbunyi:[29]

> *Pasal 18 ayat (1):*
> *Penyelenggara jasa telekomunikasi wajib mencatat/merekam secara rinci pemakaian jasa telekomunikasi yang digunakan oleh pengguna telekomunikasi.*
> *Pasal 18 ayat (2):*
> *Apabila pengguna memerlukan catatan/rekaman pemakaian jasa telekomunikasi sebagaimana dimaksud pada ayat (1), penyelenggara telekomunikasi wajib memberikannya.*

Selanjutnya dalam Pasal 40 juga diatur, bahwasanya penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dilarang dalam bentuk apapun. Ini memperlihatkan bahwa perlindungan pribadi dari pengguna jasa telekomunikasi atas data pribadi miliknya yang ditransmisikan melalui penyelenggaraan telekomunikasi. Prinsipnya informasi yang dimiliki seseorang adalah hal pribadi yang wajib dilindungi sehingga pada dasarnya penyadapan merupakan hal yang dilarang.[30]

Dalam Pasal 42 ayat (1) UU Telekomunikasi, mewajibkan penyelenggara jasa telekomunikasi untuk merahasiakan informasi. Pengecualian terhadap kerahasiaan itu antara lain untuk kepentingan proses peradilan pidana atas permintaan tertulis jaksa agung atau kepala kepolisian serta atas permintaan penyidik.[31] Pengaturan mengenai sanksi-sanksi pidana terkait dengan perlindungan data pribadi pengguna jasa telekomunikasi diatur dalam Pasal 56 dan Pasal 57 UU Telekomunikasi, dengan diancam berupa sanksi pidana, baik pidana denda dan pidana penjara.

2) Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

Undang-undang Perlindungan Konsumen pada prinsipnya menjamin data dan informasi mengenai barang dan jasa, bukan berupa informasi mengenai data pribadi konsumen.[32] Pasal 1 ayat (6) UU Perlindungan Konsumen mengatur mengenai promosi, dalam undang-undangnya dijelaskan mengenai pengertian promosi tersebut adalah kegiatan pengenalan atau penyebarluasan informasi suatu barang dan/atau untuk menarik minat beli konsumen terhadap barang dan atau jasa yang akan dan sedang diperdagangkan.[33] Permasalah terjadi saat kegitan promosi ini dilakukan oleh penyedia jasa untuk mempromosikan produknya menggunakan data pribadi orang lain tanpa persetujuan dari konsumen yang memiliki data.

UU perlindungan Konsumen tidak melarang promosi yang menggunakan data-data pribadi seseorang yang didapatkan tanpa persetujuannya. Dalam Pasal 9 hanya melarang menawarkan, memproduksikan, mengiklankan suatu barang dan/atau jasa secara tidak benar dan beberapa cara lain yang diatur dalam Pasal 9 UU Perlindungan Konsumen ini. Kemudian berdasarkan Pasal 9 ayat (3) mengatur pelaku usaha yang melakukan pelanggaran terhadap hal-

[28]Sinta Dewi Rosadi, Cyber Law…, hlm. 96
[29]*Undang-Undang Tentang Telekomunikasi*, UU Nomor 36 Tahun 1999, selanjutnya disebut UU Telekomunikasi, Pasal 18 ayat (1) dan (2).
[30] Penjelasan Pasal 40 *Undang-Undang Tentang Telekomunikasi*, UU Nomor 36 Tahun 1999, selanjutnya disebut UU Telekomunikasi.
[31]Pasal 42 ayat (2) dan Penjelasan Pasal 42 ayat (2) *Undang-Undang Tentang Telekomunikasi*, UU Nomor 36 Tahun 1999, selanjutnya disebut UU Telekomunikasi.
[32]Sinta Dewi Rosadi, Cyber Law…, hlm. 97
[33]*Undang-Undang Tentang Perlindungan Konsumen*, UU Nomor 8 Tahun 1999, selanjutnya disebut UU Perlindungan Konsumen, Pasal 1 ayat (6).

hal tersebut dilarang untuk melanjutkan penawaran, promosi, dan pengiklanan barang dan jasa tersebut.[34] Berdasarkan Pasal 62 diatur ketentuan pidana yang dapat dijatuhkan yaitu pidana penjara paling lama 5 Tahun atau denda paling banyak dua milyar rupiah.[35]

3) Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (UU HAM)

Undang-Undang tentang HAM dalam Pasal 29 disebutkan:

"Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak miliknya".

Kemudian dalam Pasal 14 ayat (2) UU HAM disebutkan bahwa setiap orang berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis sarana yang tersedia.[36] Selanjutnya Pasal 31 disebutkan kemerdekaan dan rahasia dalam hubungan surat-menyurat termasuk hubungan komunikasi melalui sarana elektronik tidak boleh diganggu, kecuali atas perintah hakim atau kekuasaan lain yang sah sesuai dengan ketentuan peraturan perundang-undangan.[37]

Sesuatu yang diatur dalam Pasal 14 dan Pasal 32 UU HAM ini menjelaskan bahwa adanya keseimbangan yang diatur dalam hal memperoleh hak yaitu mencari, memperoleh, memiliki, menyimpan dan menyampaikan informasi, dengan hak atas diakuinya kerahasiaan dalam komunikasi termasuk didalamnya mengenai data pribadi seseorang. Pasal 32 ini dapat dilihat bahwa ketentuannya merupakan jaminan dalam perlindungan terhadap informasi serta data pribadi seseorang.[38]

4) Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (UU KIP)

Informasi merupakan kebutuhan pokok setiap orang. Dalam Pasal 1 ayat (1) UU KIP disebutkan bahwa informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun nonelektronik.[39] Sedangkan informasi publik adalah informasi yang dihasilkan, disimpan, dikelola, dikirim, dan/atau diterima oleh suatu badan publik yang berkaitan dengan penyelenggara dan penyelenggaraan negara dan/atau penyelenggara dan penyelenggaraan badan publik lainnya yang sesuai dengan Undang-Undang ini serta informasi lain yang berkaitan dengan kepentingan publik.[40]

Dalam UU KIP ini disebutkan bahwa pengumpulan data informasi dilakukan oleh suatu badan publik. Perlindungan terhadap data dan informasi publik yang dihimpun oleh badan

[34]*Undang-Undang Tentang Perlindungan Konsumen*, UU Nomor 8 Tahun 1999, selanjutnya disebut UU Perlindungan Konsumen, Pasal 9 ayat (3).
[35]*Undang-Undang Tentang Perlindungan Konsumen*, UU Nomor 8 Tahun 1999, selanjutnya disebut UU Perlindungan Konsumen, Pasal 62.
[36] *Undang-Undang Tentang Hak Asasi Manusia*, UU Nomor 39 Tahun 1999, selanjutnya disebut UU HAM, Pasal 14 ayat (2).
[37]*Undang-Undang Tentang Hak Asasi Manusia*, UU Nomor 39 Tahun 1999, selanjutnya disebut UU HAM, Pasal 32.
[38]Sinta Dewi Rosadi, Cyber Law…, hlm. 100
[39]*Undang-Undang Tentang Keterbukaan Informasi Publik*, UU Nomor 14 Tahun 2008, selanjutnya disebut UU KIP, Pasal 1 ayat (1).
[40]*Undang-Undang Tentang Keterbukaan Informasi Publik*, UU Nomor 14 Tahun 2008, selanjutnya disebut UU KIP, Pasal 1 ayat (2).

publik tersebut diatur dalam Pasal 6 ayat (3), salah satu informasi yang tidak dapat di informasikan oleh badan publik merupakan informasi yang berkaitan dengan hak-hak pribadi.[41] Pelanggaran yang dilakukan oleh badan publik tersebut dapat dikenakan sanksi pidana sebagaimana yang diatur dalam Pasal 52 yaitu:[42]

> *"Badan Publik yang dengan sengaja tidak menyediakan, tidak memberikan, dan/atau tidak menerbitkan Informasi Publik berupa Informasi Publik secara berkala, Informasi Publik yang wajib diumumkan secara serta-merta, Informasi Publik yang wajib tersedia setiap saat, dan/atau Informasi Publik yang harus diberikan atas dasar permintaan sesuai dengan Undang-Undang ini, dan mengakibatkan kerugian bagi orang lain dikenakan pidana kurungan paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp5.000.000,00 (lima juta rupiah)".*

5) Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan (UU Perbankan)

Mekanisme perlindungan hukum terhadap nasabah dalam lembaga perbankan salah satu kegiatan perekonomian yang penting adalah kegiatan perbankan.[43] Di Indonesia pengaturan mengenai perbankan diatur dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Dalam UU Perbankan, perlindungan terhadap data pribadi nasabah diatur sebagai rahasia bank. Rahasia bank merupakan segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpanan dan simpanannya.[44] Kemudian dalam Pasal 40 disebutkan bahwa bank wajib merahasiakan keterangan mengenai Nasabah Penyimpan dan simpanannya, kecuali dalam hal tertentu yang diperbolehkan.[45]

Pasal 47 ayat (2) juga menyebutkan bahwa yang memegang teguh rahasia bank adalah anggota dewan komisaris, direksi, pegawai bank atau pihak terafiliasi lainnya, dan jika mereka sengaja memberikan keterangan yang wajib dirahasiakan menurut Pasal 40, diancam dengan pidana penjara sekurang-kurangnya 2 (dua) tahun serta denda sekurang-kurangnya Rp 4.000.000.000,00 (empat miliar rupiah) dan paling banyak Rp 8.000.000.000,00 (delapan miliar rupiah).[46]

6) Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan (UU Kesehatan)

Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan mengatur mengenai perlindungan terhadap riwayat kesehatan pasien dalam Pasal 57 ayat (1) yang menyatakan hak seseorang atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada

[41]*Undang-Undang Tentang Keterbukaan Informasi Publik*, UU Nomor 14 Tahun 2008, selanjutnya disebut UU KIP, Pasal 6 ayat (3).
[42]*Undang-Undang Tentang Keterbukaan Informasi Publik*, UU Nomor 14 Tahun 2008, selanjutnya disebut UU KIP, Pasal 52.
[43]Shidarta, Hukum Perlindungan Konsumen Indonesia, (Jakarta: Grasindo, 2006), hlm. 8
[44]*Undang-Undang Tentang Perbankan*, UU Nomor 10 Tahun 1998, selanjutnya disebut UU UU Perbankan, Pasal 1 ayat (28).
[45]*Undang-Undang Tentang Perbankan*, UU Nomor 10 Tahun 1998, selanjutnya disebut UU UU Perbankan, Pasal 40.
[46]*Undang-Undang Tentang Perbankan*, UU Nomor 10 Tahun 1998, selanjutnya disebut UU UU Perbankan, Pasal 47.

penyelenggara pelayanan kesehatan.[47] Sedangkan dalam ayat (2) diatur mengenai pengecualian atas rahasia kondisi kesehatan pribadi yang tidak berlaku dalam hal:[48]

a. *perintah undang-undang;*
b. *perintah pengadilan;*
c. *izin yang bersangkutan;*
d. *kepentingan masyarakat;*
e. *kepentingan orang tersebut.*

Meski ada pengakuan mengenai hak pasien untuk mendapatkan perlindungan atas data privasinya berupa riwayat kesehatan, akan tetapi perlindungan data pribadi pasien tidak secara penuh diatur dalam UU Kesehatan. Di dalam UU Kesehatan tidak ditemukan pengaturan mengenai sanksi bagi pelanggaran mengenai privasi seseorang baik secara administratif maupun sanksi pidana, baik itu atas akses yang tidak sah maupun penyalahgunaan dari data pribadi pasien oleh pihak yang tidak memiliki kewenangan.[49]

7) Undang-Undang Nomor 24 Tahun 2013 Perubahaan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (UU Adminduk)

Pasal 1 UU Adminduk menyebutkan bahwa data kependudukan merupakan data perseorangan dan/atau data agregat yang terstruktur sebagai hasil dari kegiatan Pendaftaran Penduduk dan Pencatatan Sipil.[50] Kemudian dijelaskan juga dalam Pasal 1 ayat (22) perihal data pribadi, bahwa data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.[51] Berkaca kepada ketentuan dalam beberapa angka di Pasal 1 ini dapat kita simpulkan bahwa UU Adminduk sebenarnya telah terdapat upaya dalam perlindungan data pribadi warga negara.

Kemudian dalam pasal 8 ayat (1) huruf (e) disebutkan juga bahwa instansi pelaksana melaksanakan urusan administrasi kependudukan mempunyai kewajiban untuk menjamin kerahasiaan dan keamanan data atas peristiwa kependudukan dan peristiwa penting.[52] kerahasiaan dan keamanan data peristiwa kependudukan dan peristiwa penting telah menjadi tanggungjawab dari ninstansi pelaksana administrasi kependudukan.

Data Penduduk yang dihasilkan oleh sistem informasi dan tersimpan di dalam database kependudukan dapat dimanfaatkan untuk berbagai kepentingan, seperti dalam menganalisa dan merumuskan kebijakan kependudukan, menganalisa dan merumuskan perencanaan pembangunan, pengkajian ilmu pengetahuan. Dengan demikian baik pemerintah maupun non pemerintah untuk kepentingannya dapat diberikan izin terbatas dalam arti terbatas waktu dan peruntukkannya.[53]

---

[47]*Undang-Undang Tentang Kesehatan*, UU Nomor 36 Tahun 2009, selanjutnya disebut UU UU Kesehatan, Pasal 57 ayat (1).
[48]*Undang-Undang Tentang Kesehatan*, UU Nomor 36 Tahun 2009, selanjutnya disebut UU UU Kesehatan, Pasal 57 ayat (2).
[49]Sinta Dewi Rosadi, Cyber Law…, hlm. 106
[50]*Undang-Undang Tentang Administrasi Kependudukan*, UU Nomor 24 Tahun 2013 Perubahan Atas UU Nomor 23 Tahun 2006, selanjutnya disebut UU UU Adminduk, Pasal 1 ayat (9).
[51]*Undang-Undang Tentang Administrasi Kependuduakn*, UU Nomor 24 Tahun 2013 Perubahan Atas UU Nomor 23 Tahun 2006, selanjutnya disebut UU UU Adminduk, Pasal 1 ayat (22).
[52]*Undang-Undang Tentang Administrasi Kependudukan*, UU Nomor 24 Tahun 2013 Perubahan Atas UU Nomor 23 Tahun 2006, selanjutnya disebut UU UU Adminduk, Pasal 8 ayat (1).
[53]Penjelasan Pasal 83 ayat (1) *Undang-Undang Tentang Administrasi Kependudukan*, UU Nomor 24 Tahun 2013 Perubahan Atas UU Nomor 23 Tahun 2006, selanjutnya disebut UU UU Adminduk,

Mengenai larangan terhadap akses yang ilegal dalam bentuk manipulasi data dan penyalahgunaan data pribadi atau dokumen kependudukan diatur dalam Pasal 77 dengan ancaman bagi pelanggarnya berupa ancaman pidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 50.000.000,00 (lima puluh juta rupiah).[54] Selanjutnya ancaman pidana juga terhadap orang yang mengakses database kependudukan, orang atau badan hukum yang tanpa hak mencetak, menerbitkan, dan mendistribusikan blanko dokumen kependudukan.

8) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

UU ITE mengatur mengenai data pribadi seperti yang tertuang dalam Pasal 26 ayat (1) yang menyatakan bahwa penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan.[55] Dalam penjelasan pasal tersebut juga dimuat makna data pribadi tersebut sebagai bagian dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*). Hak pribadi mengandung pengertian sebagai berikut:[56]

a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai.
c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

UU ITE juga mengatur tentang perbuatan yang dilarang berkaitan dengan bidang informasi elektronik yang tidak secara spesifik dalam data pribadi yaitu dalam Pasal 27 sampai dengan Pasal 37. Secara garis besar pasal-pasal tersebut melarang adanya perbuatan tanpa hak dan dengan sengaja menyalahgunakan informasi elektronik yang dapat merugikan orang lain terutama pemilik informasi.

Dapat dilihat pada Pasal 26 angka 1 UU ITE, yang menyebutkan bahwa penggunaan setiap informasi melaui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Selanjutnya disebutkan bahwa jika terjadi pelanggaran perihal data pribadi tersebut maka dapat ditembuh dengan gugatan ganti rugi. Disini UU ITE hanya menyediakan mekanisme penyelesaian dengan menggunakan gugatan perdata. Proses hukum dan mekanisme yang ditawarkan oleh UU ITE tidak dapat menjamin kepastian hukum terhadap data pribadi bagi setiap pengguna di ruang digital. Aturan yang ada dalam UU ITE membuat negara sebagai penjamin terlindunginya hak privasi seseorang hanya mampu bersifat pasif.

9) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)

[54]*Undang-Undang Tentang Administrasi Kependudukn,* UU Nomor 24 Tahun 2013 Perubahan Atas UU Nomor 23 Tahun 2006, selanjutnya disebut UU UU Aadminduk, Pasal 93.
[55]*Undang-Undang Tentang Informasi dan Transaksi Elektronik,* UU Nomor 19 Tahun 2016 Perubahan Atas UU Nomor 11 Tahun 2008, selanjutnya disebut UU ITE, Pasal 26 ayat (1).
[56]Penjelasan Pasal 26 ayat (1) *Undang-Undang Tentang Informasi dan Transaksi Elektronik,* UU Nomor 19 Tahun 2016 Perubahan Atas UU Nomor 11 Tahun 2008, selanjutnya disebut UU ITE

Disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mejadi suatu harapan perlindungan hukum dari banyaknya kasus kejahatan dari penyalahgunaan data pribadi di Indonesia yang berasal dari kebocoran-kebocoran data serta pencurian data pribadi. Hadirnya UU PDP memebri kewenangan kepada pemerintah dalam mengawasi tata kelola data pribadi yang dilakukan oleh penyelenggara sistem elektronik.

Dalam UU PDP dinyatakan mengenai data pribadi sebagai data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.[57] Sedangkan yang dimaksud dengan perlindungan data pribadi adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi.[58]

Agar perlindungan data pribadi dapat dilakukan dengan tepat memenuhi semua kriteria dalam pengaturannya, UU PDP membagi data pribadi kedalam dua jenis data, yaitu data pribadi yang bersifat spesifik dan data pribadi yang bersifat umum. Sebagaimana yang tercantu didalam Pasal 4 ayat (2), jenis data pribadi yang bersifat spesifik tersebut meliputi:[59]

1. *data dan informasi kesehatan;*
2. *data biometrik;*
3. *data genetika;*
4. *catatan kejahatan;*
5. *data anak;*
6. *data keuangan pribadi;*
7. *data lainnya sesuai dengan ketentuan peraturan perundang-undangan.*

Dalam data yang bersifat spesifik ini posisi catatan kejahatan termasuk dalam jenis data pribadi kategori spesifik, menurut hemat penulis pengaturan mengenai catatan kejahatan dalam kriteria data yang spesifik di mana catatan kejahatan seseorang mendapat perlakuan yang berbeda dibandingkan data bersifat umum, seperti pada Pasal 34 yang menyatakan bahwa pengendali data pribadi wajib melakukan penilaian dampak pelindungan data dalam hal pemrosesan data pribadi memiliki potensi risiko tinggi terhadap subjek data pribadi. Pemrosesan data pribadi memiliki potensi risiko tinggi sebagaimana dimaksud salah satunya adalah pemrosesan atas data pribadi yang bersifat spesifik. Hal dianggap semakin mempermudah posisi koruptor setelah menjalani masa tahanannya kembali lagi menjadi pejabat publik dan mencalon dalam proses pemilihan umum, karena masyarakat tidak dapat mengetahui rekam catatan kejahatannya.

Sedangkan data pribadi yang bersifat umum termuat dalam ayat (3) yang jenis-jenisnya meliputi:[60]

1. *Nama lengkap;*
2. *Jenis kelamin;*
3. *Kewarganegaraan*
4. *Agama;*

[57]*Undang-Undang Tentang Perlindungan Data Pribadi*, UU Nomor 27 Tahun 2022, selanjutnya disebut UU UU PDP, Pasal 1 ayat (1).
[58]*Undang-Undang Tentang Perlindungan Data Pribadi*, UU Nomor 27 Tahun 2022, selanjutnya disebut UU UU PDP, Pasal 1 ayat (2).
[59]*Undang-Undang Tentang Perlindungan Data Pribadi*, UU Nomor 27 Tahun 2022, selanjutnya disebut UU UU PDP, Pasal 4 ayat (2).
[60]*Undang-Undang Tentang Perlindungan Data Pribadi*, UU Nomor 27 Tahun 2022, selanjutnya disebut UU UU PDP, Pasal 4 ayat (3).

5. *Status perkawinan;*
6. *Data pribadi yang dikombinasikan mengidentifikasi seseorang.*

Selama ini pengaturan mengenai perlindungan data pribadi masih bersifat sektoral, yang diatur dalam berbagai bidang yang terkait denga penyelenggaraan sistem elektronik. Namun, dalam UU PDP ini mulai diidentifikasi terhadap pihak-pihak yang terlibat dalam pemrosesan data pribadi yaitu pengendali data pribadi dan prosesor data pribadi. Pengendali data pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan data pribadi. Sedangkan prosesor data pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam melakukan pemrosesan data pribadi atas nama pengendali data pribadi.

Sebagai bagian dan upaya dalam perlindungan data pribadi, UU PDP mengatur setiap hal yang wajib dipenuhi oleh pengendali dat pribadi tersebut. Diantaranya seperti yang diatur dalam Pasal 20, bahwa pengendali data pribadi wajib memiliki dasar pemrosesan data pribadi. Pengendali juga wajib melakukan pemrosesan data pribadi secara terbatas dan spesifik, sah secara hukum, dan transparan seperti yang diatur dalam Pasal 27. Pasal 36 menagtur tentang kewajiban menjaga kerahasiaan dan Pasal 37 melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan data pribadi di bawah kendali pengendali data pribadi.

Pengendali data pribadi juga wajib untuk mencegah data pribadi diakses secara tidak sah. Kemudian bertanggung jawab atas pemrosesan data pribadi dan menunjukkan pertanggungjawaban dalam pemenuhan kewajiban pelaksanaan prinsip pelindungan data pribadi. Kewajiban-kewajiban tersebut tersebar dalam beberapa pasal dalam uu pdp. sedangkan untuk prosesor data pribadi, pemrosesan data pribadi yang dilakukan olehnya melakukan dilakukan atas nama dan berdasarkan perintah pengendali data pribadi. sehingga, kewajiban perlindungan data pribadi yang berlaku kepada pengendali data pribadi juga berlaku kepada prosesor data pribadi.

Berbagai larangan dan ancaman sanksi juga diatur dalam UU PDP, larangan dan sanksi tersebut diantaranya:

1. Larangan untuk memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi dengan sanksi yang dapat diberikan berupa dipidana dengan pidana penjara paling lama lima tahun dan/atau pidana denda paling banyak Rp5 miliar.[61]
2. Larangan untuk mengungkapkan data pribadi yang bukan miliknya, dengan ancaman bagi yang pelanggarnya dikenai pidana penjara paling lama empat tahun dan/atau pidana denda paling banyak Rp4 miliar.[62]
3. Larangan untuk menggunakan data pribadi yang bukan miliknya, dengan ancaman pidana penjara paling lama lima tahun dan/atau pidana denda paling banyak Rp5 miliar.[63]
4. Larangan untuk membuat data pribadi palsu atau memalsukan data pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan

[61]*Undang-Undang Tentang Perlindungan Data Pribadi*, UU Nomor 27 Tahun 2022, selanjutnya disebut UU UU PDP, Pasal 67 ayat (1).
[62]*Undang-Undang Tentang Perlindungan Data Pribadi*, UU Nomor 27 Tahun 2022, selanjutnya disebut UU UU PDP, Pasal 67 ayat (2).
[63]*Undang-Undang Tentang Perlindungan Data Pribadi*, UU Nomor 27 Tahun 2022, selanjutnya disebut UU UU PDP, Pasal 67 ayat (3).

kerugian bagi orang lain, bagi pelanggran terhadap ketentuan ini dikenai pidana penjara paling lama enam tahun dan/atau pidana denda paling banyak Rp6 miliar rupiah.[64]

Dalam rangka mengoptimalkan upaya perlindungan data pribadi, UU PDP mengamanatkan bahwa melahirkan suatu lembaga yang berperan sebagai ujung tombak pelaksanaan pelindungan data pribadi di Indonesia. Lembaga tersebut ditetapkan dan bertanggungjawab secara langsung kepada presiden.[65] Lembaga ini memiliki tugas antara lain untuk:

1. Perumusan dan penetapan kebijakan dan strategi pelindungan data pribadi yang menjadi panduan bagi subjek data pribadi, pengendali data pribadi, dan prosesor data pribadi;
2. Pengawasan terhadap penyelenggaraan pelindungan data pribadi;
3. Penegakan hukum administratif terhadap pelanggaran undang-undang ini;
4. Fasilitasi penyelesaian sengketa di luar pengadilan.

Pada prinsipnya, UU PDP mencoba untuk memberikan harapan baru bagi keamanan data pribadi di Indonesia. UU PDP memiliki posisi yang lebih kuat jika dibandingkan dengan peraturan-peraturan yang ada selama ini yang mengatur perlindungan data pribadi yang masih bersifat sektoral dan peraturan yang memiliki tingkat di bawah undang-undang. UU PDP juga memberikan dasar hukum untuk perlindungan data pribadi yang lebih luas.

Proses Penegakan Hukum dan Pertanggungjawaban Hukum Pengendali dan Prosesor Data Pribadi Dalam Hal Terjadi Penyalahgunaan Data Pribadi

Kasus kejahatan yang berkaitan dengan data pribadi merupakan realita yang sudah sering terjadi di Indonesia. Berdasarkan laporan data trafik BSSN 2021, sepanjang tahun 2020, Indonesia mengalami serangan terhadap siber sampai pada angka 495,3 juta dan meningkat 41 persen dari tahun sebelumnya yang hanya sebesar 290,3 juta. Dalam periode tersebut, sektor pemerintah merupakan sektor tertinggi yang mengalami kebocoran data akibat pencuri informasi yakni dengan sebaran 45,5%, yang kemudian disusul oleh sektor keuangan (21,8%), telekomunikasi (10,4%), penegakan hukum (10,1%), transportasi (10,1%), dan BUMN lainnya (2,1%).[66]

Sedangkan pada Tahun 2022 Menurut data BSSN, total 714.170.967 anomali trafik atau serangan siber yang terjadi di sepanjang 2022, dengan angka serangan paling tinggi terjadi pada Januari dengan angka serangan 272.962.734.[67] Lebih lanjut lagi, berdasarkan laporan konten kasus kejahatan siber di Indonesia pada periode Januari hingga September 2021, laporan paling banyak merupakan tentang kejahatan penipuan di dunia siber yaitu sebanayak 4.601 kasus. Selain itu masyarakat juga melaporkan pengancaman dan penghinaan serta tindak

[64]*Undang-Undang Tentang Perlindungan Data Pribadi*, UU Nomor 27 Tahun 2022, selanjutnya disebut UU UU PDP, Pasal 68.

[65]*Undang-Undang Tentang Perlindungan Data Pribadi*, UU Nomor 27 Tahun 2022, selanjutnya disebut UU UU PDP, Pasal 58.

[66]Pusat Kajian Anggaran Badan Keahlian DPR RI, Tantangan Penguatan Keamanan Siber dalam Menjaga Stabilitas Keamanan, (Jakarta: Pusat Kajian Anggaran DPR RI, 2021) hlm. 4

[67]RI Dihantam 700 Juta Serangan Siber di 2022, Modus Pemerasan Dominan, diakses dalam https://www.cnnindonesia.com/teknologi/20220701164212-192-816150/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan

pemerasan. Bahkan total kerugian yang ditimbulkan berdasarkan laporan kejatan tersebut mencapai 3,88 triliun.[68]

Pencurian data pribadi seringkali diperjualbelikan dengan tujuan untuk melakukan pinjaman secara *online*, maraknya kasus ini terjadi dikarenakan, *pertama*, mudahnya pendaftaran dan pengajuan peminjaman dana, yang hanya membutuhkan e-KTP, rekening bank, dan nomor telepon. *Kedua*, data-data pribadi masyarakat Indonesia sangat mudah tersebar, diakses, hingga dipalsukan. Contohnya, e-KTP bisa saja tersebar saat kita melakukan fotokopi atau registrasi. Bahkan ada masyarakat yang secara terang-terangan mengunggah e-KTP miliknya di media sosial. Padahal hal ini sangat berbahaya karena berpotensi disalahgunakan untuk pinjaman online.

Beberapa contoh kasus yang berkaitan dengan data pribadi di Indonesia berupa kebocoran data dan jual beli data, diantaranya adalah:

a. Kasus Kebocoran Data Nasabah BRI Life

Tahun 2021 dua juta dari nasabah BRI Life mengalami kebocoran dan dijual secara *online*. Informasi bocornya data nasabah BRI Life diunggah sebuah akun *Twitter* pada Selasa, 27 Juli 2021. Dalam unggahannya, tertulis bahwa pelaku mengancam menjual data sensitif milik BRI Life. Peretas disinyalir mencuri 250 *gigabyte* data nasabah perusahaan asuransi tersebut dan dijual seharga US$ 7.000 atau Rp 101,5 juta.[69] Data-data tersebut berisi sejumlah informasi seperti foto KTP, rekening, nomor wajib pajak, akte kelahiran, hingga drekam medis.[70]

b. Kasus Kebocoran Data Pengguna Tokopedia

Tahun 2020, sebanyak 91 Juta data pengguna dan 7 juta data *merchan* aplikasi Tokopedia bocor dan dikabarkan dijual di situs gelap atau *dark web*.[71] Berdasarkan kasus ini, pihak Tokopedia bahkan mengkonfirmasi bahwa kebocoran data pengguna ini memang terjadi dan mengklaim dilakukan oleh pihak ketiga.[72] Pengelola dalam hal ini pihak Tokopedia mengkonfirmasi bahwa kejadian pencurian data pengguna ini sudah dilakukan investigasi dan bekerjasama dengam pemerintah dalam hal ini Badan Siber dan Sandi Negara (BSSN) dan Kementerian Komunikasi dan Informatika.[73]

c. Kasus Kebocoran Data BPJS Kesehatan

Tahun 2021 juga terjadi kebocoran data warga Indonesia yang merupakan data dari BPJS Kesehatan. Data-data tersebut memuat diantaranya 20 Juta foto pribadi, kemuadian data tersebut juga berisi Nomor Induk Kependudukan (NIK), nomer telepon, e-mail, alamat dan

---

[68]Kerugian Akibat Kejahatan Siber Capai Rp 3,88 Triliun, Apa Saja Bentuknya?, databoks.katadata.co.id

[69]Kebocoran Data Nasabah BRI Life Bukti Lemahnya Proteksi dan Regulasi, Focus.tempo.co, diakses dalam https://fokus.tempo.co/read/1488710/kebocoran-data-nasabah-bri-life-bukti-lemahnya-proteksi-dan-regulasi#:~:text=Data%20dua%20juta%20nasabah%20BRI,data%20sensitif%20milik%20BRI%20Life.

[70] Data Nasabah Asuransi BRI Life Diduga Bocor dan Dijual Online, Kompas.com, diakses dalam https://tekno.kompas.com/read/2021/07/27/19234397/data-nasabah-asuransi-bri-life-diduga-bocor-dan-dijual-online?page=all

[71]Data 91 Juta Pengguna Tokopedia dan 7 Juta Merchant Dilaporkan Dijual di *Dark Web*, Kompas.com diakses dalam https://tekno.kompas.com/read/2020/05/03/10203107/data-91-juta-pengguna-tokopedia-dan-7-juta-merchant-dilaporkan-dijual-di-dark?page=all

[72]Surati Pengguna, CEO Tokopedia Akui Pihak Ketiga Mencuri Data, Katadata.co.id, diakses dalam https://katadata.co.id/desysetyowati/digital/5eba4c2354ace/surati-pengguna-ceo-tokopedia-akui-pihak-ketiga-mencuri-data

[73]*Ibid*

gaji. Bahkan data tersebut juga termasuk data penduduk yang sudah meninggal.[74] Data-data pribadi tersebut dijual dengan harga 0,15 bitcoin yang jika dikonversi ke nilai rupiah saat itu, yaitu senilai Rp 81,6 juta.

d. Kasus Kebocoran Data Bank Indonesia

Bank Indonesia mengalami kebocoran data pada 16 komputer di Kantor Cabang Bank Indonesia Bengkulu dan 20 kota lainnya dan hal ini dikonformasi kebenarannya oleh Badan Siber dan Sandi Negara (BSSN). Kebocoran data tersebut sebanyak 52 Ribu dokumen yang berasal dari 200 komputer bank Indonesia.[75]

e. Kasus Kebocoran Data PLN

Pada Agustus 2022 terjadi kebocoran data 17 Juta pelanggan PLN dan data tersebut diperjualbelikan di sebuah situs online. Data-data tersebut terdiri atas informasi pribadi milik pelanggan PLN, seperti ID pelanggan, nama konsumen, alamat, informasi tagihan listrik dan tipe energi yang digunakan.[76]

Beberapa contoh kasus diatas merupakan sebagian dari jumlah kasus kebocoran data pribadi di Indonesia, beberapa data yang mengalami kebocoran dan diperjualbelikan secara ilegal tersebut berasal dari data-data pemerintahan, BUMN, dan perusahaan-perusahaan swasta. Kasus tersebut memperlihatkan bukti rentannya Indonesia perihal keamanan data pribadi.

Data dari *Surfshark*, sebuah perusahaan keamanan siber, menempatkan Indonesia sebagai urutan ketiga negara dengan jumlah kasus kebocoran data terbanyak di dunia. Data *Surfshark* tersebut mencatat 12,74 juta akun yang mengalami kebocoran data di Indonesia selama kuartal 3 di Tahun 2022.[77] Kebocoran data paling banyak terjadi di Rusia kemudian diikuti oleh Prancis.[78]

Sebelum disahkan dan diundangkannya UU PDP, penegak hukum belum mampu secara optimal dalam hal menangani persoalan kejahatan penyalahgunaan data pribadi, hal ini terbukti dari banyaknya kasus-kasus penyalahgunaan data pribadi yang terjadi di Indonesia belum ada yang mampu menjerat pelaku secara spesifik dikaitkan dengan kejahatan penyalahgunaan data pribadi. Selama ini penegak hukum menggunakan instrumen dalam undang-undang yang tersebar secara sektoral dengan spesifikasinya masing-masing. Seperti penyalahgunaan data untuk pinjaman online dan korban mendapat ancaman pemerasan, maka penegak hukum akan bertindak terhadap tindak pidana pemerasan dan pengancaman sebagaimana Pasal 368 KUHP.

---

[74]Kronologi Kasus Kebocoran Data WNI, Dijual 0,15 Bitcoin hingga Pemanggilan Direksi BPJS, Kompas.com diakses dalam https://tekno.kompas.com/read/2021/05/22/09450057/kronologi-kasus-kebocoran-data-wni-dijual-0-15-bitcoin-hingga-pemanggilan

[75]Kasus Dugaan Kebocoran Data Pribadi Sepanjang 2022, Tempo.co diakses dalam https://nasional.tempo.co/read/1632043/inilah-7-kasus-dugaan-kebocoran-data-pribadi-sepanjang-2022

[76]Kasus Kebocoran Data di Indonesia dalam Sebulan, dari PLN, IndiHome, hingga Nomor SIM Card, Kompas.com diakses dalam https://tekno.kompas.com/read/2022/09/02/10260777/3-kasus-kebocoran-data-di-indonesia-dalam-sebulan-dari-pln-indihome-hingga?page=all#:~:text=Dugaan%20kebocoran%20data%20pelanggan%20PLN&text=Kasus%20ini%20mencuat%20pada%2019%20Agustus%202022.&text=Data%20yang%20diperjualbelikan%20terdiri%20atas,hingga%20tipe%20energi%20yang%20digunakan.

[77]Indonesia Masuk 3 Besar Negara dengan Kasus Kebocoran Data Terbanyak Dunia, Katadata.co.id diakses dalam https://databoks.katadata.co.id/datapublish/2022/09/13/indonesia-masuk-3-besar-negara-dengan-kasus-kebocoran-data-terbanyak-dunia#:~:text=Menurut%20data%20perusahaan%20keamanan%20siber,tercatat%20hingga%2013%20September%202022.

[78]*Ibid*

Hal ini juga dapat dilihat dari penanganan aparat penegak hukum pada kasus yang terjadi terhadap ratusan mahasiswa Institut Pertanian Bogor yang mengalami kasus penipuan dengan dalih atau modus pinjaman online.[79] Aparat penegak hukum dalam hal ini kepolisian menjerat pelaku dengan Pasal 372 KUHP tentang penggelapan dan Pasal 378 KUHP perihal perbuatan curang.

Belum optimalnya penegakan hukum oleh aparat penegak hukum terhadap kejatan penyalahgunaan data pribadi selama ini karena memang belum ada payung hukum yang kuat untuk menyelesaikannya. Lahirnya UU PDP saat ini yang sudag mengatur berbagai bentuk larangan dan sanksi terhadap kejahatan yang berkaitan dengan data pribadi dapat menjadi landasan yang kuat untuk aparat penegak hukum kedepannya untuk menindak dan melakukan penegakan hukum secara maksimal.

UU PDP telah mengatur mengenai penyelesaian sengketaserta hukum acara yang digunakan oleh penegak hukum dalam menyelesaikan kasus kejahatan yang berkaitan dengan data pribadi ini. Didalam Pasal 64 ayat (1) disebutkan bahwa penyelesaian sengketa data pribadi dilakukan melalui arbitrase, pengadilan, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan peraturan perundang-undangan. Selanjutnya pada ayat 2 disebutkan bahwa hukum acara yang berlaku dalam penyelesaian sengketa dan proses peradilan pelindungan data pribadi sebagaimana dilaksanakan berdasarkan hukum acara yang berlaku dalam hal ini tetap merujuk kepada KUHAP.

UU PDP juga menyatakan alat bukti yang sah dalam UU PDP ini meliputi:

1. Alat bukti sebagaimana dimaksud dalam hukum acara
2. Alat bukti lain berupa informasi elelrtronik dan/ atau dokumen elektronik sesuai dengan ketentuan peraturan perundang-undangan.

Kemudian dalam hal diperlukan untuk melindungi data pribadi, proses persidangan dalam rangka penegakan hukum kasus yang berkaitan dengan data pribadi dapat dilakukan secara tertutup.

Pada prinsipnya upaya penegak hukum dalam menjalankan tugasnya yakni melakukan pencegahan dan penanggulangan tindak pidana merupakan sub sistem yang tidak dapat berdiri sendiri akan tetapi dalam upaya penegakan hukum, para penegak hukum harus dapat memiliki spirit dalam mencegah dan menanggulangi terjadinya tindak pidana yang diakibatkan dalam penyalahgunaan data pribadi. Peran penegak hukum selain berperan aktif dalam menerapkan hukuman juga wajib mengetahui faktor-faktor penyebabnya serta alternatif pencegahannya. Oleh karena itu, sekiranya sangat penting untuk mengetahui adanya kelemahan-kelemahan keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggungjawab.

Disahkan dan diundangkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) diharapkan mampu menjadi awal yang baik dalam menyelesaikan permasalahan kebocoran data pribadi di Indonesia, serta menjadi payung hukum yang optimal dalam melakukan penindakan dan penegakan hukum terhadap segala bentuk penyalahgunaan data pribadi. Kehadiran UU PDP menjadikan perlindungan terhadap data pribadi dan pengelolaannya diatur dalam suatu ketentuan yang khusus.

[79]Kronologi Ratusan Mahasiswa IPB Terlibat Pinjol, Berawal dari Tawaran Bisnis Online, Dijanjikan Keuntungan 10 Persen, Kompas.com diakses dalam https://regional.kompas.com/read/2022/11/16/081100378/kronologi-ratusan-mahasiswa-ipb-terlibat-pinjol-berawal-dari-tawaran-bisnis?page=all

Berdasarkan undang-undang yang ada, penyelenggara sistem elektronik dapat dimintai pertanggungjawaban secara hukum atas segala tindakan yang tidak sesuai dengan aturan hukum yang berlaku. Atas ketidakpatuhan terhadap aturan tersebut, penyelenggara dapat dimintai pertanggungjawaban baik itu pertanggungjawaban administratif, pertanggungjawaban perdata dan pertanggungjawaban pidana.

1) Pertanggungjawaban Administratif

Berdasarkan peraturan perundnag-undangan yang telah ada sebelumnya, setidaknya ada kewajiban administratif dari kementerian atau lembaga yang memiliki kewenangan yang terkait pelindungan data pribadi yaitu antara lain Kementerian Kominfo terkait penyelenggara sistem elektronik, Kementerian Perdagangan serta Badan Pelindungan Konsumen Nasional dalam hal perlindungan konsumen, karena tentunya pemilik data pribadi adalah pengguna sistem sebagai konsumen. Lembaga-lembaga tersebut mempunyai kewenangan, tugas pokok dan fungsi sesuai sektornya masing-masing untuk melakukan pembinaan, pengawasan, pencegahan dan penindakan.

Sebelum hadirnya UU PDP, korporasi seharusnya dapat diberikan sanksi administratif oleh Kominfo sesuai dengan PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Kominfo juga dapat melakukan *blocking* terhadap sistem korporasi tersebut guna mencegah terjadinya hal yang serupa kepada pengguna yang lain. Kondisi pemulihan ataynormalisasi untuk keluar dari daftar hitam, selayaknya hanya dapat diperkenankan jika semua permasalahan kebocoran data telah jelas fakta sesungguhnya berikut penyelesaian atau penanganan insidennya, serta telah memulihkan kembali hak-hak dari pengguna/konsumen yang dirugikan.[80]

Sedangkan dalam UU PDP saat ini, sudah diatur dengan jelas mengenai sanksi administratif tersebut didalam bab 8. Pengendali dan prosesor data pribadi dapat dikenakan sanksi administratif terhadap pelanggaran ketentuan beberapa pasal dalam UU PDP. Dalam Pasal 57 ayat (2) disebutkan bahwa sanksi administratif tersebut dapat diberikan oleh lembaga yang berwenang dalam penyelenggaraan perlindungan data pribadi yang telah diamanatkan oleh UU PDP, sanksi-sanksi administratif tersebut dapat berupa:

1. *Peringatan tertulis;*
2. *Penghentian sementara kegiatan pemrosesan Data Pribadi;*
3. *Penghapusan atau pemusnahan Data Pribadi;*
4. *Denda administratif.*

2) Pertanggungjawaban Perdata

Mengenai pertanggungjawaban perdata, UU PDP tidak secara spesifik mengatur hal tersebut, perihal gugatan UU PDP dalam Pasal 12 memberikan legitimasi kepada subjek data pribadi untuk dapat dan berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan. UU PDP tidak mengatur bagaimana proses gugatan ini dapat dilakukan, namun memberi delegasi kepada peraturan pemerintah untuk mengaturnya.

[80]Edmon Makarim, Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi, Hukumonline.com diakses dalam https://www.hukumonline.com/berita/a/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-lt5f067836b37ef?page=2

Dalam Pasal 26 UU ITE sebelumnya juga telah mengatur dan memberi jaminan untuk bisa dilakukannya gugatan secara keperdataan oleh orang yang dilanggar haknya dalam hal penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang dilakukan tanpa adanya persetujuan orang yang bersangkutan. Setidaknya terhadap pelanggaran terhadap perlindungan data pribadi dapat digugat sebagai perbuatan melawan hukum atas dasar kesalahan berdasarkan ketentuan undang-undang dalam hal ini Pasal 1365 KUHPerdata, maupun atas dasar ketidakpatutan atau ketidakhati-hatian sebagaimana Pasal1366 KUHPerdata. Pasal 3 UU ITE telah menyatakan adanya prinsip kehati-hatian dan juga memberikan tanggung jawab kepada setiap penyelenggara sistem elektronik baik korporasi maupun pemerintah untuk menerapkan akuntabilitas sistem elektronik, yakni harus andal, aman dan bertanggung jawab.[81]

Di dalam Pasal 15 UU ITE terdapat prinsip *presumed-liability*, artinya setiap penyelenggara sistem elektronik senantiasa bertanggung jawab secara hukum, kecuali pada saat kesalahan bukan terjadi karena mereka melainkan karena kesalahan konsumen atau pengguna sistem elektronik atau karena kejadian alam (*force majeure*). Beban pembuktian tentunya diemban oleh penyelenggara tersebut, sekiranya ternyata penyelenggara tidak berbicara yang sebenarnya terhadap insiden kebocoran data pribadi, maka justru akan berpotensi timbul masalah berikutnya yaitu kebohongan publik dan melanggar hak atas kejelasan informasi kepada pengguna/konsumen selaku pemilik data pribadi yang bersangkutan.[82] Berdasarkan ketentuan tersebut, maka setiap pengguna sistem elektronik dapat menggugat ganti kerugian kepada korporasi dan/atau instansi pemerintah sebagai pengendai dan prosesor data pribadi yang membocorkan data tersebut. Hanya saja untuk membuktikan kerugian immaterial relatif bukanlah sesuatu yang mudah didalam peradilannya.

3) Pertanggungjawaban Pidana

Kebocoran data bisa saja terjadi karena kegiatan intrusi dari luar (*illegal access*) ke dalam sistem atau di luar sistem (*interception* ataupun *man in the middle attack*). Kebocoran mungkin juga terjadi dari tindakan pembocoran dari pihak orang dalam yang mengirimkan data tersebut ke luar sistem yang seharusnya menjaga kerahasiaan data penggunanya. Sebagai pengendali dan proseor data, maka korporasi harus bertanggung jawab atas sistem keamanan baik secara fisik maupun logis.

Kehadiran UU PDP setidaknya juga mempertegas payung hukum dalam penegakan hukum pidana pada penyalahgunaan data pribadi. UU PDP dalam ketentuan pidananya, mengatur mengenai sanksi pidana bagi setiap orang yang melanggar ketentuan UU PDP, begitu juga sanksi bagi korporasi yang menjadi pengendali dan prosesor data pribadi. Sanksi pidana yang dapat dikenakan tersebut dapat berupa pidana penjara, pidana denda serta juga dapat dijatuhi pidana tambahan berupa perampasan keuntungan dan/ atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian.

Terkhusus jika tindak pidana dilakukan oleh korporasi, maka pidana dapat dljatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/ atau korporasi

[81] Edmon Makarim, Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi…
[82] *Ibid*

tersebut.[83] Pidana yang dapat dijatuhkan terhadap korporasinya hanyalah pidana denda. Namun, Korporasi juga dapat dijatuhi pidana tambahan seperti pembubaran korporasi.

Berdasarkan pengaturan sanksi yang ada dalam UU PDP, dapat dilihat bahwa negara memiliki landasan hukum untuk memaksa kepada penyelenggara sistem elektronik baik itu pengendali data dan prosesor data agar mampu mengamankan data dan sistem yang mereka kelola secara optimal. Hal ini dikarenakan selama ini data pribadi masyarakat tidak terjamin karena adanya potensi kebocoran data dan penyalahgunaannya untuk melakukan suatu kejahatan.

KESIMPULAN

Kajian dalam artikel ini menyimpulkan dua hal. *Pertama*, kejahatan penyalahgunaan data pribadi sebagai kejahatan siber telah mulai dan berkembang sejalan dengan berkembangnya dunia digital teknologi dan informasi. Hukum positif di Indonesia selama ini yang berkaitan dengan upaya perlindungan terhadap kejahatan penyalahgunaan data pribadi masih tersebar dengan karakteristik sektoral. Hingga akhirnya Oktober 2022 ini disahkan dan diundangkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai suatu undang-undang khusus yang mengatur persoalan data pribadi di Indonesia. Sebelum adanya UU PDP ini, pengaturan hukum di Indonesia belum ada yang secara spesifik mengatur persoalan perlindungan hukum mengenai kejahatan penyalahgunaan data pribadi tersebut. Sehingga korban-korban kejahatan seringkali tidak dapat keadilan dan tidak ada kepastian hukum. Terlebih produk hukum yang ada sangat minim pengaturannya dalam melindungi data pribadi seseorang, seperti minimnya jalur hukum yang dapat ditempuh oleh korban kejahatan tersebut. Hingga hadirnya UU PDP ini diharapkan menjadi angin segar bagi perlindungan data pribadi di Indonesia, dengan kompleksitas substansi yang sudah diatur didalamnya, diharapkan dapat menjadi acuan dalam proses pencegahan dan penegakan hukum kejahatan penyalahgunaan data pribadi.

Kedua, proses penegakan hukum dan pertanggungjawaban hukum terhadap pengendali dan prosesor data pribadi selama ini jika terjadi kejahatan penyalahgunaan data pribadi masih sangat jauh dari yang seharusnya. Hal ini disebabkan karena selama ini belum adanya pengaturan yang spesifik mengatur kejahatan ini sebelum lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lahirnya UU PDP telah mengatur berbagai kewajiban pengendali dan prosesor data pribadi, serta larangan dan sanksi jika tidak patuh terhadap aturan tersebut. UU PDP mengamanatkan lahirnya suatu lembaga yang fokus dalam penyelenggaraan sistem data pribadi ini dengan kewenangan penetapan kebijakan, pengawasan dan perlindungan, serta penegakan hukum administratif. Hal ini juga dapat membantu aparat penegak hukum dimasa mendatang dalam melaksanakan penegakan hukum lainnya, di mana UU PDP dan undang-undang sebelumnya yang mengatur perlindungan data pribadi, setidaknya mengatur pertanggungjawaban hukum yang dapat dimintai kepada pengendali dan prosesor tersebut berupa pertanggungjawaban administratif, perdata dan pidana.

[83] *Undang-Undang Tentang Perlindungan Data Pribadi*, UU Nomor 27 Tahun 2022, selanjutnya disebut UU UU PDP, Pasal 70.

DAFTAR PUSTAKA

Afitrahim, "Yurisdiksi Dan Transfer of Proceeding Dalam Kasusu Cybercrime", (Tesis Magister Universitas Indonesia, Jakarta, 2012)

Data 91 Juta Pengguna Tokopedia dan 7 Juta Merchant Dilaporkan Dijual di Dark Web, Kompas.com diakses dalam https://tekno.kompas.com/read/2020/05/03/10203107/data-91-juta-pengguna-tokopedia-dan-7-juta-merchant-dilaporkan-dijual-di-dark?page=all

Edmon Makarim, *Pengantar Hukum Telematika* (Jakarta: Raja Grafindo Persada, 2005)

Edmon Makarim, "Tanggungjawab Penyelenggara Terhadap Tata Kelola Yang Baik Dalam Penyelenggaraan Sistem Elektronik (Good Electronic Governance)", (Disertasi Doktor Universitas Indonesia, Depok, 2009)

ELSAM, Perlindungan Data Pribadi Konsep, Instrumen, Dan Prinsipnya (Jakarta: Elsam, 2019)

Fakhurohman, 2004, *Memahami Keberadaan Mahkamah Konstitusi di Indonesia*, (Bandung: Citra Aditya Bakti, 2004)

F. Sugeng Istanto, *Penelitian Hukum*, (Yogyakarta: CV. Ganda, 2007)

Gomgom T.P Siregar, Suatu analisis mengenai tindak pidana pencemaran nama baik melalui media elektronik, (Bandung: Refika Aditama, 2020)

Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*, (Jakarta: Rajawali Pres, 2012)

Muladi, Kapita Selekta Sistem Peradilan Pidana, (Semarang: Badan Penerbit Undip, 2004)

Orla Lynskey,"*Deconstructing Data Protection: the 'Added-Value' of a Right to Data Protection in the EU Legal Order"*. (International and Comparative Law Quarterly, 2014)

Philipus M Hadjon, 1987, *Perlindungan Bagi Rakyat Indonesia*, (Surabaya: PT Bina Ilmu, 1987)

Rulli Nasrullah, *Media Sosial Perspektif Komunikasi, Budaya, dan Sosioteknologi*, (Bandung: Simbiosa Rekatama Media, 2017)

Satjipto, Rahardjo, *Ilmu Hukum*, (Bandung: PT Citra Aditya Bakti, 2000)

Shidarta, Hukum Perlindungan Konsumen Indonesia, (Jakarta: Grasindo, 2006)

Sinta Dewi Rosadi, Cyber Law, (Bandung: Refika Aditama, 2015)

Soerjono Soekanto dan Sri Mamudji, Penelitian Hukum Normatif: Suatu Tinjauan Singkat, (Jakarta: PT Rajagrafindo Persada, 2001)

Wahyudi Djafar, Bernhard Ruben Fritz, dan Blandina Lintang, "Perlindungan Data Pribadi; Usulan Pelembagaan Kebijakan dari Perspektif HAM", (Jakarta: ELSAM, 2016)

Wahyudi Djafar dan Asep Komarudin, Perlindungan Hak Atas Privasi Di Internet: Beberapa Penjelasan Kunci, (Jakarta: ELSAM, 2014)

Wahyudi Djafar dan M. Jodi Santoso, 2019, *Perlindungan Data Pribadi Konsep, Instrumen, dan Prinsipnya*, (Jakarta: ELSAM, 2019)

Yasraf Amir Piliang, *Dunia yang Dilipat, Tamasya Melampaui Batas-batas Kebudayaan*, (Bandung: Jalasutra, 2004)

Lia Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia; Studi Perbandingan Hukum Inggris Dan Malaysia", Kanun Jurnal Ilmu Hukum 2, (Agustus, 2018)

Puslitbang Hukum dan Peradilan, Naskah Akademis Kejahatan Internet (*cyber crimes*), (Mahkamah Agung, 2004)

Kepaniteraan Dan Sekretariat Jenderal Mahkamah Konstitusi, Perlindungan Hak Privasi atas Data Diri di Era Ekonomi Digital, (Jakarta: Kepaniteraan Dan Sekretariat Jenderal Mahkamah Konstitusi, 2019)

Pusat Kajian Anggaran Badan Keahlian DPR RI, Tantangan Penguatan Keamanan Siber dalam Menjaga Stabilitas Keamanan, (Jakarta: Pusat Kajian Anggaran DPR RI, 2021)

Hootsuite WeareSocial, Indonesian Digital Report 2021
Undang-Undang Tentang Telekomunikasi, UU Nomor 36 Tahun 1999.
Undang-Undang Tentang Perlindungan Konsumen, UU Nomor 8 Tahun 1999.
Undang-Undang Tentang Hak Asasi Manusia, UU Nomor 39 Tahun 1999.
Undang-Undang Tentang Keterbukaan Informasi Publik, UU Nomor 14 Tahun 2008.
Undang-Undang Tentang Perbankan, UU Nomor 10 Tahun 1998.
Undang-Undang Tentang Kesehatan, UU Nomor 36 Tahun 2009.
Undang-Undang Tentang Administrasi Kependudukan, UU Nomor 24 Tahun 2013 Perubahan Atas UU Nomor 23 Tahun 2006.
Undang-Undang Tentang Informasi dan Transaksi Elektronik, UU Nomor 19 Tahun 2016 Perubahan Atas UU Nomor 11 Tahun 2008.
Undang-Undang Tentang Perlindungan Data Pribadi, UU Nomor 27 Tahun 2022
Edmon Makarim, Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi, Kolom Hukumonline.com
Tribun News.com, "Dituding Akan Salah Gunakan Data Peserta Tryout Tes Cpns 2019, Klarifikasi Akun Cpns Indonesia.Id," Tribun News .Com
Kerugian Akibat Kejahatan Siber Capai Rp 3,88 Triliun, Apa Saja Bentuknya?, databoks.katadata.co.id
Cindy Mutiara Annur, Pencurian Data Pribadi dalam Pusaran Bisnis Fintech Ilegal, diakses dalam katadata.co.id
Indonesia Masuk 3 Besar Negara dengan Kasus Kebocoran Data Terbanyak Dunia, Katadata.co.id
Kebocoran Data Nasabah BRI Life Bukti Lemahnya Proteksi dan Regulasi, Focus.tempo.co.
Data Nasabah Asuransi BRI Life Diduga Bocor dan Dijual Online, Kompas.com, diakses dalam https://tekno.kompas.com/read/2021/07/27/19234397/data-nasabah-asuransi-bri-life-diduga-bocor-dan-dijual-online?page=all
Office of Privacy and Civil Liberties, Privasi Act of 1974, (U.S Department of Justice). Diakses dalam https://www.justice.gov/opcl/privacy-act-1974#:~:text=The%20Privacy%20Act%20of%201974%2C%20as%20amended%2C%205%20U.S.C.,of%20records%20by%20federal%20agencies.
Kasus Kebocoran Data di Indonesia dalam Sebulan, dari PLN, IndiHome, hingga Nomor SIM Card, Kompas.com
RI Dihantam 700 Juta Serangan Siber di 2022, Modus Pemerasan Dominan, diakses dalam https://www.cnnindonesia.com/teknologi/20220701164212-192-816150/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan
Surati Pengguna, CEO Tokopedia Akui Pihak Ketiga Mencuri Data, Katadata.co.id, diakses dalam https://katadata.co.id/desysetyowati/digital/5eba4c2354ace/surati-pengguna-ceo-tokopedia-akui-pihak-ketiga-mencuri-data
Kronologi Kasus Kebocoran Data WNI, Dijual 0,15 Bitcoin hingga Pemanggilan Direksi BPJS, kompas.com diakses dalam https://tekno.kompas.com/read/2021/05/22/09450057/kronologi-kasus-kebocoran-data-wni-dijual-0-15-bitcoin-hingga-pemanggilan
Kasus Dugaan Kebocoran Data Pribadi Sepanjang 2022, Tempo.co diakses dalam https://nasional.tempo.co/read/1632043/inilah-7-kasus-dugaan-kebocoran-data-pribadi-sepanjang-2022
Kronologi Ratusan Mahasiswa IPB Terlibat Pinjol, Berawal dari Tawaran Bisnis Online, Dijanjikan Keuntungan 10 Persen, Kompas.com diakses dalam https://regional.kompas.com/read/2022/11/16/081100378/kronologi-ratusan-mahasiswa-ipb-terlibat-pinjol-berawal-dari-tawaran-bisnis?page=all
https://kbbi.kemdikbud.go.id/