

# ANALISIS YURIDIS TRANSFER DATA PADA PERANGKAT DIGITAL BERBASIS INTERNET

**Evelyn Angelita Pinondang Manurung<sup>1</sup>**

<sup>1</sup>*Dosen Program Studi Teknik Informatika, STMIK STIKOM Indonesia*

Email : evelynangelita@stiki-indonesia.ac.id

## ABSTRAK

Perangkat teknologi digital saat ini dimanfaatkan oleh hampir semua orang secara masiv karena salah satu cara berkomunikasi modern dan untuk berbagi informasi tentunya. Dewasa ini masyarakat lebih memilih berkomunikasi secara modern dengan berbagi informasi berupa data digital melalui media digital berbasis internet dengan tujuan penyampaian informasi. Metode pengiriman data atau informasi yang cepat, mudah dan dilengkapi fitur modern dengan bergantung pada internet sesuai kebutuhan penggunanya menjadi pilihan efektif bagi masyarakat urban dalam menggunakan perangkat digital. Penggunaan perangkat digital dalam melakukan transfer data digital saat ini juga membuat masyarakat mulai menyadari pentingnya keamanan dalam transfer data. Tingginya aktivitas masyarakat yang mengirim data pribadi melalui perangkat digital juga harus seimbang dengan tingkat keamanan dan kerahasiaan data pada perangkat digital berbasis internet tersebut. Penelitian ini bertujuan untuk mengetahui aspek hukum dalam transfer data digital melalui perangkat digital berbasis internet agar masyarakat mengerti akan keamanan dan perlindungan data digital. Penelitian ini menggunakan metode penelitian yuridis normatif dengan menggunakan sumber hukum kepustakaan. Fakta banyaknya kasus pelanggaran data di media elektronik berbasis internet merupakan tanda atau bukti bahwa data pribadi adalah hak privasi yang harus mendapat perlindungan oleh negara. Adanya payung hukum akan peraturan yang komprehensif sangat diperlukan berupa undang-undang untuk menjamin keamanan, kerahasiaan dan perlindungan data pribadi.

Kata kunci: transfer data digital, keamanan data, perlindungan data

## PENDAHULUAN

Masivnya penggunaan platform pesan singkat digital berbasis internet saat ini telah mengubah kebiasaan komunikasi masyarakat dalam bertukar informasi secara global dan hal itu tentu saja memengaruhi perkembangan sosial, budaya, ekonomi, bahkan hukum yang ada. Penggunaan aktivitas internet masyarakat Indonesia di hampir seluruh sektor kegiatan masyarakat utamanya dalam pengiriman pesan yang berupa data atau informasi dewasa ini dirasakan sangat signifikan dan berpengaruh bagi kelancaran kegiatan atau aktivitas masyarakat. Menurut hasil survei Asosiasi Penyelenggara Jasa Internet Indonesia di tahun 2019 sampai 2020, presentase pengguna internet di Indonesia mencapai 73,7% dengan kalkulasi 196,71 juta jiwa merupakan pengguna internet dari total jumlah penduduk Indonesia 266,91 juta jiwa (APJII, 2020).

Salah satu kemudahan teknologi yang dirasakan masyarakat adalah dengan adanya internet. Penggunaan internet dalam berbagai bidang kehidupan tidak saja membuat segala sesuatunya menjadi lebih mudah, namun juga memunculkan sejumlah permasalahan termasuk dalam bidang hukum. Salah satu masalah hukum yang dapat muncul yakni berkaitan dengan perlindungan data pribadi (Lembaga Studi dan Advokasi Masyarakat, 2019). Sejalan dengan sifat keterbukaan platform digital dalam mengakses data dan informasi, maka perlindungan terhadap data dan informasi juga hal yang perlu disadari dan dilindungi.

Berikut adalah beberapa pengertian data diantaranya:

1. Data adalah setiap informasi yang diproses melalui peralatan yang berfungsi secara otomatis menanggapi instruksi-instruksi yang diberikan bagi tujuannya dan disimpan dengan maksud untuk dapat diproses (*Data Protection Act* Inggris tahun 2018).
2. Menurut Kamus Umum Bahasa Indonesia (KUBI), “Data adalah bukti yang ditemukan dari hasil penelitian yang dapat dijadikan dasar kajian atau pendapat” (*sdm.data.kemdikbud.go.id*).
3. Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya (Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Pasal 1 ayat 1).

Dalam perkembangan teknologi dan informasi data pribadi yang terdiri dari nama, alamat tempat tinggal, alamat surat elektronik, nomor telepon genggam merupakan data yang sangat berharga karena ada nilai ekonomis yang didapatkan dalam dunia bisnis dengan data tersebut. Penyalagunaan data melalui pengiriman pesan singkat digital menjadi perhatian khusus. Banyak pelanggaran data yang terjadi karena implementasi yang buruk atau tidak adanya kontrol keamanan baik diantara pengguna bahkan pihak ketiga. Banyak negara yang berusaha meningkatkan persyaratan keamanan dan menerapkannya di undang-undang mereka. Namun, sebagian besar kerangka keamanan bersifat reaktif dan tidak mengatasi ancaman yang relevan (Sungmi Park, 2018).

Era digital sebagai tanda kemajuan teknologi di seluruh negara menandakan pertumbuhan penggunaan perangkat digital bagi hampir seluruh masyarakat urban. Salah satu kebiasaan masyarakat urban adalah berkomunikasi dengan media/perangkat digital yang mengandalkan jaringan internet. Hal tersebut dikarenakan masyarakat urban lebih mengutamakan efektifitas dan efisiensi waktu, cara berkomunikasi mereka terbentuk pada perangkat digital berbasis internet. Perangkat tersebut digunakan sebagai media berkomunikasi sebagai cara paling efektif dan efisien. Platform digital berbasis internet seperti WhatsApp, Telegram, Messenger, Facebook, Instagram, dan lainnya adalah contoh platform digital yang digunakan untuk bertukar informasi dan data. Bukan hanya data atau sekedar informasi yang dikirimkan melalui platform digital tersebut, tapi data pribadi pun tidak jarang dikirimkan ke sesama pengguna platform digital.

## **METODE**

Permasalahan yang akan dibahas dalam penelitian ini terkait judul penelitian maka penelitian ini dilakukan dengan menggunakan metode penelitian yuridis normatif (metode penelitian hukum normatif). Metode penelitian yuridis normatif adalah penelitian hukum kepustakaan yang dilakukan dengan cara meneliti bahan-bahan kepustakaan atau data sekunder belaka. Penelitian ini dilakukan guna untuk mendapatkan bahan-bahan berupa: teori-teori, konsep-konsep, asas-asas hukum serta peraturan hukum yang berhubungan dengan pokok bahasan. Dengan demikian objek yang dianalisis dengan pendekatan yang bersifat kualitatif adalah metode penelitian yang mengacu pada norma-norma hukum yang terdapat dalam peraturan perundang-undangan (Soerjono Soekanto, 2003).

## PEMBAHASAN

Revolusi 4.0 merupakan *disruption era* yaitu yaitu era disrupsi dimana cara kerja berpindah atau berubah dari cara yang konvensional menjadi modern, dengan pendekatan digital. Oleh sebab itu semua lapisan harus dapat bersahabat dengan yang namanya teknologi supaya dapat mengikuti perkembangan jaman yang semakin maju (Sinaga, E. M. C & Putri, M. C, 2020). Tidak dapat dipungkiri bahwa platform layanan digital saat ini merupakan kebutuhan pokok masyarakat luas khususnya masyarakat urban. Perangkat digital digunakan untuk bertukar informasi dan data digital dengan berbasis internet. Maka itu platform digital yang memiliki fitur transfer data atau informasi sudah banyak menyimpan data pribadi dalam jumlah yang besar dan hal itu sudah sepatutnya diikuti dengan payung hukum untuk mencegah atau meminimalisir penyalahgunaan data seperti kebocoran/pelanggaran data pribadi seseorang. Data tersebut diantaranya yakni Kartu Tanda Penduduk (KTP), alamat tempat tinggal, nomor telepon, alamat surel, tanggal lahir, nomor paspor, dan lainnya. Sebagai pengguna platform digital berbasis internet, masyarakat luas sering tidak menyadari secara langsung dampak buruk yang ditimbulkan dari adanya kebocoran/pelanggaran data tersebut.

Masyarakat pengguna internet perlu memahami dan menyadari bahwa perlindungan data adalah penting untuk saat ini dan jangka panjang. Banyaknya kasus kebocoran data melalui platform pengiriman data digital memunculkan urgensi terhadap perlindungan data dari penyalahgunaan data oleh pihak yang tidak bertanggungjawab. Perlindungan data pribadi adalah upaya yang dilakukan oleh pengguna data pribadi, penyelenggara sistem elektronik baik secara preventif (pencegahan), persuasive (pengarahan), represif ataupun kuratif terhadap data pribadi yang dihimpun oleh pemilik data pribadi atau konsumen ke dalam sistem elektronik penyelenggara supaya data tersebut dijaga, dilindungi, dan terhindar dari penyalahgunaan yang merugikan pemilik data atau konsumen tersebut (Rizky P.P. Karo Karo, 2020).

Pesatnya perkembangan industri berbasis teknologi informasi membuat masyarakat sadar akan pentingnya menjaga kerahasiaan data pribadi miliknya dari berbagai ancaman penyalahgunaan data (Evelyn A.P. Manurung, 2020). Di era digital saat ini data merupakan unsur penting dan rahasia mengenai identitas seseorang yang menjadi kebutuhan utama dalam aktivitas bertukar informasi dan data di media digital berbasis internet. Contohnya fungsi memasukkan atau mengirimkan data secara digital dalam proses registrasi untuk mendapatkan layanan platform digital dengan mengisi identitas pribadi yang tanpa disadari pengendali data

atau penyedia layanan digital kemungkinan tidak bisa menjamin keamanan data pribadi. Memang hampir tidak bisa dihindari saat ini platform digital sudah menjadi media penting dalam aktivitas rutin masyarakat luas.

Perlindungan data pribadi berhubungan dengan konsep privasi. Konsep privasi sendiri adalah gagasan untuk menjaga integritas dan martabat pribadi. Hak privasi juga merupakan kemampuan individu untuk menentukan siapa yang memegang informasi tentang mereka dan bagaimana informasi tersebut digunakan (Wahyudi Djafar, 2014). Dalam bidang pekerjaan, pengelolaan data yang berjumlah sangat banyak dapat dikelola dengan baik, cepat, efektif dan efisien serta meminimalisir kesalahan. Dalam bidang perekonomian, promosi-promosi dan potensi-potensi dalam meningkatkan kesejahteraan masyarakat dilakukan dengan cepat tanpa batasan tempat atau wilayah dan menjangkau semua lapisan masyarakat baik nasional maupun internasional. Akan tetapi perkembangan teknologi dan informasi ini tidak saja memberikan manfaat melainkan juga mengakibatkan masalah yang dapat merugikan masyarakat, seperti halnya penyalahgunaan data, pencurian data pribadi, penjualan data pribadi, penipuan dan lain-lain (Sahat M.T. Situmeang, 2021). Perlindungan data pribadi itu menjadi sangat penting karena jika disalahgunakan oleh pihak penyedia data atau pihak ketiga, maka hal ini dapat bertentangan dengan hak dasar manusia untuk mendapatkan perlindungan privasi terhadap data pribadi.

Data atau informasi yang menyangkut identitas sudah sepatutnya mendapat perlindungan utamanya yang menyangkut data pribadi individu atau pun kelompok individu atau organisasi. Berdasarkan konstitusi bangsa Indonesia yang termaktub dalam UUD NRI 1945 sesungguhnya telah mengakui akan adanya hak terhadap perlindungan diri pribadi warganya dimana tercantum dalam Pasal 28 huruf G yaitu “Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”. Pasal tersebut menegaskan bahwa negara menjamin hak dan perlindungan atas privasi warga negaranya.

Maraknya kasus pelanggaran atau penyalahgunaan data yang ditransfer secara digital di banyak negara mendorong banyak negara untuk dapat melindungi data pribadi warga negaranya. Sejalan dengan hal itu negara-negara yang tergabung dalam Uni Eropa (EU) sepakat membuat sebuah regulasi tentang perlindungan data yang disebut *The EU General Data Protection Regulation (The EU GDPR)*. Prinsip GDPR sendiri adalah untuk melindungi hak asasi warga di era digital saat ini. GDPR dipandang sebagai solusi atas perlindungan data publik di internet sehingga mendorong pengendali data untuk lebih waspada dalam melindungi data milik subjek data (pengguna) (Tommy Kurnia, 2018). Berikut beberapa aturan yang tercantum dalam GDPR yang menyatakan perlindungan terhadap pengiriman data penggunanya:

Chapter II Article 9 (1): “*Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited*”. Berikutnya Chapter III Section 3 Article 17:

*“The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies”*. Begitu juga dalam Chapter III Section 5 Article 23 number 2 (d): *“the safeguards to prevent abuse or unlawful access or transfer”*.

Pasal tersebut melarang untuk membongkar segala informasi yang mengungkap identitas ras, etnis, agama, keyakinan, data biometrik, data atau data kesehatan pemilik data. Pemilik data harus terlebih dahulu setuju apabila data-data tersebut diproses. Demikian juga pada pasal 17 GDPR, pemilik data berhak atas data miliknya agar dihapus secara keseluruhan tanpa ditunda oleh pengendali data (penyedia layanan digital). Apabila pemilik data menyetorkan datanya di sebuah platform situs (penyedia layanan digital), maka platform tersebut wajib menghapus semua data pengguna. Dengan demikian maka sebuah platform digital tidak dapat menyimpan data pengguna yang sudah tidak menggunakan layanan digital tersebut. Pemilik data juga berhak untuk mendapat konfirmasi tentang pengelolaan data miliknya. Seperti tujuan dari pengelolaan data, siapa yang mengelola data pribadi miliknya. Demikian halnya bila data pengguna ditransfer ke pihak ketiga atau organisasi internasional, maka pemilik data berhak mendapat informasi.

Di negara Singapura sendiri perlindungan data pribadi juga terdapat pada *Personal Data Protection Act* (PDPA). Undang-Undang tersebut menjadi acuan dasar untuk perlindungan data pada sektor swasta. PDPA mengatur pihak-pihak yang terlibat untuk mematuhi Undang-Undang dalam pengelolaan dan pemrosesan data. Dalam PDPA dijelaskan mengenai perlindungan dalam pengiriman/transfer data pribadi ke pihak lain yaitu termaktub dalam Bab VI Perlindungan Data Pribadi:

Pasal 24. *An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent: (a). unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b). the loss of any storage medium or device on which personal data is stored.*

Pasal di atas menjelaskan mengenai pengaturan keamanan yang layak untuk mencegah akses pengumpulan/penyalinan yang tidak sah.

Pasal 26 (1). *An organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act.*

Pasal di atas menyatakan larangan mentransfer data pribadi apa pun ke wilayah di luar Singapura untuk memastikan adanya standar perlindungan terhadap data pribadi yang ditransfer sebagaimana diatur dalam Undang-Undang.

Diketahui di Indonesia ada regulasi yang secara umum mengatur tentang perlindungan data dalam proses pengiriman/transfer/transmisi data diantaranya Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik:

- a. Pasal 2 ayat 1. Perlindungan Data Pribadi Dalam Sistem Elektronik mencakup perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan Data Pribadi.
- b. Pasal 2 ayat 2 huruf b. Data Pribadi bersifat rahasia sesuai persetujuan dan/atau berdasarkan ketentuan peraturan perundang-undangan.
- c. Pasal 21 ayat 1 huruf a. Menampilkan, mengumumkan, mengirimkan, menyebarluaskan, dan/atau membuka akses Data Pribadi dalam sistem elektronik hanya dapat dilakukan atas persetujuan kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan.

Dalam pasal tersebut dijelaskan bahwa proses transfer atau penyebarluasan data mendapat perlindungan tetapi belum secara spesifik menyangkut perlindungan privasi individu dan apabila dikirimkan atau disebarluaskan kepada pihak ketiga harus mendapatkan persetujuan. Demikian juga dengan persetujuan yang diberikan oleh pemilik data pribadi menyangkut kebenaran atas data pribadi yang dimilikinya. Pihak penyedia layanan digital juga dianggap memiliki tanggung jawab dan kewajiban untuk menyimpan dan mengelola data pribadi seseorang karena berhubungan dengan etika kerahasiaan warga negaranya.

Maka dari itu sudah sepatutnya bangsa Indonesia memiliki perangkat hukum berupa Undang-Undang mengenai perlindungan data guna menjamin keamanan, kenyamanan dan hak-hak pengguna platform pesan digital dalam melaksanakan aktivitasnya. Saat ini regulasi mengenai perlindungan data di Indonesia masih dalam bentuk Rancangan Undang-Undang tentang Perlindungan Data Pribadi dimana pengaturan mengenai perlindungan terhadap pengiriman/transfer data oleh pengguna platform pesan digital dan pihak pengendali data (penyedia layanan digital) terlihat telah diatur sedemikian rupa, berikut diantaranya :

- a. Pasal 4. Pemilik Data Pribadi berhak meminta informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan Data Pribadi, dan akuntabilitas pihak yang meminta Data Pribadi.
- b. Pasal 13. Pemilik Data Pribadi berhak menuntut dan menerima ganti rugi atas pelanggaran Data Pribadi miliknya sesuai dengan ketentuan peraturan perundang-undangan.
- c. Pasal 47. Pengendali Data Pribadi yang mentransfer Data Pribadi dan yang menerima transfer Data Pribadi wajib melakukan perlindungan Data Pribadi sebagaimana dimaksud dalam Undang-Undang ini.
- d. Pasal 48 ayat 3. Dalam hal Pengendali Data Pribadi berbentuk badan hukum melakukan pembubaran atau dibubarkan, penyimpanan, transfer, penghapusan, atau pemusnahan Data Pribadi dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.
- e. Pasal 48 ayat 4. Penyimpanan, transfer, penghapusan, atau pemusnahan Data Pribadi sebagaimana dimaksud pada ayat (3) diberitahukan kepada Pemilik Data Pribadi.
- f. Pasal 61 ayat (1), misalnya, menyebutkan bahwa setiap orang yang dengan sengaja memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian Pemilik Data dipidana dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak Rp50 miliar. Sementara ayat (2) berbunyi

setiap orang yang dengan sengaja dan melawan hukum mengungkapkan data pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 51 ayat (2) dipidana dengan pidana penjara paling lama dua tahun atau pidana denda paling banyak Rp20 miliar. Sedangkan ayat (3) berisi setiap orang yang dengan sengaja dan melawan hukum menggunakan data pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 51 ayat (3) dipidana dengan pidana penjara paling lama tujuh tahun atau pidana denda paling banyak Rp70 miliar.

- g. Pasal 62 menyatakan setiap orang yang dengan sengaja dan melawan hukum memasang dan/atau mengoperasikan alat pemroses atau pengolah data visual di tempat umum atau fasilitas pelayanan publik yang dapat mengancam atau melanggar perlindungan data pribadi sebagaimana dimaksud dalam Pasal 52, dipidana dengan pidana penjara paling lama satu tahun atau pidana denda paling banyak Rp10 miliar.
- h. Pasal 63 disebutkan setiap orang yang dengan sengaja dan melawan hukum menggunakan alat pemroses atau pengolah data visual yang dipasang di tempat umum dan/atau fasilitas pelayanan publik yang digunakan untuk mengidentifikasi seseorang sebagaimana dimaksud dalam Pasal 53 dipidana dengan pidana penjara paling lama satu tahun atau pidana denda paling banyak Rp10 miliar.

Beberapa pasal di atas menyatakan bahwa data pribadi yang dikirimkan/ditransfer kepada platform penyedia layanan digital dilindungi oleh Undang-Undang demikian juga dengan pengaturan pengelolaan data. Jika dicermati RUU mengenai Perlindungan Data di Indonesia harusnya mendapat respon pemerintah dengan cepat bahwa Indonesia harus segera memiliki perangkat hukum komprehensif mengenai perlindungan data utamanya data digital.

Perlindungan dalam pengiriman/transfer data merupakan hal yang sangat mendesak saat ini dikarenakan kita telah masuk dalam era digital apabila ada penyalahgunaan atau pelanggaran oleh pihak ketiga, maka hal tersebut sangat bertentangan dengan hak atas privasi seseorang untuk mendapat perlindungan privasi terhadap data pribadinya. Bukti banyaknya kasus pelanggaran atau penyalahgunaan transfer data melalui platform digital berbasis internet adalah bagian dari pelanggaran data pribadi. Maka itu Indonesia patut memiliki payung hukum yang tegas dan menyeluruh untuk meminimalisir pelanggaran dan dapat mencegah penyalahgunaan data seperti kebocoran data.

## **SIMPULAN**

Belum adanya payung hukum yang komprehensif tentang perlindungan data dalam hal transfer data digital yang mengatur proses pengiriman/transfer data menjadi faktor penyebab banyaknya pelanggaran dan penyalahgunaan data di era digital ini. Demikian juga faktor pemahaman masyarakat luas yang belum melek terhadap privasi dan perlindungan data. Begitu pun perangkat hukum atau payung hukum mengenai perlindungan data di Indonesia masih lemah karena pengaturan perlindungan data yang ada saat ini terpisah-pisah di beberapa peraturan. Hingga saat ini Indonesia masih belum memiliki Undang-Undang mengenai perlindungan data pribadi, karena pengaturan tersebut masih berupa draft Rancangan Undang-Undang Perlindungan Data Pribadi. Menilik banyak negara yang telah memiliki dan

menerapkan Undang-Undang mengenai perlindungan data pribadi utamanya yang mengatur pengiriman/transfer data, sudah selayaknya Indonesia juga mengesahkan dan menerapkannya, mengingat masyarakat Indonesia sebagian besar telah menggunakan platform digital. Keberadaan Undang-Undang tentang perlindungan data memang merupakan suatu harapan besar bagi masyarakat Indonesia yang sangat dinantikan karena banyak kepentingan publik menyangkut regulasi tersebut.

## REFERENSI

1. <https://apjii.or.id/survei>
2. Lembaga Studi dan Advokasi Masyarakat (2019), Pentingnya Melindungi Data Pribadi bagi Perusahaan <https://elsam.or.id/pentingnya-melindungi-data-pribadi-bagiperusahaan>
3. Data Protection Act Inggris 2018
4. kemdikbud.go.id, <https://sdm.data.kemdikbud.go.id/upload/files/15Arus%20Siswa%20Revisi.pdf>
5. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.
6. Sungmi Park, dkk, (2018). *A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement*. DFRWS 2018 Europe-Proceedings of the Fifth Annual DFRWS Europe. [Volume 24, Supplement, March 2018, Pages S93-S100. https://doi.org/10.1016/j.diin.2018.01.012](https://doi.org/10.1016/j.diin.2018.01.012)
7. Soekanto S., & Mahmudji S,. (2003). *Penelitian Hukum Normatif, Suatu Tinjauan Singkat*. Jakarta: Raja Grafindo Persada.
8. Sinaga, E. M. C. & Putri, M. C. (2020). Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0. *Jurnal Recht Vinding*, 9 (2), 237-256. <http://dx.doi.org/10.33331/rechtsvinding.v9i2.428>
9. Prasetyo, T., & Karo-Karo, R. (2020). *Pengaturan Perlindungan Data Pribadi di Indonesia (Perspektif Teori Keadilan Bermartabat)*. Bandung: Nusa Media.
10. Manurung, E., & Lestari, E. (2020). Kajian Perlindungan E-Payment Berbasis Qr-Code Dalam E-Commerce. *Jurnal Penelitian dan Pengembangan Sains dan Humaniora*, 4(1), 28-36. <http://dx.doi.org/10.23887/jppsh.v4i1.24323>
11. Djafar W., & Komarudin A. (2014). *Perlindungan Hak Atas Privasi Di Internet-Beberapa Penjelasan Kunci*. Jakarta: Elsam.
12. Situmeang, S.M. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *SASI*, 27(1), 38-52. <https://doi.org/10.47268/sasi.v27i1.394>
13. Kurnia, T., [Liputan6.com https://www.liputan6.com/tekno/read/3431122/perlindungan-data-uni-eropa-terganas-di-dunia-berikut-7-faktanya](https://www.liputan6.com/tekno/read/3431122/perlindungan-data-uni-eropa-terganas-di-dunia-berikut-7-faktanya)
14. The EU General Data Protection Regulation 2016
15. Personal Data Protection Act Singapore 2012
16. RUU Perlindungan Data Pribadi Republik Indonesia