

# IMPLIKASI HUKUM TERHADAP PERLINDUNGAN DATA PRIBADI DI ERA DIGITAL

Sepiyah<sup>1</sup>, Idul Adnan<sup>2</sup>, Rahmatun Ulfa<sup>3</sup>, Elpipit,<sup>4</sup>

<sup>1</sup> Dosen Sekolah Tinggi Ilmu Syari'ah Darussalam Bermi, Indonesia

<sup>2</sup> Dosen Sekolah Tinggi Ilmu Syari'ah Darussalam Bermi, Indonesia

<sup>4</sup> Dosen Sekolah Tinggi Ilmu Syari'ah Darussalam Bermi, Indonesia

<sup>4</sup> Dosen Sekolah Tinggi Ilmu Syari'ah Darussalam Bermi, Indonesia

Email koresponden: *sepiyah311293@gmail.com*

## Abstrak

Dalam era digital yang terus berkembang, perlindungan data telah menjadi isu sentral yang memerlukan perhatian serius. Artikel ini menyelidiki tantangan dan solusi terkait perlindungan data di era digital. Peningkatan penggunaan teknologi informasi dan internet telah membuka pintu bagi pertukaran informasi yang cepat, namun juga meningkatkan risiko terhadap keamanan data pribadi. Faktor-faktor seperti serangan siber, pencurian identitas, dan eksploitasi data telah menunjukkan dampak negatif yang dapat merugikan individu maupun organisasi. Dengan demikian, implikasi hukum atas perlindungan data memainkan peran penting dalam memastikan bahwa data pribadi diproses dan dikelola dengan cara yang adil, transparan, dan aman. Perusahaan harus memperhatikan peraturan yang berlaku dan mengimplementasikan praktik-praktik terbaik dalam pengelolaan data agar menghindari risiko pelanggaran dan sanksi hukum yang berpotensi merugikan. Adapun kemudian pendekatan yang digunakan dalam penelitian ini adalah mengkaji sumber-sumber bacaan yang relevan dengan pembahasan, lalu kemudian memberikan perspektif oleh peneliti terkait dengan rumusan masalah yang ada.

**Kata Kunci :** *Perlindungan Data Pribadi, Era Digital, Implikasi Hukum*

Article history: Received :01/04/2022 Approved : 20/05/2022	<b>STIS Darussalam Bermi</b> <a href="https://ejournal.stisdarussalam.ac.id/index.php/jurdar">https://ejournal.stisdarussalam.ac.id/index.php/jurdar</a>
---	---

## Pendahuluan

Kejadian pelanggaran data yang melibatkan pencurian atau akses tidak sah terhadap informasi pribadi merupakan kekhawatiran utama. Kasus seperti ini dapat mengakibatkan kerugian finansial, pencurian identitas, dan dampak emosional bagi individu yang terkena dampak. Banyak kekhawatiran masyarakat terkait penggunaan data pribadi tanpa izin mereka. Ini bisa melibatkan penjualan data oleh perusahaan kepada pihak ketiga tanpa persetujuan, atau penggunaan data untuk tujuan yang tidak diinginkan seperti targeting iklan yang invasif. Sebagian besar masyarakat mungkin

tidak sepenuhnya memahami konsekuensi dari informasi yang mereka bagikan secara online. Kekhawatiran tentang apa yang terjadi dengan data mereka setelah dikumpulkan oleh perusahaan atau situs web menjadi perhatian utama.

Masyarakat juga khawatir tentang penggunaan algoritma dan kecerdasan buatan dalam membuat keputusan, seperti penentuan kredit, penilaian kesehatan, atau penerimaan pekerjaan. Ketidaktransparan dalam cara algoritma bekerja dan risiko diskriminasi dapat memunculkan kekhawatiran. Beberapa masyarakat merasa bahwa mereka kehilangan kontrol atas informasi pribadi mereka, terutama ketika berbagai platform online mengumpulkan data tanpa memberikan opsi kontrol yang memadai kepada pengguna. Kekhawatiran tentang keamanan perangkat dan layanan online yang rentan terhadap serangan siber dan malware juga merupakan masalah. Hal ini diperparah oleh ketidakpahaman sebagian masyarakat terhadap praktik keamanan digital yang baik. Pengelolaan kata sandi yang kompleks dan unik dapat menjadi tugas yang menantang bagi banyak individu. Penggunaan kata sandi yang lemah atau penggunaan kata sandi yang sama untuk berbagai layanan dapat meningkatkan risiko keamanan.

Masyarakat juga harus memahami konsep dari perlindungan data pribadi tersebut, oleh sebab pengertian data pribadi menurut Pasal 1 Ayat 1 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi adalah: Data pribadi tertentu yang disimpan, dipelihara, dan dijaga kebenaran dan kerahasiaannya. Pasal 3 Undang - Undang Nomor 43 Tahun 2009 Tentang Kearsipan menyebutkan bahwa untuk menjaga perlindungan dan keamanan data, maka arsip harus tertata rapi<sup>1</sup>. Definisi lain dari data pribadi disediakan dalam Undang - Undang Perlindungan Data Inggris tahun 1998, yang menyatakan bahwa itu adalah informasi apa pun yang berhubungan dengan individu hidup yang dapat dikenali dari informasi atau dari informasi lain yang dimiliki atau akan dimiliki oleh pengontrol data. Informasi pribadi juga dapat dikaitkan dengan karakteristik responden, seperti jenis kelamin, usia, nama, dan lain-lain.

Sistem elektronik yang mengontrol integrasi data pribadi dengan teknologi informasi, media, dan telekomunikasi bertujuan untuk data itu sendiri.<sup>2</sup> Undang - Undang Perlindungan Data Pribadi (UU PDP) yang telah berjalan sejak tahun 2019, adalah akhirnya diratifikasi pada 2019, sama seperti ada lebih banyak contoh data pribadi orang yang disusupi. Seperti yang dia katakan dalam pemikirannya, undang-undang ini bertujuan untuk membela hak privasi warga negara, meningkatkan pemahaman publik tentang perlunya menjaga informasi pribadi, dan memastikan hak-hak itu diakui dan

---

<sup>1</sup> 4 ELSAM dan Komisi I DPR RI. (2021). Termof Reference(TOR) Perwakilan Sekretariat Komisi I DPR dan TimAsistensi RUU PDP Sekjen DPRRI "Pembahasan Daftar Inventaris Masalah (DIM) RUU Pelindungan Data" Pribadi Focus Group Discussion.

<sup>2</sup> Makarim, E. (2010). *Tanggung jawab hukum penyelenggara sistem elektronik*. Rajajawali Pers.  
Miller, A. R. (1971). *Assault on privacy*.

ditegakkan. Undang-undang ini diharapkan dapat berfungsi sebagai kerangka hukum yang kuat untuk administrasi dan perlindungan data pribadi orang dan pegawai negeri. Salah satu hak asasi manusia yang terkait dengan perlindungan pribadi adalah perlindungan informasi pribadi. Pasal 28G UUD 1945 mengatur hak atas perlindungan pribadi ini. Dalam arti banyak negara mengakuinya, keamanan atau privasi pribadi ini bersifat universal. Mengenai informasi pribadi, sejak Tuhan menciptakan manusia, mereka memiliki informasi tentang diri mereka sendiri, khususnya informasi Biometrik.

Dalam era digital yang terus berkembang, data pribadi menjadi mata uang yang paling berharga. Seiring dengan kemajuan teknologi informasi, pertukaran data menjadi semakin cepat dan luas, memungkinkan informasi pribadi untuk tersebar dengan cara yang belum pernah terjadi sebelumnya. Namun, di balik kemudahan dan keunggulan teknologi ini, timbul pula kekhawatiran akan privasi dan keamanan data pribadi.

Dengan memperhatikan kerangka hukum yang ada dan perkembangan terkini dalam regulasi perlindungan data, kita dapat memahami tantangan yang dihadapi oleh individu, perusahaan, dan pemerintah dalam menjaga keamanan dan privasi informasi pribadi. Dengan munculnya peraturan baru seperti General Data Protection Regulation (GDPR) di Uni Eropa dan peraturan serupa di negara lain, dunia sedang menyaksikan perubahan signifikan dalam cara data pribadi diatur dan dilindungi. Sejalan dengan perkembangan di atas, banyak negara dan yurisdiksi telah merespon dengan mengenalkan peraturan dan undang-undang yang dirancang khusus untuk mengatasi tantangan perlindungan data di era digital. Pembahasan mengenai hak individu, kewajiban perusahaan, dan tanggung jawab pemerintah dalam melindungi data pribadi menjadi sorotan utama dalam konteks hukum.

Artikel ini akan menjelajahi implikasi hukum terhadap perlindungan data pribadi di era digital, dengan menyoroti dan fokus kajian sebagai berikut (1) Bagaimanakah Teknologi digital mempengaruhi perlindungan data pribadi dalam ranah hukum (2) Apakah kerangka hukum yang ada sudah cukup efektif dalam menangani kasus pelanggaran data pribadi. Dua itulah kemudian yang menjadi fokus kajian pada penelitian ini.

### **Metode Penelitian**

Peneliti menggunakan metodologi penelitian normatif, meninjau prinsip dan aplikasi setiap artikel sambil memasukkan literatur dari buku, jurnal, makalah, media cetak, dan sumber berita internet yang berkaitan dengan perlindungan data. Data target yang dikumpulkan terkait dengan kasus kejahatan dunia maya, perlindungan data, makna, dan undang-undang terkait. Pendekatan hukum, pendekatan kasus, dan metode komparatif semuanya digunakan untuk mejadi sumber-sumber informasi yang akurat.

## Pembahasan dan Hasil

Perlindungan data pribadi merupakan elemen integral dalam era digital yang terus berkembang. Kepentingan menjaga kerahasiaan informasi pribadi mencakup sejumlah dimensi yang memiliki relevansi yang substansial bagi individu dan masyarakat.<sup>3</sup> Pada tingkat pertama, perlindungan data pribadi melibatkan landasan dari hak privasi individu. Hak ini mencakup kontrol yang dimiliki individu atas data pribadi mereka, seperti nama, alamat, nomor telepon, dan informasi yang bersifat sensitif. Dengan keberadaan perlindungan data ini, individu dapat menjaga privasi mereka, mengendalikan penggunaan informasi mereka, dan secara efektif mencegah penyalahgunaan, penipuan, atau penggunaan data mereka untuk tujuan yang tidak dikehendaki.

Perlindungan data pribadi juga memiliki relevansi penting dalam mencegah pencurian identitas<sup>4</sup>. Identitas digital yang terungkap secara tidak sah dapat menjadi sarana bagi pihak yang bermaksud jahat untuk mendapatkan keuntungan pribadi, seperti melakukan penipuan keuangan, membuka rekening palsu, atau menyalahgunakan informasi pribadi lainnya. Dengan demikian, menjaga kerahasiaan data pribadi menjadi langkah pertahanan yang signifikan terhadap potensi kerentanannya identitas digital.

Di tengah era globalisasi yang kita alami saat ini, teknologi informasi memegang peran yang sangat sentral dalam membentuk lingkungan tanpa batasan yang melibatkan peningkatan produktivitas dan efisiensi.<sup>5</sup> Perkembangan pesat dalam teknologi informasi dan komunikasi telah membawa perubahan mendasar dalam cara masyarakat berinteraksi, bertransaksi, dan berkomunikasi.<sup>6</sup> Dalam era digital ini, pengaruh teknologi informasi terhadap sistem pengelolaan data, baik di sektor pemerintahan maupun sektor swasta, telah membantu memfasilitasi pelaksanaan berbagai kegiatan

---

<sup>3</sup> Weley, N. C., & Disemadi, H. S. (2022). Implikasi Hukum Pemasangan CCTV di Tempat Umum secara Tersembunyi terhadap Perlindungan Data Pribadi. *Amnesti Jurnal Hukum*, 4(2), 79-93.

<sup>4</sup> Nurfitri, N., Sudirman, L., & Disemadi, H. S. (2022). Tiktok Phenomenon: Exoneration Clause Vs. Personal Data Protection. *Jurnal Pendidikan Kewarganegaraan Undiksha*, 10(1), 441-453.

<sup>5</sup> Disemadi, H. S., Silviani, N. Z., Jaya, D., Haiti, R., Gea, L. K. B., Tobing, J. J., & Kasturi, M. I. (2022). Literasi Masyarakat Pesisir terhadap Perlindungan Data Pribadi dalam Transaksi Financial Technology. *Jurnal ABDIMASA Pengabdian Masyarakat*, 5(2), 68-76.

<sup>6</sup> Suharyanti, N. P. N., & Sutrisni, N. K. (2021). Urgensi Perlindungan Data Pribadi Dalam Menjamin Hak Privasi Masyarakat. *Prosiding Seminar Nasional Fakultas Hukum Universitas Mahasaraswati Denpasar* 2020.

secara digital, yang pada gilirannya meningkatkan efisiensi kinerja. Dalam konteks ini, informasi yang diperoleh melalui media elektronik, khususnya data individu, memiliki nilai yang sangat berharga, seperti data kependudukan dan demografis di Indonesia, termasuk Kartu Tanda Penduduk (KTP) dan Kartu Keluarga (KK).<sup>7</sup> Data-data semacam ini telah menjadi komoditas berharga dalam ekosistem digital, dan oleh karena itu, perlindungan mereka menjadi esensial untuk melindungi individu dan masyarakat dari potensi risiko yang berkaitan dengan eksploitasi data pribadi.

Perkembangan era digital telah memberikan kontribusi yang signifikan dalam mengubah paradigma kehidupan sehari-hari masyarakat.<sup>8</sup> Perubahan ini mencakup peningkatan signifikan dalam aliran informasi yang lebih cepat dan mudah diakses, peningkatan efisiensi serta efektivitas dalam berbagai aspek pekerjaan, ekspansi peluang pembelajaran daring, serta kemungkinan interaksi yang tak terbatas dengan individu yang berjarak jauh. Adopsi teknologi informasi dan komunikasi telah mengubah lanskap bisnis secara fundamental, dengan munculnya berbagai aplikasi dan layanan perdagangan daring (e-commerce) yang merevolusi cara transaksi dan berbisnis secara keseluruhan.<sup>9</sup> Dalam konteks inovasi digital ini, terdapat elemen-elemen yang menantang yang mempengaruhi bagaimana individu, bisnis, dan lembaga-lembaga terlibat dengan data pribadi dan keamanannya.

Kemajuan teknologi informasi, seiring dengan segala kenyamanannya, telah memunculkan sarana bagi aksi ilegal yang tak kalah canggih, dikenal sebagai kejahatan dunia maya atau *cybercrime*. Kejahatan semacam itu memanfaatkan kemajuan teknologi informasi sebagai wadah untuk berbagai bentuk kejahatan, seperti penipuan kartu kredit, pencurian data ATM/EDC, peretasan sistem komputer, penyusupan, penipuan internet banking, serta penyebaran perangkat lunak berbahaya seperti virus, worm, trojan, dan bot. Selain itu, aspek lain dari kejahatan dunia maya mencakup praktik-praktik seperti perebutan domain (*cybersquatting*), penyebaran konten pornografi, perjudian daring, serta kejahatan transnasional seperti perdagangan narkoba, kelompok mafia, tindakan terorisme, pencucian uang, perdagangan manusia, dan ekonomi gelap.<sup>10</sup>

Dalam beberapa tahun terakhir, Indonesia sendiri menjadi saksi terjadinya insiden-insiden serius terkait dengan kebocoran data yang mengkhawatirkan. Sebagai contoh, pada tanggal 17 April 2020, terjadi kebocoran data pribadi pengguna platform e-

---

<sup>7</sup> Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi. *Jurnal Hukum*, 37(2), 119. <https://doi.org/10.26532/jh.v37i2.16272>

<sup>8</sup> Winarso, T., Disemadi, H. S., & Prananingtyas, P. (2020). Protection of private data consumers p2p lending as part of e-commerce business in indonesia. *Tadulako Law Review*, 5(2), 206-221.

<sup>9</sup> Siahaan, A. L. S. (2022). Urgensi Perlindungan Data Pribadi Di Platform Marketplace Terhadap Kemajuan Teknologi. *Majalah Hukum Nasional*, 52(2), 211.

<sup>10</sup> Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi. *Jurnal Hukum*, 37(2), 119. <https://doi.org/10.26532/jh.v37i2.16272>

commerce terkemuka, Tokopedia, yang melibatkan setidaknya 12.115.583 akun pengguna. Tak berselang lama, peristiwa serupa terjadi di Bhinneka.com, sebuah platform toko online, ketika kelompok peretas yang dikenal sebagai Shiny Hunters mengklaim memiliki akses terhadap data pribadi 1,2 juta pengguna Bhinneka.com. Data tersebut kemudian dijual dengan nilai yang mencapai USD12.000 atau setara dengan Rp17.800.000. Sebelumnya, platform e-commerce Bukalapak juga mengalami insiden serupa, di mana lebih dari 12.957.573 akun pengguna dari platform tersebut tercatat telah berpindah tangan melalui transaksi illegal. Dengan demikian, perlu adanya perhatian serius dan tindakan hukum yang kuat untuk mengatasi ancaman yang semakin meluas ini dalam ranah siber.<sup>11</sup>

Lantas bagaimanakah peran pemerintah dalam hal membuat regulasi dan undang-undang agar masyarakat luas tidak khawatir terhadap data-data pribadi mereka. Beberapa Pengaturan Perlindungan Data Pribadi Di Indonesia adalah sebagai berikut :

**Definisi Data Pribadi:** UU ITE dan peraturan pelaksanaannya memberikan definisi yang jelas terkait apa yang dimaksud dengan data pribadi. Data pribadi dianggap sebagai bagian dari informasi elektronik yang dapat mengidentifikasi seseorang secara langsung atau tidak langsung.

**Pemrosesan Data Pribadi:** Pemrosesan data pribadi harus mematuhi prinsip-prinsip tertentu, seperti keberlanjutan, proporsionalitas, dan persetujuan dari pemilik data. Pemrosesan data dapat melibatkan pengumpulan, penyimpanan, penggunaan, pengungkapan, dan penghapusan data pribadi.

**Pemberitahuan dan Izin:** UU ITE menetapkan bahwa setiap pemilik data pribadi harus memberikan izin sebelum data pribadi mereka diproses. Selain itu, entitas yang mengumpulkan data pribadi wajib memberikan pemberitahuan secara jelas dan transparan tentang tujuan pemrosesan data tersebut.

**Keamanan Data:** Entitas yang memproses data pribadi diwajibkan untuk memberikan perlindungan yang memadai terhadap data tersebut. Hal ini mencakup langkah-langkah keamanan teknis dan organisasional untuk mencegah akses yang tidak sah, kebocoran, atau kerusakan data.

**Pemindahan Data ke Luar Negeri:** Pemindahan data pribadi ke luar negeri hanya dapat dilakukan dengan memperoleh izin dari Badan Autoritas Perlindungan Data Pribadi (BPDP). BPDP bertanggung jawab sebagai badan otoritas yang mengawasi implementasi perlindungan data pribadi di Indonesia.

**Sanksi:** Pelanggaran terhadap ketentuan perlindungan data pribadi dapat dikenai sanksi administratif dan pidana, termasuk denda dan hukuman penjara. Sanksi ini bertujuan untuk mendorong kepatuhan terhadap peraturan perlindungan data.

---

<sup>11</sup> 4 ELSAM dan Komisi I DPR RI. (2021). Termof Reference(TOR) Perwakilan Sekretariat Komisi I DPR dan Tim Asistensi RUU PDP Sekjen DPRRI "Pembahasan Daftar Inventaris Masalah (DIM) RUU Pelindungan Data" Pribadi Focus Group Discussion.

Seiring dengan perkembangan teknologi dan kesadaran akan pentingnya perlindungan data pribadi, Indonesia sedang mempertimbangkan revisi UU ITE untuk lebih menyesuaikan dengan tantangan dan perubahan terkini dalam dunia digital. Langkah-langkah ini bertujuan untuk memastikan bahwa data pribadi warga negara terlindungi dengan baik di tengah era digital yang terus berkembang.

Pasal-pasal yang juga mengatur perlindungan data pribadi :

**Pasal 15: Pengolahan Data Pribadi**

- Menetapkan bahwa setiap pengolahan data pribadi harus memperoleh izin dari pemilik data pribadi.
- Pemrosesan data pribadi hanya boleh dilakukan untuk tujuan tertentu dan sesuai dengan persetujuan dari pemilik data.

**Pasal 17: Pemberitahuan dan Persetujuan**

- Menekankan pentingnya memberikan pemberitahuan kepada pemilik data pribadi sebelum data diproses.
- Persetujuan harus diperoleh dengan cara yang jelas, transparan, dan dapat dipahami oleh pemilik data.

**Pasal 19: Keamanan Data**

- Menyatakan bahwa setiap entitas yang memproses data pribadi wajib memberikan perlindungan yang memadai terhadap data tersebut.
- Menetapkan bahwa keamanan data mencakup langkah-langkah teknis dan organisasional untuk mencegah akses yang tidak sah dan kerugian data.

**Pasal 22: Hak Pemilik Data Pribadi**

- Memberikan hak kepada pemilik data untuk mengetahui apakah data pribadinya diolah.

**Pasal 26: Pemindahan Data ke Luar Negeri**

- Menetapkan bahwa pemindahan data pribadi ke luar negeri hanya dapat dilakukan dengan izin dari Badan Autoritas Perlindungan Data Pribadi (BPDP).
- Pemindahan data pribadi harus memenuhi standar keamanan dan persyaratan tertentu.

**Pasal 29: Tanggung Jawab Pemilik dan Pengelola Sistem Elektronik**

- Menetapkan kewajiban bagi pemilik dan pengelola sistem elektronik untuk menjaga kerahasiaan data pribadi yang mereka kelola.

**Pasal 34: Sanksi Administratif dan Pidana**

- Sanksi ini dapat berupa denda dan/atau hukuman penjara, tergantung pada tingkat pelanggaran.

Penting untuk dicatat bahwa peraturan ini dapat mengalami perubahan atau amendemen, dan ketersediaan informasi terkini dari Badan Autoritas Perlindungan Data

Pribadi (BPDP) atau instansi terkait sangat disarankan untuk memahami dengan tepat kerangka hukum yang berlaku.

Di Indonesia, upaya peraturan perlindungan data pribadi tengah berlangsung, dan Badan Autoritas Perlindungan Data Pribadi (BPDP) dibentuk untuk memainkan peran penting dalam pengawasan dan penegakan kebijakan perlindungan data pribadi. Pemerintah Indonesia juga sedang mempertimbangkan revisi UU ITE, yang bisa saja melibatkan penambahan ketentuan yang lebih khusus terkait perlindungan data pribadi.

Penting untuk selalu memantau perkembangan hukum terkait perlindungan data pribadi di Indonesia, karena dunia hukum dan regulasi dapat mengalami perubahan. Mengikuti pembaruan dari sumber resmi seperti situs web Badan Autoritas Perlindungan Data Pribadi (BPDP) atau sumber hukum resmi lainnya adalah cara terbaik untuk memahami efektivitas dan perkembangan hukum tersebut.

Di tengah pesatnya mobilitas manusia, baik yang nampak maupun yang melalui media sosial, tidak dapat dipungkiri bahwasanya mereka setiap saat dihadapkan dengan media-media sosial dan lain sebagainya yang justru bisa menjebak mereka terlibat kasus-kasus ITE bila tidak memahami peraturan-peraturan yang sudah ditetapkan, namun yang menjadi pertanyaannya adalah apakah sudah efektif UU tersebut. Data terbaru Per Maret 2024, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia, yang memasukkan sejumlah ketentuan terkait perlindungan data pribadi, telah menjadi pusat perhatian dan kritik. Meskipun UU ITE mencakup beberapa ketentuan mengenai perlindungan data pribadi, masih ada kekhawatiran dan pandangan bahwa UU tersebut belum maksimal dalam mengatasi tantangan terkini terkait privasi dan keamanan data.

Kasus-kasus yang menjadi perhatian bersama bahwa peretasan data dan sebagainya sangat mungkin bisa dilakukan oleh orang-orang yang memiliki keahlian dan sangat merugikan pihak korban, di Indonesia bahkan perusahaan-perusahaan ternama tidak luput dari gangguan-gangguan tersebut: Pada tahun 2018, Facebook menghadapi skandal besar setelah diketahui bahwa data pribadi pengguna, yang diperoleh oleh perusahaan analitik Cambridge Analytica, digunakan untuk memengaruhi pemilihan umum dan kampanye politik di berbagai negara. Jutaan pengguna terkena dampak dari pelanggaran data ini. Yahoo mengalami dua pelanggaran besar pada tahun 2013 dan 2014. Pada 2013, sekitar satu miliar akun Yahoo terkena dampak, sedangkan pada 2014, sekitar 500 juta akun pengguna Yahoo diretas, termasuk informasi pribadi seperti nama, alamat email, dan data keamanan.

Pada tahun 2018, Marriott mengumumkan bahwa sistem reservasi hotelnya telah diakses oleh pihak yang tidak sah, mengungkap data pribadi lebih dari 500 juta tamu. Informasi yang bocor termasuk nama, alamat email, nomor paspor, dan detail pembayaran. Kasus Solar Winds adalah serangan siber yang terjadi pada tahun 2020, di mana peretas menggunakan perangkat lunak manajemen jaringan SolarWinds yang terinfeksi malware untuk menyusup ke sejumlah besar organisasi, termasuk lembaga pemerintah dan perusahaan swasta. Serangan ini memungkinkan para penyerang mengakses dan mencuri data sensitif. JBS, salah satu produsen daging terbesar di dunia, menjadi target serangan ransomware pada tahun 2021. Serangan ini menyebabkan gangguan produksi dan distribusi di sektor daging global.

Sedangkan di Indonesia Beberapa kritik dan kekhawatiran yang sering muncul terkait dengan UU ITE, terhadap perlindungan data pribadi di era digital adalah :

**Ketidakjelasan Definisi dan Lingkup Perlindungan Data:** Beberapa pihak berpendapat bahwa UU ITE masih belum memberikan definisi dan lingkup yang cukup jelas terkait dengan perlindungan data pribadi, yang dapat menimbulkan ketidakpastian dalam penerapan dan penegakan.

**Ketidaksesuaian dengan Standar Perlindungan Data Internasional:** Beberapa pihak mengkritik bahwa UU ITE belum sepenuhnya sejalan dengan standar internasional terkait perlindungan data pribadi, seperti General Data Protection Regulation (GDPR) di Uni Eropa.

**Kekhawatiran Terkait Penegakan Hukum yang Tidak Konsisten:** Ada ketakutan bahwa penegakan hukum di bawah UU ITE dapat dianggap tidak konsisten dan dapat disalahgunakan untuk membungkam kritik dan pendapat di dunia maya.

**Perlindungan Hak Kebebasan Berekspresi:** Beberapa pihak mengkhawatirkan bahwa UU ITE dapat mengancam hak kebebasan berekspresi dan berpendapat bahwa reformasi atau revisi diperlukan untuk lebih memastikan perlindungan hak-hak tersebut.

Pemerintah Indonesia menyadari kebutuhan untuk mereformasi UU ITE dan sedang mempertimbangkan revisi untuk mengatasi berbagai masalah dan meningkatkan ketahanannya terhadap perkembangan terkini di dunia digital. Pembaruan dan perubahan dapat terjadi seiring waktu, dan perhatian terus menerus terhadap pengembangan hukum dan peraturan di bidang perlindungan data pribadi adalah penting.

Kritikan-kritikan tersebut menjadi salah satu bukti belum sepenuhnya UU ITE perihal perlindungan data pribadi belum maksimal keberadaannya di tengah masyarakat dan belum bisa menjamin keamanan serta perlindungan terhadap data pribadi. Adapun kemudian efek jera bagi pelaku penyalahgunaan data belum terlihat memberikan sanksi

hukum yang tegas, sebab itu masih saja oknum-oknum bisa memanfaatkan kesempatan dan peluang yang ada serta implikasi hukum yang masih harus diperbaiki.

### **Kesimpulan**

Implikasi hukum terhadap perlindungan data pribadi di era digital mengharuskan pemangku-pemangku kekuasaan harus mulai berbenah dan memperbaiki serta merevisi UU perlindungan terhadap data pribadi. Kenapa demikian? masyarakat merasakan ketidakjelasan konsep yang ada pada UU tersebut, kemudian kritikan dan desakan dari masyarakat menggambarkan betapa rentannya kejahatan-kejahatan yang dapat terjadi dalam penyalahgunaan data pribadi. Perkembangan teknologi saat ini juga harus diwaspadai oleh khalayak, karna salah dalam mengambil sebuah keputusan akan berdampak fatal bagi pribadi mereka, perusahaan dan sebagainya. Berbicara masalah efektifitas UU ITE dan juga UU yang mengatur masalah sanksi belum sepenuhnya membuat pelaku mendapatkan efek jera, terlihat dengan semakin maraknya oknum-oknum yang bisa melakukan penyalahgunaan tersebut untuk keuntungan pribadi atau kelompok. Oleh sebab itu menjadi tugas bersama terutama pemerintah dalam memberikan rasa aman dan kebertanggungjawaban pihak-pihak yang memiliki otoritas terhadap data pribadi masyarakat.

### **Daftar Pustaka**

- 4 ELSAM dan Komisi I DPR RI. (2021). Termof Reference(TOR) Perwakilan Sekretariat Komisi I DPR dan TimAsistensi RUU PDP Sekjen DPRRI "Pembahasan Daftar Inventaris Masalah (DIM) RUU Pelindungan Data" Pribadi Focus Group Discussion.
- Makarim, E. (2010). *Tanggung jawab hukum penyelenggara sistem elektronik*. Rajajawali Pers.
- Miller, A. R. (1971). *Assault on privacy*.
- Weley, N. C., & Disemadi, H. S. (2022). Implikasi Hukum Pemasangan CCTV di Tempat Umum secara Tersembunyi terhadap Perlindungan Data Pribadi. *Amnesti Jurnal Hukum*, 4(2), 79-93.
- Nurfitri, N., Sudirman, L., & Disemadi, H. S. (2022). Tiktok Phenomenon: Exoneration Clause Vs. Personal Data Protection. *Jurnal Pendidikan Kewarganegaraan Undiksha*, 10(1), 441-453.
- Disemadi, H. S., Silviani, N. Z., Jaya, D., Haiti, R., Gea, L. K. B., Tobing, J. J., & Kasturi, M. I. (2022). Literasi Masyarakat Pesisir terhadap Perlindungan Data Pribadi dalam Transaksi Financial Technology. *Jurnal ABDIMASA Pengabdian Masyarakat*, 5(2), 68-76.
- Suharyanti, N. P. N., & Sutrisni, N. K. (2021). Urgensi Perlindungan Data Pribadi Dalam Menjamin Hak Privasi Masyarakat. *Prosiding Seminar Nasional Fakultas Hukum Univeritas Mahasaraswati Denpasar 2020*.

- Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi. *Jurnal Hukum*, 37(2), 119.  
<https://doi.org/10.26532/jh.v37i2.16272>
- Winarso, T., Disemadi, H. S., & Prananingtyas, P. (2020). Protection of private data consumers p2p lending as part of e-commerce business in indonesia. *Tadulako Law Review*, 5(2), 206-221.
- Siahaan, A. L. S. (2022). Urgensi Perlindungan Data Pribadi Di Platform Marketplace Terhadap Kemajuan Teknologi. *Majalah Hukum Nasional*, 52(2), 211.
- Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi. *Jurnal Hukum*, 37(2), 119.  
<https://doi.org/10.26532/jh.v37i2.16272>