



Perlindungan Hak Privasi sebagai Bagian dari Hak Asasi Manusia dalam Sistem Hukum Nasional Indonesia

I Gede Pasek Eka Wisanjaya¹

¹Fakultas Hukum Universitas Udayana, E-mail: pasekwisanjaya@gmail.com

Info Artikel

Masuk: 18 September 2023

Diterima: 26 Desember 2023

Terbit: 30 Desember 2023

Keywords:

Right to Privacy, ICCPR, Data Protection, Cybercrime, dan Social Media

Kata kunci:

Hak atas Privasi, ICCPR, Perlindungan Data, Kejahatan Siber, and Media Sosial

Corresponding Author:

I Gede Pasek Eka Wisanjaya, E-mail:

pasekwisanjaya@gmail.com

DOI:

10.24843/JMHU.2023.v12.i04.p08

Abstract

The development of technology has brought us into a borderless world, which can be a challenge or an opportunity depending on how we approach it. Recent cases have shown that an individual's personal data, which is part of their privacy, can be leaked and misused by irresponsible parties. Examples such as the Facebook data breach during the U.S. presidential election, hacking attacks carried out by Bjorka, and the leakage of data from various government agencies are real examples of this issue. In this context, the protection of privacy has become more crucial than ever. The purpose of this writing is to investigate how Indonesian regulations protect individual privacy. This research uses a normative approach by analyzing the applicable laws and relevant facts. The research findings indicate that Indonesia has regulations that indirectly provide protection for individual privacy. This is in line with Indonesia's constitution and its international responsibility as a party that has ratified the ICCPR. Furthermore, these regulations also include sanctions that can be imposed in cases of privacy violations. However, challenges persist in terms of supervision and the implementation of these regulations, as well as the presence of extraterritorial threats beyond the jurisdiction of the country. Therefore, the challenge of protecting privacy in the digital era needs to be continuously addressed through rigorous supervision and international cooperation.

Abstrak

Perkembangan teknologi telah membawa kita ke dalam dunia yang tidak mengenal batas, yang dapat menjadi tantangan atau peluang tergantung pada bagaimana kita menghadapinya. Kasus-kasus terbaru menunjukkan bahwa data pribadi seseorang, yang merupakan bagian dari privasi mereka, dapat bocor dan disalahgunakan oleh pihak yang tidak bertanggung jawab. Contoh-contoh seperti kebocoran data Facebook selama pemilihan presiden Amerika Serikat, serangan peretasan yang dilakukan oleh Bjorka, dan bocornya data dari berbagai lembaga pemerintah menjadi contoh nyata dari masalah ini. Dalam konteks ini, perlindungan privasi menjadi lebih krusial daripada sebelumnya. Penulisan ini bertujuan untuk menyelidiki bagaimana peraturan perundang-undangan di Indonesia melindungi privasi individu. Penelitian ini menggunakan pendekatan normatif dengan menganalisis hukum yang berlaku dan fakta-fakta terkait. Hasil penelitian menunjukkan bahwa Indonesia telah memiliki peraturan-peraturan yang secara tidak langsung memberikan

perlindungan terhadap privasi individu. Hal ini sejalan dengan konstitusi Indonesia dan tanggung jawab internasionalnya sebagai pihak yang telah meratifikasi ICCPR. Selain itu, dalam peraturan tersebut juga telah diatur sanksi yang dapat diberlakukan dalam kasus pelanggaran privasi. Namun, kendala tetap muncul dalam hal pengawasan dan penerapan peraturan tersebut, serta adanya ancaman ekstrateritorial yang berada di luar yurisdiksi negara. Oleh karena itu, tantangan perlindungan privasi dalam era digital ini perlu terus diatasi dengan ketatnya pengawasan dan kerja sama lintas negara.

I. Pendahuluan

Seiring berkembangnya zaman maka semakin maju pula teknologi informasi dan komunikasi ("TIK") yang dimiliki oleh manusia. Perkembangan ini bagaikan pisau bermata dua dimana dapat membawa suatu kebermanfaatan tetapi juga apabila tidak diatur dapat menyebabkan lebih banyak kerugian (kejahatan) daripada kebaikan.¹ Perkembangan TIK telah memunculkan apa yang kita kenal sekarang sebagai Internet, sebuah platform komunikasi digital yang menggunakan metode "packet switching" yang dimana berbeda dengan teknologi sebelumnya, internet memecah data menjadi paket-paket digital, mengirimkannya melalui rute jaringan yang berbeda, dan merangkainya kembali di tempat tujuan. Keunggulan ini memungkinkan Internet mencakup wilayah yang lebih luas, dan menampung lebih banyak pengguna serta tidak terbatas pada suatu wilayah tertentu (*Borderless World*).² Teresa Fuentes-Camacho mendefinisikan ranah internet atau yang umum disebut dunia maya (*cyberspace*) sebagai berikut³:

"Cyberspace is a new human and technological environment. It involves people from all countries, cultures and languages and of all ages and occupations supplying and demanding information, as well as a worldwide network of computers interconnected by means of telecommunication infrastructures enabling information to be processed and transmitted digitally. Synonyms of the term 'cyberspace' include 'information superhighways' and 'infosphere'."

Dalam beberapa tahun terakhir, segala aspek kehidupan kita telah menyatu dengan dunia maya.⁴ Mulai dari komunikasi, pertukaran informasi, perbankan, berbelanja, bisnis, pelayanan publik, pemerintahan, pengawasan hukum, keamanan nasional, dan masih

¹ I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, and I Nyoman Gede Sugiarta, "Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime)," *Jurnal Konstruksi Hukum* 1, no. 2 (October 28, 2020): 334.

² Nicholas Tsagourias and Russell Buchan, eds., *Research Handbook on International Law and Cyberspace* (United Kingdom: Edward Elgar Publishing, 2021), 131, <https://doi.org/10.4337/9781789904253>.

³ Bruno De padirac, ed., *The International Dimensions of Cyberspace Law*, vol. 1 (London: Routledge, Taylor & Francis Group : UNESCO Publishing, 2018), 35.

⁴ United Nations General Assembly, "Report of the Secretary General 69/112: Developments in the Fields of Information and Telecommunications in the Context of International Security," 2014, <http://undocs.org/A/69/112>.

banyak lagi.⁵ Semua ini terjadi tanpa menghiraukan batas-batas negara, baik untuk tujuan yang positif maupun negatif.

Berdasarkan data yang tersedia pada tahun 2022, tercatat bahwa sekitar 5.3 miliar atau sekitar 66% dari populasi dunia telah menggunakan internet.⁶ Namun, perkembangan teknologi dan konektivitas internet juga membawa dampak negatif, terutama dalam bentuk kejahatan siber. Ada ungkapan yang mengatakan bahwa “kejahatan adalah produk dari masyarakat itu sendiri”⁷ yang mengindikasikan bahwa dalam setiap masyarakat, akan selalu ada potensi untuk terjadinya tindakan kriminal.

Salah satu contoh kasus yang mencuat dalam benak kita adalah kasus dugaan kebocoran data yang dilaporkan melibatkan peretas yang mengklaim telah mencuri data dari penduduk Indonesia. Kasus tersebut mencakup data pelanggan Indihome, data registrasi SIM, MyPertamina, Peduli Lindungi, serta dokumen pemerintah seperti paspor.⁸ Sayangnya, ini hanyalah salah satu dari banyak laporan tentang kebocoran data yang masih terjadi di Indonesia. Baru-baru ini, juga muncul laporan terkait dugaan bocornya data dari Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementerian Dalam Negeri dengan melibatkan total 337 juta data.⁹

Kejadian-kejadian semacam ini memperlihatkan adanya permasalahan serius terkait perlindungan data pribadi di Indonesia. Selain itu, berdasarkan data, Indonesia menempati peringkat ketiga di dunia dalam hal jumlah kejahatan siber yang terjadi.¹⁰ Ini adalah peringatan serius tentang betapa pentingnya menjaga keamanan data dan privasi individu dalam dunia yang semakin terhubung.

Sebagai negara, Indonesia memiliki tanggung jawab untuk melindungi warga negaranya, termasuk melindungi data pribadi mereka. Hal ini sejalan dengan semangat yang terkandung dalam alinea ke-4 pembukaan Undang-Undang Dasar Negara Republik Indonesia tahun 1945 (“UUD NRI 1945”). Permasalahan ini seharusnya menjadi prioritas dan menjadi bahan evaluasi dalam upaya meningkatkan perlindungan data pribadi,

⁵ Tsagourias and Buchan, *Research Handbook on International Law and Cyberspace*, 1.

⁶ *Measuring Digital Developments: Facts and Figures 2022* (ITU Publications, 2022), 1.

⁷ Abdul Wahid and Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, Cet. 1 (Bandung: Refika Aditama, 2005), 39.

⁸ Ilyas Fadilah, “Kilas Balik Aksi Bjorka Curi-Curi Data, Dijual Demi Cuan!,” *Detikfinance*, January 11, 2023, <https://finance.detik.com/berita-ekonomi-bisnis/d-6508922/kilas-balik-aksi-bjorka-curi-curi-data-dijual-demi-cuan/2>; kumparanTECH, “Hacker Bjorka Klaim Curi 34 Juta Data Paspor Orang Indonesia,” *Kumparan*, July 3, 2023, <https://kumparan.com/kumparantech/hacker-bjorka-klaim-curi-34-juta-data-paspor-orang-indonesia-20jaXTAD4VO/full>; “10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-Ramai Bantah,” *CNNIndonesia*, Desember 2022, <https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah/2>.

⁹ BBC News Indonesia, “Ratusan Juta Data Dukcapil Kemendagri Diduga Bocor, Pakar Siber: ‘Ini Peretasan Paling Parah,’” *BBC*, July 18, 2023, <https://www.bbc.com/indonesia/articles/c51v25916zlo>.

¹⁰ Indriana Firdaus, “Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan,” *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia* 4, no. 2 (December 14, 2022): 24, <https://doi.org/10.52005/rechten.v4i2.98>.

meningkatkan kesadaran akan risiko siber, dan menguatkan kapasitas dalam menghadapi ancaman keamanan siber di masa depan.

Isu mengenai kebocoran data tidak berhenti hanya pada pencurian data itu sendiri; sebaliknya, ada tindak kejahatan lain yang mengikuti setelah memperoleh data tersebut. Contoh kasus yang menggambarkan hal ini adalah: **Pertama**, tindak kejahatan yang sangat signifikan terjadi dalam kampanye yang ditargetkan yang telah dipersonalisasi untuk kelompok-kelompok berdasarkan data yang diperoleh. Salah satu contoh kasus terkait adalah skandal Cambridge Analytica yang menggunakan data dari Facebook untuk membuat profil pemilih guna menargetkan pemilih di Amerika pada waktu tersebut.¹¹ **Kedua**, tindakan mengirimkan surel elektronik yang mengandung elemen botnet atau tautan yang bertujuan untuk merancang penipuan dan perolehan data yang berpotensi merugikan, dimana hal ini dijalankan dengan menyamar sebagai entitas perusahaan atau bank tertentu.¹² Situasi ini mungkin muncul akibat informasi kontak korban yang bocor, sehingga menyebabkan individu tersebut menjadi rentan terhadap praktik penipuan. Contoh kasus yang terjadi sebelumnya adalah munculnya kerugian senilai tiga juta dolar Amerika Serikat akibat pencurian kartu kredit, dengan fakta bahwa 25 persen dari surel spam dikirimkan secara spesifik kepada akun akuntansi di situ.¹³

Dari permasalahan *a quo*, sebenarnya "perlindungan data pribadi" merupakan bagian dari konsep yang kita kenal sebagai Hak Privasi. Hak tersebut yang akan menjadi fokus pada penulisan kali ini. Perlindungan terhadap privasi seseorang saat ini menjadi sangat penting dari pada sebelumnya mengingat, perangkat elektronik dan akses internet dapat dimiliki oleh siapa saja dengan harga yang terjangkau. Seperti yang telah dijelaskan sebelumnya, meskipun perangkat elektronik dan internet dapat digunakan untuk tujuan yang baik, namun kita juga harus menyadari potensi penyalahgunaan digital yang mengancam atau merampas privasi seseorang.¹⁴

Pasal 28G ayat (1) UUD NRI 1945 menggariskan hak privasi sebagai hak fundamental. Dalam pasal tersebut ditegaskan bahwa setiap individu memiliki hak untuk dilindungi dalam aspek-aspek pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kendali mereka. Tak hanya itu, setiap orang juga berhak merasa aman dan mendapatkan perlindungan dari ancaman atau ketakutan, sehingga dapat dengan bebas mengambil keputusan sesuai dengan hak asasinya, tanpa ada tekanan eksternal

¹¹ Nicholas Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far," *The New York Times*, April 4, 2018, <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>; Alex Hern, "Cambridge Analytica: How Did It Turn Clicks into Votes?," *The Guardian*, May 6, 2018, <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie>.

¹² Ian Goldberg, "Privacy-Enhancing Technologies for the Internet III: Ten Years Later," in *Digital Privacy: Theory, Technologies, and Practices* (New York: Auerbach Publications, 2008), 13; T. Editors of Encyclopaedia Britannica, "Phishing," *Encyclopedia Britannica*, August 8, 2023, <https://www.britannica.com/technology/phishing>.

¹³ Candra Kresna Wijaya, "Tanggung Jawab Negara Terhadap Akibat Accidental Unilateral Transborder Access Melalui Government Hacking" (Bali, Universitas Udayana, 2023), 9.

¹⁴ Kriangsak Kittichaisaree, *Public International Law of Cyberspace*, vol. 32, Law, Governance and Technology Series (Cham: Springer International Publishing, 2017), 45.

yang membahayakan. Hak ini memastikan bahwa kehidupan pribadi dan hak asasi individu dihormati dan terjaga dengan baik.

Pasal ini menciptakan dasar konstitusional yang kuat untuk melindungi hak privasi individu di Indonesia. Hak privasi ini mencakup hak untuk tidak terganggu dalam kehidupan pribadi, keluarga, dan kehormatan seseorang. Selain itu, pasal ini juga mengakui hak individu untuk memiliki perlindungan atas harta benda mereka dan merasa aman dari ancaman atau ketakutan terkait dengan hak-hak dasar mereka. Dengan adanya dasar konstitusional ini, negara memiliki kewajiban yang jelas untuk melindungi hak privasi individu. Ini mencakup upaya untuk mencegah penyalahgunaan data pribadi, perlindungan terhadap keamanan data, serta tindakan hukum yang tegas terhadap pelanggaran privasi.

Berdasarkan deskripsi diatas, maka dirasa penting untuk dilakukannya suatu penulisan tentang perlindungan Privasi itu sendiri terkhususnya di Indonesia. Untuk menghindari kesamaan dalam penulisan, judul, dan topik pembahasan, penting untuk melakukan pencarian terhadap penulisan terdahulu agar dapat meminimalisir tumpang tindih topik. Dari penelusuran yang telah dilakukan, terdapat beberapa penulisan yang hampir serupa. Pertama, "Upaya Perlindungan Hukum Privasi Data Pribadi dari Tindak Peretasan" oleh Indriana Firdaus, membahas solusi untuk melindungi hak privasi individu yang menjadi korban kejahatan peretasan dan menggambarkan bagaimana penegak hukum menangani tindak pidana peretasan. Kedua, "Perlindungan Hukum Data Pribadi sebagai Aspek Hak Privasi" oleh Sekaring Ayumeida Kusnadi dan Andy Usmina Wijaya, mencoba menjelaskan esensi hak privasi terhadap data pribadi dan bagaimana data pribadi dilindungi secara hukum sebagai hak privasi di Indonesia.

Berdasarkan hasil pencarian sebelumnya, penulisan ini akan memiliki perbedaan dari yang sebelumnya. Dalam penulisan ini, akan mencoba menjawab rumusan masalah berikut: Pertama, bagaimana Perlindungan Privasi dalam Hukum Nasional Indonesia? Kedua, apakah Norma Hukum Nasional Indonesia telah memberikan Perlindungan yang Maksimal terhadap Perlindungan terhadap Hak Privasi? Harapannya, penulisan ini akan memberikan penjelasan yang jelas mengenai hak privasi yang sebenarnya harus dilindungi dan bagaimana pengaturannya di Indonesia, serta bagaimana implementasinya dalam kenyataan. Selain itu, diharapkan penulisan ini akan menjadi pertimbangan penting dalam proses pengaturan hukum di Indonesia ke depan, terutama dalam upaya melindungi Hak Asasi Manusia ("HAM") secara keseluruhan, dan hak privasi secara khusus, dalam perundang-undangan yang akan datang.

2. Metode Penelitian

Penelitian hukum normatif, sering dikenal sebagai *normative legal research*,¹⁵ akan menjadi metode utama dalam penulisan ini. Pendekatan ini melibatkan analisis mendalam terhadap hukum positif, mencakup peraturan-perundang-undangan yang berlaku, asas-asas hukum, norma-norma hukum, kaidah hukum, putusan pengadilan, perjanjian, dan doktrin hukum. Pendekatan ini ditujukan untuk menawarkan solusi terhadap berbagai

¹⁵ Ronny Hanitijo Sumitro, *Metodologi Penelitian Hukum* (Jakarta: Ghalia Indonesia, 1994), 15.

permasalahan hukum yang timbul, dengan menggunakan sumber-sumber hukum utama dan sekunder seperti buku, jurnal, serta sumber-sumber online.

Dalam penelitian hukum normatif, informasi yang ditemukan dari sumber-sumber ini akan dianalisis secara sistematis dan diuraikan dalam penelitian ini dengan menggunakan pendekatan perundang-undangan dan pendekatan fakta. Ini berarti bahwa analisis akan didasarkan pada hukum yang berlaku dan informasi faktual yang relevan untuk memahami isu-isu hukum yang sedang dibahas.

3. Hasil Dan Pembahasan

3.1. Pengaturan Perlindungan Hak atas Privasi di Indonesia

HAM adalah hak yang berlaku secara universal dan tidak terbatas pada suatu wilayah tertentu. Semua individu memilikinya hanya karena mereka merupakan bagian dari spesies manusia. Hal ini memiliki signifikansi yang besar. Beberapa pakar meyakini bahwa memiliki status moral dan hak-hak moral serta hukum bergantung pada status sebagai individu.¹⁶

Perlindungan terhadap HAM berlaku di semua tempat, termasuk dalam lingkup dunia maya.¹⁷ Pada masa lalu, perlindungan terhadap HAM sering kali dianggap sebagai tanggung jawab suatu negara saja, namun setelah Perang Dunia Kedua, negara-negara mulai menyadari bahwa tindakan ini harus dihindari agar tragedi serupa tidak terulang.¹⁸ Oleh karena itu, penghormatan terhadap HAM menjadi faktor penting dalam menjaga perdamaian dan keamanan internasional. Selain itu, upaya ini juga bertujuan untuk menegaskan bahwa hak-hak yang mendasar tidak boleh dicabut, sehingga perlindungan terhadap HAM tidak lagi hanya menjadi hak diskresi nasional.¹⁹ Tapi walaupun begitu, kedaulatan sebuah negara masih memiliki peran penting dalam menjalankan perlindungan HAM, sebagaimana juga ditegaskan oleh Tunkin yang menyatakan bahwa penghormatan terhadap HAM difokuskan pada tanggung jawab negara.²⁰

¹⁶ Miriam Budiardjo, *Dasar-Dasar Ilmu Politik*, Cet. pert. rev (Jakarta: Gramedia Pustaka Utama, 2008), 211-12.; A. Masyhur Effendi, *Dimensi/Dinamika Hak Asasi Manusia dalam Hukum Nasional dan Internasional*, Cet. 1 (Jakarta: Ghalia Indonesia, 1994), 199.

¹⁷ Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Second edition (Cambridge, United Kingdom: Cambridge University Press, 2017), 182.

¹⁸ Kent Revelino Chandra, "Perlindungan Hak Kebebasan Berpendapat Dan Berekspresi Berdasarkan Hukum Internasional Di Indonesia (Studi Kasus: Pembatasan Hak Kebebasan Berpendapat Dan Berekspresi Pada Putusan No.210/Pid.B/2020/PN.Amb. Mengenai Tindak Pidana Makar)" (Bali, Universitas Udayana, 2023), 36.

¹⁹ Alette Smeulers and Fred Grünfeld, *International Crimes and Other Gross Human Rights Violations* (Leiden: Martinus Nijhoff Publishers, 2011), 5.

²⁰ G. I. Tunkin, *Theory of International Law* (Cambridge, Mass: Harvard University Press, 1974), 81-83.

Pernyataan *a quo* ditegaskan kembali dalam salah satu dokumen hukum internasional yaitu *General Comment No.31*,²¹ yang menegaskan bahwa negara-negara pihak yang terikat oleh ICCPR²² serta semua lembaga di dalamnya (termasuk eksekutif, legislatif, yudikatif, dan otoritas publik lainnya) memiliki tanggung jawab untuk memastikan perlindungan terhadap HAM di wilayahnya.²³

Pengaturan mengenai perlindungan privasi sendiri telah ada dan berkembang di negara-negara modern. Contohnya, di Amerika Serikat,²⁴ ini terlihat dalam Amandemen Keempat Konstitusi yang menyatakan, "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures*" Prinsip ini juga diterapkan dalam keputusan-keputusan Mahkamah Agung Amerika. Di India, meskipun tidak ada peraturan khusus tentang perlindungan privasi, Mahkamah Agung India telah menginterpretasikan bahwa hak privasi ini termasuk dalam hak 'kehidupan' dan 'kebebasan pribadi' yang dijamin oleh negara dan tidak dapat dibatasi kecuali berdasarkan prosedur yang telah ditetapkan oleh hukum. Demikian pula, Kanada, meskipun tidak secara tegas diatur dalam Canadian Charter of Rights and Freedoms 1982, jaminan keamanan dari penyelidikan dan penyitaan yang tidak wajar dianggap sebagai hak untuk 'harapan wajar terhadap privasi'.²⁵

Sebelum membahas regulasi perlindungan privasi di Indonesia, penting untuk memahami konsep privasi dengan baik. Privasi oleh J. Michael dijelaskan sebagai keinginan individu akan kesendirian, kedekatan, anonimitas, dan ketertutupan. Beberapa definisi menyebut privasi sebagai "hak untuk tidak diganggu," baik secara umum maupun dalam artian lebih sempit yaitu hak untuk mengendalikan informasi tentang diri sendiri.²⁶ Upaya untuk merangkul beragam konsep privasi menghasilkan definisi kompromi yang mencakup "kebebasan dari gangguan yang tidak sah dan tidak wajar dalam aktivitas yang diakui masyarakat sebagai bagian dari ranah otonomi individu."²⁷ Ranah otonomi individu adalah tempat individu dapat menjalani kehidupan sesuai dengan keinginan dan harapannya tanpa mengganggu kebebasan individu lainnya.²⁸

Proteksi terhadap privasi individu di Indonesia telah diamanatkan oleh konstitusi, terutama Pasal 28G ayat (1) UUD NRI 1945. Selain itu, hak ini juga dijamin oleh Pasal 17

²¹ UN Human Rights Committee (HRC), "General Comment No. 31 [80], The Nature of the General Legal Obligation Imposed on States Parties to the Covenant" (United Nations, May 26, 2004), CCPR/C/21/Rev.1/Add.13. Para. 3-4.

²² International Covenant on Civil and Political Rights (ICCPR) adalah salah satu perjanjian internasional yang memiliki signifikansi paling penting dan bersifat universal, dirancang dengan tujuan untuk menjaga dan melindungi hak-hak sipil dan politik. (Lihat UN General Assembly, "International Covenant on Civil and Political Rights" (United Nations, December 16, 1966), Art. 19, 999 UNTS 171.)

²³ Tunkin, *Theory of International Law*, 28

²⁴ William A. Schabas, *The Customary International Law of Human Rights*, 1st ed. (Oxford University Press, 2021), 218, <https://doi.org/10.1093/oso/9780192845696.001.0001>.

²⁵ Nihal Jayawickrama, *The Judicial Application of Human Rights Law: National, Regional and International Jurisprudence*, Second edition (Cambridge, United Kingdom New York Port Melbourne Delhi Singapore: Cambridge University Press, 2017), 647.

²⁶ Joseph and Castan, *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary*, 533-34.

²⁷ *Ibid.*

²⁸ Nowak, *U.N. Covenant on Civil and Political Rights*, 378.

dalam International Convention on Civil and Political Rights (“ICCPR”), yang telah disahkan oleh Indonesia melalui Undang-Undang No. 12 tahun 2005 tentang Pengesahan International Covenant on Civil and Political Rights. ICCPR merupakan perjanjian internasional kunci di bidang HAM yang mengharuskan negara-negara anggotanya untuk melindungi hak-hak sipil dan politik individu, termasuk hak privasi.

Dengan merujuk pada prinsip *Pacta Sunt Servanda*, yang mengindikasikan bahwa sebuah negara yang telah bersedia menjadi pihak dalam suatu perjanjian berkewajiban untuk memenuhi kewajiban-kewajiban yang telah disepakati dalam perjanjian tersebut dengan itikad baik.²⁹ Dalam situasi keterlibatan Indonesia sebagai negara peserta dalam ICCPR, hal ini mencerminkan kesediaan untuk memenuhi tanggung jawab perjanjian tersebut dengan itikad baik. Sebagai konsekuensi dari keterlibatan tersebut, Indonesia dihadapkan pada kewajiban untuk menjaga dan melindungi privasi warganya. Tindakan ini dianggap sebagai bentuk implementasi dari itikad baik, terutama mengingat ICCPR telah menjadi bagian dari hukum internasional yang mengikat Indonesia setelah melewati proses ratifikasi dan diakui sebagai hukum kebiasaan internasional.³⁰

Lebih lanjut, menurut *General Comment 16*, perlindungan terhadap privasi mencakup kerahasiaan korespondensi yang tidak boleh diintervensi.³¹ Ini juga mencakup informasi pribadi yang disimpan dalam komputer, basis data, dan perangkat lainnya.³² Sebagaimana perlindungan data dan privasi menjadi bagian yang berhubungan dan tidak dapat terlepas satu sama lainnya.³³ Negara harus mengatur hal ini dan memastikan bahwa data-data tersebut tidak jatuh ke tangan yang tidak sah atau tanpa otorisasi.³⁴ Dokumen "*Rights to Privacy in the Digital Age*" juga menguatkan hak privasi tidak hanya berlaku dalam ruang pribadi seperti di dalam rumah, tetapi juga mencakup ranah publik.³⁵ Privasi memberikan individu kekuatan untuk mengendalikan identitas mereka, baik dalam dunia nyata maupun dalam standar kehidupan di dunia maya.

Apabila kita melihat pengaturan di Indonesia yang mengatur tentang privasi, kebebasan pribadi, atau perlindungan data. Beberapa undang-undang yang mungkin mengatur aspek-aspek tersebut dapat ditemukan namun tidak terbatas dalam peraturan perundang-undangan berikut:

²⁹ Malcom D. Evans, *International Law Documents (12th ed.)*. (Oxford: Oxford University Press, 2015), 134.; Talya Uçaryılmaz, “The Principle of Good Faith In Public International Law”, *Estudios De Deusto* 68, no. 1 (December,2019): 53.

³⁰ Kent Revelino Chandra and I Gusti Ngurah Parikesit Widiatedja, “Perang Rusia-Ukraina Dan Ancaman Terhadap Kebebasan Berpendapat Dan Berekspresi Di Rusia,” *Jurnal Magister Hukum Udayana* 12, no. 2 (July 29, 2023): 406–7.

³¹ UN Human Rights Committee (HRC), “CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation” (United Nations, April 8, 1988). Para. 8.

³² Jayawickrama, *The Judicial Application of Human Rights Law*, 691.

³³ Ida Ayu Agung Rasmi Wulan and Ni Luh Gede Astariyani, “Urgensi Dalam Meratifikasi Convention On Cybercrime Sebagai Pemenuhan HAM Di Indonesia,” *Kertha Patrika* 45, no. 2 (August 30, 2023): 226, <https://doi.org/10.24843/KP.2023.v45.i02.p06>.

³⁴ *Ibid.* Para.10.

³⁵ UN Human Rights Committee (HRC), “Concluding Observations on the Seventh Periodic Report of Colombia.” (United Nations, 2016), U.N. Doc. CCPR/C/COL/CO/7. Para. 32.

Pertama, Undang-Undang Nomor 8 tahun 1992 tentang Perbankan yang di amandemen dengan Undang-undang nomor 10 tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 tahun 1992 tentang Perbankan (“UU Perbankan”). adalah peraturan hukum yang secara umum mengatur sektor perbankan di Indonesia. Fokus utama dari undang-undang ini adalah untuk mengatur dan mengawasi kegiatan perbankan, termasuk operasi bank, pemberian kredit, pengelolaan dana nasabah, serta perlindungan kepentingan nasabah.

Terkait dengan perlindungan privasi, undang-undang ini biasanya mencakup ketentuan yang mengharuskan bank untuk menjaga kerahasiaan informasi dan data nasabah. Bank diwajibkan untuk melindungi data pribadi nasabah dan menjaga kerahasiaannya sesuai dengan ketentuan yang berlaku. Hal ini penting untuk menjaga kepercayaan nasabah terhadap sistem perbankan.

Selain itu, undang-undang ini juga dapat mencakup ketentuan mengenai penyediaan informasi kepada pihak ketiga, seperti pemberian informasi nasabah kepada otoritas perbankan atau pihak berwenang yang berhubungan dengan investigasi atau penegakan hukum. Dalam hal ini, peraturan biasanya mengatur batasan dan persyaratan untuk pengungkapan informasi tersebut. Hal ini sebagaimana tercantum dalam Pasal 40 UU Perbankan: “(1) Bank Wajib merahasiakan keterangan mengenai Nasabah Penyimpan dan simpanannya, kecuali dalam hal sebagaimana dimaksud dalam Pasal 41, Pasal 41A, Pasal 42, Pasal 44, dan Pasal 44A. (2) Ketentuan sebagaimana dimaksud dalam ayat (1) berlaku pula bagi Pihak Terafiliasi.”

Kedua, Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi, yang sering disebut sebagai UU Telekomunikasi, adalah kerangka hukum yang mengatur sektor telekomunikasi di Indonesia secara menyeluruh. Peraturan ini mencakup berbagai aspek, termasuk perizinan, alokasi spektrum frekuensi, privatisasi, hak dan kewajiban operator, serta perlindungan konsumen.

Dalam konteks perlindungan privasi, undang-undang ini juga mengandung ketentuan untuk melindungi kerahasiaan komunikasi pribadi dan mencegah tindakan penyadapan ilegal serta pengungkapan informasi pribadi oleh penyedia layanan telekomunikasi. Pasal 40 UU Telekomunikasi dengan tegas melarang siapa pun untuk melakukan penyadapan terhadap informasi yang dikirimkan melalui jaringan telekomunikasi, dalam bentuk apa pun. Ini menunjukkan larangan yang kuat terhadap tindakan penyadapan yang dapat mengancam privasi komunikasi individu. Selain itu, Pasal 42 ayat (1) UU Telekomunikasi mengamanatkan bahwa penyelenggara jasa telekomunikasi memiliki kewajiban untuk menjaga kerahasiaan informasi yang dikirim dan diterima oleh pelanggan melalui jaringan telekomunikasi mereka. Ini berarti bahwa penyedia layanan telekomunikasi harus mempertahankan kerahasiaan informasi yang ditransmisikan melalui jaringan mereka dan tidak boleh mengungkapkannya tanpa izin yang tepat.

Ketentuan-ketentuan ini menegaskan pentingnya melindungi privasi komunikasi dalam lingkungan telekomunikasi dan memberikan dasar hukum yang kuat untuk menegakkan hak privasi individu dalam konteks penggunaan layanan telekomunikasi di Indonesia.

Ketiga, Undang-Undang Nomor 23 tahun 2006 tentang Administrasi Kependudukan (“UU Aminduk”) yang telah mengalami perubahan melalui Undang-Undang Nomor 24

tahun 2013 adalah peraturan hukum yang mengatur berbagai aspek terkait administrasi kependudukan di Indonesia (UU 24/2013). Peraturan ini mencakup sejumlah aspek penting, seperti pendaftaran kependudukan, pemberian identitas melalui Kartu Tanda Penduduk (KTP), dan juga perlindungan data pribadi penduduk. Salah satu aspek yang sangat vital adalah perlindungan privasi, yang mencakup berbagai ketentuan untuk menjaga kerahasiaan data pribadi penduduk, mencegah akses yang tidak sah, dan memastikan bahwa data pribadi dikelola secara cermat sesuai dengan hukum yang berlaku.

Pasal 79 ayat (1) dalam undang-undang ini dengan tegas menyatakan bahwa "Negara berkewajiban untuk menyimpan dan menjaga kerahasiaan data pribadi dan dokumen kependudukan." Ketentuan ini menggarisbawahi tanggung jawab negara dalam menjaga kerahasiaan informasi yang bersifat sangat pribadi dan sensitif milik penduduk. Data pribadi merupakan informasi yang sangat rahasia dan penting untuk memastikan bahwa data ini tidak disalahgunakan atau diakses oleh pihak yang tidak berhak. Selain itu, Pasal 84 ayat (1) "Data Pribadi Penduduk yang harus dilindungi memuat: a. keterangan tentang cacat fisik dan/atau mental; b. sidik jari; c. iris mata; d. tanda tangan; dan e. elemen data lainnya yang merupakan aib seseorang," merujuk pada informasi pribadi seseorang. Pasal ini menegaskan pentingnya melindungi data pribadi yang sangat sensitif ini dan memastikan bahwa data tersebut tidak disalahgunakan atau diungkapkan tanpa izin yang sesuai.

Perlindungan privasi dalam UU Aminduk merupakan aspek yang sangat penting dalam menjaga kepercayaan masyarakat terhadap sistem administrasi kependudukan dan melindungi hak-hak individu terkait data pribadi mereka. Hal ini juga sesuai dengan prinsip-prinsip perlindungan data pribadi yang semakin relevan di era digital saat ini

Keempat, Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang mengalami perubahan melalui Undang-Undang Nomor 19 tahun 2016 ("UU 19/2016"), merupakan kerangka hukum yang mengatur berbagai aspek terkait teknologi informasi dan transaksi elektronik di Indonesia. Undang-undang ini meliputi regulasi transaksi elektronik, kepemilikan dan penggunaan data elektronik, serta memiliki peran penting dalam perlindungan privasi. Dalam konteks perlindungan privasi, UU ITE mencakup ketentuan-ketentuan yang mengatur bagaimana data pribadi harus diolah, disimpan, dan dilindungi, sehingga mencegah penyadapan ilegal dan pengungkapan informasi pribadi tanpa izin. Selain itu, UU ITE juga mengatur masalah keamanan jaringan dan sistem untuk melindungi data dari ancaman siber yang semakin meningkat. Perlindungan privasi dalam kerangka hukum ini menjadi sangat penting dalam era digital yang terus berkembang, untuk memastikan bahwa data pribadi individu terlindungi dan privasi dihormati dalam lingkungan teknologi informasi yang semakin kompleks. Sebagaimana dituukan pada Pasal 26 - Pasal 35 UU ITE

Kelima, Undang-Undang Nomor 43 tahun 2009 tentang Kearsipan adalah kerangka hukum yang mengatur manajemen, pelestarian, dan akses terhadap dokumen dan arsip di berbagai entitas, termasuk pemerintah dan lembaga swasta di Indonesia. UU ini mencakup aspek-aspek seperti pengelolaan kearsipan, prosedur pencatatan, penyimpanan, pemeliharaan, dan penggunaan dokumen dan arsip. Salah satu fokus utama undang-undang ini adalah mendorong pelestarian dokumen yang memiliki nilai

penting, baik dari segi hukum, sejarah, maupun administratif, untuk memastikan transparansi dan akuntabilitas.

Dalam konteks perlindungan privasi, UU Kearsipan juga dapat mencakup ketentuan-ketentuan yang terkait dengan perlindungan data pribadi yang mungkin terdapat dalam dokumen dan arsip. Ini termasuk aturan untuk menjaga kerahasiaan informasi pribadi yang terdapat dalam dokumen atau arsip, serta upaya untuk melindungi data pribadi dari akses yang tidak sah atau penyalahgunaan. Ketentuan ini ditemukan dalam Pasal 44 ayat (1) g dan h, "Pencipta arsip dapat menutup akses atas arsip dengan alasan apabila arsip dibuka untuk umum dapat: g. mengungkapkan isi akta autentik yang berisi fakta pribadi dan kemauan terakhir ataupun wasiat seseorang kecuali kepada yang berhak secara hukum; h. mengungkapkan rahasia atau data pribadi."

Meskipun UU Kearsipan mencakup beberapa ketentuan yang berhubungan dengan privasi dalam kaitannya dengan dokumen dan arsip, peraturan perlindungan privasi yang lebih terperinci dan spesifik biasanya diatur dalam undang-undang terpisah atau peraturan yang berkaitan dengan perlindungan data pribadi di Indonesia. Hal ini menunjukkan pentingnya menggabungkan perlindungan data pribadi ke dalam manajemen arsip untuk memastikan bahwa data pribadi tetap aman dan terlindungi dalam kerangka yang lebih luas.

Keenam, Undang-Undang Nomor 14 tahun 2008 tentang Keterbukaan Informasi Publik. adalah landasan hukum yang memastikan hak masyarakat untuk mengakses informasi publik yang dimiliki oleh entitas publik di Indonesia. Informasi Publik sendiri diartikan dalam Pasal 1 ayat (2), yaitu:

"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."

Peraturan ini mendorong transparansi dalam pemerintahan dengan mengharuskan lembaga-lembaga publik untuk secara proaktif memberikan informasi yang relevan kepada masyarakat. Tujuannya adalah untuk meningkatkan akuntabilitas dan partisipasi publik dalam proses pengambilan keputusan.

UU ini menetapkan kewajiban bagi entitas publik untuk menjaga catatan dan dokumen secara teratur dan memberikan akses yang mudah diakses kepada masyarakat. Meskipun peraturan ini mengadvokasi akses terbuka, ada pengecualian yang dapat digunakan untuk melindungi informasi yang bersifat pribadi, keamanan nasional, atau kepentingan tertentu lainnya. Kondisi ini diatur dalam Pasal 6 ayat (3) dimana

"Informasi Publik yang tidak dapat diberikan oleh Badan Publik, sebagaimana dimaksud pada ayat (1) adalah: a. informasi yang dapat membahayakan negara; b. informasi yang berkaitan dengan kepentingan perlindungan usaha dari persaingan usaha tidak sehat; c. informasi yang berkaitan dengan hak-hak pribadi; d. informasi yang berkaitan dengan rahasia jabatan; dan/atau e. Informasi Publik yang diminta belum dikuasai atau didokumentasikan."

UU Keterbukaan Informasi Publik berfokus pada hak masyarakat untuk mengakses informasi yang penting sambil menciptakan keseimbangan yang diperlukan antara transparansi pemerintah dan perlindungan privasi individu

Ketujuh, Undang-undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi (“UU PDP”). Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) adalah tonggak penting dalam pengaturan perlindungan data pribadi di Indonesia. UU ini secara umum mengatur cara pemrosesan dan perlindungan data pribadi individu. Dalam rangka menciptakan keseimbangan antara kemajuan teknologi dan privasi individu, UU PDP mewajibkan pemilik data dan pengolah data untuk memproses informasi pribadi dengan itikad baik dan transparansi, menjaga keamanan data dari ancaman siber, serta memberikan hak kepada individu untuk mengontrol data mereka. Dengan adanya UU PDP, Indonesia mengambil langkah penting untuk melindungi hak privasi masyarakat dalam era digital yang semakin berkembang pesat dan meningkatkan kepercayaan dalam penggunaan data pribadi.

Kedelapan, Undang-Undang Nomor 17 tahun 2023 tentang Kesehatan (“UU Kesehatan”) adalah payung hukum yang mengatur berbagai aspek penting dalam sektor kesehatan Indonesia. Secara umum, undang-undang ini mencakup perizinan dan pengaturan sistem kesehatan nasional, promosi kesehatan, serta pengaturan pelayanan kesehatan, termasuk regulasi obat dan alat kesehatan. Di dalamnya juga mengatur hak dan kewajiban pasien serta aspek etika dalam praktik medis. Dalam upaya memberikan pelayanan kesehatan yang berkualitas, UU Kesehatan mungkin juga mencakup ketentuan-ketentuan yang berhubungan dengan perlindungan privasi, terutama dalam hal penggunaan data kesehatan pasien dan informasi pribadi yang terkait dengan layanan medis. Hal ini bertujuan untuk menjaga kerahasiaan informasi medis individu dan mencegah potensi penyalahgunaan data pribadi pasien. Sebagaimana terlihat dalam Pasal 4 ayat (1) huruf i “Setiap Orang berhak: i. memperoleh kerahasiaan data dan informasi Kesehatan pribadinya”

3.2. Analisis Perlindungan Hak Privasi melalui Norma Hukum Indonesia

Sebelum mengeksplorasi lebih jauh implementasi peraturan yang berlaku, penting untuk memahami terlebih dahulu prinsip legalitas. Seperti yang sudah tertera dalam Pasal 1 ayat 1 Kitab Undang-Undang Hukum Pidana (KUHP), "Suatu perbuatan tidak dapat dipidana, kecuali berdasarkan kekuatan ketentuan perundang-undangan pidana yang telah ada." Dalam ranah hukum pidana, terdapat prinsip legalitas yang menyatakan bahwa tidak ada tindakan yang dapat dianggap sebagai pelanggaran pidana dan diancam dengan hukuman kecuali sudah diatur secara eksplisit dalam undang-undang. Dalam bahasa Latin, prinsip ini dikenal sebagai “*Nullum delictum nulla poena sine praevia lege poenalli*” yang dapat diartikan sebagai tidak ada perbuatan melanggar hukum, tidak ada hukuman tanpa aturan hukum yang telah ditetapkan terlebih dahulu.³⁶

Secara sederhana, prinsip legalitas menegaskan bahwa keberadaan undang-undang yang mengatur suatu tindakan adalah syarat yang harus dipenuhi sebelum tindakan tersebut dapat dikenai sanksi pidana. Prinsip ini bertujuan untuk menjamin kejelasan dan kepastian hukum, sambil melindungi individu dan HAM yang dimilikinya. Hukum hadir untuk menjaga masyarakat dari tindakan kejahatan, terutama dalam hal ini yang

³⁶ Moeljatno, *Asas-asas Hukum Pidana*, (Jakarta: Rineka Cipta, 2000), 23.

mengancam privasi individu. Mengingat perkembangan TIK, ancaman terhadap privasi individu semakin besar. Oleh karena itu, perlu untuk mengevaluasi bagaimana Indonesia mengimplementasikan perlindungan terhadap hak privasi individu melalui aplikasi dan sanksi yang tertuang dalam peraturan-peraturan yang ada, mengingat pentingnya menjaga keseimbangan antara inovasi teknologi dan keamanan privasi.

Perlindungan privasi di Indonesia dapat diilustrasikan melalui salah satu kasus yang sangat penting, yaitu Putusan Mahkamah Konstitusi (“MK”) No. 5/PUU-VIII/2010. Dalam kasus ini, diuji konstitusionalitas Pasal 34 ayat (4) UU ITE yang memberikan pemerintah kewenangan untuk mengeluarkan peraturan terkait penyadapan. MK memutuskan untuk membatalkan Pasal *a quo*, sehingga pemerintah tidak lagi memiliki wewenang untuk mengatur penyadapan melalui peraturan pemerintah. Penyadapan sekarang harus diatur melalui undang-undang. Keputusan MK ini menyatakan bahwa Pasal tersebut bertentangan dengan Pasal 28G UUD NRI 1945 dalam Konstitusi yang mengatur hak privasi, sehingga Pasal tersebut tidak berlaku lagi.

Selain itu, seperti yang telah dijelaskan sebelumnya, beberapa pasal dalam undang-undang yang telah disebutkan *supra* menunjukkan komitmen untuk melindungi hak atas privasi juga, termasuk namun tidak terbatas pada hal-hal berikut:

Pasal 26 ayat (1) UU 19/2016 yang berbunyi “Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan,” peraturan sebelumnya mengindikasikan bahwa penggunaan informasi yang mencakup data pribadi seseorang melalui media elektronik harus didasarkan pada persetujuan dari individu yang bersangkutan, terkecuali diatur lain dalam peraturan.

Pasal 65 UU PDP, yang menyatakan:

- “(1) Setiap Orang dilarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi.
- (2) Setiap Orang dilarang secara melawan hukum mengungkapkan Data Pribadi yang bukan miliknya.
- (3) Setiap Orang dilarang secara melawan hukum menggunakan Data Pribadi yang bukan miliknya.”

Pasal ini mengatur larangan hukum bagi individu terkait dengan data pribadi yang bukan milik mereka. Pertama, mereka tidak boleh mengumpulkan atau mengakses data pribadi tersebut dengan niat untuk memperoleh keuntungan pribadi atau keuntungan orang lain yang dapat merugikan pemilik data pribadi tersebut. Kedua, mereka tidak boleh mengungkapkan informasi pribadi yang tidak berhak. Ketiga, mereka tidak boleh memanfaatkan informasi pribadi tersebut yang tidak sah kepemilikannya.

Hal ini menekankan pentingnya melindungi data pribadi individu dari penyalahgunaan dan pengungkapan yang tidak sah, serta menjaga integritas privasi data pribadi tersebut. Larangan ini dirancang untuk mencegah tindakan yang dapat merugikan pemilik data pribadi dan mempromosikan perlindungan data yang tepat dalam hukum. Dengan

demikian, menjaga privasi data pribadi adalah tanggung jawab bersama untuk melindungi hak-hak individu dalam konteks digital yang semakin maju.

Pasal 1 ayat (1) Permenkominfo 20/2016, "Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya." Pasal ini mengenali Data Pribadi sebagai data individual yang harus dipelihara, dijaga keakuratannya, dan dijaga kerahasiaannya sesuai dengan hukum.

Dalam beberapa peraturan nasional juga, jika terjadi pelanggaran terhadap hak privasi, sanksi pidana dan/atau ganti rugi dapat dikenakan. Ini terlihat dalam beberapa peraturan, Pertama, terkait dengan UU 19/2016, di mana Bab IX mengatur tentang "Ketentuan Pidana", salah satu pasalnya, yaitu Pasal 45 UU 19/2016, mengatur hal tersebut.

"(1) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(2) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian sebagaimana dimaksud dalam Pasal 27 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(3) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik sebagaimana dimaksud dalam Pasal 27 ayat (3) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).

(4) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman sebagaimana dimaksud dalam Pasal 27 ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(5) Ketentuan sebagaimana dimaksud pada ayat (3) merupakan delik aduan."

Selain itu, dalam regulasi lain seperti UU PDP, jika terjadi pelanggaran terhadap data pribadi, perusahaan atau lembaga dapat dikenakan sanksi administratif dan juga sanksi pidana, sebagaimana tertuang pada pasal-pasal berikut: Pasal 57 ayat (2) UU PDP "(2)Sanksi administratif sebagaimana dimaksud pada ayat (1) berupa: a. peringatan tertulis; b. penghentian sementara kegiatan pemrosesan Data Pribadi dan c. penghapusan atau pemusnahan Data Pribadi; dan/atau d. denda administratif." Ketentuan Pidana dapat dilihat Bab XIV salah satu pasalnya yaitu pada Pasal 67 UU PDP

"(1) Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk

menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

(2) Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).

(3) Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah)."

Walaupun pengaturan tentang perlindungan privasi sekarang telah diatur akan tetapi hal inipun menyisahkan permasalahan. Sebagaimana dijelaskan dalam era digital, privasi tidak hanya terkait dengan informasi komunikasi. Metadata, yang mengandung informasi penting, juga menjadi bagian integral dari privasi, dan jenis data ini dapat melampaui informasi komunikasi dalam hal signifikansinya.³⁷ Ini mengindikasikan perluasan apa yang dapat dianggap sebagai wilayah privasi, khususnya dalam konteks di mana data pribadi seseorang telah menjadi sangat berharga, seperti "minyak baru".³⁸ Seiring dengan dinamika perkembangan TIK, yang saat ini dikenal sebagai Revolusi Industri Keempat, teknologi terus berkembang dan memfasilitasi konvergensi antara dunia nyata dan maya. Hal ini mengakibatkan produksi dan pertukaran informasi pribadi antar individu menjadi lebih mudah, terutama dengan munculnya internet dan perdagangan elektronik yang merambah hampir ke seluruh penjuru dunia.

Penyimpanan informasi pribadi oleh perusahaan teknologi di dunia maya telah meningkatkan risiko eksploitasi data ini oleh pihak-pihak yang tidak berwenang, seperti pelaku kejahatan cyber atau bahkan pemerintah. Oleh karena itu, perlindungan terhadap hak privasi sebagaimana dijelaskan *supra* yang berlaku di dunia nyata juga harus berlaku dan diterapkan dalam era virtual yang saat ini kita alami.³⁹

Dalam dokumennya yang berjudul "*The Right to Privacy in the Digital Age*,"⁴⁰ Komite Hak Asasi Manusia menyebutkan bahwa banyak negara menghadapi kesulitan dalam melindungi privasi karena terungkapnya kekurangan dalam undang-undang dan/atau penegakan hukum nasional yang memadai, perlindungan prosedural yang lemah, serta pengawasan yang tidak efektif. Semua hal ini telah berkontribusi pada kurangnya akuntabilitas terhadap campur tangan sewenang-wenang atau ilegal dalam hak privasi.

Penting untuk diingat bahwa beroperasi di ruang siber berarti memasuki wilayah tanpa batas. Meskipun tidak ada negara yang dapat mengklaim kedaulatan atas ruang siber itu

³⁷ Metadata memiliki potensi untuk mengungkap informasi yang mendalam tentang cara individu berperilaku, interaksi sosial, pilihan pribadi, dan identitas mereka (Lihat "United Nations General Assembly, 2013. The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights. U.N. Doc. A/HRC/39/29", paragraf 6).

³⁸ *Personal Data: The Emergence of a New Asset Class* (World Economic Forum., 2011), 7.

³⁹ United Nations General Assembly, "Resolution Adopted by the General Assembly: The Rights to Privacy in the Digital Age," 2015, 3, U.N. Doc. A/6/166.

⁴⁰ Human Rights Committee, "The Right to Privacy in the Digital Age" (UN Commission on Human Rights, June 30, 2014), 16.

sendiri, negara-negara memiliki kewenangan kedaulatan terhadap seluruh infrastruktur siber yang berada di wilayah mereka dan aktivitas yang terkait dengan infrastruktur siber tersebut.⁴¹ Dengan adanya layanan melalui internet hal ini menimbulkan tantangan baru dalam penegakan hukum. Komputasi awan, atau komputasi berbasis Internet, menyediakan layanan informasi dan informasi melalui Internet, tanpa perlu perangkat keras atau perangkat lunak tertentu di titik akses fisik.⁴² Masalah ekstrateritorialitas mengambil dimensi baru dalam konteks komputasi awan karena tidak adanya perangkat keras yang terletak secara fisik dan lokasi data dapat melintasi batas nasional dan mungkin tidak diketahui oleh pengguna.⁴³

Isu ekstrateritorialitas menjadi kompleks karena dalam hukum internasional, terutama dalam kasus S.S. Lotus,⁴⁴ prinsip yang ditegaskan adalah suatu negara hanya dapat menjalankan yurisdiksinya di wilayahnya sendiri. Sebagaimana dinyatakan berikut: *"it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention."* Sebagaimana juga dijelaskan, namun, ada pengecualian terhadap prinsip tersebut yang diperbolehkan ketika didasari berdasarkan perjanjian internasional, kebiasaan hukum internasional, atau persetujuan dari negara yang terlibat, yang memungkinkan penerapan prinsip ekstrateritorialitas.⁴⁵

Dalam situasi saat ini, Indonesia masih belum mencapai tingkat perlindungan privasi yang optimal bagi masyarakatnya, terutama mengingat banyaknya kasus pelanggaran yang telah dijelaskan sebelumnya. Oleh karena itu, Indonesia memiliki peluang untuk memperkuat peraturan yang ada, meningkatkan pengawasan, dan mengembangkan kerja sama nasional dan internasional sebagai upaya untuk melindungi privasi warga negaranya lebih baik.

4. Kesimpulan

Berdasarkan penjelasan di atas, dapat disimpulkan bahwa Indonesia memiliki tanggung jawab, baik di tingkat nasional maupun internasional, untuk melindungi hak privasi masyarakatnya. Perlindungan terhadap hak privasi telah diatur dalam hukum internasional melalui perjanjian ICCPR yang telah diadopsi dan diimplementasikan dalam undang-undang Indonesia. Selain itu, hak privasi juga diperkuat oleh Pasal 28G ayat (1) UUD NRI 1945 serta diimplementasikan melalui beberapa peraturan perundang-undangan nasional.

Apabila kita melihat lebih dalam pada kerangka hukum di Indonesia, perlindungan privasi telah diatur dalam berbagai undang-undang, dan sanksi administratif atau pidana dapat diberlakukan jika terdapat pelanggaran. Namun, terdapat beberapa kekhawatiran terkait kelemahan dalam peraturan, pengawasan, dan penerapan yang menghambat

⁴¹ Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 15-16.

⁴² Kittichaisaree, *Public International Law of Cyberspace*, 32:26.

⁴³ Nancy J. King and V.T. Raja, "What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data," *American Business Law Journal* 50, no. 2 (June 2013): 418, <https://doi.org/10.1111/ablj.12012>.

⁴⁴ *France v. Turkey, The Case of the S.S. "Lotus,"* Judgment No, 9, PCIJ (ser A), 18-19 (Permanent Court of International Justice 1927).

⁴⁵ Candra Kresna Wijaya, "Tanggung Jawab Negara Terhadap Akibat Accidental Unilateral Transborder Access Melalui Government Hacking," 130.

efektivitas perlindungan privasi. Permasalahan ini belum sepenuhnya teratasi, terutama dengan kemajuan teknologi yang memungkinkan kegiatan di dunia maya menyeberangi batas negara, menciptakan isu ekstrateritorial. Meskipun demikian, ada potensi perbaikan melalui perketatan pengawasan dan kerja sama lintas negara untuk mengatasi masalah yang memiliki dampak ekstrateritorial. Dengan meningkatkan pengawasan dan kerja sama internasional, kita dapat lebih efektif dalam menjaga privasi masyarakat dalam lingkup yang semakin terbuka dan terhubung secara global.

Daftar Pustaka

- Abdul Wahid and Mohammad Labib. *Kejahatan Mayantara (Cyber Crime)*. Cet. 1. Bandung: Refika Aditama, 2005.
- Alex Hern. "Cambridge Analytica: How Did It Turn Clicks into Votes?" *The Guardian*, May 6, 2018. <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie>.
- BBC News Indonesia. "Ratusan Juta Data Dukcapil Kemendagri Diduga Bocor, Pakar Siber: 'Ini Peretasan Paling Parah.'" *BBC*, July 18, 2023. <https://www.bbc.com/indonesia/articles/c51v25916zlo>.
- Britannica, T. Editors of Encyclopaedia. "Phishing." *Encyclopedia Britannica*, August 8, 2023. <https://www.britannica.com/technology/phishing>.
- Bruno De padirac, ed. *The International Dimensions of Cyberspace Law*. Vol. 1. London: Routledge, Taylor & Francis Group : UNESCO Publishing, 2018.
- Budiardjo, Miriam. *Dasar-Dasar Ilmu Politik*. Cet. pert. rev. Jakarta: Gramedia Pustaka Utama, 2008.
- Candra Kresna Wijaya. "Tanggung Jawab Negara Terhadap Akibat Accidental Unilateral Transborder Access Melalui Government Hacking." Universitas Udayana, 2023.
- Chandra, Kent Revelino, and I Gusti Ngurah Parikesit Widiatedja. "Perang Rusia-Ukraina Dan Ancaman Terhadap Kebebasan Berpendapat Dan Berekspresi Di Rusia." *Jurnal Magister Hukum Udayana* 12, no. 2 (July 29, 2023): 402. <https://doi.org/10.24843/JMHU.2023.v12.i02.p12>.
- CNNIndonesia. "10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-Ramai Bantah." Desember 2022. <https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah/2>.
- Donnelly, Jack. *Universal Human Rights in Theory and Practice*. 2nd ed. Ithaca: Cornell University Press, 2003.
- — —. *Universal Human Rights in Theory and Practice*. 3rd ed. Ithaca: Cornell University Press, 2013.
- Effendi, A. Masyhur. *Dimensi/Dinamika Hak Asasi Manusia dalam Hukum Nasional dan Internasional*. Cet. 1. Jakarta: Ghalia Indonesia, 1994.
- France v. Turkey. The Case of the S.S. "Lotus," Judgment No, 9, PCIJ (ser A), (Permanent Court of International Justice 1927).
- Human Rights Committee. "The Right to Privacy in the Digital Age." UN Commission on Human Rights, June 30, 2014.
- I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, and I Nyoman Gede Sugiarta. "Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime)." *Jurnal Konstruksi Hukum* 1, no. 2 (October 28, 2020): 334-39.

- Ian Goldberg. "Privacy-Enhancing Technologies for the Internet III: Ten Years Later." In *Digital Privacy: Theory, Technologies, and Practices*, 470. New York: Auerbach Publications, 2008.
- Ida Ayu Agung Rasmi Wulan and Ni Luh Gede Astariyani. "Urgensi Dalam Meratifikasi Convention On Cybercrime Sebagai Pemenuhan HAM Di Indonesia." *Kertha Patrika* 45, no. 2 (August 30, 2023): 221–35. <https://doi.org/10.24843/KP.2023.v45.i02.p06>.
- Ilyas Fadilah. "Kilas Balik Aksi Bjorka Curi-Curi Data, Dijual Demi Cuan!" *Detikfinance*, January 11, 2023. <https://finance.detik.com/berita-ekonomi-bisnis/d-6508922/kilas-balik-aksi-bjorka-curi-curi-data-dijual-demi-cuan/2>.
- Indriana Firdaus. "Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan." *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia* 4, no. 2 (December 14, 2022): 23–31. <https://doi.org/10.52005/rechten.v4i2.98>.
- Jayawickrama, Nihal. *The Judicial Application of Human Rights Law: National, Regional and International Jurisprudence*. Second edition. Cambridge, United Kingdom New York Port Melbourne Delhi Singapore: Cambridge University Press, 2017.
- Joseph, Sarah, and Melissa Castan. *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary*. Third edition. Oxford, United Kingdom: Oxford University Press, 2013.
- Kent Revelino Chandra. "Perlindungan Hak Kebebasan Berpendapat Dan Berekspresi Berdasarkan Hukum Internasional Di Indonesia (Studi Kasus: Pembatasan Hak Kebebasann Berpendapat Dan Berekspresi Pada Putusan No.210/Pid.B/2020/PN.Amb. Mengenai Tindak Pidana Makar)." Universitas Udayana, 2023.
- King, Nancy J., and V.T. Raja. "What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data." *American Business Law Journal* 50, no. 2 (June 2013): 413–82. <https://doi.org/10.1111/ablj.12012>.
- Kittichaisaree, Kriangsak. *Public International Law of Cyberspace*. Vol. 32. Law, Governance and Technology Series. Cham: Springer International Publishing, 2017. <https://doi.org/10.1007/978-3-319-54657-5>.
- kumparanTECH. "Hacker Bjorka Klaim Curi 34 Juta Data Paspor Orang Indonesia." *Kumparan*, July 3, 2023. <https://kumparan.com/kumparantech/hacker-bjorka-klaim-curi-34-juta-data-paspor-orang-indonesia-20jaXTAD4VO/full>.
- Malcom D. Evans, *International Law Documents* (12th ed.). Oxford: Oxford University Press, 2015.
- Measuring Digital Developments: Facts and Figures 2022*. ITUPublications, 2022.
- Moeljatno, *Asas-asas Hukum Pidana*, Jakarta: Rineka Cipta, 2000.
- Muladi. *Demokratisasi, Hak Asasi Manusia, dan Reformasi Hukum di Indonesia*. Cet. 1. Jakarta: Habibie Center, 2002.
- Nicholas Confessore. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far." *The New York Times*, April 4, 2018. <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>.
- Nowak, Manfred. *U.N. Covenant on Civil and Political Rights: CCPR Commentary*. 2nd, rev. ed ed. Kehl: Engel, 2005.
- Personal Data: The Emergence of a New Asset Class*. World Economic Forum., 2011.
- Ronny Hanitijo Sumitro. *Metodologi Penelitian Hukum*. Jakarta: Ghalia Indonesia, 1994.

- Schabas, William A. *The Customary International Law of Human Rights*. 1st ed. Oxford University Press, 2021. <https://doi.org/10.1093/oso/9780192845696.001.0001>.
- Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Second edition. Cambridge, United Kingdom: Cambridge University Press, 2017.
- Smeulers, Alette, and Fred Grünfeld. *International Crimes and Other Gross Human Rights Violations*. Leiden: Martinus Nijhoff Publishers, 2011.
- Talya Uçaryılmaz, "The Principle of Good Faith In Public International Law", *Estudios De Deusto* 68, no. 1 (December, 2019).
- Tsagourias, Nicholas, and Russell Buchan, eds. *Research Handbook on International Law and Cyberspace*. United Kingdom: Edward Elgar Publishing, 2021. <https://doi.org/10.4337/9781789904253>.
- Tunkin, G. I. *Theory of International Law*. Cambridge, Mass: Harvard University Press, 1974.
- UN Human Rights Committee (HRC). "CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation." United Nations, April 8, 1988.
- — —. "Concluding Observations on the Seventh Periodic Report of Colombia." United Nations, 2016. U.N. Doc. CCPR/C/COL/CO/7.
- — —. "General Comment No. 31 [80], The Nature of the General Legal Obligation Imposed on States Parties to the Covenant." United Nations, May 26, 2004. CCPR/C/21/Rev.1/Add.13.
- United Nations General Assembly. "Report of the Secretary General 69/112: Developments in the Fields of Information and Telecommunications in the Context of International Security," 2014. <http://undocs.org/A/69/112>.
- — —. "Resolution Adopted by the General Assembly: The Rights to Privacy in the Digital Age," 2015. U.N. Doc. A/6/166.

Peraturan Perundang-Undangan

- Undang-Undang Dasar Negara Republik Indonesia 1945
- Undang-Undang Nomor 8 tahun 1992 tentang Perbankan, Lembaran Negara Republik Indonesia tahun 1992 nomor 31, Tambahan Lembaran Negara Republik Indonesia nomor 3473.
- Undang-undang nomor 10 tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 tahun 1992 tentang Perbankan, Lembaran Negara Republik Indonesia tahun 1998 nomor 182, Tambahan Lembaran Negara Republik Indonesia nomor 3790.
- Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi, Lembaran Negara Republik Indonesia tahun 1999 nomor 154, Tambahan Lembaran Negara Republik Indonesia nomor 3881.
- Undang-Undang Nomor 12 tahun 2005 tentang Pengesahan International Covenant on Civil and Political Rights (Kovenan Internasional tentang Hak-Hak Sipil dan Politik), Lembaran Negara Republik Indonesia tahun 2005 nomor 119, Tambahan Lembaran Negara Republik Indonesia nomor 4558.
- Undang-Undang Nomor 23 tahun 2006 tentang Administrasi Kependudukan, Lembaran Negara Republik Indonesia tahun 2006 nomor 124, Tambahan Lembaran Negara Republik Indonesia nomor 4674.
- Undang-Undang Nomor 24 tahun 2013 tentang perubahan atas Undang-Undang Nomor 23 tahun 2006 tentang Administrasi Kependudukan, Lembaran Negara Republik Indonesia tahun 2013 nomor 232, Tambahan Lembaran Negara Republik Indonesia nomor 5475.

- Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia tahun 2008 nomor 58, Tambahan Lembaran Negara Republik Indonesia nomor 4843.
- Undang-Undang Nomor 19 tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia tahun 2016 nomor 251, Tambahan Lembaran Negara Republik Indonesia nomor 5952.
- Undang-Undang Nomor 43 tahun 2009 tentang Kearsipan, Lembaran Negara Republik Indonesia tahun 2009 nomor 152, Tambahan Lembaran Negara Republik Indonesia nomor 5071.
- Undang-Undang Nomor 14 tahun 2008 tentang Keterbukaan Informasi Publik, Lembaran Negara Republik Indonesia tahun 2008 nomor 61, Tambahan Lembaran Negara Republik Indonesia nomor 4846.
- Undang-undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi, Lembaran Negara Republik Indonesia tahun 2022 nomor 196, Tambahan Lembaran Negara Republik Indonesia nomor 6820.
- Undang-Undang Nomor 17 tahun 2023 tentang Kesehatan, Lembaran Negara Republik Indonesia tahun 2023 nomor 105, Tambahan Lembaran Negara Republik Indonesia nomor 6887.