DISIPLIN
JURNAL ILMU HUKUM
http://disiplin.stihpada.ac.id/
P-ISSN: 1411-0261 | E-ISSN: 2746-394X
Volume 30 Issue 4 Desember 2024 Page : 163-170

Alamat:
Jl. Kol. H. Animan Achyad (d/h. Jl. Sukabangun II) KM. 6,5 No. 1610
Kelurahan Sukabangun Kecamatan Sukarami. Palembang.
Telp: 0711-418873/ email: jurnaldisiplin@gmail.com

Perlindungan Data Pribadi Dalam Cloud Computing: Perspektif Hukum

Tobi Haryadi[1]
[1]*Sekolah Tinggi Ilmu Hukum Sumpah Pemuda, E-mail : tobi@stihpada.ac.id*

Info Artikel

Kata Kunci:
Perlindungan Data Pribadi, Cloud Computing, Hukum.

Abstrak

Perkembangan teknologi informasi yang pesat telah mendorong adopsi cloud computing sebagai solusi penyimpanan dan pengelolaan data. Namun, penggunaan teknologi ini menimbulkan tantangan dalam perlindungan data pribadi, terutama dari perspektif hukum. Fokus utama kajian ini mencakup prinsip-prinsip perlindungan data, kewajiban penyedia layanan cloud, hak-hak pengguna, serta tantangan hukum dalam penegakan perlindungan data pribadi. Bahwa meskipun telah ada regulasi yang mengatur perlindungan data pribadi, masih terdapat celah hukum dan tantangan dalam implementasinya, terutama terkait yurisdiksi, tanggung jawab penyedia layanan, serta keamanan data. Oleh karena itu, diperlukan peningkatan regulasi dan kerja sama antara berbagai pihak guna memastikan perlindungan data pribadi dalam lingkungan cloud computing yang lebih optimal.

Abstract: *The rapid development of information technology has encouraged the adoption of cloud computing as a data storage and management solution. However, the use of this technology poses challenges in the protection of personal data, especially from a legal perspective. This study analyses the protection of personal data in cloud computing based on the applicable legal framework, both at the national and international levels. The main focus of this study includes the principles of data protection, the obligations of cloud service providers, the rights of users, as well as legal challenges in the enforcement of personal data protection. The results show that although there are regulations governing the protection of personal data, there are still legal gaps and challenges in their implementation, especially regarding jurisdiction, service provider responsibilities, and data security. Therefore, it is necessary to improve regulations and cooperation between various parties to ensure more optimal protection of personal data in the cloud computing environment.*

Keywords: Personal Data Protection, Cloud Computing, Law.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam cara individu, perusahaan, dan pemerintah menyimpan serta mengelola data. Salah satu inovasi yang semakin berkembang adalah *cloud computing*, yaitu model komputasi berbasis internet yang memungkinkan pengguna untuk menyimpan, mengelola, dan mengakses data melalui jaringan tanpa harus memiliki infrastruktur fisik secara langsung (Mell, P., & Grance, T. 2011). Teknologi ini menawarkan berbagai keuntungan, seperti efisiensi biaya operasional, fleksibilitas dalam akses data, serta peningkatan kapasitas penyimpanan yang dapat disesuaikan dengan kebutuhan pengguna (Rittinghouse, J. W., & Ransome, J. F. 2017).

Namun, di balik berbagai manfaatnya, *cloud computing* juga menghadirkan tantangan baru, terutama dalam aspek perlindungan data pribadi. Data pribadi yang disimpan dalam

layanan *cloud* umumnya dikelola oleh penyedia layanan pihak ketiga yang sering kali beroperasi di berbagai yurisdiksi hukum yang berbeda. Hal ini menimbulkan berbagai risiko, seperti akses tidak sah oleh pihak yang tidak berwenang, kebocoran data akibat serangan siber, serta ketidakjelasan dalam tanggung jawab hukum jika terjadi pelanggaran (Solove, D. J. 2020). Selain itu, perbedaan regulasi antara satu negara dengan negara lainnya menimbulkan kesulitan dalam menegakkan hak-hak pengguna atas data pribadinya.

Di Indonesia, perlindungan data pribadi telah mendapatkan perhatian khusus dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang-undang ini mengatur berbagai aspek perlindungan data, termasuk hak-hak subjek data, kewajiban pengendali data, serta sanksi atas pelanggaran yang terjadi (Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi). Namun, penerapan perlindungan data dalam konteks *cloud computing* masih menghadapi berbagai tantangan, seperti kepatuhan terhadap regulasi lintas negara serta tanggung jawab hukum dalam hubungan antara pengguna dan penyedia layanan *cloud*. Sistem yang mengumpulkan, menyimpan, memproses, memproduksi, dan mengirimkan informasi secara efisien dan cepat ke masyarakat dan sektor bisnis termasuk dalam teknologi informasi.

Karena data disimpan di tempat yang aman, pengguna hanya membayar untuk apa yang mereka gunakan, dan tidak ada biaya lisensi yang terkait dengan komputasi awan, komputasi awan dapat membantu bisnis mengurangi biaya. Penyimpanan data/informasi elektronik yang dilakukan penyedia layanan CC itu sendiri pada dasarnya merupakan bagian dari sebuah perjanjian layanan atau *Service Level Agreement* ("SLA") yang disepakati antara penyelenggara CC dengan *customer*. Penempatan data/informasi elektronik oleh penyedia layanan CC secara teknis dapat dilakukan di mana saja sesuai dengan pertimbangan masing-masing penyedia. Dengan demikian, aspek keamanan dan kepastian hukum harus dipertimbangkan saat memanfaatkan teknologi informasi, media, dan komunikasi secara optimal. Oleh karena itu, untuk menjaga keamanan di dunia maya, ada tiga cara: hukum, teknologi, sosial, budaya, dan etika. Karena tanpa kepastian hukum, masalah pemanfaatan teknologi informasi menjadi tidak optimal, pendekatan hukum bersifat mutlak untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem secara elektronik.

METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian hukum normatif, yaitu penelitian yang berfokus pada kajian hukum dengan menganalisis peraturan perundang-undangan, doktrin hukum, serta prinsip-prinsip hukum yang relevan.

PEMBAHASAN

Cloud computing adalah model komputasi berbasis internet yang memungkinkan pengguna untuk menyimpan, mengelola, dan mengakses data melalui layanan pihak ketiga tanpa perlu memiliki infrastruktur fisik sendiri (Mell, P., & Grance, T. 2011). *National Institute of Standards and Technology* (NIST) mendefinisikan *cloud computing* sebagai model yang memungkinkan akses jaringan sesuai permintaan terhadap sekumpulan sumber

daya komputasi yang dapat dikonfigurasi (seperti jaringan, server, penyimpanan, aplikasi, dan layanan) dengan upaya pengelolaan minimal (Rittinghouse, J. W., & Ransome, J. F. 2017). *Cloud computing* telah menjadi salah satu inovasi teknologi yang signifikan dalam beberapa dekade terakhir. Dengan kemampuan untuk menyimpan, mengelola, dan mengakses data dari mana saja, *cloud computing* menawarkan kemudahan dan efisiensi yang luar biasa. Namun, kemajuan ini juga menimbulkan kekhawatiran tentang perlindungan data pribadi yang disimpan di *cloud*. Dari perspektif hukum, ada beberapa tantangan dan isu yang perlu diperhatikan dalam rangka melindungi data pribadi dalam *sistem cloud computing. Cloud computing* memiliki beberapa karakteristik utama, yaitu:

1. *On-Demand Self-Service*: Pengguna dapat mengakses layanan kapan saja tanpa interaksi langsung dengan penyedia layanan.
2. *Broad Network Access: Layanan cloud* dapat diakses melalui berbagai perangkat, seperti komputer, tablet, dan ponsel pintar.
3. *Resource Pooling*: Sumber daya komputasi dikumpulkan dan dialokasikan secara dinamis kepada berbagai pengguna.
4. *Rapid Elasticity*: Kapasitas layanan dapat diperbesar atau diperkecil sesuai kebutuhan pengguna.
5. *Measured Service*: Penggunaan sumber daya dipantau dan diukur secara transparan (Kuner, C. 2013).

Data pribadi merujuk pada setiap informasi yang berkaitan dengan individu yang dapat diidentifikasi secara langsung maupun tidak langsung. Dalam konteks *cloud computing*, data pribadi meliputi informasi seperti nama, alamat, nomor identitas, riwayat transaksi, hingga data sensitif seperti informasi medis dan *biometric* (Solove, D. J. 2020). Dalam layanan *cloud*, data pribadi disimpan di pusat data yang dapat berada di berbagai lokasi di dunia. Hal ini menimbulkan tantangan dalam hal yurisdiksi hukum dan perlindungan terhadap data pribadi yang diunggah ke dalam layanan cloud (Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi). Tantangan hukum dalam perlindungan data pribadi di *cloud computing* meliputi: Kurangnya kesadaran masyarakat, Infrastruktur yang belum memadai, Koordinasi antar-lembaga yang kurang, Risiko keamanan yang signifikan. Untuk mengatasi tantangan-tantangan tersebut, diperlukan upaya untuk meningkatkan kesadaran dan kemampuan dalam melindungi data pribadi.

Berikut beberapa upaya yang dapat dilakukan:

1. Meningkatkan kesadaran masyarakat dan organisasi kecil tentang pentingnya perlindungan data
2. Melakukan sosialisasi dan pelatihan untuk karyawan
3. Memilih penyedia layanan *cloud* yang dapat dipercaya dan memiliki fitur keamanan yang handal
4. Menerapkan kebijakan keamanan yang ketat
5. Menggunakan enkripsi data
6. Mengimplementasikan mekanisme otentikasi yang kuat
7. Membuat kata sandi yang kuat
8. Menggunakan VPN untuk mengakses *cloud* dari jaringan *Wi-Fi* umum

Salah satu tantangan terbesar dalam perlindungan data pribadi di *cloud computing* adalah masalah kedaulatan data. Data yang disimpan dalam *cloud* tidak selalu berada dalam yurisdiksi hukum negara asal pengguna, melainkan dapat disimpan di berbagai pusat data di negara yang berbeda. Hal ini menimbulkan pertanyaan hukum mengenai:

1. Hukum mana yang berlaku jika terjadi pelanggaran data
2. Siapa yang bertanggung jawab jika terjadi kebocoran data
3. Bagaimana mekanisme penegakan hukum atas pelanggaran data pribadi (European Parliament and Council. 2016).

Sebagai contoh, penyedia layanan *cloud* besar seperti *Amazon Web Services* (AWS) dan *Google Cloud* memiliki pusat data di berbagai negara. Jika seorang pengguna di Indonesia menyimpan data pribadinya di layanan *cloud* yang berbasis di Amerika Serikat atau Eropa, maka data tersebut dapat tunduk pada hukum negara tempat pusat data berada. Indonesia tidak terlibat dalam perlindungan dan privasi data instrumen internasional. Negara-negara Asia seperti Jepang, Singapura, Korea Selatan, dan Cina adalah pemimpin dalam perlindungan data pribadi dan dekat dengan Indonesia. Indonesia, sebagai kekuatan Asia baru, harus mempertimbangkan peran mereka dalam melindungi rakyatnya. Saat ini, Indonesia memiliki dasar hukum untuk membuat hukum internasional yang berlaku di tingkat nasional karena hukumnya dapat meratifikasi instrumen hukum internasional. Indonesia telah menandatangani Pedoman Organisasi Kerja Sama Ekonomi dan Pembangunan (OECD) pada tahun 2004, yang bertujuan untuk memastikan bahwa peraturan yang mengatur privasi dan perlindungan data diterapkan dengan benar.

Legislasi negara anggota didorong oleh keanggotaan ini untuk mempromosikan perlindungan privasi dan kerja sama ekonomi, terutama dalam perdagangan elektronik antara anggota. Tidak hanya karena alasan ekonomi, kebijakan privasi harus dimasukkan ke dalam hukum hak asasi manusia. Privasi adalah hak asasi manusia, dan salah satu cara untuk menghormati hak ini adalah dengan melindungi data pribadi. Karena belum ada undang-undang yang jelas yang mengatur privasi dan perlindungan data di Indonesia, orang khawatir tentang keamanan data mereka. Oleh karena itu, perlindungan data pribadi dan privasi telah menjadi prioritas utama di era kontemporer saat ini. Meskipun banyak negara telah menetapkan hukum yang kuat untuk melindungi data pribadi, hukum Indonesia tidak.

Kebutuhan akan privasi dan perlindungan data pribadi telah meningkat seiring dengan globalisasi, kekuatan media, dan ilmu pengetahuan dan teknologi. Sejarah Indonesia sendiri adalah sumber tantangan untuk privasi dan perlindungan data regulasi. Indonesia mengalami kesulitan besar dalam menentukan dan mengatur privasi sebagai negara Asia. Privasi belum menjadi perhatian sebagian besar negara Asia. Dalam banyak negara Asia, termasuk Indonesia, privasi belum dianggap sebagai masalah "serius". Kebanyakan orang Asia tinggal dalam komunitas konvensional yang tidak memperhatikan privasi. Di era teknologi informasi dan komunikasi, istilah privasi sebagai hak asasi manusia menjadi penting. Bisnis dan organisasi yang terus mengumpulkan, berbagi, mengolah, menyimpan, dan bahkan menjual data pribadi sebagai komoditas saat ini sangat berharga, terutama yang berkaitan dengan konsumen. Sekarang, sejumlah besar data pribadi dapat dikumpulkan dan digabungkan dari pengguna internet dalam lingkungan jaringan untuk membuat profil dari

aktivitas dan preferensi online mereka. Dalam beberapa kasus, pemilik data mungkin tidak tahu bahwa ini terjadi. Menjaga privasi konsumen jauh lebih mudah di dunia jaringan daripada di dunia fisik.

Pasal 26 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik membahas bagaimana melindungi data pribadi di media elektronik, dan menyatakan bahwa:

(1) Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.
(2) Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

Pada masa lalu data dan *software* komputer tidak termasuk dalam suatu hal yang dapat diterpakan prinsip *strict liability* karena data dan *software* dikategorikan sebagai *intangible asset*, namun ternyata hal tersebut justru telah mengakibatkan perkembangan industrinya menjadi negative bagi kepentingan perlindungan konsumen (Makarim, 2010:225). Dalam hal ini, tanggung jawab penyedia layanan komputasi awan dapat dikaitkan dengan teori tanggung jawab penyelenggara sistem elektronik. Dalam praktik, pembuatan sistem biasanya dilakukan dalam rangka hubungan bisnis dengan konsumen, atau pihak ketiga, jika sistem tersebut tidak dirancang untuk digunakan sendiri. Selain itu, penyelenggara harus mempertimbangkan untuk mengasuransi sistem sebelum berkomunikasi dengan pelanggan, seperti yang biasanya dilakukan. Penyelenggara bertanggung jawab kepada masyarakat umum, terutama mereka yang menjadi pelanggan atau konsumennya, dengan berupaya sebaik mungkin untuk meminimalkan segala macam risiko.

Selain bertanggung jawab kepada konsumen, penyedia juga bertanggung jawab untuk mengikuti standar lokal dan pedoman pemerintah untuk melakukan upaya terbaik dan menjaga kualitas layanan *(Quality of Services)*. Pada dasarnya, ia bertanggung jawab secara mutlak atas semua kerugian yang ditimbulkannya kepada pihak lain. Namun, jika ada mekanisme tertentu yang mengukur *best practices*, tanggung jawabnya dapat dibatasi. Dalam hal tanggung jawab hukum, ada dua hal yang membedakan tanggung jawab hukum jika dilihat dari adanya kewajiban sebelum atau setelah peristiwa tak tentu (kejadian):

1. tanggung jawab sebelum terjadi suatu kerjadian dan
2. tanggung jawab setelah kejadian (Makarim, 2010:159).

Tanggung jawab sebelum suatu kejadian (*ex-ante liability*) adalah tanggung jawab untuk mematuhi semua Undang-Undang dan/atau regulasi administrasi negara dalam rangka memberikan suatu yang layak kepada *public* (Makarim, 2010:160). Namun, dalam kasus tanggung jawab setelah kejadian, atau tanggung jawab setelah kejadian, orang yang dirugikan bertanggung jawab untuk memulihkan keadaan mereka ke keadaan yang semula. Kepentingan tersebut ditunjukkan dengan membayar sejumlah kompensasi yang sebanding dengan kerugian yang dialami, sebagai bentuk kompensasi dari perbuatan tersebut (Makarim, 2010). Dalam hal tanggung jawab penyedia layanan komputasi awan, ada 4 (empat) masalah yang ingin diketahui, yaitu:

1. Pihak yang memiliki otentikasi atau akses kontrol kepada data pelanggan.

2. Lokasi pusat data pelanggan disimpan.
3. Tindakan yang dilakukan oleh penyedia layanan komputasi awan untuk melindungi data pelanggan.
4. Pertanggung jawaban dari penyedia layanan komputasi awan apabila data pelanggan tersebut bocor atau disalahgunakan.

Dalam hal autentikasi atau akses kontrol terhadap data pelanggan, layanan *Microsoft* memiliki dua jenis autentikasi yang berbeda berdasarkan lokasi *server*. Jika layanan awan berada di *server Microsoft*, maka kontrol akses dan autentikasi ada di *Microsoft*; jika layanan awan berada di server mitra *Microsoft*, seperti Telkom atau Infinys, maka kontrol akses dan autentikasi ada di perusahaan-perusahaan mitra *Microsoft* tersebut. *Microsoft* melakukan sertifikasi layanan komputasi awannya untuk memastikan desain dan keamanan yang baik. Teknologi terkini, seperti virtualisasi, partisi, *firewall*, manajemen hak informasi, enkripsi, dan desain pusat data tersebar, melindungi data pelanggan dalam layanan komputasi awan *Microsoft*. IBM sebagai penyedia teknologi dan layanan berupaya semaksimal mungkin untuk memberikan layanan secara teknis dalam melindungi data pelanggan. Keamanan mencakup privasi, integritas, dan aksesibilitas sesuai dengan tingkat keamanan yang diinginkan pelanggan dalam Perjanjian Tingkat Layanan. Perjanjian Tingkat Layanan juga mencakup kebijakan, prosedur, standar layanan, dan bantuan yang berkaitan dengan tingkat keamanan yang diinginkan pelanggan.

Microsoft tidak akan membocorkan atau menyalahgunakan data pelanggan karena *Microsoft* menghargai privasi pelanggan dan melindunginya. *Microsoft* tidak akan mengungkapkan informasi pribadi Anda di luar Microsoft dan anak perusahaan yang dikendalikan dan afiliasi tanpa persetujuan Anda (Microsoft *Online Privacy Statement*, 2021). Pasal privasi dan keamanan data Undang-Undang ITE dapat menjerat *Microsoft* jika terjadi pelanggaran. Untuk meningkatkan perlindungan data pribadi dalam *cloud computing*, beberapa langkah yang dapat dilakukan antara lain:

1. Penguatan Implementasi Undang-Undang Perlindungan Data Pribadi dengan memastikan kepatuhan oleh penyedia layanan *cloud* yang beroperasi di Indonesia.
2. Peningkatan Kesadaran Pengguna tentang hak-hak mereka dalam perlindungan data pribadi.
3. Kolaborasi Internasional untuk harmonisasi regulasi lintas negara guna mengatasi permasalahan yurisdiksi hukum.

Untuk meningkatkan perlindungan data pribadi dalam *cloud computing*, diperlukan tiga langkah utama:

1. Penguatan regulasi dan penegakan hukum guna memastikan kepatuhan penyedia layanan *cloud* terhadap standar perlindungan data yang ketat.
2. Peningkatan kesadaran pengguna mengenai hak-hak mereka dalam pengelolaan data pribadi serta pentingnya menerapkan langkah-langkah keamanan.
3. Kolaborasi internasional untuk menciptakan mekanisme perlindungan data yang lebih terpadu dan mampu mengatasi tantangan lintas negara.

Dengan implementasi perlindungan data pribadi yang efektif dan komprehensif, risiko terkait keamanan dan privasi dalam *cloud computing* dapat diminimalkan. Ke depan, perlu

ada sinergi antara pemerintah, penyedia layanan *cloud*, dan masyarakat guna menciptakan ekosistem digital yang aman dan berkelanjutan.

KESIMPULAN

Perlindungan data pribadi dalam *cloud computing* menjadi aspek yang sangat penting dalam era digital, mengingat semakin banyak individu dan organisasi yang bergantung pada layanan *cloud* untuk menyimpan dan mengelola informasi. Meskipun *cloud computing* menawarkan berbagai manfaat, seperti fleksibilitas, efisiensi, dan skalabilitas, teknologi ini juga menghadirkan tantangan hukum yang kompleks, terutama dalam hal keamanan data, yurisdiksi hukum, serta hak pengguna atas data pribadinya. Salah satu tantangan utama adalah ketidakjelasan yurisdiksi hukum, karena data yang disimpan dalam *cloud* dapat berada di berbagai negara dengan regulasi yang berbeda. Hal ini menimbulkan permasalahan terkait hukum mana yang berlaku dan bagaimana mekanisme penegakan hukum dapat diterapkan jika terjadi pelanggaran. Selain itu, ancaman terhadap keamanan data pribadi, seperti peretasan, akses tidak sah, dan kebocoran data, semakin meningkat seiring dengan berkembangnya teknologi serangan siber. Di Indonesia, perlindungan data pribadi telah mendapatkan landasan hukum melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)**.** Regulasi ini memberikan hak kepada subjek data serta menetapkan kewajiban bagi pengendali dan pemroses data. Namun, jika dibandingkan dengan regulasi internasional seperti *General* Data *Protection Regulation* (GDPR) di Uni Eropa, Undang-Undang Perlindungan Data Pribadi masih memerlukan penguatan dalam hal implementasi, mekanisme pengawasan, serta harmonisasi dengan regulasi *global*.

DAFTAR PUSTAKA

Cameron G. Shilling, 2011. *Privacy and Data Security : New Challenges of The Digital Age,* New Hampshire Bar Journal.

Diaz Gwijangge*, Peran TIK Dalam Pembangunan Karakter Bangsa*, Makalah : Pusat Teknologi Informasi dan Komunikasi Pendidikan Kementerian Pendidikan Nasional, Sulawesi Selatan, 14 Juni 2011.

Edmon Makarim, 2010. *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*, Raja Grafindo Persada, Jakarta.

Jerry Kang, *Information Privacy in Cyberspace Transaction*, Stanford Law Review Vol 50, April 1998.

Kuner, C. 2013. *Transborder Data Flows and Data Privacy Law*. Oxford University Press.

La Porta, R., Florencio Lopez, A. Shleifer, dan R. Vishny, *Investor Protection and Corporate Governance*. Journal of Financial Economics 58, 1999.

Mell, P., & Grance, T. 2011. The NIST Definition of Cloud Computing. National Institute of Standards and Technology.

Microsoft Online Privacy Statement, http://privacy.microsoft.com/

Miles Mattew dan Michael Huberman, 1992. *Analisis Data Kualitatif,* Universitas Indonesia, Jakarta.

Peter Mell dan Timothy Grance, *The NIST Definition of Cloud Computing*.

Purwanto, 2007. *Penelitian Tentang Perlindungan Hukum Data Digital*, Badan Pembinaan Hukum Nasional, Jakarta.

Richardus Eko Indrajit, *Fenomena Kebocoran Data : Mencari Sumber Penyebab dan Akar Permasalahannya*, http://www.idsirtii.or.id

Rittinghouse, J. W., & Ransome, J. F. 2017. Cloud Computing: Implementation, Management, and Security. CRC Press.

Shinta Dewi, 2009. *Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional*, Widya Padjajaran, Bandung.

Solove, D. J. 2020. The Digital Person: Technology and Privacy in the Information Age. New York: NYU Press.

Sonny Zulhuda, *Data Privacy in Indonesia-Quo Vadis?*, http://sonnyzulhuda.wordpress.com

Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik.

W. Michael Ryan dan Christopher M. Leoffler, 2010. *Insights into Cloud Computing*, Intellectual Property and Technology Law Journal, 22 (11).