Jurnal Ilmu Hukum "THE JURIS" Vol. VIII, No. 2, Desember 2024
ISSN 2580-0299, e-ISSN 2580-8370
http://ejournal.stih-awanglong.ac.id/index.php/juris

PERLINDUNGAN TERHADAP DATA PRIBADI DALAM BERSELANCAR DI DUNIA MAYA

Johan Wijaya[1*], Aji Titin Roswitha Nursanthy[2], Muhammad Arganata Thamrin[3]
[1.2,3]Sekolah Tinggi Ilmu Hukum Awang Long, Samarinda, Indonesia
jwijaya07@gmail.com, withaayu77@yahoo.co.id, arga@stih-awanglong.ac.id

Abstract

Cyberspace is an electronic medium connected through a computer network, used for online communication. Cyberspace is an integration of various communication technology tools and computer networks that connect communication devices across the globe. Cyberspace has transformed the way people live, work, and interact with one another. Examples of cyberspace include online gaming platforms and social networks. This research addresses the issue of protecting personal data while navigating cyberspace. It is a library research study based on a literature review. In this paper, the author employs a normative juridical approach. Due to its methodology, this type of legal research is referred to as normative legal research. Legal provisions serve as the primary legal materials, particularly Law Number 27 of 2022 on Personal Data Protection (PDP Law). The PDP Law aims to guarantee citizens' rights to personal protection and to raise public awareness of the importance of personal data protection. This study also refers to the Electronic Information and Transactions Law (ITE Law) and its amendments. Article 26, paragraph (1) of Law Number 19/2016 stipulates that the use of personal information through electronic media must be carried out with the consent of the concerned individual. Additionally, the 1945 Constitution of the Republic of Indonesia (UUD NRI 1945) is referenced. Article 28G, paragraph (1) of the 1945 UUD NRI states that everyone has the right to the protection of themselves, their family, their honor, their dignity, and their property.

Keywords: *Personal data protection; cyberspace; ITE Law*

✉Alamat korespondensi:
Program Sarjana Strata 1Ilmu Hukum, Sekolah Tinggi Ilmu Hukum Awang Long, Samarinda, Indonesia
E-mail : jwijaya07@gmail.com

I. PENDAHULUAN

Seiring pesatnya perkembangan teknologi informasi dan komunikasi, data pribadi menjadi aset atau komoditas bernilai tinggi di era *big data* dan ekonomi digital. Konsekuensinya, data pribadi merupakan hak yang harus dilindungi, sebagai bagian dari Hak Asasi Manusia (HAM) dan amanat yang disampaikan oleh konstitusi Negara Republik Indonesia serta Undang-Undang Dasar 1945.

Data Pribadi adalah 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. Data pribadi, dalam Undang Undang Perlindungan Data Diri (UU PDP) Nomor 27 Tahun 2022, setiap data tentang seseorang, baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya, baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik. Adapun data diri pribadi terdiri dari: Nama lengkap, tempat dan tanggal lahir (kota, tanggal, bulan, tahun), alamat lengkap (jalan, nomor, desa, kecamatan, kabupaten, provinsi, negara, kode pos), jenis kelamin, agama, nomor telepon, email, berat dan tinggi badan (opsional).

Data Pribadi Berdasarkan Fungsi:

1. Identitas Pribadi: Termasuk nama lengkap, alamat, tanggal lahir, nomor identifikasi nasional atau paspor.
2. Data Keuangan: Informasi seperti nomor rekening bank, kartu kredit, atau rincian transaksi keuangan.
3. Informasi Kesehatan: Catatan medis, riwayat kesehatan, dan informasi lain yang berkaitan dengan kondisi medis seseorang.
4. Data Biometrik: Data yang dihasilkan dari pengukuran biologis manusia, seperti sidik jari, iris mata, atau wajah.

Data Pribadi Berdasarkan Undang-Undang

Indonesia telah mengatur data pribadi di dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Berdasarkan UU PDP, jenis-jenis data pribadi dikategorikan menjadi dua, yaitu:

1. Data Pribadi Umum
   Data Pribadi Umum adalah informasi yang secara langsung maupun tidak langsung terkait dengan identitas seseorang yang dapat diidentifikasi, seperti: nama lengkap, nomor telepon, alamat email, nomor KTP, tempat dan tanggal lahir, jenis kelamin, pekerjaan, pendidikan, agama, status perkawinan, foto/video.
2. Data Pribadi Spesifik
   Data Pribadi Spesifik adalah informasi yang secara langsung maupun tidak langsung terkait dengan identitas seseorang yang bersifat sensitif dan/atau rahasia, seperti: riwayat kesehatan, riwayat keuangan, kehidupan seksual, keanggotaan organisasi politik, kepercayaan agama, keyakinan politik, catatan criminal, data biometric, data genetic.
   Penting untuk diketahui bahwa UU PDP juga mengatur kategori lain, yaitu Data Pribadi Anak.
3. Data Pribadi Anak meliputi: nama anak dan orang tua, alamat rumah dan sekolah, nomor telepon anak dan orang tua, foto/video anak, riwayat kesehatan anak, nilai akademik anak.

Kasus kejahatan yang marak terjadi dunia maya saat ini, dimana data pribadi disalahgunakan untuk pembobolan rekening Bank, pembobolan kartu pra bayar, penipuan berkedok cinta (love scammer), pencabulan, pelecehan seksual. Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 juga menjamin hak warga negara atas perlindungan pribadi, meningkatkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan terhadap pentingnya perlindungan data pribadi. Dari kasus diatas yang menjadi pertanyaan adalah

efektifitas UU Perlindungan Data Pribadi terhadap perlindungan data pribadi dan apakah dengan adanya UU Perlindungan Data Pribadi ini dapat mengurangi angka kebocoran data pada pengguna jejaring sosial. Oleh karena itu, berdasarkan permasalahan yang telah diuraikan di atas, penulis ingin melakukan penelitian lebih lanjut mengenai perlindungan data pribadi dalam berselancar didunia maya.

II. METODE PENELITIAN

Dalam tulisan ini penulis menggunakan pendekatan yuridis normatif, karena pendekatannya maka penelitian hukum model ini disebut dengan penelitian hukum normatif. Dalam hal ini, penulis juga memakai dua pendekatan yaitu pendekatan perundang-undangan dan pendekatan konseptual. Pendekatan perundang-undangan merupakan pendekatan dengan melakukan telaah terhadap peraturan perundang undangan, peraturan, dan kebijakan yang relevan dengan isu dalam penelitian ini. Sedangkan, pendekatan konseptual merupakan pendekatan yang beranjak dari pandangan atau doktrin yang berkembang di dalam ilmu hukum. Pendekatan ini digunakan untuk mencermati dan melakukan kajian.

Dalam tulisan ini penulis menggunakan pendekatan yuridis normatif, karena pendekatannya maka penelitian hukum model ini disebut dengan penelitian hukum normative. Ketentuan-ketentuan hukum merupakan bahan hukum primer Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU PDP ini bertujuan untuk menjamin hak warga negara atas perlindungan diri pribadi, serta menumbuhkan kesadaran masyarakat akan pentingnya perlindungan data pribadi. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan perubahannya. Pasal 26 ayat (1) UU 19/2016 mengatur bahwa penggunaan informasi pribadi melalui media elektronik harus dilakukan dengan persetujuan orang yang bersangkutan. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945). Pasal 28G ayat (1) UUD NRI 1945 menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda.

Penulis menggunakan metode library research atau kajian pustaka. Riset kajian kepustakaan ini adalah melakukan penelitian dari buku-buku perpustakaan, majalah, jurnal dan artikel dan sumber dari internet yang relevan dengan masalah yang dibahas. Sedangkan, bahan hukum sekunder adalah bahan hukum yang dapat mendukung bahan hukum primer. Contohnya kepustakaan yang ada hubunganya dengan penelitian tentang pasal menguntungkan terpidana, dan upaya hukum pidana di Indonesia. Maka dari itu, metode pengumpulan bahan hukum dalam penelitian akan mencari peraturan perundang-undangan yang berkaitan dengan isu hukum dalam penelitian ini, kemudian mencari bahan hukum lain berupa hasil penelitian, jurnal, buku, kamus dan literatur lainya yang berkaitan dengan isu penelitian, kemudian diklasifikasi dan dianalisis yang selanjutnya dituangkan dalam penulisan.

III. HASIL DAN PEMBAHASAN

Perlindungan data pribadi merupakan salah satu hak asasi manusia yang merupakan bagian dari perlindungan diri pribadi. Perlindungan diri pribadi ini tercantum dalam Pasal 28G UUD 1945. Perlindungan diri pribadi atau privasi ini bersifat universal, dalam arti diakui banyak negara. Industri 4.0 telah mendorong perkembangan dunia digital di Indonesia. Hingga saat ini, data Hootsuite (We are Social) 2022 menunjukkan 204,7 juta penduduk Indonesia menggunakan internet dan 93,5 persen di antaranya aktif sebagai pengguna media sosial. Perkembangan dunia digital juga melahirkan beberapa budaya dan perilaku baru, mulai mengunggah apa pun hingga transaksi online. Kondisi tersebut belum diikuti kesadaran masyarakat dan pemerintah untuk melindungi data pribadi. Padahal, pengungkapan data pribadi tanpa kendali terbukti menimbulkan banyak risiko beragam tindak kriminalitas. Perundungan, ancaman, penipuan, hingga pembobolan akun menjadi hal yang tidak terhindarkan. Yang paling baru adalah peretas Bjorka yang mengaku telah memiliki data pribadi milik warga Indonesia, termasuk beberapa pejabat publik.

Kasus penyalahgunaan data pribadi juga terjadi pada proses pinjaman online yang menggunakan data milik orang lain, penyalinan data dan informasi ATM (skimming), hingga penyebarluasan informasi pribadi kepada publik, dimana hal seperti ini termasuk pelanggaran hak privasi yang terjadi di dunia digital. Saat ini, regulasi hukum yang menyinggung terkait dengan hak

privasi pemilik data digital terdapat dalam Pasal 26 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang -Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang menyebutkan "*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.*

Beberapa kasus hukum yang berkaitan dengan perlindungan data pribadi yang pernah terjadi di Indonesia, antara lain:

1. Penjualan data peserta BPJS di Raid Forums pada Mei 2021. Data yang dijual meliputi NIK, nama, alamat, nomor telepon, dan data BPJS Kesehatan. Kebocoran yang terjadi pada 12 Maret 2023 lalu itu diperkirakan membobol sebanyak 19,56 juta data yang kemudian di jual di situs dark web. Kasus ini pertama kali diketahui setelah hacker bernama Bjorka di Breach Forums mengunggah konten dengan deskripsi "BPJS Ketenagakerjaan Indonesia 19 Million." Biar ada yang tertarik, Bjorka membagikan 100.000 contoh data pengguna yang berisi informasi pribadi seperti Nomor Induk Kependudukan (NIK), nama lengkap, dan alamat. Bjorka menjual 19 juta data tersebut sebesar US$10.000 atau setara Rp154 juta.
2. Pada Mei 2023 kemarin, Bank Syariah Indonesia (BSI) menjadi 641ensi pembicaraan setelah menjadi korban ransomware atau serangan siber dengan modus pemerasan yang dilakukan oleh Lockbit atau kelompok hacker. Pihak Lockbit meminta tebusan sebesar US$20 juta atau setara Rp309 miliar untuk mengembalikan data sebesar 1,5 TB yang berisi 15 juta data pribadi pengguna, termasuk kata sandi, data karyawan, dan dokumen legal. Namun pihak BSI hanya 641ens memberikan penawaran sebesar US$10 juta atau setara Rp154 miliar.
3. Kasus bocornya data kembali menjadi sorotan pada Juni 2023. Kali ini, Bjorka, yang seringkali terlibat dalam insiden serupa di Indonesia, kembali menjadi pelakunya. Hacker yang mengklaim berasal dari Polandia ini mempublikasikan data tersebut di forum gelap Breach Forums, yang telah berhasil mengakses 35 juta data pengguna My IndiHome dan menawarkannya dengan harga US$ 5.000 atau sekitar Rp 77 juta. My Indihome menolak berita ini.
4. Bjorka kembali menjadi sorotan setelah diduga membocorkan data paspor sebanyak 34,9 juta milik Warga Negara Indonesia (WNI) pada tanggal 5 Juli 2023. Data yang berisi informasi pribadi terkait paspor itu dijual di situs gelap dengan harga US$ 10.000, atau sekitar Rp 154 juta.
5. Pada tanggal 16 Juli 2023, kembali ada insiden kebocoran data yang mencakup sebanyak 337 juta data di Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil) Kementerian Dalam Negeri. Data yang terbocor ini mengandung informasi personal yang lengkap, termasuk NIK hingga nomor akta lahir atau pernikahan. Tetapi pihak Dukcapil menolak berita ini.
6. Komisi Pemilihan Umum (KPU) menjadi korban serangan siber sebanyak dua kali. Kasus pertama terjadi pada September 2022, peretas bernama Bjorka mengklaim telah mengakses 105 juta data pemilih dari website KPU. Kasus kedua terjadi pada Selasa, 28 November 2023, oleh peretas Jimbo mengklaim telah mengakses data pemilih tetap (DPT) dari situs KPU. Jimbo mempublikasikan 500.000 sampel data yang diretas di forum online Breach Forums.
7. Pada bulan September 2022, peretas dunia ini kembali mencuri 1,3 miliar data kartu SIM Card yang dijual di forum breached.to. Melalui situs itu, Bjorka mengaku memiliki 87 GB data yang berisi Nomor Induk Kependudukan (NIK), nomor telepon, dan tanggal registrasi.
8. Pada Januari 2022, terjadi kebocoran data yang mengincar data-data medis rumah sakit di Indonesia.Data 641ensitive itu diketahui dijual di forum online bernama Raidforums oleh akun bernama GOD User.Dalam postingannya tersebut, dia mengaku memiliki 720 GB data yang diambil dari server Kementerian Kesehatan dan BPJS Kesehatan.
9. Di bulan yang sama seperti data medis, grup ransomware Conti berhasil mencuri 228 GB data yang diambil dari Bank Indonesia.Kebocoran ini tentu menjadi viral, sebab bank sentral utama Indonesia yang seharusnya memiliki 641ensit keamanan paling baik, ternyata 641ens diretas oleh hacker.Kepala Departemen Komunikasi BI, Erwin Haryono menjelaskan bahwa benar adanya upaya berupa serangan ransomware. Tapi dia mengaku tidak ada data yang diretas dalam aksi tersebut.
10. Kasus kebocoran data di Indonesia terakhir terjadi kepada Jasa Marga. Insiden kebocoran yang terjadi pada Agustus 2022 lalu itu dilakukan oleh hacker bernama Desorden.Setelah memiliki

sekitar 252 GB data pelanggan, perusahaan, dan karyawan, Desorden memasarkan data-data tersebut di breached.to.

Kebocoran data termasuk kejahatan dunia maya atau cyber crime. Kebocoran data adalah ketika data sensitif yang seharusnya disimpan secara aman dan rahasia bocor ke tangan yang salah. Data yang bocor bisa berupa informasi pribadi, bisnis, atau organisasi. Kebocoran data bisa terjadi secara elektronik, seperti melalui email atau internet, atau secara fisik, seperti melalui perangkat penyimpanan atau laptop. Kebocoran data bisa berdampak besar dan merugikan bagi korban, baik perorangan maupun perusahaan.

Tindak pidana cyber merupakan salah satu kejahatan transnasional dimana kejahatan ini terjadi tanpa batas, dalam hal ini akan terdapat permasalahan terkait dengan yurisdiksi suatu negara dalam hal menegakan hukum apabila terjadi kejahatan siber. Negara Indonesia telah memiliki payung hukum terkiat peraturan perundang-undangan yang khusus mengatur mengenai kejahatan siber dan didalamnya termuat aturan mengenai yurisdiksi yang telah memiliki asas universal yaitu Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Undang-Undang ITE) Hal ini dapat dilihat dalam Pasal 2 Undang-Undang ITE yang menyebutkan bahwa : "Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia. Undang-undang ini memiliki jangkauan yurisdiksi yang sangat luas, pada pokoknya menjelaskan mengenai bahwa Undang-Undang ITE mengatur mengenai perbuatan hukum yang dilakukan di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga dapat berlaku untuk perbuatan hukum yang dilakukan diluar wilayah negara Indonesia dan/atau dilkukan oleh warga negara Indonesia maupun warga negara asing yang memiliki akibat hukum di wilayah negara Indonesia dengan menimbulkan kerugian. Yang dimaksud dengan merugikan meliputi tetapi tidak terbatas pada kepentingan ekonomi nasioanl, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamnan negara, kedaulatan negara, warga negara serta badan hukum Indonesia.

Pihak yang menyimpan data, seperti perusahaan atau pemerintah, memiliki kewajiban untuk transparan dalam penggunaan data, mendapatkan izin pemilik sebelum memproses data, dan menjaga keamanan data agar terhindar dari kebocoran. Perlindungan data pribadi adalah hal yang krusial untuk menjaga kepercayaan masyarakat terhadap penggunaan teknologi dan layanan digital. Berikut beberapa alasan pentingnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).

1. Mencegah Penyalahgunaan Data: Dengan adanya UU PDP, kasus penyalahgunaan data pribadi dapat diminimalisir. Contohnya, penggunaan data pribadi untuk keperluan ilegal seperti pencurian identitas atau penipuan dapat dicegah.
2. Meningkatkan Keamanan dan Privasi Individu: UU PDP memastikan bahwa data pribadi dilindungi dengan baik, sehingga memberikan rasa aman bagi individu atas informasi pribadi mereka.
3. Mematuhi Standar Internasional: Menyesuaikan regulasi Indonesia dengan standar perlindungan data pribadi internasional, seperti General Data Protection Regulation (GDPR) di Uni Eropa.
4. Perlindungan Hak Asasi Manusia: Hak atas privasi adalah bagian dari hak asasi manusia. UU PDP melindungi hak ini dengan mencegah penyalahgunaan data pribadi oleh pihak yang tidak bertanggung jawab.

Dalam Penerapan UU PDP ini, pemerintah berharap dapat meminimalisir insiden kebocoran data yang selama ini kerap menghantui berbagai perusahaan teknologi di Indonesia. Keamanan siber telah menjadi isu global, dan Indonesia tidak luput dari ancaman tersebut. Kasus kebocoran data di Indonesia, mulai dari sektor perbankan hingga platform digital, telah menimbulkan kekhawatiran besar di kalangan masyarakat. UU PDP mencakup berbagai aspek penting yang sebelumnya diabaikan dalam regulasi terkait data di Indonesia. Undang-undang ini mengatur segala sesuatu mulai dari bagaimana data dikumpulkan, disimpan, diproses, hingga dihapus. UU PDP memberikan hak kepada individu untuk meminta akses, koreksi, dan bahkan penghapusan data pribadi mereka jika dirasa perlu.

Pasal 1 poin 2, UU UDP menyatakan pelindungan data pribadi sebagai seluruh upaya untuk melindungi data dalam rangkaian pemrosesan data pribadi untuk menjamin hak konstitusional subjek data pribadi, serta mengatur bagaimana data tersebut akan diberikan dan digunakan oleh pihak lain. Pada Pasal 4, UU UDP secara lebih rinci disebutkan tentang Jenis Data Pribadi.

Jenis data pribadi

- UU PDP membagi data pribadi menjadi dua jenis, yaitu data pribadi umum dan data pribadi spesifik. Data pribadi umum boleh digunakan secara umum, seperti nama, alamat, status, agama, nomor telepon dan lainnya. Untuk data pribadi spesifik adalah data yang sensitif, seperti data kesehatan, data biometrika, atau catatan kriminal.

Hak pemilik data

1. Salah satu hal penting dalam UU PDP adalah hak pemilik data. Setiap individu berhak mengetahui bagaimana data mereka digunakan, siapa yang menggunakannya, memperbaiki data atau menolak penggunaan data, dan dapat meminta penghapusan data jika diperlukan. Konsep ini ini memberikan hak penuh kepada pemilik data terhadap penggunaan informasi pribadi mereka.

Peran pengelola data

1. UU PDP juga mengatur kewajiban pihak yang mengelola data pribadi, seperti perusahaan atau lembaga. Mereka harus memastikan data yang telah disimpan tetap aman, bertanggungjawab atas penggunaan data, dan tidak disebarluaskan tanpa izin pemilik. Jika kebocoran data, pengelola data wajib memberi tahu informasi tersebut atau memungkinkan dapat dikenakan sanksi hukum, termasuk denda besar atau hukuman pidana.

Verifikasi data pribadi adalah proses untuk memastikan bahwa data yang disimpan atau digunakan adalah milik individu yang sah. Proses ini penting untuk melindungi data pribadi dari pencurian, penipuan, dan akses tidak sah ke informasi pribadi. Ada beberapa metode verifikasi yang dapat digunakan untuk mengamankan data pribadi, yaitu:

1. Verifikasi Email dan Telepon. Metode verifikasi ini melibatkan pengiriman kode verifikasi atau kode OTP ke alamat email maupun nomor telepon yang terdaftar. Pengguna kemudian harus memasukkan kode ini ke dalam sistem (aplikasi atau website) untuk mengonfirmasi identitas mereka.
2. Verifikasi Dua Faktor (2FA). Verifikasi dua faktor adalah langkah menambahkan lapisan keamanan ekstra dengan memasukkan kode verifikasi setelah pengguna memasukkan kata sandi mereka. Verifikasi 2FA bisa dikirim melalui SMS, WA, email, atau aplikasi autentikasi.
3. Verifikasi Biometri. Verifikasi biometrik adalah salah satu cara paling aman untuk melindungi data pribadi. Metode ini menggunakan karakteristik unik individu seperti sidik jari atau wajah untuk memverifikasi identitas. Karena karakteristik biometrik sulit dipalsukan dan kemungkinan hanya dimiliki oleh satu orang di dunia, saat ini verifikasi biometrik dianggap memiliki tingkat keamanan tertinggi.

Setelah memahami apa itu data pribadi dan jenis-jenisnya, maka penting untuk mengetahui cara melindungi data pribadi agar terhindar dari ancaman di dunia maya, adalah:

1. Enkripsi Data, pastikan data pribadi disimpan dalam format terenkripsi untuk meningkatkan keamanan dan mencegah akses yang tidak sah.
2. Waspadai WiFi Publik, hati-hati saat menggunakan Wifi, karena sering kali jaringannya telah diretas untuk mencuri informasi pribadi pengguna.
3. Hindari Mengklik Tautan Mencurigakan, jangan mengklik tautan yang mencurigakan, baik dari nomor yang dikenal maupun tidak dikenal, karena ini menjadi serangan phishing yang memungkinkan pencurian data pribadi.
4. Hindari Membagikan Data Pribadi di Media Sosial, berhati-hati saat membagikan data pribadi di media 643ensit, seperti nomor KTP, kartu kredit, atau informasi pribadi lainnya yang dapat digunakan untuk membobol data sensitive lainnya.
5. Hindari Aplikasi Palsu, unduh aplikasi hanya dari sumber terpercaya untuk menghindari aplikasi berbahaya yang dapat membocorkan data pribadi. Jangan sembarangan mengunduh aplikasi dari website tidak resmi hanya karena ingin menghindari biaya aplikasi resmi.

Kemunculan UU PDP, sebaiknya harus diikuti dengan peningkatan edukasi literasi digital pada masyarakat soal pentingnya menjaga data pribadi. Tingkat literasi digital masyarakat Indonesia masih sangat rendah. Perlu sosialisasi dari pemerintah untuk menghimbau agar warga masyarakat

melindungi datanya, mencegah berbagai kebocoran data pribadi yang dipegang badan publik dalam beberapa tahun terakhir sehingga badan publik sebagai pemangku kepentingan untuk ditingkatkan kesadarannya dalam perlindungan data,

IV. KESIMPULAN

Setelah membaca uraian diatas maka dapat disimpulkan bahwa Perlindungan data pribadi merupakan salah satu hak asasi manusia yang merupakan bagian dari perlindungan diri pribadi. Perlindungan diri pribadi ini tercantum dalam Pasal 28G UUD 1945. Perlindungan diri pribadi atau privasi ini bersifat universal, dalam arti diakui banyak negara.Industri 4.0 telah mendorong perkembangan dunia digital di Indonesia.. Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) diharapkan menjadi payung hukum yang kuat bagi tata kelola dan perlindungan data personal warga negara dan para penyelenggara pemerintahan.khususnya data kependudukan. UU ini berfungsi untuk menjamin hak warga negara atas perlindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya perlindungan data pribadi.

REFERENSI

Ayu Media Kusnadi, S., & Wijaya, A. U. (n.d.). Perlindungan hukum pribadi sebagai hak pribadi. *Jurnal Al-Wasath, 2*(1), 19-32.

Bayu Indra Pratama. (2017, January). *Etnografi dunia maya*. UB Press.

CSA, Lesmana, T., Elis, E., & Hamimah, S. (2022). Urgensi undang-undang perlindungan data pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak atas privasi masyarakat Indonesia. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia, 3*(2).

Hanifan, N. (2020). Perlindungan data pribadi sebagai bagian hak asasi manusia atas perlindungan diri pribadi: Suatu tinjauan komparatif dengan peraturan perundang-undangan di negara lain. *Selisik, 6*(1), 2685-6816.

Hidayatullah Arham, M. R., & Risal, M. C. (2023). Perlindungan data pribadi bagi pengguna media sosial. *Jurnal Al Tasyri'iyyah, 3*(2).

https://indonesia.go.id//kategori/editorial/8725/era-baru-perlindungan-data-pribadi?lang=1?lang=1. Diakses pada 31 Desember 2024.

https://vida.id/id/blog/tag/cybersecurity. Diakses pada 26 Desember 2024.

https://www.inilah.com/kasus-kebocoran-data-di-indonesia. Diakses pada 26 Desember 2024.

Maruli Situmeang, S. (2020, November). *Cyber law*. CV. Cakra.

Moh Hamzah, H. (2021). Urgensi rancangan undang-undang (RUU) perlindungan data pribadi. *Jurnal Hukum Unissula, 37*(2), 119-133.

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

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).