Jurnal Serina Abdimas
Vol. 1, No. 1, Feb 2023: hlm 157-165 ISSN-L 2986-6065 (Versi Elektronik)

SOSIALISASI PERLINDUNGAN DATA PRIBADI BAGI MASYARAKAT KABUPATEN INDRAMAYU

Moody R. Syailendra[1], Samantha Elizabeth Fitzgerald[2] & Malvin Santoso[3]
[1]Fakultas Hukum, Universitas Tarumanagara Jakarta
Email: moodys@fh.untar.ac.id
[2]Program Studi Sarjana Hukum, Universitas Tarumanagara Jakarta
Email: samelizabethf@gmail.com
[3]Program Studi Sarjana Hukum, Universitas Tarumanagara Jakarta
Email: malvinsantoso39@gmail.com

ABSTRACT

From the various cases of personal data leakage that have occurred, the urgency of efforts to protect one's self from cyber threats is very clear. In the framework of the Indonesian constitution itself, in 2022 a legal basis was promulgated in the form of Law Number 27 of 2022 concerning the Protection of Personal Data (UU PDP). The existence of the PDP Law is important to be socialized to the public, so the authors/researchers of this scientific work are interested in conducting legal counseling and reviewing the effectiveness as well as changes that arise from its existence. The research method applied is normative and empirical legal methods. Normative legal research is carried out by means of conducting literature study towards primary and secondary legal materials, whereas empirical legal research is carried out by conducting legal counseling at the Regional Secretariat Office of Indramayu Regency in West Java. The counseling begins with a presentation session on material related to personal data protection which is followed by an interactive discussion with the audience. The approach used in this research is a sociological juridical and legislation approach. The results obtained are insights related to the PDP Law, such as the rights of the community as personal data owners and sanctions related to criminal acts against a person's personal data. The Indonesian government has issued a legal basis that prioritizes cyber security for all Indonesian people, especially in the realm of personal data protection, namely Law Number 27 of 2022 concerning Personal Data Protection. On the other hand, the public needs to prioritize the principles of prudence, selectivity, and discretion in protecting personal data. Thus, active participation from all walks of life in Indonesia in the form of repressive and preventive measures will increase the security of Indonesia's digital ecosystem.

***Keywords**: Law, Protection, Data, Privacy*

ABSTRAK

Dari berbagai kasus kebocoran data pribadi yang sudah terjadi, urgensi terkait upaya-upaya untuk melindungi diri seseorang dari ancaman-ancaman siber sudah sangat jelas. Dalam tatanan konstitusi Indonesia sendiri, pada tahun 2022 sudah diundangkan dasar hukum berupa Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Eksistensi UU PDP penting untuk disosialisasikan kepada masyarakat, sehingga penulis tertarik untuk melakukan penyuluhan hukum dan mengkaji efektivitas serta perubahan yang timbul dari keberadaannya. Metode penelitian yang diterapkan adalah metode hukum normatif dan empiris. Penelitian hukum normatif dilakukan dengan studi pustaka terhadap bahan hukum primer dan sekunder, sedangkan penelitian hukum empiris dilakukan dengan melaksanakan penyuluhan hukum di Kantor Sekretariat Daerah Kabupaten Indramayu. Penyuluhan diawali dengan sesi pemaparan materi terkait perlindungan data pribadi yang dilanjut dengan sesi diskusi bersama para hadirin. Pendekatan yang digunakan dalam penelitian ini merupakan pendekatan peraturan perundang-undangan dan yuridis sosiologis. Hasil yang diperoleh merupakan wawasan terkait UU PDP, seperti hak-hak masyarakat sebagai pemilik data pribadi dan sanksi-sanksi yang berkenaan dengan tindak pidana terhadap data pribadi seseorang. Pemerintah Indonesia sudah mengeluarkan dasar hukum yang mengedepankan keamanan siber bagi seluruh rakyat Indonesia, khususnya dalam ranah perlindungan data pribadi, yaitu dengan Undang Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Di sisi lain, masyarakat perlu mengutamakan prinsip kehati-hatian, keselektifan, dan kebijaksanaan dalam melindungi data pribadi. Dengan demikian, adanya partisipasi aktif dari seluruh kalangan di Indonesia dalam bentuk tindakan represif sekaligus preventif akan meningkatkan keamanan ekosistem digital Indonesia.

Kata kunci: Undang-Undang, Perlindungan, Data, Pribadi

1. PENDAHULUAN

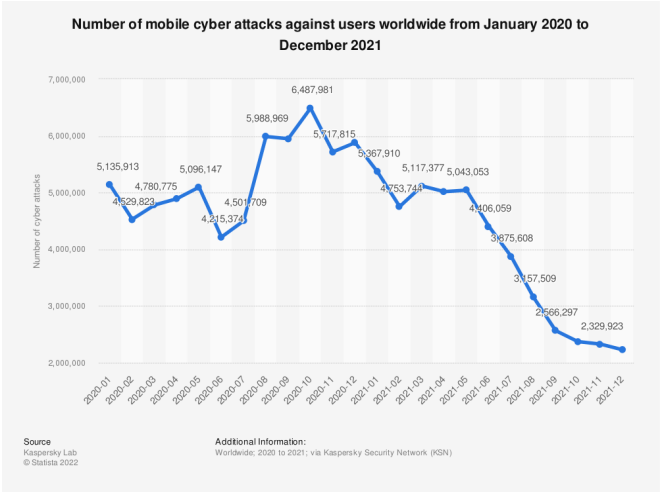
Digitalisasi pada zaman ini bukan suatu hal asing di telinga kita semua. Digitalisasi sudah menjadi suatu bagian dari realita masyarakat di mana ada berbagai informasi yang bisa kita akses dan cari tahu melalui berbagai platform secara daring. Sewaktu kita masuk ke pembahasan terkait digitalisasi maka kita tidak akan lepas dari yang namanya data pribadi. Pada umumnya, saat kita mengakses suatu situs web atau mencoba *login* ke dalam aplikasi, penyedia layanan tersebut akan meminta data pribadi kita agar bisa mengakses layanan mereka. Data-data yang diminta di antaranya seperti nama, alamat, tempat dan tanggal lahir, nomor telepon, email dan lain sebagainya. Dengan adanya pemberian data kepada pihak-pihak ketiga maka muncul potensi terjadinya *cybercrime*.

Cybercrime merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia internasional (Barda Nawawi Arief, 2006). *Cybercrime* atau kejahatan dunia maya adalah jenis kejahatan yang terkait dengan penggunaan teknologi informasi sehingga memiliki karakteristik tidak dibatasi. *Cybercrime* meliputi seluruh tindak pidana yang berasosiasi dengan sistem informasi, sistem informasi (*information system*) itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi kepada pihak lainnya (*transmitter/originator to recipient*) (Dikdik M. Arief Mansur dan Elisatris Gultom, 2005). Dengan demikian, *cybercrime* berhubungan dengan tingkat keamanan dan keabsahan informasi yang dikirimkan dan diakses oleh konsumen internet.

Cybercrime dapat terjadi dalam berbagai bentuk, salah satunya secara khusus merupakan *"infringements of privacy"* atau invasi/pelanggaran privasi. Invasi privasi merupakan kejahatan terhadap informasi seorang individu yang merupakan hal yang sangat personal dan rahasia (Maskun, 2013). Kejahatan ini biasanya ditujukan terhadap informasi pengenal pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara komputerisasi, yang apabila diketahui oleh orang lain, maka dapat merugikan orang secara materiil maupun immateriil, seperti nomor kartu kredit, nomor PIN ATM, keterangan tentang cacat atau penyakit tersembunyi, dan sebagainya (Maskun, 2013). Data dari Kaspersky Lab memaparkan jumlah serangan siber yang terjadi di seluruh dunia pada tahun 2020-2021.

Gambar 1

Grafik Jumlah Serangan Siber Seluler terhadap Pengguna di Seluruh Dunia dari Januari 2020 - Desember 2021



Dengan demikian, urgensi terkait upaya-upaya untuk melindungi diri seseorang dari ancaman-ancaman siber sudah sangat jelas. Dalam tatanan konstitusi Indonesia sendiri, pada tahun 2022 sudah diundangkan dasar hukum berupa Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang-undang ini merupakan langkah afirmatif yang

https://doi.org/10.24912/jsa.v1i1.23845

mendukung keamanan siber di Indonesia sebab terdapat hal-hal yang belum tercakup dalam perangkat hukum yang telah tersedia berkenaan dengan perlindungan data pribadi sebelum adanya UU PDP, yaitu:

a. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE);
b. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE);
c. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik;

Contohnya secara lebih spesifik terdapat dalam Pasal 27 Ayat (1) UU ITE,

"Setiap Orang 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."

Dari pasal tersebut, diuraikan dalam bagian penjelasan bahwa,

a. "Mendistribusikan" adalah mengirimkan dan/atau menyebarkan informasi elektronik dan/ atau dokumen elektronik kepada banyak orang atau berbagai pihak melalui sistem elektronik;
b. "Mentransmisikan" adalah mengirimkan informasi elektronik dan/ atau dokumen elektronik yang ditujukan kepada satu pihak lain melalui sistem elektronik;
c. "Membuat dapat diakses" adalah semua perbuatan lain selain mendistribusikan dan mentransmisikan melalui sistem elektronik yang menyebabkan informasi elektronik dan/atau dokumen elektronik dapat diketahui pihak lain atau publik;

Pasal 27 beserta penjelasannya mengungkapkan bagaimana hukum menjerat pengumpul data pribadi yang secara aktif memberikan atau mendistribusikan data tersebut kepada pihak ketiga sedangkan tidak ada ancaman pidana bagi pengumpul data pribadi apabila data tersebut dirampas oleh seorang peretas. Oleh karena itu, ada celah bagi pengumpul data pribadi untuk tidak memperhatikan tingkat keamanan siber sistem pengolah data yang mereka miliki dan menyalahkan peretas atas kebocoran data yang terjadi. Dengan demikian, dapat disimpulkan bahwa kurang adanya sanksi bagi penyelenggara sistem elektronik yang mengalami kebocoran data akibat kelalaiannya sendiri.Pada saat ini, dengan eksistensi UU PDP, penulis tertarik mengkaji efektivitas dan perubahan yang timbul dari keberadaannya.

Bagaimana cara memilah dan mengetahui berbagai bentuk modus penipuan yang dapat dilakukan oleh oknum-oknum yang memiliki *mens rea* (niat jahat) dalam bermedia online sehingga dapat mengurangi tingginya angka pembocoran, pencurian ataupun penipuan data pribadi?

Bagaimana bentuk perlindungan represif dan preventif yang konkret dalam rangka mewujudkan keamanan serta perlindungan bagi para pengguna media sosial yang seringkali mengalami kasus pembocoran, pencurian, maupun penipuan data pribadi tersebut?

2. METODE PELAKSANAAN PKM

Metode penelitian yang diterapkan adalah metode hukum normatif dan empiris. Penelitian hukum normatif dilakukan dengan studi pustaka terhadap bahan hukum primer, seperti peraturan perundang-undangan dan bahan hukum sekunder, seperti buku teks dan jurnal hukum yang berkaitan dengan tema yang dibahas. Dari kajian normatif, peneliti bertujuan untuk memperoleh fondasi dan materi yang akan mendukung pelaksanaan pengabdian kepada masyarakat di Kabupaten Indramayu. Sebagai lanjutan dari penelitian hukum normatif, tim peneliti melaksanakan penelitian hukum empiris dengan mengadakan penyuluhan hukum di Kantor Sekretariat Daerah Kabupaten Indramayu pada hari Senin, 31 Oktober 2022 sampai dengan hari Kamis, 3 November 2022. Penyuluhan diawali dengan sesi pemaparan materi terkait perlindungan data pribadi yang dilanjut dengan sesi diskusi bersama para hadirin. Melalui penelitian hukum empiris, peneliti memperoleh perspektif dari warga masyarakat Kabupaten Indramayu terkait dengan perlindungan data pribadi. Dengan demikian, pendekatan yang digunakan dalam penelitian ini merupakan pendekatan peraturan perundang-undangan dan yuridis sosiologis.

Gambar 2
Foto Tim Peneliti melakukan Penyuluhan Hukum di Kantor Sekretariat Daerah Kabupaten Indramayu

Gambar 3
Foto Bersama Tim Pengabdian Kepada Masyarakat (PKM) Indramayu

https://doi.org/10.24912/jsa.v1i1.23845

3. HASIL DAN PEMBAHASAN

Data Pribadi, sebagaimana dengan yang diamanatkan definisinya dalam Rancangan Undang Undang Perlindungan Data Pribadi (RUU PDP), dan kemudian disahkan menjadi Undang Undang Perlindungan Data Pribadi (UU PDP) pada tahun 2022, terkhususnya Pasal 1 ayat (1) merupakan "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". Kemudian, yang dimaksud dengan Perlindungan Data Pribadi pada Pasal 1 ayat (2), adalah " Keseluruhan upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak konstitusional subjek Data Pribadi". Dari kedua definisi yang sudah dipaparkan, dapat diketahui seberapa esensialnya menjaga informasi-informasi sensitif yang disimpan dalam handphone, laptop, komputer, dan objek penyimpan data lainnya.

Jika kita telusuri dalam substansi yang termuat dalam Pasal 28G UUD 1945 yang berbunyi, "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," maka dapat kita simpulkan bahwa penggunaan teknologi digital sepatutnya menitikberatkan pada peningkatan keamanan dan kesejahteraan masyarakat Indonesia serta dimanfaatkan sebaik-baiknya untuk memudahkan mobilitas sosial rakyat dalam bertransaksi, bersosialisasi, media hiburan, dan berbagai aktivitas lainnya.

Terdapat begitu banyak informasi yang kita distribusikan kepada orang lain dalam bersosialisasi sehari-harinya. Oleh sebab itu, fluktuasi data yang menyangkut kehidupan pribadi kita sangat mudah ditransmisikan melalui dunia maya. Identitas diri seperti Nomor Induk Kependudukan (NIK), data Kartu Keluarga dan KTP, tidak luput hingga foto-foto serta dokumen pribadi kita yang bersifat privat pun berada dalam posisi rentan sehingga membutuhkan pengawasan serta perlindungan maksimal. Semakin maju dan modern kehidupan masyarakat, maka semakin maju dan modern pula jenis dan modus operandi kejahatan yang terjadi di masyarakat (Budi Suhariyanto, 2012). Seperti pada saat ini, sedang marak terjadi kasus pembobolan data pribadi yang merugikan banyak pihak.

Dilansir dari CNN Indonesia, pada tahun 2020, Tokopedia dilaporkan mengalami peretasan hingga 91 juta akun pengguna dan 7 juta akun penjual berhasil diambil datanya oleh peretas. Pelaku menjual data di *dark web* berupa user ID, email, nama lengkap, tanggal lahir, jenis

kelamin, nomor handphone dan password yang masih ter-hash atau tersandi. Semua data tersebut dijual dengan harga US$5.000 atau sekitar Rp 74 juta (CNN Indonesia, 2020).

Pada Mei 2021, seorang pengguna RaidForums bernama Kotz menjual database informasi pribadi tentang penduduk Indonesia. Data yang dijual meliputi NIK KTP, gaji, nomor handphone, alamat dan email. Kotz mengatakan bahwa ia memperoleh data tersebut dari situs web bpjs-kesehatan.go.id dan mengonfirmasi untuk menjual database tersebut seharga 0,15 BTC (setara dengan Rp84,3 juta atau sekitar US$6.000).

Dengan demikian, dilatarbelakangi polemik perlindungan data pribadi yang merupakan masalah serius, penulis akan mengelaborasikan analisis dari dua rumusan masalah yang sudah disampaikan terlebih dahulu di awal. Rumusan masalah pertama adalah mengenai adanya upaya untuk mengetahui munculnya intensi buruk (*mens rea*) orang lain untuk mencuri data pribadi milik kita. Salah satu langkah preventif untuk mengurangi potensi terjadinya tindak pidana terhadap data pribadi adalah setiap orang sebagai pemilik data pribadi perlu mengedepankan prinsip kehati-hatian dan selektif dalam memberikan izin akses kepada pihak ketiga terhadap data-data yang termuat dalam handphone maupun laptop dirinya masing-masing. Secara lebih detail, berikut merupakan beberapa kiat yang bisa dilakukan oleh subjek data pribadi sebagai langkah preventif dalam melindungi data pribadi:

1. Menggunakan kata sandi (*password*) yang kuat.

   Penggunaan kata sandi yang lemah, seperti mudah ditebak dan umum digunakan merupakan faktor utama mengapa akun yang kita miliki mudah untuk diretas. Kasus yang kerap terjadi setelah seorang peretas sudah membobol akun pribadi adalah mencuri data yang terdapat di dalamnya dan mengancam untuk mengeksposnya apabila si pemilik akun tidak melakukan apa yang diinginkan si peretas. Oleh karena itu, setiap orang perlu membuat kata sandi dengan variasi karakter yang lebih kompleks sehingga lebih sulit untuk ditebak, seperti menggunakan huruf kapital, angka, tanda baca, dan kombinasi huruf yang tidak membentuk kata. Perlu diperhatikan juga bahwa akun yang sudah diretas lazimnya tidak digunakan kembali sebab berisiko diretas kembali;

2. Aktif mencari tahu perkembangan modus penipuan digital yang terbaru.

   Kurangnya pemahaman terhadap modus penipuan yang kian hari semakin canggih membuat seseorang rentan untuk ditipu oleh pihak-pihak yang tidak bertanggung jawab. Modus penipuan yang cukup marak terjadi saat ini adalah penyebaran link *phising* atas nama organisasi/kelompok tertentu yang memberikan keuntungan besar dan menawarkan hadiah menarik terhadap kita apabila kita memencet link tersebut. Namun, ketika memencet link tersebut, pemilik data pribadi terkena malware atau virus, lalu data pribadinya diretas. Dengan demikian, setiap orang perlu membekali diri sendiri dengan mencari tahu secara berkala mengenai modus-modus penipuan yang sedang marak terjadi;

3. Selektif dalam memberikan informasi dan data pribadi melalui media digital.

   Rekam jejak digital sangat sulit untuk dihilangkan atau dihapuskan setelah kita membagikan data tersebut. Ketiadaan penyaringan terhadap informasi yang kita bagikan, baik foto-foto, video, tulisan, maupun data pribadi akan meningkatkan kerentanan data kita disalahgunakan sebab begitu banyak informasi terkait diri pemilik data pribadi yang terekspos dan diungkapkan secara terbuka. Oleh karena itu, setiap orang perlu memperhatikan informasi apa yang ia bagikan ke platform-platform digital;

https://doi.org/10.24912/jsa.v1i1.23845

4. Jangan tergesa-gesa memberikan izin akses kepada pihak pengumpul data pribadi terhadap data yang terdapat di *handphone*, laptop, maupun media elektronik lain.

   Ketika dihadapkan dalam situasi di mana suatu aplikasi atau situs web mewajibkan seseorang untuk memberikan izin akses data terhadap daftar kontak, isi Email, atau pesan-pesan Whatsapp maka jangan buru-buru memberikan izin tersebut. Riset terlebih dahulu tanggapan pengguna lain terhadap aplikasi atau situs web tersebut. Tidak hanya itu, pemilik data pribadi juga perlu membaca syarat dan ketentuan yang ditetapkan oleh penyedia layanan aplikasi maupun situs web;

Selain langkah preventif yang dapat ditempuh oleh setiap orang, perusahaan-perusahaan yang bergerak dalam bidang *Information and Communication Technology* (ICT) juga perlu untuk menerbitkan penetapan kewajiban pemberlakuan fitur verifikasi dua langkah (*2-step verification*), kode cadangan keamanan, dan verifikasi identitas pembuat akun, seperti melalui Email, Whatsapp, SMS, dan lain sebagainya. Dengan demikian, keterlibatan dari orang perorangan maupun korporasi akan mendukung jaminan keamanan dan perlindungan negara. Hal ini selaras dengan perkataan dari Roscoe Pound, yaitu *"Law is a tool of social engineering"* di mana artinya merupakan kehadiran partisipasi rakyat linear dengan kemajuan negara dan rakyat itu sendiri.

Selanjutnya, dari segi represif, konstitusi Indonesia telah mengundangkan beberapa regulasi yang bertujuan untuk meningkatkan keamanan digital di Indonesia, seperti UU ITE dan PP PSTE. Namun, peraturan tersebut dalam tataran praktik masih tidak cukup efektif dalam melindungi data pribadi sebab tidak sepenuhnya berfokus pada perlindungan data pribadi. Oleh karena itu, pada tahun 2022, DPR bersama presiden mengesahkan UU PDP yang disebutkan dalam bagian menimbangnya,

1. "Ditujukan untuk menjamin hak warga negara atas perlindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya perlindungan data pribadi";

2. "Bahwa perlindungan data pribadi merupakan salah satu hak asasi manusia yang merupakan bagian dari perlindungan diri pribadi maka perlu diberikan landasan hukum untuk memberikan keamanan atas data pribadi, berdasarkan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945";

Ada beberapa hal yang patut diperhatikan dengan adanya UU PDP ini, seperti:

1. Data pribadi terbagi menjadi 2 jenis.

   Dalam Pasal 4 UU PDP, diuraikan bahwa data pribadi digolongkan menjadi data pribadi yang bersifat umum dan spesifik. Data pribadi yang bersifat umum berupa nama, jenis kelamin, kewarganegaraan, dan lainnya sedangkan yang bersifat spesifik dapat berupa data dan informasi kesehatan, data biometrik, data genetika, data kejahatan, dan data anak;

2. Pemilik data pribadi memiliki hak-hak yang disebutkan secara eksplisit dalam Bab IV Pasal 5 hingga 18 dari UU PDP.

   Subjek pemilik data pribadi berhak untuk mengakses, mengelola, mengedit, menggunakan, mengubah, hingga menetapkan kewenangan data yang dimilikinya untuk dibagikan kepada orang lain;

3. Terdapat 3 jenis sanksi yang termaktub dalam UU PDP.

Ketiga jenis sanksi tersebut merupakan sanksi administratif (Pasal 57), sanksi tambahan (Pasal 69 - 70), dan sanksi pidana (Pasal 67 - 68). Adanya asas Ultimum Remedium dalam hukum pidana atau yang berarti "hukum sebagai obat terakhir" dapat diterapkan bagi para pelaku pidana pencuri data pribadi dan pembobolan data pribadi. Hal tersebut merupakan solusi yang tepat untuk dilakukan, apabila dengan adanya pemberian sanksi yang lebih ringan masih tidak membuat jera para pelaku pidana pencuri data pribadi;

Pada dasarnya niat jahat (*mens rea*) tidak dapat dihilangkan dan sangat sulit dibuktikan, tetapi adanya eksistensi UU PDP diharapkan dapat mengurangi kejahatan-kejahatan yang berhubungan dengan data pribadi. Sasaran tersebut diharapkan dapat tercapai dengan adanya penegasan kewajiban pihak-pihak pengumpul data untuk memaksimalkan keamanan tempat penyimpanan data mereka. Dengan demikian, seluruh penduduk Indonesia serta lembaga-lembaga atau instansi baik swasta maupun negara berperan aktif dalam upaya perlindungan data pribadi di Indonesia.

4. KESIMPULAN

Perkembangan zaman saat ini di mana negara-negara mulai memasuki era Society 5.0 menyebabkan data pribadi mengalami digitalisasi sehingga makin mudah transmisinya dalam dunia maya. Pemerintah Indonesia sudah mengeluarkan dasar hukum yang mengedepankan keamanan siber bagi seluruh rakyat Indonesia, khususnya dalam ranah perlindungan data pribadi, yaitu dengan Undang Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Di sisi lain, masyarakat perlu mengutamakan prinsip kehati-hatian, keselektifan, dan kebijaksanaan dalam melindungi data pribadi. Dengan demikian, adanya partisipasi aktif dari seluruh kalangan di Indonesia dalam bentuk tindakan represif sekaligus preventif akan meningkatkan keamanan ekosistem digital Indonesia.

Ucapan terima kasih *(Acknowledgement)*

Tim pelaksana Pengabdian Kepada Masyarakat (PKM) mengucapkan terima kasih kepada Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) Universitas Tarumanagara, Pimpinan Fakultas Hukum, serta pihak-pihak lainnya yang tidak bisa disebutkan satu per satu atas kepercayaan dan dukungannya dalam pelaksanaan PKM ini. Terima kasih juga disampaikan kepada Pemprov Indramayu, Jawa Barat, atas kesediaannya untuk menjadi mitra pelaksana PKM ini sehingga PKM dapat berjalan dengan lancar.

REFERENSI

Arief Mansur, D.M. dan Gultom, E. (2005). Cyber Law: Aspek Hukum Teknologi Informasi. Bandung: Refika Aditama.

Maskun. (2013). Kejahatan Siber (Cyber Crime): Suatu Pengantar. Jakarta: Kencana.

Nawawi Arief, B. (2006). Tindak Pidana Mayantara: Perkembangan Kajian Cybercrime di Indonesia. Jakarta: RajaGrafindo Persada.

Suhariyanto, B. (2012). Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya. Jakarta: RajaGrafindo Persada.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

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

Sidharta, S. (2019, September). Data Pribadi dan Perseorangan Tertentu. Diakses dari https://business-law.binus.ac.id/2019/09/12/data-pribadi-dan-data-perseorangan-tertentu/

https://doi.org/10.24912/jsa.v1i1.23845

Pratiwi, T.H. (2021, October 17). Pentingnya Perlindungan Data Pribadi di Era Digital. Diakses dari https://aptika.kominfo.go.id/2021/10/pentingnya-pelindungan-data-pribadi-di-era-digital/

Kaspersky Lab. (2022, Februari). Number of mobile cyber attacks against users worldwide from January 2020 to December 2021. Diakses dari https://www.statista.com/statistics/1305965/mobile-users-cyber-attacks/

Acer Indonesia. (2021, March 22). Mengapa Perlindungan Data Pribadi Penting Saat Ini. Diakses dari https://commercial.acerid.com/support/articles/mengapa-perlindungan-data-pribadi-penting-saat-ini/