



Proceeding of Conference on Law and
Social Studies

<http://prosiding.unipma.ac.id/index.php/COLaS>

Held in Madiun on October 14th 2023

e-ISSN: 2798-0103

Jaminan Perlindungan Hukum Terhadap Pemilik Data Pribadi dalam Penyelesaian Sengketa dengan Pengendali Data di Luar Negeri

Nurul Husna Khoirani Rozannah¹, Hari Purwadi², Isharyanto³

¹Universitas Sebelas Maret, nurulhsna11@gmail.com

²Universitas Sebelas Maret, hpurwadie@gmail.com

³Universitas Sebelas Maret, masis_uns@yahoo.com

Abstrak

Ditengah era digitalisasi ini, kebocoran data pribadi yang disebabkan lalainya pengendali data pribadi dalam melindungi data pribadi, cukup menjadi momok bagi masyarakat indonesia karena rentannya penyalahgunaan data pribadi untuk menguntungkan salah satu pihak tertentu. Tak jarang pengelola atau pengendali dari data pribadi tidak berkedudukan di Indonesia sehingga muncul masalah jika sengketa terjadi antara subjek data pribadi dengan pengendali data pribadi di luar negeri. Penelitian ini bertujuan untuk mengetahui perlindungan hukum bagi pemilik data pribadi dalam penyelesaian sengketa dengan pengendali data pribadi di luar negeri. Penelitian ini merupakan penelitan yuridis normatif dengan pendekatan undang-undang. Hasil dari penelitian ini adalah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi belum mengatur secara eksplisit tentang perlindungan hukum bagi pemilik data pribadi yang bersengketa dengan pengendali data pribadi yang berkedudukan di luar negeri. Sehingga masih terdapat kekosongan hukum jika terjadi sengketa antara pemilik data pribadi dengan pengendali data pribadi yang tidak berkedudukan di Indonesia.

Kata kunci: data pribadi, pengendali data pribadi, pemilik data pribadi.

Abstract

Abstract is a general description of research with a maximum of 250 words with the contents: background, research objectives, problem formulation, research methods, and conclusions.

Keywords: keyword 1, keyword 2, next (maximum 5)

Abstract

In the midst of this era of digitalization, personal data leaks caused by personal data controllers' negligence in protecting personal data

are quite a scourge for Indonesian society because of the vulnerability of personal data being misused to benefit one particular party. It is not uncommon for the manager or controller of personal data not to be domiciled in Indonesia, so problems arise if a dispute occurs between the personal data subject and the personal data controller abroad. This research aims to determine legal protection for personal data owners in resolving disputes with personal data controllers abroad. This research is normative juridical research with a statutory approach. The results of this research are that Law Number 27 of 2022 concerning Personal Data Protection does not yet explicitly regulate legal protection for personal data owners who are in dispute with personal data controllers based abroad. So there is still a legal vacuum if a dispute occurs between the owner of personal data and a personal data controller who is not domiciled in Indonesia.

Keywords: *personal data, personal data controller, personal data owner.*

I. Pendahuluan

Perkembangan teknologi di era sekarang semakin menunjukkan kemajuan yang signifikan. Penggunaan teknologi yang hampir selalu ada dalam setiap segmen kehidupan bermasyarakat semakin mempengaruhi pola pikir setiap manusia guna menyesuaikan dengan perkembangan tersebut. Hal ini akhirnya membuat teknologi kian hari menjadi kebutuhan bagi manusia terutama dalam penyampaian informasi. Teknologi yang berkaitan dengan pengambilan, pengumpulan, pengolahan, penyebaran dan penyajian informasi biasa disebut sebagai teknologi informasi dan komunikasi atau *Information and Communication Technologies (ICT)* (Darmawan, 2011).

Kehadiran internet merupakan contoh nyata dalam perkembangan teknologi informasi dan komunikasi. Jaringan internet biasa berbentuk website dimana terdapat nama domain atau URL (*Uniform Resource Locator*) yang berbeda-beda untuk mengidentifikasi setiap *website* (Rozannah, 2021). Dengan hadirnya internet menimbulkan gaya baru dalam berkomunikasi dalam jaringan tanpa harus bertatap muka dengan tetap menggunakan waktu seefisien mungkin (Djaja & Permatasari, 2022). Setiap orang dapat mencari dan menyebarkan data atau informasi secara lebih leluasa tanpa dibatasi oleh tempat dan waktu mereka berada. Dikarenakan bentuk internet yang tidak memiliki batas, memunculkan kekhawatiran akan kemungkinan adanya kebocoran informasi atau data pribadi dalam penggunaan internet. Kebocoran data pribadi ini akan membawa pada kejahatan atau biasa disebut *cybercrime* dimana kejahatan dilakukan dengan komputer dan atau internet (Irawati et al., 2021).

Pengaturan umum hukum perdata juga mengatur tentang data pribadi. Data pribadi dalam hukum perdata dapat dipersamakan dengan hak kebendaan karena dalam buku II KUHPerdata benda meliputi barang dan hak. Sehingga data pribadi sebagai hak selalu mengikuti dan melekat dimana pun benda berada atau disebut asas *droit de suite*. (Fikri & Rusdiana, 2023). Kemudian dalam Undang- Undang Dasar Negara Republik Indonesia Tahun 1945 (untuk selanjutnya disebut UUD 1945) juga menyinggung terkait Informasi atau data yang bersifat pribadi yang dikategorikan sebagai salah satu hak asasi manusia yaitu perlindungan pribadi. Hak atas perlindungan pribadi diatur dalam Pasal 28G UUD 1945. Kemudian ditegaskan kembali dalam Pasal 1 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik yang berbunyi “Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat dan dijaga kebenaran serta dilindungi kerahasiannya”. Hal ini juga diatur dalam Pasal 1 angka 2 Undang- Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (selanjutnya disebut UU Perlindungan Data Pribadi), “Perlindungan Data Pribadi adalah keseluruhan upaya untuk melindungi data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak konstitusional subjek Data Pribadi.” Sehingga data pribadi harus dijaga kerahasiannya oleh pengendali data pribadi dan tidak disebarluaskan dengan kesengajaan oleh pihak tertentu tanpa persetujuan dari pemilik data pribadi itu sendiri.

Kejahatan yang menyebabkan bocornya data pribadi yaitu peretasan (*hack*) sebagai bentuk langkah awal untuk melakukan kejahatan siber (*cybercrime*) lainnya (Akbar, 2021). Berdasarkan keterangan dari Kepala Badan Siber dan Sandi Negara (BSSN) yang dikutip dalam Detik News (Anggrainy, 2023) pada tahun 2022 terdapat

250 kasus dugaan kebocoran data pribadi dan pada tahun 2023 terdapat 126 kasus dugaan kebocoran data pribadi. Kebocoran data pribadi tidak hanya menjadi masalah dalam lingkup nasional, kebocoran data lintas negara juga dapat dimungkinkan terjadi. Seperti pada tahun 2022 diduga terdapat 487 juta data pengguna aplikasi *WhatsApp* dari 84 negara di dunia bocor dan dijual dalam forum *online* (Riyanto & Pratomo, 2022).

Ditengah era digitalisasi ini, kebocoran data pribadi cukup menjadi momok bagi masyarakat Indonesia karena rentannya penyalahgunaan data pribadi untuk menguntungkan salah satu pihak tertentu. Kebocoran data pribadi merupakan hal yang merugikan bagi pemilik data pribadi karena dimungkinkan dapat menyebabkan kerugian materiil maupun immateriil bagi warga yang data pribadinya disalahgunakan (Fikri & Alhakim, 2022). Banyaknya kasus dugaan kebocoran data pribadi di Indonesia menjadi alasan yang kuat untuk dibentuknya suatu peraturan perundang-undangan baru yang mengatur terkait perlindungan data pribadi di Indonesia.

Perlindungan data pribadi telah diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mana undang-undang tersebut akan berlaku bagi warga negara Indonesia atau di wilayah hukum negara Indonesia, namun bagaimana jika pengendali data pribadi dan/atau prosesor data pribadi tidak berada dalam wilayah hukum Indonesia? Sehingga muncul sebuah rumusan masalah yaitu bagaimana pengaturan jaminan perlindungan hukum terhadap pemilik data pribadi dalam menghadapi penyelesaian sengketa dengan pengendali data pribadi di luar negeri. Hal ini lah yang menjadi tujuan penulis dalam menulis artikel ini, yaitu untuk mengkaji terkait perlindungan hukum terhadap pemilik data pribadi dalam menghadapi penyelesaian sengketa dengan pengendali data pribadi di luar negeri.

II. Metode Penelitian

Metode Penelitian yang digunakan adalah penelitian yuridis- normatif yaitu penelitian yang dilakukan dengan meneliti bahan-bahan kepustakaan (Soekanto & Mahmudji, 2003). Jenis data yang digunakan adalah data primer dan sekunder. Data primer diperoleh dari Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sedangkan data sekunder diperoleh dari buku-buku, jurnal- jurnal serta artikel yang relevan. Teknik pengumpulan data dilakukan dengan studi pustaka. Teknik analisis yang digunakan adalah teknik analisis kualitatif.

III. Pembahasan

1. Pengaturan Jaminan Perlindungan Hukum Terhadap Pemilik Data Pribadi dalam Menghadapi Penyelesaian Sengketa dengan Pengendali Data Pribadi di Luar Negeri

Kemudahan berbagi data dan informasi melalui internet membuat pengguna internet di Indonesia melonjak naik setiap tahunnya. Berdasarkan Laporan We Are Social yang dikutip dalam DataIndonesia.id pengguna internet di Indonesia pada tahun 2022 mencapai 205 juta jiwa, kemudian pada awal tahun 2023 pengguna internet di Indonesia berjumlah 212,9 juta jiwa atau setara 77% dari populasi Indonesia (Rizaty, 2023). Artinya lebih dari setengah jumlah penduduk Indonesia telah mengakses internet dan memungkinkan para pengguna internet ini telah menggunakan data pribadinya untuk mengakses berbagai *website* di seluruh dunia. Kemudahan pengaksesan internet ini akan membawa masalah baru ketika data yang diberikan mengalami kebocoran (Ilhafa et al., 2021).

Penggunaan data pribadi telah masuk dalam segala bidang seperti perdagangan, keuangan bahkan pemerintahan. Pencatatan data terkait informasi pribadi seorang individu tidak lagi dilakukan secara manual di era digitalisasi ini. Bahkan proses pendaftaran Tanah telah

menggunakan peralatan elektronik, walaupun produknya belum elektronik atau masih sertifikat (Rohman, 2022). Bentuk pencatatan elektronik yang kemudian disimpan dalam sebuah *database* besar sudah menjadi hal lumrah. Pencatatan elektronik dalam bidang-bidang ini juga dikatakan sebagai data pribadi seorang individu. Pendaftaran aplikasi seperti akun *e-commerce* atau *e-wallet* juga membutuhkan proses penginputan data pribadi yang mana ini digunakan untuk melakukan konfirmasi terhadap *database* yang dimiliki oleh masing-masing perusahaan tersebut. Perusahaan, organisasi atau perseorangan yang menyimpan dan mengelola data pribadi seseorang biasa disebut sebagai Pengendali Data.

Perlindungan terhadap data pribadi pada dasarnya merupakan hak dasar bagi setiap individu. Hal ini sesuai dengan Pasal 28 G UUD 1945 yang mana menyatakan bahwa setiap orang mempunyai hak atas perlindungan diri pribadi dan harta benda yang dibawah kekuasaannya. Kemudian pada Pasal 21 Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia juga mengatur tentang hak setiap orang atas keutuhan pribadi yang mana hal tersebut tidak dapat menjadi objek penelitian tanpa memperoleh izin darinya. Dalam Penjelasan Pasal 21 UU HAM kembali diterangkan lebih rinci tentang objek penelitian yang dimaksud adalah keterangan atau pendapat terkait kehidupan pribadi atau data-data pribadinya. Hal ini yang kemudian menjadi salah satu urgensi adanya peraturan perundang-undangan yang secara khusus mengatur tentang perlindungan terhadap data pribadi seseorang agar terciptanya kepastian hukum terkait perlindungan dari data pribadi (Maruli & Situmeang, 2021).

Data pribadi merupakan data yang berkaitan langsung dengan seorang individu atau data yang menjadi ciri khusus dari seorang individu. Definisi data pribadi dirumuskan secara lebih rinci dalam Pasal 1 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi “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”. Artinya data yang terkait informasi diri atau ciri khusus seorang individu yang digunakan pada saat proses pencarian atau penyebaran data informasi terkait hal tertentu melalui internet termasuk sebagai data pribadi dan dilindungi. Sehingga pihak manapun yang menjadi pengendali data tidak dapat menyebarluaskan atau menyalahgunakan data pribadi yang dikelolanya untuk kepentingan pribadi tanpa izin dari subjek data pribadi. Hal tersebut dapat menimbulkan kejahatan dunia maya yang dapat merugikan dengan jumlah kerugian yang tidak dapat diukur (Irawati et al., 2021).

Data pribadi sendiri terbagi menjadi 2 (dua) sifat yaitu data pribadi bersifat umum dan khusus. Data pribadi yang bersifat umum menurut

Pasal 4 ayat (3) UU Perlindungan Data Pribadi adalah nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan dan/atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang. Kemudian Data pribadi yang bersifat khusus diatur dalam Pasal 4 ayat (2) UU Perlindungan Data Pribadi meliputi: data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi dan/atau data lainnya sesuai dengan ketentuan perundang-undangan. Perbedaan yang cukup spesifik adalah kerincian tentang informasi pribadi tersebut, dimana jika bersifat umum maka hal tersebut cukup relevan untuk diketahui banyak orang, sedangkan yang bersifat khusus hanya boleh digunakan untuk kepentingan pribadi dari pemilik data pribadi tersebut dan bentuknya lebih spesifik dalam mencirikan seorang individu.

Hampir sebagian besar sistem operasi dalam penggunaan internet mengharuskan seorang individu menggunakan data pribadinya. Berbagai aplikasi yang membutuhkan jaringan internet juga membutuhkan informasi yang bersifat pribadi seperti nama, email dan nomor telepon. Data pribadi tersebut disimpan dan dikelola oleh sebuah perusahaan atau bisa disebut pengendali data pribadi. Dalam pemrosesan data pribadi tersebut, pengendali data pribadi harus memiliki izin secara tertulis dari subjek data pribadi tersebut. Hal ini sesuai dengan Pasal 22 ayat (1) UU Perlindungan Data Pribadi yang berbunyi “Persetujuan pemrosesan Data Pribadi dilakukan melalui persetujuan tertulis atau terekam”.

Penyimpanan data yang dilakukan oleh pengendali data pribadi ini ternyata masih dapat terjadi kebocoran data. Terdapat beberapa pihak yang dengan sengaja membobol *database* sebuah perusahaan dengan tujuan menjual data pribadi tersebut. Lemahnya tingkat keamanan dari *database* sebuah perusahaan menjadi faktor yang menambah tingginya angka kebocoran data pribadi. Kebocoran data pribadi ini secara tidak langsung dapat membawa kerugian kepada subjek data pribadi karena besarnya kemungkinan penyalahgunaan data pribadi yang akan dilakukan oleh pihak tertentu. Bahkan kerugian tersebut juga dapat berbentuk kerugian immateriil yang cukup besar bagi subjek data pribadi.

Dilansir dalam laman berita Metro TV News (Metro TV News, 2023), pada tahun 2022 telah terjadi kebocoran data pengguna SIM Card di Indonesia dengan jumlah 1,3 miliar data dari para pendaftar SIM Card. Kemudian di tahun 2023 terdapat beberapa kali kebocoran data yaitu kebocoran data Bank Syariah Indonesia (BSI), data paspor yang mencapai 34 juta data berhasil dibobol dan pada bulan juli terjadi kebocoran data dukcapil sebesar 337 juta data pribadi. Tingginya kasus pembobolan data pribadi di Indonesia menunjukkan bahwa kegagalan sistem dalam perlindungan data pribadi di Indonesia masih tinggi. Pertanggungjawaban terhadap kegagalan sistem yang dapat

menimbulkan kerugian pada pihak lain tidak tegas dalam menyatakan adanya unsur sanksi pidana, melainkan hanya terdapat sanksi administratif (Thalib et al., 2021).

Pembentukan UU Perlindungan Data Pribadi sebagai bentuk perlindungan hukum yang dapat diberikan negara kepada setiap subjek data pribadi. Dalam undang-undang ini diatur dengan rinci terkait perlindungan terhadap data pribadi dari masing-masing individu agar lebih terlindungi secara hukum. Sebagaimana tercantum dalam Pasal 47 UU Perlindungan Data Pribadi, "Pengendali data Pribadi wajib bertanggung jawab atas pemrosesan Data Pribadi dan menunjukkan pertanggungjawaban dalam pemenuhan kewajiban pelaksanaan prinsip perlindungan data pribadi". Dengan adanya pasal ini membuat pengendali data pribadi dapat lebih bertanggung jawab dalam menjaga kerahasiaan dan penggunaan data atau informasi agar data pribadi tetap terlindungi. Selain itu, sebagai bentuk keseriusan dari pemerintah, maka akan dibentuk suatu lembaga khusus dalam rangka mewujudkan terselenggaranya perlindungan data pribadi sesuai dengan konsep UU Perlindungan Data Pribadi. Lembaga ini nantinya akan ditetapkan oleh Presiden dan bertanggung jawab secara langsung kepada Presiden sesuai dengan ketentuan pada Pasal 58 UU Perlindungan Data Pribadi.

Apabila terjadi kebocoran data yang disebabkan oleh kelalaian pengendali data sehingga mengakibatkan tidak terlaksananya perlindungan data pribadi, maka pengendali data dapat dikenakan sanksi administratif. Berdasarkan Pasal 57 ayat (2) UU Perlindungan Data Pribadi, pengenaan sanksi administratif dapat berupa peringatan tertulis, penghentian sementara atas kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi dan denda administratif.

Luasnya ruang lingkup dalam penggunaan internet di berbagai negara membuat penyebaran data pribadi pun dapat dilakukan lintas negara. Hal ini membuat yurisdiksi dari UU Perlindungan Data Pribadi akan bersifat ekstrateritorial sebagaimana yang tercantum dalam Pasal 2 ayat (1) UU Perlindungan Data Pribadi. Dimana UU Perlindungan Data Pribadi tidak hanya berlaku di wilayah hukum Negara Republik Indonesia, akan tetapi juga berlaku diluar wilayah hukum Negara Republik Indonesia. Yang artinya Indonesia akan melaksanakan yurisdiksinya terhadap warga negaranya di wilayah negara lain (Suryokusumo, 2005). Dalam Pasal 56 UU Perlindungan Data Pribadi juga menerangkan bahwasanya pengendali data dapat melakukan transfer data pribadi kepada pengendali data yang berada di luar negeri dengan beberapa syarat yaitu negara tempat pengendali data yang menerima transfer memiliki tingkat perlindungan hukum yang setara atau lebih tinggi dari yang diatur di Indonesia atau memastikan adanya perlindungan data pribadi yang memadai dan mengikat atau adanya persetujuan dari subjek data pribadi tersebut.

Sifat ekstrateritorial digunakan pula untuk mencakup perusahaan multinasional seperti *Google*, *Whatsapp*, *Meta Platforms* dan beberapa perusahaan multinasional lainnya. Penginputan data pribadi yang dilakukan oleh subjek data pribadi diarahkan langsung kepada masing-masing perusahaan yang berada diluar wilayah hukum Indonesia. Hal ini dapat mengakibatkan adanya tumpang tindih aturan antar negara apabila terjadi sengketa terkait perlindungan data pribadi. Pada tahun 2022 diduga terdapat 487 juta data pengguna aplikasi *WhatsApp* dari 84 negara di dunia bocor dan dijual dalam forum *online* (Riyanto & Pratomo, 2022). Indonesia masuk menjadi salah satu dari 84 negara yang data pribadinya bocor dan dijual di forum *online*. Hal ini termasuk sebagai bentuk sengketa terhadap perlindungan data pribadi antar negara.

Penyelesaian sengketa yang diatur dalam UU Perlindungan Data Pribadi dilakukan melalui arbitrase, pengadilan atau lembaga penyelesaian sengketa alternatif lainnya yang tertuang dalam Pasal 64 ayat (1) UU Perlindungan Data Pribadi. Salah satu bentuk alternatif penyelesaian sengketa yang mungkin bisa digunakan yaitu *Online Dispute Resolution (ODR)* yang dapat menghemat waktu dan uang serta dapat terhindar dari rasa intimidasi dari pihak lain (Rifai, 2022). Namun hal tersebut belum dapat digunakan untuk kasus pengendali data pribadi yang berada di luar negeri karena tidak adanya kejelasan hukum yang akan digunakan. Kemudian dalam Pasal 64 ayat (2) UU Perlindungan Data Pribadi menegaskan bahwa apabila penyelesaian sengketa yang dipilih adalah proses peradilan, maka hukum acara yang akan dipakai adalah hukum acara yang sesuai dengan ketentuan dalam peraturan perundang-undangan di Indonesia. Klasusul terkait penyelesaian sengketa tidak menyinggung tentang pihak pelanggar yang berada dalam kekuasaan atau wilayah hukum negara lain yang membuat adanya celah hukum dalam undang-undang ini.

Ketika warga negara pemilik data pribadi dan negara kedudukan pengendali data pribadi merupakan negara yang berbeda, maka hukum mana yang akan digunakan untuk penyelesaian sengketa tersebut. Belum adanya klausul dalam UU Perlindungan Data Pribadi yang secara eksplisit menerangkan terkait *choice of law* yang digunakan jika terjadi masalah lintas negara seperti contoh diatas. Adanya celah hukum ini membuat belum terpenuhinya hak perlindungan diri terhadap perlindungan data pribadi di Indonesia.

IV. Simpulan dan Saran

Simpulan

Data pribadi adalah suatu data yang berisi informasi yang mengidentifikasi atau menjadi ciri dari seorang individu. Pentingnya data pribadi bagi setiap individu membuat data pribadi harus mendapat perlindungan secara hukum. Indonesia telah mengatur terkait perlindungan data pribadi dalam Undang-Undang Nomor 27 Tahun 2022

tentang Perlindungan Data Pribadi. Meskipun UU Perlindungan Data Pribadi bersifat multinasional, masih terdapat kekosongan aturan terkait pengendali data pribadi yang berada diluar negeri. Tidak adanya aturan yang secara eksplisit dapat digunakan apabila terjadi sengketa antara subjek data pribadi di dalam negeri dengan pengendali data yang berada di luar negeri membuat perlindungan data pribadi di Indonesia belum terlindungi secara sempurna.

Saran

Adapun dari penelitian ini, penulis menyarankan sebaiknya Pemerintah melakukan kajian lebih lanjut terkait Undang-Undang Perlindungan Data Pribadi dengan tujuan agar lebih terjaminnya perlindungan data pribadi bagi subjek data pribadi di Indonesia dari penyalahgunaan data oleh pengendali data pribadi di luar negeri.

V. Ucapan Terima Kasih

Ucapan terimakasih yang sebesar-besarnya kami sampaikan kepada semua pihak yang terlibat dalam penelitian dan penulisan karta ini, kepada dosen Fakultas Hukum Universitas Sebelas Maret dan seluruh penyelenggaran kegiatan COLaS.

Daftar Pustaka

Akbar, G. (2021). Pertanggungjawaban Pidana Cybercrime dalam Penyebaran Virus dan Trojan Horse berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *Proceeding of Conference on Law and Social Studies*.

Anggrainy, F. C. (2023). Rapat di DPR, BSSN Ungkap 376 Dugaan Kebocoran Data Vital di 2022-2023. *Detik News*.
<https://news.detik.com/berita/d-6890194/rapat-di-dpr-bssn-ungkap-376-dugaan-kebocoran-data-vital-di-2022-2023>

Darmawan, D. (2011). *Teknologi Pembelajaran*. PT Remaja Rosdakarya.
Djaja, B., & Permatasari, S. J. (2022). The Implications of Electronic Mortgage Right ' s Implementation to Non-Bank Creditors. *Activa Yuris*, 2(February), 1–13.

Fikri, M., & Alhakim, A. (2022). Urgensi Pengaturan Hukum Terhadap Pelaku Tindak Pidana Pencurian Data Pribadi di Indonesia. *Yustisi*, 9(1), 1–13. <http://ejournal.uika-bogor.ac.id/index.php/YUSTISI/article/viewFile/7474/3650>

Fikri, M., & Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia. *Ganesha Law Review*, 5(1), 39–57.

Ihafa, F., Nur, A. I., Faresi, F., & Tiara, W. (2021). Upaya Hukum Terhadap Keamanan Data Pribadi Korban Pinjaman Online. *Proceeding of Conference on Law and Social Studies*.

Irawati, A., Fadholi, H. B., & Alamsyah, A. N. (2021). URGENSI CYBER LAW DALAM KEHIDUPAN MASYARAKAT INDONESIA DI ERA

DIGITAL. *Proceeding of Conference on Law and Social Studies*.
<http://prosiding.unipma.ac.id/index.php/COLaS>

Maruli, S., & Situmeang, T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber. *S A S I*, 27(28), 38–52. <https://doi.org/10.47268/sasi.v27i1.394>

Metro TV News. (2023). Deretan Kasus Kebocoran Data Pribadi di Indonesia Sepanjang 2022-2023.

<https://www.metrotvnews.com/play/NA0CXWqa-deretan-kasus-kebocoran-data-pribadi-di-indonesia-sepanjang-2022-2023>

Rifai, A. (2022). The Settlement of Electronic Commerce Transactions Through Online Dispute Resolution Mediation (ODR) in Indonesia. *Activa Yuris*, 2(1), 1–10. <http://doi.org/10.25273/ayWebsite:http://ejournal.unipma.ac.id/index.php/AYhttps://dx.doi.org/10.23887/jp.p.v53i1.24127>

Riyanto, G. P., & Pratomo, Y. (2022). 487 Juta Data WhatsApp Diduga Bocor, Ada Data Pengguna Indonesia. Kompas.Com.

<https://tekno.kompas.com/read/2022/11/28/07360197/487-juta-data-whatsapp-diduga-bocor-ada-data-pengguna-indonesia?page=all>

Rizaty, M. A. (2023). Pengguna Internet di Indonesia Sentuh 212 Juta pada 2023. DataIndonesia.Id.

<https://dataindonesia.id/internet/detail/pengguna-internet-di-indonesia-sentuh-212-juta-pada-2023>

Rohman, N. (2022). Urgence and Security of Digitalization of Land Electronic Certificate Issuance Documents. *Activa Yuris*, 2(1), 1–7.

Rozannah, N. H. K. (2021). Perlindungan Hukum Terhadap Hak Cipta atas Film yang Dipublikasikan Melalui Website.

<https://digilib.uns.ac.id/dokumen/detail/93835/Perlindungan-Hukum-Terhadap-Hak-Cipta-Atas-Film-yang-Dipublikasikan-Melalui-Website>.

Soekanto, S., & Mahmudji, S. (2003). *Penelitian Hukum Normatif, Suatu Tinjauan Singkat*. Raja Grafindo Persada.

Suryokusumo, S. (2005). *Yurisdiksi Negara vs. Yurisdiksi Ekstrateritorial*.

Jurnal Hukum Internasional, 2.

Thalib, E. F., Putu, N., & Meinarni, S. (2021). Liability of Marketplace as Electronic System Provider in Regard to System Failure Occured on Online Transactions. *Activa Yuris*, 1, 1–9.

Kitab Undang-Undang Hukum Perdata

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi