JURNAL HUKUM SASANA, Volume 10, Iss. 1 (2024), pp. 70-83
ISSN 2461-0453 (print) | ISSN 2722-3779 (online)
Available online at: http://ejurnal.ubharajaya.ac.id/index.php/SASANA

Perlindungan Keamanan Atas Data Pribadi Di Dunia Maya

Edi Saputra Hasibuan[1], **Elfirda Ade Putri**[2]

[1,2]Universitas Bhayangkara Jakarta Raya
Email: edi.hasibuan@dsn.ubharajaya.ac.id, elfirdade.putri@gmail.com

DOI: https://doi.org/10.31599/sasana.v10i1.2134

Received:
25-04-2024

Revised:
01-06-2024

Accepted:
05-06-2024

Abstract: *The development of technology from the traditional era to the current millennial era has changed the way humans communicate. Social media is one example, social media has become an integral part of life to obtain, share and disseminate information. With the development of social media, information security and privacy issues are also important today. Social media is a source of disclosure of confidential information has become common today. So that a lot of data about one's privacy has been spread in cyberspace. Scattered privacy data can be caused by negligence or service providers. Information system security is an asset that must be protected. Security is generally defined as "the quality or state of being secure to be free from danger". Crimes related to personal data, such as hacking and fraud, are increasing in Indonesia, threatening the right to privacy guaranteed by the Constitution. To address this, the Government responded by issuing Law No. 27 of 2022 on Personal Data Protection which regulates principles, types of data, rights of data subjects, and prohibitions on the use of personal data, reflecting attention to privacy in the health sector. The research method used is the normative method. This research is conducted by searching and understanding literature or related to information security on social media and literature research. Six main points that must be considered when using online application systems related to data privacy are security and data protection, user awareness, control settings, risk management, transparency, and ethics. It is necessary to build trust into the design of Internet services, both through the design activities of managing a system that prioritizes user priority. Allowing, users are given a choice of control mechanisms on whether or not to disclose personal information and its use.*

Keywords: *Legal Protection, Personal Data, Technology Development.*

Abstrak

Perkembangan teknologi dari era tradisonal ke era milenial saat ini mengubah cara manusia dalam melakukan komunikasi. Media social merupakan salah satu contohnya, media sosial sudah satu kesatuan dari kehidupan untuk memperoleh, membagikan dan menyebarluaskan informasi. Berkembangnya media sosial maka masalah keamanan informasi dan privasi juga menjadi hal yang penting saat ini. Media sosial merupakan satu sumber terbongkarnya informasi rahasia sudah menjadi hal yang umum saat ini. Sehingga banyak data mengenai privasi seseorang yang telah tersebar di dunia maya. Data privasi yang tersebar bisa disebabkan oleh kelalaian maupun penyedia layanan. Keamanan sistem informasi merupakan aset yang harus dilindungi keamanannya. Keamanan secara umum diartikan sebagai "quality or state of being secure to be free from danger". Kejahatan terkait data pribadi, misalnya hacking dan penipuan, semakin meningkat di Indonesia, mengancam hak privasi yang dijamin konstitusi. Untuk mengatasi hal ini, Pemerintah merespons dengan mengeluarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mengatur

prinsip, jenis data, hak subjek data, dan larangan penggunaan data pribadi, mencerminkan perhatian terhadap privasi di sektor kesehatan. Metode penelitian dilakukan adalah menggunakan metode normatif. Penelitian ini dilakukan dengan cara mencari dan serta memahami literatur atau yang berhubungan keamanan informasi pada media social dan penelitian pustaka. Enam poin utama yang harus dipertimbangkan saat menggunakan system aplikasi online terkait privasi data yaitu keamanan dan data perlindungan, kesadaran pengguna, pengaturan kontrol, manajemen risiko, transparansi, dan etika. Perlu dibangun kepercayaan ke dalam rancangan layanan Internet, baik melalui kegiatan rancang bangun pengelolaan suatu sistem yang lebih mengedepankan user priority. Memungkinkan, user diberikan pilihan mekanisme kontrol terhadap perlu tidaknya dalam mengungkapkan informasi pribadi dan penggunaannya.

Keywords: Perlindungan Hukum, Data Pribadi, Perkembangan Teknologi

PENDAHULUAN

Kejahatan-kejahatan yang timbul pada bidang data pribadi di Indonesia biasa dilakukan dengan menggunakan jaringan internet, seperti penipuan, hacking, penyadapan data orang lain, spaming email, dan manipulasi data untuk mengakses data milik orang lain.Kemajuan teknologi informasi telah mengakibatkan batas privasi semakin berkurang, sehingga berbagai data pribadi semakin mudah tersebar dan/atau didapatkan oleh orang-orang yang tidak bertanggungjawab.Padahal, Data pribadi adalah suatu hal yang melekat pada diri setiap orang tanpa terkecuali, dimana data pribadi merupakan hal yang wajib dilindungi dan tergolong kedalam hak privasi seseorang. Hak privasi di Indonesia adalah hak konstitusional warga negara yang telah diatur di dalam Undang-Undang Dasar Republik Indonesia Tahun 1945.[1]

Media sosial merupakan salah satu media yang trend saat ini, karena menyediakan kemudahan dan kecepatan yang memungkinkan seseorang membuat dan mendistribusikan sebuah konten. Media sosial didefinisikan sebagai sekelompok aplikasi berbasis Internet yang membangun fondasi ideologis dan teknologi Web 2.0, dan memungkinkan penciptaan dan pertukaran konten yang dibuat penggunanya . Internet of Things didefinisikan sebagai infrastruktur jaringan global yang dinamis dengan konfigurasi sendiri dan komunikasi yang dapat dioperasikan. Secara sederhana dapat didefenisikan yakni kemampuan untuk membuat segala sesuatu di sekitar kita mulai dari (mis. mesin, perangkat, ponsel, dan mobil) bahkan (kota dan jalan) dapat terhubung ke Internet dengan perilaku yang cerdas dan dengan mempertimbangkan keberadaan jenis otonomi dan privasi. Kemajuan teknologi informasi dan komunikasi, menghasilkan data dalam jumlah yang luar biasa. Data yang dihasilkan tidak akan bernilai jika mereka tidak dapat dianalisis, ditafsirkan dan dipahami. Menurut Boyd, situs

[1] Ririn Aswandi, Putri Rofifah Nabilah Muchsin, Muhammad Sultan, Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (Idps), Legislatif, Vol. 3, No. 2, hal. 169

jejaring sosial adalah layanan berbasis web yang memungkinkan individu untuk (1) membuat profil publik atau semi-publik dalam sistem, (2) mengartikulasikan daftar pengguna lain dengan siapa mereka dapat berbagi koneksi, dan (3) melihat dan mencari daftar koneksi mereka dan yang dibuat oleh orang lain dalam sistem. Lebih jauh, Kaplandan Haenlein mendefinisikan media sosial sebagai "sekelompok aplikasi berbasis Internet yang dibangun di atas fondasi ideologis dan teknologi Web 2.0, dan memungkinkan pembuatan dan pertukaran konten yang dibuat pengguna".[2]

Perkembangan teknologi komunikasi dan informasi harus dilihat sebagai sarana pendukung. Penguasaan teknologi komunikasi dan informasi bukan dalam konteks sebagai user (pengguna) semata, namun harus benar-benar dapat dilakukan penguasan keilmuanny.[3] Perlindungan data sendiri secara umum pengertiannya mengacu pada praktik, perlindungan, dan aturan mengikat yang diberlakukan untuk melindungi informasi pribadi dan memastikan bahwa subjek data tetap mengendalikan informasinya. Singkatnya, pemilik data harus dapat memutuskan apakah ingin membagikan beberapa informasi atau tidak, siapa yang memiliki akses, untuk berapa lama, untuk alasan apa, dan dapat memodifikasi beberapa informasi ini, dll. Sedangkan data pribadi jika mengacu pada EU GDPR adalah: "Setiap informasi terkait seseorang ('subjek data') yang dapat mengenali atau dapat dikenali; mengenali secara langsung atau tidak lansung seseorang tersebut, terutama dengan merujuk pada sebuah tanda pengenal seperti nama, nomor identitas, data lokasi, data pengenal daring atau pada satu factor atau lebih tentang identitas fisik, psikologis, genetik, mental, ekonomi, atau sosial orang tersebut". Data pribadi umumnya dibedakan menjadi dua kategori: Data Pribadi Bersifat Umum, seperti: Nama, Alamat, Alamat e-mail, Data lokasi, IP address, web cookie; dan Data Pribadi Spesifik (Sensitif), seperti: ras, etnis, agama, pandangan politik, orientasi seksual, genetik, biometrik, kondisi mental dan kejiwaan, catatan kriminal.[4]

Masalah determinisme dan indeterminisme merupakan problem filosofis yang berada di luar ruang lingkup kebijakan pidana dan hukum pidana. Akan tetapi, ditegaskan bahwa kebijakan pidana yang modern hampir selalu mensyaratkan adanya kebebasan individu. Tujuan utama dari setiap perlakuan readaptasi sosial harus diarahkan pada perbaikan terhadap penguasaan diri sendiri. Oleh karena itu, masalah pertanggungjawaban seharusnya

[2] Mesra Betty Yel, Mahyuddin K. M. Nasution, Kemamanan, Keamanan Informasi Data Pribadi Pada Media Sosial, Jurnal Informatika Kaputama, Vol. 6, No.1 hal. 93

[3] Edi Saputra Hasibuan, Wajah Polisi Presisi Melahirkan Banyak Inovasi dan Prestasi, Rajawali Pres, PT. Grafindo Persada, 2022,hal.20

[4] https://aptika.kominfo.go.id/2019/05/pentingnya-melindungi-data-pribadi/ diakses tanggal 29 April 2024 lihat juga Wahyudi Djafar, Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan, tt

tidak boleh diabaikan, malahan justru harus diperkenalkan kembali sebagai suatu pertanggungjawaban pribadi.[5]

Dalam konteks kekinian, para pengguna media sosial di Indonesia, umumnya secara terbuka menyantumkan tempat tinggal asli (alamat rumah); tanggal, bulan dan tahun lahir; nomor telepon; juga hubungan kekerabatan dengan orang tua atau saudara kandung. Hal ini memperlihatkan masih besarnya problem kesadaran untuk melindungi privasi atau data pribadi, sebagai bagian dari properti pribadi. Klaim yang menyatakan privasi sebagai konsep barat sesungguhnya tidak sepenuhnya benar di Indonesia, studi yang dilakukan Alan Westin (1967), terutama ketika dia memberikan gambaran mengenai konsep privasi dalam era pra modern atau dalam struktur masyarakat tradisional, justru menggunakan contoh privasi rumah tangga dalam tatanan masyarakat Jawa dan Bali di Indonesia, dengan merujuk pada studi yang dilakukan oleh Clifford Geertz. Memang sebagai sebuah konsep hukum perlindungan terhadap privasi seseorang memang baru hadir bersamaan dengan hadirnya peraturan perundang-undangan kolonial, terutama setelah disahkannya KUHPerdata pada 1848, dan KUHP pada 1915, oleh pemerintah colonial Hindia Belanda. Hal ini salah satunya dapat diidentifikasi dengan hadirnya konsep larangan untuk memasuki rumah atau pekarangan orang lain tanpa ijin, atau adanya larangan untuk melakukan pembukaan surat tanpa ijin dari Ketua Pengadilan, yang diatur dalam Postordonnantie 1935 (Staatsblad 1934 No. 720).

Dalam perkembangannya, khususnya pasca amandemen konstitusi UUD 1945, hak atas privasi termasuk di dalamnya perlindungan data pribadi diakui sebagai salah hak konstitusional warga negara. Hal ini sejalan dengan dimasukannya bab khusus tentang hak asasi manusia (bill of rights) dalam konstitusi hasil amandemen (Bab XA—Pasal 28 A-J). Ketentuan memgenai jaminan perlindungan data pribadi dapat ditemukan di dalam Pasal 28G ayat (1) UUD 1945 yang menyatakan, "Setiap orang berhak atas perlindungan 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.". Selain perlindungan konstitusional, keterlibatan Indonesia sebagai negara pihak dari *International Covenant on Civil and Political Rights* (ICCPR), yang telah disahkan melalui UU No. 12/2005, juga menegaskan kewajiban pemerintah Indonesia untuk melindungi privasi dan data pribadi warga negaranya.

[5] Edi Saputra Hasibuan, Hukum Kepolisian dan Criminal Policy Dalam Penegakan Hukum, Rajawali Pres, PT. Grafindo Persada, 2021,hal.101

Saat ini Indonesia sebagai negara hukum telah berusaha untuk mengatasi permasalahan yang berkaitan dengan data pribadi tersebut dengan terbitnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi ("UU PDP"). Adapun UU PDP telah mengatur mengenai asas, jenis data pribadi, hak subjek data pribadi, pemerosesan data pribadi, larangan dalam penggunaan data pribadi, dan beberapa hal terkait data pribadi lainnya. Berkaitan dengan bidang kesehatan, UU PDP mengatur megenai data pribadi yang speifik seperti informasi kesehatan, data bimetrik, data genetika, catatan kesehatan, dan data lainnya. Hal ini menunjukkan bahwa UU PDP juga mengatur dan memperhatikan mengenai pentingnya privasi dalam pengelolaan data pada bidang kesehatan, namun demikian implementasi terhadap perlindungan data pribadi tersebut belum banyak diterapkan dan/atau dipersiapkan, meningat UU PDP memberikan waktu selama 2 (dua) tahun untuk dilakukan penyesuaian. Lebih lanjut, lahirnya UU PDP menimbulkan berbagai tantangan pada bidang kesehatan, termasuk namun tidak terbatas pada penyesuaian peraturan dan praktik kesehatan, penyelarasan dengan etika medis, danberbagai macam hal lainnya. Berdasarkan konteks yang telah dijelaskan di atas, Penulis merasa tertarik untuk melakukan penelitian terkait urgensi kenapa data pribadi harus dilindungi mengingat sudah disyahkannya Undang-Undang Nomor 27 Tahun 2022.

METODE PENELITIAN

Penelitian yang di gunakan adalah yuridis normatif, dimana penelitian yang dilakukan dengan cara menelusuri bahan hukum melalui studi kepustakaan. Penelitian ini bersifat deskriptif analitis yaitu untuk menganalisis data secara sistematis, factual dan akurat mengenai masalah yang diteliti. Dengan sifat penelitian yang dilakukan adalah sifat penelitian secara deskriptif analisis yaitu untuk memberikan data yang seteliti mungkin dilakukan penelitian terhadap tingakat kepercayaan masyarakat pada polri. Adapun alat pengumpul data yang digunakan, yakni: Bahan Hukum primer, skunder dan tersier yang kemudian dianalisis dengan analisis kualitatif kemudian disajikan secara deskriptif, yaitu dengan menjelaskan, menguraikan, dan menggambarkan permasalahan serta penyelesaiannya yang berkaitan dengan rumusan masalah yang dibuat.

PEMBAHASAN

Pentingnya regulasi dalam perlindungan data pribadi menjadi semakin signifikan di tengah era ekonomi digital. Hal ini bertujuan untuk menjaga agar data pribadi tidak disalahgunakan, terutama ketika data tersebut memiliki nilai ekonomis yang tinggi dandimanfaatkan dalam

kegiatan bisnis11. Peningkatan perlindungan data pribadi akan mengarahkan Indonesia pada posisi sejajar dengan negara-negara yang memiliki perekonomian maju, selain itu akan menguatkan dan memperkuat posisi Indonesia sebagai pusat bisnis dan investasi. Fenomena ini muncul karena setiap informasi yang tersimpan memiliki potensi untuk berdampak pada transformasi digital dalam ekonomi suatu negara.Seperti yang kita pahami, penghimpunan dan pengolahan informasi pribadi tidak hanya dilakukan oleh pihak Pemerintah untuk keperluan layanan masyarakat dan urusan politik, tetapi juga oleh entitas swasta dengan motivasi yang bersifat ekonomis. Masyarakat mungkin akan merasa ragu dan cemas untuk melakukan transaksi digital jika mereka merasa bahwakerahasiaan dan integritas data pribadi mereka berada dalam risiko yang signifikan. Bahkan berpotensi menimbulkan stagnasi pertumbuhan ekonomi yang berimbas padakerugian finansial negarakarena membuat gairah dan kepercayaan investor untuk berinvestasimenjadi berkurang.Rosadi dan Pratama juga menegaskan bahwa perlindungan data pribadi memiliki peran krusial dalam membentuk tingkat kepercayaan dalam lingkungan daring (online trust),yang pada gilirannya akan semakin mendorong pertumbuhan digital economydi Indonesia.[6]

Perlindungan data pribadi seseorang sangat dekat kaitannya terhadap hak privasi. Secara tata aturan hal tersebut telah diatur secara jelas dalam berbagai dokumen yang memuat tentang Hak Asasi Manusia. Sebelum pembahasannya lebih jauh, tulisan ini akan lebih dahulu meunculkan berbagai doktrin yang berkaitan dengan perlindungan tersebut. Merujuk pada artikel 12 Deklarasi Universal HAM (UDHR) menyaatakan dengan tegas bahwa "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".[7] Dalam pembahasan tersebut menegaskan apabila kebebasan menjaga privasi adalah hak setiap individu. Ketentuannya sudah diatur sebagaimana tertuang dalam banyak dasar hukum dan tidak boleh dilanggar oleh siapapun tanpa terkeculi. Selain itu, pada pengaturan lanjutannya yang tertuang dalam artikel 17 Konvensi Internasional Hak Sipil & Politik (ICCPR) kembali menegaskan apa yang tercantum dalam UDHR.[8] Oleh karenanya hak privasi haruslah ditegakkan oleh semua pihak agar tidak mencederai makna dari perlindungan atas dasar kemanusiaan.

[6] Sinta Dewi Rosadi dan Garry Gumelar Pratama, "Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia," Veritas et Justitia No. 4, No. 1 2018, hal. 88–110,
[7] United Nations, "Universal Declaration of Human Rights | United Nations," https://www.un.org/en/about-us/universal-declaration-of-human-rights Diakses Tanggal 29 April 2024
[8] International Covenant on Civil and Political Rights | OHCHR," https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights diakses tanggal 29 April 2024

Data Pribadi merupakan data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secaratersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsungmelalui sistem elektronik atau nonelektronik. edUU PDP membagi data pribadi menjadi dua bagian yaitu data pribadi yang bersifat spesifik dan data pribadi yang bersifat umum. Adapun yang termasuk dan tergolong dari data pribadi yang bersifat spesifik adalah; (i) data dan informasi kesehatan;(ii) data biometrik;(iii) data genetika;(iv) catatan kejahatan;(v) data anak;(vi) data keuangan pribadi; dan/atau(vii) data lainnya sesuai dengan ketentuan peraturan perundang-undangan.Lebih lanjut, data pribadi yang bersifat umum sebagaimana diatur dalam UU PDP merupakan data yang meliputi nama, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan/atau data pribadi yang dikombinasikan untuk identifikasi seseorang.Adapun terhadap kedua golongan data pribadi tersebut wajib dilindungi dan termasuk kedalam data pribadi yang perlu dilindungan berdasarkan UU PDP.

Pengendali Data Pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan DataPribadi, sedangkan Prosesor Data Pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindaksendiri-sendiri atau bersama-sama dalam melakukan pemrosesan Data Pribadi atas nama PengendaliData Pribadi.Dalam melakukan pemerosesan data pribadi, Pengendali Data Pribadi wajib memiliki dasar pemerosesan data pribadi seperti persetujuan dari Subjek Data Pribadi, pemenuhan kewajiban dalam perjanjian dengan Subjek Data Pribadi, dan lain-lain. Lebih lanjut, persetujuan terhadap pemerosesan Data Pribadi wajib dilakukan melalui persetujuan tertulis atau terekam yang dapat disampaikan secara elektronik maupun non-elektronik.Apabila persetujuan pemerosesan Data Pribadi tidak dilakukan secara tertulis atau terekam, maka akibatnya persetujuan tersebut dinyatakan batal demi hukum berdasarkan peraturan perundang-undangan. Adapun pengaturan mengenai kewajiban-kewajiban yang perlu dilakukan oleh Pengendali Data Pribadi diatur pada Pasal 20 sampai dengan Pasal 50 UU PDP. Selain itu, pengaturan mengenai kewajiban dari Prosesor Data Pribadi juga diatur dalam Pasal 51 dan Pasal 52 UU PDP.

Perlindungan data pribadi harus memiliki prinsip-prinsip:[9]

a. Adil, sah dan transparan,

[9] https://aptika.kominfo.go.id/2019/05/pentingnya-melindungi-data-pribadi/ diakses tanggal 29 April 2024

b. Ketepatan,

c. Batasan yujuan,

d. Batasan penyimpanan,

e. Akuntabilitas,

f. Minimalisasi,

g. Integritas dan kerahasiaan.

Sebagai contoh dalam transaksi e-commerce, kebutuhan informasi pribadi untuk verifikasi akun dalam transaksi elektronik terlihat jelas. Namun, ketika menangani tindakan hukum terhadap kasus kebocoran data yang mengarah pada penjualan data pribadi di situs web tertentu, tantangan muncul karena ketidaknyamanan yang dihadapi oleh individu yang datanya bocor seperti korban kejahatan skimming.22 Dampak dari kebocoran data pribadi adalah adanya potensi penyalahgunaan oleh oknum tidak bertanggung jawab yang melakukan kegiatan kriminal. Pertama, kemampuan untuk mengeksploitasi data pribadi untuk mendapatkan akses tidak sah ke rekening keuangan. Kedua, penggunaan informasi pribadi yang melanggar hukum untuk penipuan kredit online. Ketiga, data pribadi warga negara yang bocor dapat dieksploitasi untuk membuat profil pemilik data, misalnya untuk tujuan politik atau iklan media sosial. Keempat, data yang diretas dari akun media social dapat dimanfaatkan untuk berbagai tujuan terlarang.

Penyelenggara Sistem Elektronik harus menerapkan kebijakan keamanan data yang kuat, mematuhi peraturan perlindungan data, dan secara proaktif menerapkan praktik perlindungan privasi di seluruh operasi mereka. Langkah-langkah ini tidak hanya penting untuk keselamatan konsumen tetapi sebagai kelangsungan bisnis dan reputasi perusahaan. Dalam konteks bisnis yang mematuhi prinsip-prinsip Islam, pelanggaran kewajiban untuk melindungi data pribadi konsumen dapat menimbulkan konsekuensi kepatuhan etika dan syariah.24 Beberapa akibat tersebut dalam perspektif hukum Islam dapat mencakup: a.) Pelanggaran nilai etika islam. Jika Penyelenggara Sistem Elektronik tidak mematuhi kewajibannya dalam melindungi data pribadi konsumen, hal ini dapat dianggap sebagai pelanggaran terhadapnilai-nilai etika Islam, antara lain keadilan, transparansi, dan integritas. Pelanggaran etika dapat merugikan reputasi perusahaan di mata konsumen dan masyarakat; b.) Kehilangan kepercayaan konsumen muslim. Hilangnya kepercayaan konsumen Muslim bisa menjadi risiko yang signifikan. Islam menekankan pentingnya kejujuran, dapat dipercaya, dan perlindungan hak-hak individu. Jika konsumen Muslim merasa data pribadinya tidak

aman, hal ini dapat merusak kepercayaan mereka terhadap perusahaan; c.) Ketidakpatuhan terhadap prinsip kewajaran dan keseimbangan. Prinsip keadilan dalam Islam mencakup perlindungan terhadap hak-hak individu, termasuk hak atas privasi. Ketidakpatuhan terhadap prinsip-prinsip keadilan dapat dianggap sebagai ketidaksetaraan dan ketidakadilan, yang dapat berdampak negatif pada reputasi bisnis; d.) Pelanggaran hukum syariah. Jika pelanggaran privasi data melibatkan transaksi keuangan atau kebijakan bisnis yang bertentangan dengan prinsip keuangan syariah, hal ini dapat dianggap sebagai pelanggaran hukum syariah; e.) Menurunnya dukungan dari stakeholder syariah. Perusahaan yang beroperasi di lingkungan bisnis yang menganut prinsip-prinsip Islam seringkali mendapat dukungan dari pemangku kepentingan syariah, seperti badan amil zakat atau lembaga keuangan Islam. Ketidakpatuhan terhadap prinsip-prinsip ini dapat menyebabkan berkurangnya dukungan dan kerja sama dari pemangku kepentingan syariah; f.) Sanksi komunitas dan otoritas keagamaan. Pelanggaran terhadap perlindungan data pribadi yang melanggar prinsip-prinsip Islam dapat menarik perhatian otoritas agama dan masyarakat. Sanksi sosial dan kemungkinan pernyataan kecaman dapat merugikan reputasi dan citra perusahaan; dan g.) Kerugian dari pasar khusus muslim. Jika Penyelenggara Sistem Elektronik beroperasi di pasar yang mayoritas penduduknya beragama Islam, ketidakpatuhan terhadap prinsip Islam dalam melindungi data pribadi konsumen dapat menyebabkan penurunan pangsa pasar di kalangan konsumen Muslim.[10]

Selanjutnya sebagai contoh bila mengacu pada apa yang dilakukan banyak negara di dunia dalam pengelolaan data pribadi masyarakatnya mereka membangun dan memberlakukan kebijakan-kebijakan seperti yang diterapkan oleh Uni Eropa yang dapat menjamin perlindungan data terhadap warga negaranya. Diantaranya yaitu menggunakan kebijakan framework yang hormat dan menjungjung tinggi hak kehidupan pribadi setiap orang.[11] kemudian prinsip-prinsip yang dibuat harus sejalan mengikuti arus perubahan digitalisasi di masyarakat. Maka dari itu setiap kebijakan yang dibangun secara menyeluruh harus dapat mencapai keamanan informasi dan pertahanan siber.

Kemudian, yang menjadi dasar pengelolaan data di Uni Eropa menampilkan bahwa aturan tentang data flow telah melarang mengeluarkan data pribadi apabila negara tujuan belum mempunyai aturan yang adequancy (setara) dibandingkan dengan aturan yang ada di

[10] Rista Maharani, Andria Luhur Prakoso, Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital, Jurnal USM Law Review, Vol. 1 No. 7, 2024, hal. 334

[11] Bal Sokhi-Bulley, "Human Rights Law Review 11:4 ß The Fundamental Rights Agency of the European Union: A New Panopticism," n.d., 686, https://doi.org/10.1093/hrlr/ngr031.

negara eropa.[12] Maka dari itu dalam hal ini The Organization for Economic and Coorperation Development (OECD) telah menerbitkan panduan baku berkaitan perlindungan data pribadi yang bernama "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data". [13] Di dalam aturan tersebut memuat beberapa prinsip-prinsip yang diantaranya adalah sebagai berikut:[14]

a. Prinsip Pengumpulan Batasan *(Collection Limitation Principle)*

b. Prinsip Kualitas *(Data Quality Principle)*

c. Prinsip Tujuan Khusus *(Purpose Specification Principle)*

d. Prinsip Batasan Penggunaan *(Use Limitation Principle)*

e. Prinsip Perlindungan Keamanan *(Security Safeguard Principle*

f. Prinsip Keterbukaan *(Openness Principle)*

g. Prinsip Partisipasi Individu *(Individual Participation Principle)*

h. Prinsip Akuntabilitas *(Accountability Principle)."*

Mengapa data pribadi perlu dilindungi ? maka kita dapat melihat fenomena pencatutan data pribadi masyarakat pada tahapan pemilu 2024 merupakan sebuah fakta yang tidak terbantahkan khususnya dalam tahapan pemilu 2024, terlebih masa pendaftaran dan verifikasi calon peserta pemilu dan pencalonan anggota DPD. Merujuk kepada PKPU No. Tahun 2022 tentang jadwal & tahapan pelaksanaan pemilu 2024 mengatakan jika tahapan pendaftaran dan verifikasi factual calon peserta pemilu telah berlangsung pada 1 Agustus 2022 hingga 14 Desember 2022, sedangkan tahapan pendaftaran calon anggota DPD telah berlangsung dari tanggal 16 Desember 2022 dan November 2023.[15]

Pendaftaran parpol calon peserta pemilu dalam pelaksanaan pemilu 2024 sedikit berbeda dengan pemilu sebelumnya, karena hari ini pendaftarannya dilaksanakan satu pintu di KPU RI dengan menggunakan aplikasi SIPOL. Pada teknisnya setiap partai politik yang berkas administrasi pendaftarannya telah dinyatakan lengkap maka akan langsung diberikan akses sipol untuk mengisi persyaratan keanggotaannya. Kemudian yang menjadi perhatian adalah pada saat pengisian keanggotaan inilah, partai politik entah mendapatkan data

[12] uhammad Saiful Rizal, "Perbandingan Perlindungan Data Pribadi Indonesia Dan Malaysia," Jurnal Cakrawala Hukum Vol. 10, No. 2, 2019, hal.222.
[13] Ian Lloyd, Information Technology Law, 9th ed. (London: University of London, 2021)
[14] OECD Privacy Principles, http://oecdprivacy.org/ dikases tanggal 29 April 2024
[15] Lihat Peraturan KPU Nomor 3 Tahun 2022 tentang Jadwal dan Tahapan Pelaksanaan Pemilihan Umum Tahun 2024

kependudukan dari mana sehingga tak jarang masyarakat yang notabenenya bukan merupakan anggota partai politik tiba-tiba terdaftar sebagai keanggotaan partai politik. Praktik ini terjadi secara massif hamper semua parpol melakukannya. Dari total 9 partai politik yang dilakukan verifikasi factual keanggotaan, baik KPU maupun Bawaslu telah banyak mendapatkan aduan masyarakat dan temuan terkait dengan pencatutan nama ini sebanyak kurang lebih 20.565 orang.[16]

Pencatutan data pribadi masyarakat oleh parpol ini jelas sangat merugikan masyarakat. Karena sebarannya memiliki latar belakang yang beragam mulai dari usia, status pekerjaan, kelompok masyarakat, sampai dengan data orang yang telah meninggal dunia pun masih ada. Kita ambil contoh dengan status pekerjaan semisal Aparatur Sipil Negara, Kepala Desa dan Peenyelenggara Pemilu, apabila melihat regulasi baik yang ada di dalam UU ASN, UU Desa dan UU Pemilu, menyatakan bahwa pihak-pihak tersebut dilarang berafiliasi atau masuk sebagai anggota partai politik dan cenderung harus menjaga netralitasnya. Dengan adanya pencatutan nama yang dilakukan oleh partai politik secara illegal dan tidak bertanggung jawab hal tersebut telah menyebabkan kerugian bagi masyarakat secara imateril. Jika kita melihat dari uraian diatss bahwa benar UU PDP sudah disahkan dan banyak mengatur tentang ketentuan penyebarluasan, pemanfaatan dan kepemilikan data pribadi diatur dengan ketat sampai dengan sanksi dari setiap perbuatan pun ada. Akan tetapi untuk apa yang terjadi hari ini hamper semua korbannya hanya menyampaikan permohonan penghapusan saja kepada pihak pencatut melalui KPU agar namanya tidak muncul di dalam SIPOL dan SILON.

Hak privat dalam perlindungan data pribadi apabila ditinjau dari sisi regulasi seperti yang sudah diuraikan diatas bahwa hal tersebut sudah dijamin tercantum dalam pengaturan pasal 28G ayat (1) UUD 1945. Kemudian regulasi lainnya terdapat dalam UU Administrasi Kependudukan dan UU PDP. Pencatutan data pribadi oleh peserta pemilu apabila ditinjau melalui Undang-Undang Perlindungan Data Pribadi telah melanggar ketentuan pasal 65 ayat (1), (2) dan (3).

Secara aturan hukum yang berlaku sudah semestinya hal tersebut dapat dikenakan sanksi sebagaimana yang tertuang pada pasal 67 ayat (1), (2) dan (3) dengan hukuman maksimal 4 dan/atau 5 tahun dengan denda RP. 4.000.000.000 (empat miliyar rupiah) dan/atau Rp. 5.000.000.0000 (lima miliyar rupiah). 30 Namun dikarenakan penyalahgunaan data pribadi ini merupakan delik aduan dan masyarakat belum mendapatkan sosialisasi

[16] Bawaslu Temukan 20.565 Data Pribadi Warga Dicatut Parpol Untuk Daftar Pemilu, 3.198 Lolos."

tentang UU perlindungan data pribadi ini untuk konteks hari ini belum dapat diterapkan secara konsekuen dan mengikat.

Data pribadi berkaitan erat dengan data atau identitas yang melekat bagi seseorang, maka setiap data yang dikeluarkan harus atas dasar sepengetahuan dan persetujuan orang bersangkutan untuk kemudian nantinya akan digunakan oleh pihak lain. Selain itu dalam pengelolaan data pribadi pun harus mengutamakan prinsip keamanan, dengan adanya pencatutan ini telah membuktikan bahwa keamanan data pribadi yang dimiliki oleh system informasi di Indonesia begitu lemah sehingga akan membahayakan apabila disalahgunakan. Data pribadi harus dilindungi karena memiliki nilai penting bagi individu tersebut serta dapat berpotensi digunakan secara salah atau merugikan jika jatuh ke tangan yang salah. Berikut beberapa alasan mengapa perlindungan data pribadi penting:

a. Privasi: Data pribadi mencakup informasi sensitif tentang individu, seperti nama, alamat, nomor telepon, dan informasi keuangan. Perlindungan data membantu menjaga privasi individu dan mencegah penyalahgunaan informasi pribadi.

b. Keamanan Finansial: Data keuangan pribadi, seperti nomor kartu kredit atau rekening bank, dapat disalahgunakan untuk pencurian identitas atau penipuan keuangan jika jatuh ke tangan yang salah.

c. Keamanan Identitas: Informasi identitas pribadi dapat digunakan untuk membuat akun palsu atau melakukan kejahatan identitas, mengakibatkan kerugian finansial dan reputasi bagi individu yang terkena dampak.

d. Risiko Pencurian Identitas: Data pribadi yang dicuri dapat digunakan untuk membuat akun palsu, mengajukan pinjaman, atau melakukan pembelian secara ilegal atas nama individu tersebut.

e. Risiko Keamanan Digital: Data pribadi yang tidak dilindungi dapat rentan terhadap serangan cyber, seperti peretasan atau malware, yang dapat menyebabkan pencurian data atau kerusakan sistem.

f. Kepatuhan Regulasi: Banyak negara telah menerapkan regulasi perlindungan data, seperti GDPR di Uni Eropa atau CCPA di California, yang mewajibkan organisasi untuk melindungi data pribadi dan memberikan hak kepada individu atas informasi mereka.

g. Kepercayaan dan Reputasi: Ketika organisasi gagal melindungi data pribadi pelanggan atau karyawan, hal itu dapat merusak kepercayaan dan reputasi mereka, yang dapat berdampak negatif pada hubungan dengan pelanggan dan citra merek.

Perlindungan data pribadi menjadi semakin penting di era digital ini, di mana informasi pribadi mudah dikumpulkan, disimpan, dan ditransmisikan secara online. Melindungi data pribadi merupakan tanggung jawab bersama bagi individu, organisasi, dan pemerintah untuk memastikan bahwa privasi dan keamanan informasi tetap terjaga.

KESIMPULAN

Data pribadi harus dilindungi sebab berkaitan dengan privasi, keamanan finansial, keamanan identitas, Risiko Pencurian Identitas, risiko keamanan digital, kepatuhan regulasi dan kepercayaan dan reputasi hal ini penting sesuai dengan hak privat dalam perlindungan data pribadi apabila ditinjau dari sisi regulasi seperti yang sudah diuraikan diatas bahwa hal tersebut sudah dijamin tercantum dalam pengaturan pasal 28G ayat (1) UUD 1945. Kemudian regulasi lainnya terdapat dalam UU Administrasi Kependudukan dan UU PDP. Pencatutan data pribadi oleh peserta pemilu apabila ditinjau melalui Undang-Undang Perlindungan Data Pribadi telah melanggar ketentuan pasal 65 ayat (1), (2) dan (3). Pengesahan UU No. 27 Tahun 2022merupakan bukti bahwa Pemerintah menyadari betapa berharganya data di era digital economysaat ini. Kehadiran UU No. 27 Tahun 2022 yang melindungi data pribadi secara rinci tentunya akan memberikan dampak positif seperti meningkatkan kepercayaan publik terhadap pelaku bisnis digital dan investor merasa aman untuk itu perlu pembentukan suatu lembaga yang berfungsi untuk mengawasi pererdaran data pribadi di Indonesia.

SARAN

Data pribadi harus dilindungi karena memiliki nilai penting bagi individu tersebut serta dapat berpotensi digunakan secara salah atau merugikan jika jatuh ke tangan yang salah. Kesadaran pengguna, pengaturan kontrol, manajemen risiko, transparansi, dan etika. Perlu dibangun kepercayaan ke dalam rancangan layanan Internet, baik melalui kegiatan rancang bangun pengelolaan suatu sistem yang lebih mengedepankan user priority. Memungkinkan, user diberikan pilihan mekanisme kontrol terhadap perlu tidaknya dalam mengungkapkan informasi pribadi dan penggunaannya.

DAFTAR PUSTAKA

Bal Sokhi-Bulley, "Human Rights Law Review 11:4 ß The Fundamental Rights Agency of the European Union: A New Panopticism," n.d., 686, https://doi.org/10.1093/hrlr/ngr031.

Bawaslu Temukan 20.565 Data Pribadi Warga Dicatut Parpol Untuk Daftar Pemilu, 3.198 Lolos."

https://aptika.kominfo.go.id/2019/05/pentingnya-melindungi-data-pribadi/ diakses tanggal 29 April 2024 lihat juga Wahyudi Djafar, Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan, tt

https://aptika.kominfo.go.id/2019/05/pentingnya-melindungi-data-pribadi/ diakses tanggal 29 April 2024

Ian Lloyd, Information Technology Law, 9th ed. (London: University of London, 2021)

International Covenant on Civil and Political Rights | OHCHR," https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights diakses tanggal 29 April 2024

Mesra Betty Yel, Mahyuddin K. M. Nasution, Kemamanan, Keamanan Informasi Data Pribadi Pada Media Sosial, Jurnal Informatika Kaputama, Vol. 6, No.1 hal. 93

Muhammad Saiful Rizal, "Perbandingan Perlindungan Data Pribadi Indonesia Dan Malaysia," Jurnal Cakrawala Hukum Vol. 10, No. 2, 2019.

OECD Privacy Principles, http://oecdprivacy.org/ dikases tanggal 29 April 2024

Peraturan KPU Nomor 3 Tahun 2022 tentang Jadwal dan Tahapan Pelaksanaan Pemilihan Umum Tahun 2024

Ririn Aswandi, Putri Rofifah Nabilah Muchsin, Muhammad Sultan, Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (Idps), Legislatif, Vol. 3, No. 2.

Rista Maharani, Andria Luhur Prakoso, Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital, Jurnal USM Law Review, Vol. 1 No. 7, 2024.

Sinta Dewi Rosadi dan Garry Gumelar Pratama, "Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia," Veritas et Justitia No. 4, No. 1 2018.

United Nations, "Universal Declaration of Human Rights | United Nations," https://www.un.org/en/about-us/universal-declaration-of-human-rights Diakses Tanggal 29 April 2024