Journal of Innovative and Creativity
Journal Homepage: https://joecy.org/index.php/joecy
e-mail: journaljoecy@gmail.com

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2775-771X (Online)
ISSN 2962-570X (Printed)
6 (1) 2026, Page: 22039-22044

Implikasi Hukum Pidana Terhadap Penyalahgunaan Data Pribadi dalam Ekosistem Digital

Sepriandison Saragih
Universitas HKBP Nommensen Pematangsiantar
Corresponding Author: sepriandison123@gmail.com

Published: April, 2026

ABSTRACT

This article examines the implications of criminal law for the misuse of personal data within the digital ecosystem. The rapid development of digital technology has positioned personal data as a strategic asset while simultaneously increasing the risk of data breaches, unauthorized use, and other forms of misuse that threaten privacy rights and legal certainty. The objective of this study is to analyze the role of criminal law in providing legal protection against personal data misuse and to assess its effectiveness in the context of the Indonesian legal system. The research object focuses on the regulation and enforcement of criminal provisions related to personal data protection in the digital environment. This study employs normative legal research using statutory, conceptual, and case approaches. Legal materials are analyzed qualitatively through systematic and teleological interpretation to obtain a comprehensive understanding of criminal liability for personal data violations. The results show that criminal law has a significant role in strengthening personal data protection through the criminalization of unlawful data processing and the recognition of corporate criminal liability. The application of criminal sanctions contributes to increased compliance by digital service providers and improved data governance. However, the study also finds that enforcement effectiveness remains constrained by challenges in digital evidence, cross-border jurisdiction, and institutional capacity. It is concluded that criminal law constitutes an essential instrument in personal data protection, but its effectiveness requires integration with administrative and civil mechanisms as well as institutional strengthening to ensure sustainable and effective protection in the digital ecosystem.

Keyword: *Ciminal Law; Prsonal Data; Digital Cosystem; Legal Protection; Data Privacy*

ABSTRAK

Artikel ini membahas implikasi hukum pidana terhadap penyalahgunaan data pribadi dalam ekosistem digital. Perkembangan teknologi digital telah menjadikan data pribadi sebagai aset strategis, namun sekaligus meningkatkan risiko kebocoran dan penyalahgunaan data yang berdampak pada pelanggaran hak privasi dan kepastian hukum. Penelitian ini bertujuan untuk menganalisis peran hukum pidana dalam memberikan perlindungan hukum terhadap penyalahgunaan data pribadi serta menilai efektivitas penerapannya dalam sistem hukum Indonesia. Objek penelitian difokuskan pada pengaturan dan penegakan ketentuan pidana terkait perlindungan data pribadi di lingkungan digital. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan peraturan perundang-undangan, konseptual, dan kasus. Bahan hukum dianalisis secara kualitatif melalui penafsiran sistematis dan teleologis. Hasil penelitian menunjukkan bahwa hukum pidana memiliki peran penting dalam memperkuat perlindungan data pribadi melalui kriminalisasi perbuatan penyalahgunaan data dan pengaturan pertanggungjawaban pidana korporasi. Penerapan sanksi pidana mendorong peningkatan kepatuhan penyelenggara sistem elektronik, meskipun efektivitas penegakannya masih menghadapi tantangan pembuktian digital dan keterbatasan kapasitas institusional. Penelitian ini menyimpulkan bahwa hukum pidana merupakan instrumen penting dalam perlindungan data pribadi, namun perlu disinergikan dengan mekanisme hukum lainnya agar perlindungan dapat berjalan secara optimal.

Kata kunci: Hukum Pidana, Data Dribadi, Ekosistem Digital, Perlindungan Hukum.

© The Author(s). 2025 Open Access This article is licensed under a Creative Commons Atibution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi besar dalam berbagai aspek kehidupan sosial, ekonomi, dan pemerintahan. Ekosistem digital yang ditandai dengan masifnya penggunaan internet, platform media sosial, layanan keuangan digital, serta sistem pemerintahan berbasis elektronik telah menjadikan data pribadi sebagai salah satu aset paling bernilai di era digital. Data pribadi

tidak hanya berfungsi sebagai identitas individu, tetapi juga menjadi dasar pengambilan keputusan, personalisasi layanan, dan efisiensi aktivitas ekonomi digital.

Namun, meningkatnya ketergantungan terhadap teknologi digital juga diiringi dengan tingginya risiko penyalahgunaan data pribadi. Berbagai kasus kebocoran data, perdagangan data ilegal, pencurian identitas, hingga pemanfaatan data pribadi untuk penipuan dan kejahatan siber menunjukkan bahwa perlindungan data pribadi masih menghadapi tantangan serius. Penyalahgunaan data pribadi tidak hanya menimbulkan kerugian ekonomi bagi individu, tetapi juga berdampak pada pelanggaran hak privasi dan menurunnya kepercayaan publik terhadap penyelenggara sistem elektronik.

Dalam konteks negara hukum, perlindungan terhadap data pribadi merupakan bagian integral dari perlindungan hak asasi manusia, khususnya hak atas privasi. Negara memiliki kewajiban untuk menyediakan instrumen hukum yang efektif guna mencegah dan menanggulangi pelanggaran tersebut. Di Indonesia, penguatan perlindungan data pribadi ditandai dengan hadirnya Undang-Undang Perlindungan Data Pribadi yang memberikan landasan hukum yang lebih komprehensif, termasuk pengaturan mengenai sanksi pidana terhadap pelaku penyalahgunaan data pribadi.

Penerapan hukum pidana dalam kasus penyalahgunaan data pribadi menimbulkan implikasi yang kompleks. Di satu sisi, hukum pidana berfungsi sebagai sarana represif dan preventif untuk memberikan efek jera serta menegaskan keseriusan negara dalam melindungi data pribadi. Di sisi lain, karakteristik kejahatan siber yang bersifat lintas batas, melibatkan teknologi tinggi, serta sering dilakukan oleh korporasi digital menimbulkan tantangan dalam hal pembuktian, penegakan hukum, dan pertanggungjawaban pidana.

Berdasarkan latar belakang tersebut, artikel ini bertujuan untuk mengkaji implikasi hukum pidana terhadap penyalahgunaan data pribadi dalam ekosistem digital. Fokus pembahasan diarahkan pada bagaimana hukum pidana berperan dalam memberikan perlindungan hukum terhadap subjek data, serta tantangan dan prospek penerapannya dalam menghadapi dinamika kejahatan digital. Kajian ini diharapkan dapat memberikan kontribusi konseptual bagi pengembangan hukum pidana di bidang perlindungan data pribadi serta menjadi rujukan bagi pembuat kebijakan dan praktisi hukum dalam memperkuat tata kelola ekosistem digital yang aman dan berkeadilan.

METODE

Penelitian ini menggunakan jenis penelitian hukum normatif (doctrinal research) dengan pendekatan konseptual dan peraturan perundang-undangan. Penelitian hukum normatif dipilih karena fokus kajian diarahkan pada analisis norma hukum pidana yang mengatur penyalahgunaan data pribadi serta implikasinya dalam ekosistem digital. Selain itu, penelitian ini juga menggunakan pendekatan kasus (case approach) untuk memperkuat analisis terhadap penerapan hukum pidana dalam praktik.

Subjek penelitian dalam kajian ini bukan individu atau responden, melainkan bahan hukum yang terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang relevan, antara lain Undang-Undang Perlindungan Data Pribadi, Kitab Undang-Undang Hukum Pidana, Undang-Undang Informasi dan Transaksi Elektronik, serta peraturan pelaksana lainnya yang berkaitan dengan perlindungan data pribadi dan kejahatan siber. Bahan hukum sekunder mencakup literatur ilmiah berupa buku teks hukum, jurnal nasional dan internasional, hasil penelitian terdahulu, serta pendapat para ahli hukum. Adapun bahan hukum tersier digunakan sebagai pendukung, seperti kamus hukum dan ensiklopedia hukum.

Penelitian ini dilaksanakan dalam rentang waktu tahun 2025 dengan lokasi penelitian bersifat studi kepustakaan (library research), sehingga tidak terikat pada wilayah geografis tertentu. Seluruh data diperoleh melalui penelusuran literatur dan dokumen hukum yang relevan dengan objek penelitian.

Instrumen penelitian berupa panduan studi dokumen, yang digunakan untuk mengidentifikasi, mengklasifikasi, dan menganalisis norma hukum, konsep hukum pidana, serta putusan pengadilan yang berkaitan dengan penyalahgunaan data pribadi. Instrumen ini membantu peneliti dalam memastikan konsistensi dan ketepatan analisis terhadap bahan hukum yang dikaji.

Prosedur penelitian dilakukan melalui beberapa tahapan, yaitu pengumpulan bahan hukum, klasifikasi bahan hukum sesuai dengan jenis dan relevansinya, serta analisis secara sistematis terhadap ketentuan hukum pidana yang mengatur penyalahgunaan data pribadi. Selanjutnya, dilakukan penafsiran

hukum dengan menggunakan metode penafsiran gramatikal, sistematis, dan teleologis untuk memperoleh pemahaman yang komprehensif terhadap norma yang berlaku.

Teknik analisis data yang digunakan adalah analisis kualitatif normatif, dengan cara mengkaji bahan hukum secara mendalam untuk menarik kesimpulan berdasarkan logika hukum dan argumentasi yuridis. Hasil analisis kemudian disajikan dalam bentuk deskriptif-analitis guna menjelaskan implikasi hukum pidana terhadap penyalahgunaan data pribadi dalam ekosistem digital serta tantangan penerapannya di Indonesia.

HASIL DAN PEMBAHASAN

Hasil penelitian menunjukkan bahwa pengaturan hukum pidana terkait penyalahgunaan data pribadi dalam ekosistem digital di Indonesia telah mengalami perkembangan signifikan, khususnya setelah diberlakukannya Undang-Undang Perlindungan Data Pribadi (UU PDP). Regulasi ini memperkuat rezim perlindungan data dengan mengkriminalisasi perbuatan tertentu yang sebelumnya hanya dikenai sanksi administratif atau perdata. Berdasarkan penelusuran bahan hukum primer dan sekunder, ditemukan bahwa penyalahgunaan data pribadi dapat dikualifikasikan sebagai tindak pidana apabila memenuhi unsur perbuatan melawan hukum, kesalahan (mens rea), serta menimbulkan akibat hukum terhadap subjek data. Selain itu, hukum pidana tidak hanya menyasar pelaku perorangan, tetapi juga memungkinkan pertanggungjawaban pidana korporasi dalam konteks ekosistem digital. Untuk memperjelas hasil kajian normatif, bentuk penyalahgunaan data pribadi dan implikasi pidananya dapat diringkas sebagai berikut:

Tabel 1. Bentuk Penyalahgunaan Data Pribadi dan Implikasi Hukum Pidana

Bentuk Penyalahgunaan Data Pribadi	Unsur Pidana yang Terpenuhi	Implikasi Hukum Pidana
Pengumpulan data tanpa persetujuan	Perbuatan tanpa hak	Ancaman pidana penjara dan/atau denda
Kebocoran data akibat kelalaian	Kelalaian yang menimbulkan kerugian	Pertanggungjawaban pidana pengendali data
Perdagangan data pribadi	Kesengajaan dan tujuan komersial	Pidana terhadap pelaku dan korporasi
Pemanfaatan data untuk penipuan	Penyalahgunaan data dan akibat kerugian	Pidana kumulatif dengan tindak pidana siber

Hasil ini menunjukkan bahwa hukum pidana berperan sebagai instrumen utama dalam memberikan perlindungan terhadap data pribadi ketika pelanggaran bersifat serius dan berdampak luas.

Pembahasan ini diarahkan untuk menjawab permasalahan penelitian mengenai bagaimana implikasi hukum pidana terhadap penyalahgunaan data pribadi dalam ekosistem digital serta sejauh mana efektivitasnya dalam memberikan perlindungan hukum.

Pertama, dari perspektif perlindungan hukum, kriminalisasi penyalahgunaan data pribadi mencerminkan pengakuan negara terhadap data pribadi sebagai bagian dari hak asasi manusia, khususnya hak atas privasi. Hukum pidana berfungsi sebagai **ultimum remedium**, yang diterapkan ketika mekanisme administratif dan perdata tidak lagi memadai. Dengan demikian, penerapan sanksi pidana memberikan efek jera (deterrent effect) dan mempertegas batasan perilaku yang dapat ditoleransi dalam pengelolaan data pribadi.

Kedua, hasil penelitian menunjukkan bahwa penerapan hukum pidana memiliki implikasi langsung terhadap tata kelola ekosistem digital. Penyelenggara sistem elektronik dituntut untuk meningkatkan kepatuhan terhadap prinsip perlindungan data, seperti legalitas pemrosesan, pembatasan tujuan, dan keamanan data. Ancaman pertanggungjawaban pidana, termasuk terhadap korporasi, mendorong pelaku usaha digital untuk mengadopsi standar keamanan informasi yang lebih tinggi dan menerapkan prinsip kehati-hatian dalam pengelolaan data.

Ketiga, meskipun secara normatif pengaturan hukum pidana telah memadai, penelitian ini menemukan adanya tantangan dalam aspek penegakan hukum. Karakteristik kejahatan digital yang bersifat lintas batas, penggunaan teknologi canggih, serta keterbatasan kapasitas aparat penegak hukum

berpotensi mengurangi efektivitas penerapan sanksi pidana. Hal ini menunjukkan bahwa keberhasilan hukum pidana tidak hanya bergantung pada norma tertulis, tetapi juga pada kesiapan institusional dan koordinasi antar lembaga.

Keempat, hasil penelitian juga menunjukkan bahwa hukum pidana tidak dapat berdiri sendiri dalam melindungi data pribadi. Diperlukan sinergi antara sanksi pidana, sanksi administratif, dan mekanisme perdata agar perlindungan data pribadi bersifat komprehensif. Dalam konteks ini, hukum pidana berfungsi sebagai pilar terakhir yang memperkuat rezim perlindungan data secara keseluruhan.

Dengan demikian, pembahasan ini menegaskan bahwa implikasi hukum pidana terhadap penyalahgunaan data pribadi bersifat strategis, baik dalam menjamin perlindungan hak subjek data maupun dalam membentuk tata kelola ekosistem digital yang bertanggung jawab dan berkeadilan.

Hasil penelitian menunjukkan bahwa penerapan hukum pidana terhadap penyalahgunaan data pribadi secara normatif telah memberikan perlindungan hukum yang kuat bagi subjek data. Kriminalisasi perbuatan seperti pengumpulan data tanpa persetujuan, perdagangan data pribadi, serta penyalahgunaan data untuk tindak kejahatan menegaskan bahwa pelanggaran data pribadi tidak lagi dipandang sebagai pelanggaran administratif semata. Dengan demikian, H1 diterima karena hukum pidana berfungsi sebagai instrumen represif dan preventif yang efektif dalam menjamin perlindungan hak atas privasi di ekosistem digital.

Temuan penelitian memperlihatkan bahwa pengaturan pertanggungjawaban pidana korporasi memiliki implikasi signifikan terhadap peningkatan kepatuhan penyelenggara sistem elektronik. Dalam ekosistem digital, pelanggaran data pribadi sering kali terjadi akibat kebijakan internal, kelemahan sistem keamanan, atau kelalaian struktural perusahaan. Dengan adanya ancaman pidana terhadap korporasi dan pengurusnya, perusahaan digital terdorong untuk menerapkan standar keamanan informasi yang lebih ketat serta prinsip kehati-hatian dalam pemrosesan data pribadi. Oleh karena itu, H2 dapat diterima karena hukum pidana berperan sebagai mekanisme kontrol terhadap perilaku korporasi digital.

Meskipun secara normatif hukum pidana telah memberikan dasar perlindungan yang memadai, hasil penelitian menunjukkan bahwa efektivitas penerapannya masih menghadapi berbagai kendala. Tantangan utama meliputi kesulitan pembuktian digital, keterbatasan kemampuan forensik siber aparat penegak hukum, serta karakteristik kejahatan data pribadi yang bersifat lintas negara. Kondisi ini mengindikasikan adanya kesenjangan antara norma hukum dan implementasinya di lapangan. Dengan demikian, H3 diterima karena keberhasilan hukum pidana dalam melindungi data pribadi sangat bergantung pada kesiapan institusional dan koordinasi lintas sektor.

Penyalahgunaan data pribadi dalam ekosistem digital menempatkan hukum pidana pada posisi strategis sebagai instrumen perlindungan terakhir terhadap pelanggaran hak privasi. Dalam perspektif hukum modern, data pribadi tidak lagi dipahami sekadar sebagai informasi teknis, melainkan sebagai bagian dari identitas dan martabat individu yang wajib dilindungi oleh negara (Warren & Brandeis, 1890; Solove, 2008). Oleh karena itu, kriminalisasi terhadap penyalahgunaan data pribadi merupakan konsekuensi logis dari perkembangan masyarakat digital yang semakin bergantung pada teknologi informasi.

Secara konseptual, penerapan hukum pidana dalam perlindungan data pribadi berfungsi untuk menegaskan batas antara pemrosesan data yang sah dan perbuatan yang melanggar hukum. Solove (2008) menegaskan bahwa kerugian akibat pelanggaran privasi sering kali bersifat kumulatif dan tidak selalu dapat diukur secara ekonomi, sehingga mekanisme perdata saja tidak cukup untuk memberikan perlindungan yang efektif. Dalam konteks ini, sanksi pidana berperan sebagai sarana represif sekaligus preventif guna mencegah penyalahgunaan data yang berpotensi menimbulkan dampak sistemik.

Hasil penelitian ini menunjukkan bahwa secara normatif, pengaturan hukum pidana terkait penyalahgunaan data pribadi di Indonesia telah sejalan dengan perkembangan global. Pengaturan pidana dalam Undang-Undang Perlindungan Data Pribadi mencerminkan adopsi prinsip-prinsip perlindungan data internasional, seperti legalitas pemrosesan, pembatasan tujuan, dan akuntabilitas pengendali data (OECD, 2021; Voigt & von dem Bussche, 2017). Dengan demikian, hukum pidana tidak hanya berfungsi menghukum pelaku, tetapi juga membentuk standar perilaku yang harus dipatuhi oleh seluruh aktor dalam ekosistem digital.

Lebih lanjut, pembahasan mengenai pertanggungjawaban pidana korporasi menjadi aspek krusial dalam perlindungan data pribadi. Dalam ekosistem digital, pelanggaran data sering kali terjadi bukan semata akibat tindakan individu, melainkan sebagai hasil dari kebijakan organisasi, kelalaian sistem keamanan, atau kegagalan tata kelola data (Janssen & van den Hoven, 2015). Lodge dan Wegrich (2014) menekankan bahwa dalam konteks governance modern, korporasi harus dipandang sebagai aktor yang memiliki tanggung jawab hukum dan sosial. Oleh karena itu, pengenaan pertanggungjawaban pidana terhadap korporasi digital merupakan langkah penting untuk memastikan adanya akuntabilitas institusional.

Namun demikian, penelitian ini juga mengonfirmasi bahwa efektivitas penerapan hukum pidana terhadap penyalahgunaan data pribadi masih menghadapi berbagai tantangan. Salah satu tantangan utama adalah kompleksitas pembuktian dalam kejahatan berbasis teknologi informasi. Yakowitz (2011) menjelaskan bahwa karakteristik data digital yang mudah direplikasi, dipindahkan lintas yurisdiksi, dan dimanipulasi secara anonim menyulitkan aparat penegak hukum dalam mengidentifikasi pelaku dan membuktikan unsur kesalahan. Kondisi ini berpotensi mengurangi daya guna hukum pidana sebagai instrumen perlindungan yang efektif.

Selain itu, sifat lintas batas dari kejahatan data pribadi menimbulkan persoalan yurisdiksi dan penegakan hukum internasional. ENISA (2021) dan ICO (2020) menekankan bahwa perlindungan data pribadi membutuhkan kerja sama lintas negara, mengingat banyak platform digital beroperasi secara global. Tanpa mekanisme koordinasi internasional yang kuat, penerapan hukum pidana nasional berisiko menjadi tidak optimal dalam menghadapi pelanggaran data yang berskala transnasional.

Dalam perspektif kebijakan hukum pidana, temuan ini menguatkan pandangan bahwa hukum pidana harus ditempatkan sebagai **ultimum remedium**, bukan satu-satunya instrumen perlindungan data pribadi. Janssen, Charalabidis, dan Zuiderwijk (2012) menegaskan pentingnya pendekatan multi-instrumen yang mengombinasikan sanksi pidana, sanksi administratif, dan mekanisme perdata. Pendekatan ini tidak hanya meningkatkan efektivitas perlindungan hukum, tetapi juga memberikan fleksibilitas dalam menangani berbagai tingkat pelanggaran data pribadi.

Dengan demikian, pembahasan ini menunjukkan bahwa implikasi hukum pidana terhadap penyalahgunaan data pribadi bersifat multidimensional. Di satu sisi, hukum pidana memperkuat perlindungan hak privasi dan meningkatkan akuntabilitas pelaku ekosistem digital. Di sisi lain, efektivitasnya sangat bergantung pada kesiapan institusional, kapasitas penegakan hukum, serta integrasi dengan rezim perlindungan data yang lebih luas. Oleh karena itu, penguatan hukum pidana harus diiringi dengan pembaruan kebijakan, peningkatan kapasitas aparat penegak hukum, dan penguatan kesadaran hukum para pelaku digital agar tujuan perlindungan data pribadi dapat tercapai secara optimal.

Implikasi Temuan

Berdasarkan hasil dan pembahasan, dapat disimpulkan bahwa hukum pidana memiliki implikasi strategis dalam memperkuat perlindungan data pribadi di ekosistem digital. Namun, efektivitasnya memerlukan dukungan kebijakan non-pidana, peningkatan kapasitas penegak hukum, serta sinergi antara pendekatan pidana, administratif, dan perdata.

KESIMPULAN

Penelitian ini menyimpulkan bahwa penerapan hukum pidana terhadap penyalahgunaan data pribadi dalam ekosistem digital memiliki peran yang penting dan strategis dalam memberikan perlindungan hukum bagi subjek data. Kriminalisasi terhadap berbagai bentuk penyalahgunaan data pribadi menunjukkan komitmen negara dalam melindungi hak atas privasi sebagai bagian dari hak asasi manusia di era digital. Dengan demikian, hukum pidana berfungsi sebagai instrumen ultimum remedium yang mempertegas batasan perilaku yang dilarang dalam pengelolaan data pribadi. Hasil penelitian juga menunjukkan bahwa pengaturan pertanggungjawaban pidana korporasi memberikan implikasi positif terhadap peningkatan kepatuhan penyelenggara sistem elektronik. Ancaman sanksi pidana mendorong korporasi digital untuk memperkuat tata kelola data, meningkatkan sistem keamanan informasi, serta menerapkan prinsip kehati-hatian dalam pemrosesan data pribadi. Hal ini berkontribusi pada terciptanya

ekosistem digital yang lebih bertanggung jawab dan berkeadilan. Namun demikian, penelitian ini menemukan bahwa efektivitas penerapan hukum pidana masih menghadapi berbagai kendala dalam praktik penegakan hukum. Kompleksitas pembuktian digital, keterbatasan kapasitas aparat penegak hukum, serta sifat kejahatan data pribadi yang lintas batas negara menjadi tantangan utama yang perlu diatasi. Oleh karena itu, keberhasilan perlindungan data pribadi tidak hanya bergantung pada kekuatan norma hukum pidana, tetapi juga pada kesiapan institusional, koordinasi lintas sektor, dan sinergi dengan instrumen hukum administratif dan perdata.

REFERENSI

Bennett, C. J., & Raab, C. D. (2018). *The governance of privacy: Policy instruments in global perspective* (2nd ed.). MIT Press.

Bygrave, L. A. (2014). *Data privacy law: An international perspective*. Oxford University Press.

Cate, F. H., & Mayer-Schönberger, V. (2013). Notice and consent in a world of big data. *International Data Privacy Law, 3*(2), 67–73. https://doi.org/10.1093/idpl/ipt005

ENISA. (2021). *Personal data protection engineering*. European Union Agency for Cybersecurity.

Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review, 34*(2), 279–288. https://doi.org/10.1016/j.clsr.2017.12.003

Greenleaf, G. (2018). Global data privacy laws 2017: 120 national data privacy laws. *Privacy Laws & Business International Report, 145*, 10–13.

ICO. (2020). *Guide to the General Data Protection Regulation (GDPR)*. Information Commissioner's Office.

ISO. (2013). *ISO/IEC 27001:2013 – Information security management systems*. International Organization for Standardization.

Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits, adoption barriers and myths of open data and open government. *Information Systems Management, 29*(4), 258–268. https://doi.org/10.1080/10580530.2012.716740

Janssen, M., & van den Hoven, J. (2015). Big and open linked data (BOLD) in government: A challenge to transparency and privacy? *Government Information Quarterly, 32*(4), 363–368. https://doi.org/10.1016/j.giq.2015.11.007

Kuner, C. (2015). *European data protection law: Corporate compliance and regulation*. Oxford University Press.

Lodge, M., & Wegrich, K. (2014). *Managing regulation: Regulatory analysis, politics and policy*. Palgrave Macmillan.

OECD. (2021). *OECD privacy guidelines*. Organisation for Economic Co-operation and Development.

Rosadi, S. D. (2023). *Perlindungan data pribadi dalam era digital*. RajaGrafindo Persada.

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Solove, D. J., & Schwartz, P. M. (2020). *Information privacy law* (6th ed.). Wolters Kluwer.

Spiekermann, S., & Cranor, L. F. (2009). Engineering privacy. *IEEE Transactions on Software Engineering, 35*(1), 67–82. https://doi.org/10.1109/TSE.2008.88

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.

Yakowitz, J. (2011). Tragedy of the data commons. *Harvard Journal of Law & Technology, 25*(1), 1–67.

Zarsky, T. Z. (2016). Incompatible: The GDPR in the age of big data. *Seton Hall Law Review, 47*(4), 995–1020.

Peraturan Perundang-undangan

Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*.

Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik* (sebagaimana telah diubah).

Indonesia. (2023). *Kitab Undang-Undang Hukum Pidana*.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2021). *Pedoman perlindungan data pribadi dalam sistem elektronik*.