

Peningkatan Kesadaran Hukum Warga Terhadap Perlindungan Data Pribadi dan Konsekuensi Hukum di Era Digital

Syukron Abdul Kadir¹⁾, Noor Rahmat²⁾, Bhenu Artha³⁾, Amirudin⁴⁾, Sumantri⁵⁾

^{1,2,3,4,5} Universitas Widya Mataram, Indonesia

Email: syukronkadir@gmail.com¹, noorrohmat@yahoo.co.id², bhenoz27@gmail.com³, amirdinn7@gmail.com⁴, triv0357@gmail.com⁵

Correspondent : bhenoz27@gmail.com³

Abstract: *The rapid development of information technology has led to an increased risk of personal data misuse in society. A lack of understanding regarding the legal basis and methods for protecting personal data often leaves the general public vulnerable to cybercrimes, such as online fraud and illegal commercial lending. This community service activity aims to provide education and legal counseling regarding the protection of personal data, the legal framework governing it, and the legal consequences for violators. The method used was legal counseling in the form of interactive lectures and question-and-answer sessions. The event was held on Friday, August 7, 2026, in the Celeban area, Umbulharjo District, Yogyakarta City, and was attended by 11 local residents. The results of this activity showed an increase in residents' understanding of the importance of maintaining the confidentiality of personal data, such as the National Identity Number (NIK) and the photo on their ID card, as well as an understanding of the legal protection mechanisms stipulated in Law No. 27 of 2022 on Personal Data Protection (PDP Law).*

Abstrak : *Perkembangan teknologi informasi yang masif membawa dampak pada rentannya penyalahgunaan data pribadi di masyarakat. Ketidaktahuan mengenai dasar hukum dan cara melindungi data pribadi sering kali menjadikan masyarakat awam sebagai korban kejahatan siber, seperti penipuan daring dan pinjaman komersial ilegal. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk memberikan edukasi dan penyuluhan hukum terkait perlindungan data pribadi, dasar hukum yang mengaturnya, serta konsekuensi hukum bagi pelanggarnya. Metode yang digunakan adalah penyuluhan hukum berupa ceramah interaktif dan diskusi tanya jawab. Kegiatan dilaksanakan pada Jumat, 7 Agustus 2026, bertempat di wilayah Celeban, Kecamatan Umbulharjo, Kota Yogyakarta, dan dihadiri oleh 11 orang warga setempat. Hasil dari kegiatan ini menunjukkan adanya peningkatan pemahaman warga mengenai pentingnya menjaga kerahasiaan data pribadi, seperti Nomor Induk Kependudukan (NIK) dan swafoto KTP, serta pemahaman mengenai instrumen perlindungan hukum yang diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).*

Keyword : *Konsekuensi Hukum, Pengabdian Masyarakat, Penyuluhan Hukum, Perlindungan Data Pribadi*

PENDAHULUAN

Pada era digitalisasi kontemporer, data telah bertransformasi menjadi salah satu aset dengan nilai signifikansi yang tinggi. Ekstensifikasi transformasi digital di berbagai sektor berimplikasi pada

tuntutan bagi masyarakat untuk menyerahkan informasi pribadinya sebagai prasyarat utama dalam mengakses ragam layanan, baik yang bersifat publik maupun komersial (Sulianta, 2025). Kendati demikian, fenomena tersebut menghadirkan sebuah paradoks. Walaupun digitalisasi menawarkan efisiensi secara administratif, disaat yang bersamaan, eskalasi risiko penyalahgunaan serta kebocoran data menjadi ancaman yang kian mengemuka (Saeed et al., 2023).

Masyarakat di tingkat akar rumput, termasuk warga di Celeban, Umbulharjo, Yogyakarta, sering kali kurang menyadari nilai penting dari data yang mereka miliki. Praktik membagikan foto Kartu Tanda Penduduk (KTP), Kartu Keluarga (KK), atau memberikan informasi pribadi kepada pihak yang tidak berwenang masih kerap terjadi (Soomro et al., 2019). Hal ini bermuara pada maraknya kasus penipuan, pemalsuan identitas, hingga jeratan pinjaman online (pinjol) ilegal yang menggunakan identitas korban tanpa izin.

Secara yuridis, negara telah hadir untuk memberikan perlindungan melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) (Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, 2022). UU PDP menjadi tonggak sejarah yang mengatur secara komprehensif mengenai hak subjek data, kewajiban pengendali data, serta sanksi hukum bagi pelanggar (<https://www.tempo.co/ekonomi/uu-pdp-disahkan-jhonny-g-plate-tonggak-sejarah-kemajuan-perlindungan-data-di-indonesia-287028>). Berdasarkan latar belakang tersebut, dipandang sangat perlu untuk melaksanakan pengabdian kepada masyarakat dalam bentuk penyuluhan hukum guna memitigasi risiko hukum di masyarakat.

METODE

Kegiatan pengabdian masyarakat ini menggunakan metode penyuluhan hukum (*Economides, 2015; Vrhovec et al., 2023*) dengan pendekatan sosialisasi dialogis (ceramah dan tanya jawab). Pelaksanaan kegiatan ini pada Jumat, 7 Agustus 2026 di Celeban, Umbulharjo, Kota Yogyakarta. Audiens dalam acara ini sebanyak 11 orang yang terdiri dari perwakilan tokoh dan warga masyarakat.

Pemaparan materi pada kesempatan ini meliputi penjelasan mengenai definisi data pribadi, dasar hukum, dan ancaman pidana serta perdata. Setelah penjelasan materi dari pengabdi, dilaksanakan sesi diskusi dan tanya jawab untuk menggali pengalaman warga terkait isu data pribadi dan memberikan solusi hukum preventif. Pada akhir sesi dilaksanakan evaluasi dengan penilaian pemahaman warga melalui konfirmasi.

HASIL DAN PEMBAHASAN

Kegiatan penyuluhan berjalan secara interaktif dengan 11 orang warga, dimana dalam sesi diskusi, beberapa warga membagikan pengalaman mereka saat dimintai foto diri memegang KTP oleh pihak yang tidak dikenal dengan dalih verifikasi undian berhadiah. Pengabdian selaku ahli hukum memberikan penekanan bahwa tindakan tersebut adalah gerbang utama terjadinya *identity theft* (pencurian identitas) (Geradts, 2023).

Dalam penyampaian materi, warga diberikan pemahaman mengenai data pribadi. Berdasarkan Pasal 4 UU No. 27 Tahun 2022 (Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, 2022), data pribadi terdiri atas data pribadi spesifik dan data pribadi yang bersifat umum. Data pribadi spesifik meliputi data dan informasi kesehatan, biometrik, genetika, catatan kejahatan, data anak, hingga data keuangan pribadi. Data pribadi yang bersifat umum meliputi nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan/atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang.



Gambar 1. Pengabdian Menyampaikan Materi
Sumber gambar: Dokumentasi Pengabdian

Dasar hukum utama yang menjadi pijakan dalam perlindungan ini adalah Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yang menjamin hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda (Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, 2024). Pengaturan teknis dan sanksi kemudian diejawantahkan

secara khusus (*lex specialis*) melalui UU No. 27 Tahun 2022 (UU PDP) (Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, 2022).

Perlindungan data pribadi sering kali digambarkan sebagai masalah teknis: kata sandi yang lebih kuat, jaringan yang aman, dan pengaturan yang cermat (Laurent & Levallois-Barth, 2015). Langkah-langkah ini memang penting, tetapi masalahnya lebih luas dari itu. Perlindungan data pribadi berkaitan dengan cara informasi mengenai seseorang dikumpulkan, ditafsirkan, dibagikan, disimpan, dan digunakan untuk mengambil keputusan. Oleh karena itu, hal ini sekaligus merupakan masalah praktik individu, tanggung jawab organisasi, dan tata kelola publik.

Dalam kehidupan masa kini, informasi pribadi dihasilkan melalui aktivitas sehari-hari: berkomunikasi, menjelajah internet, berbelanja, belajar, bekerja, dan menggunakan layanan digital. Beberapa detail dapat mengidentifikasi seseorang secara langsung; sementara detail lainnya menjadi identifikasi atau mengungkapkan identitas ketika digabungkan. Catatan lokasi, misalnya, dapat mengungkap pola tempat tinggal dan pergerakan, sedangkan riwayat penelusuran atau transaksi dapat mengungkap minat dan kerentanan. Dengan demikian, signifikansi data tidak hanya bergantung pada setiap item secara individual, tetapi juga pada bagaimana informasi tersebut saling terhubung dan tujuan penggunaannya (Kotronoulas et al., 2023).

Prinsip praktis yang dapat diterapkan adalah sebelum membagikan informasi, pertimbangkan apakah informasi tersebut diperlukan untuk layanan tersebut dan sepadan dengan tujuannya. Alamat mungkin sangat penting untuk pengiriman barang yang dibeli; sedangkan akses ke daftar kontak mungkin tidak. Apabila suatu permintaan tampak tidak relevan, seseorang dapat meninjau izin yang diberikan, mencari alternatif, atau menolak memberikan informasi tersebut.

Namun, penilaian individu tidak terjadi dalam ruang hampa. Layanan digital dirancang untuk membuat beberapa pilihan menjadi mudah dan yang lainnya menjadi sulit. Pemberitahuan yang panjang, pengaturan default, tekanan waktu, dan janji kemudahan dapat memengaruhi informasi apa yang diungkapkan oleh orang pada umumnya (Carbone & Loewenstein, 2023; Mallinson & Hatemi, 2018; Paunov et al., 2019).

Penelitian mengenai “paradoks privasi” menggambarkan adanya kesenjangan yang berulang antara kekhawatiran privasi yang diungkapkan oleh seseorang dengan perilaku pengungkapan atau perlindungan data mereka di dunia maya. Sebuah tinjauan sistematis menemukan bahwa keputusan untuk mengungkapkan informasi sering kali dipengaruhi oleh persepsi terhadap manfaat dan risiko, termasuk dalam situasi di mana risiko dinilai rendah atau dapat diabaikan (Barth & de Jong, 2017). Temuan ini menjadi peringatan agar tidak menganggap pengungkapan informasi sebagai bukti bahwa seseorang tidak menghargai privasi (Barth & de Jong, 2017). Pilihan yang diambil dalam kondisi

informasi terbatas atau pilihan yang terbatas mungkin tidak mencerminkan preferensi yang sepenuhnya didasarkan pada informasi yang memadai.

Desain yang mendukung privasi dapat membantu menutup kesenjangan tersebut. Dalam sebuah studi terhadap 1.593 pengguna aplikasi seluler di Eropa Barat, persepsi efikasi diri, kerentanan, dan kekhawatiran terhadap privasi dikaitkan dengan motivasi yang lebih tinggi untuk mengambil tindakan pengurangan risiko, sementara persepsi biaya respons dikaitkan dengan motivasi yang lebih rendah (Kropczynski et al., 2026; Wang, 2026; Wottrich et al., 2019; Yan et al., 2026). Dalam sebuah eksperimen yang telah didaftarkan sebelumnya yang melibatkan 485 peserta, informasi privasi yang disajikan dalam bentuk skor mendukung pilihan yang lebih sadar privasi dalam situasi yang diteliti; manfaat yang dirasakan juga berkorelasi positif dengan niat untuk membagikan informasi (Meier et al., 2020; Meier & Krämer, 2024; Ostendorf et al., 2020). Temuan ini menunjukkan bahwa informasi yang jelas dan tepat waktu serta kontrol yang mudah digunakan dapat mendukung pengambilan keputusan, sementara hambatan dan kompleksitas dapat melemahkannya, serta tidak menyiratkan bahwa setiap keputusan privasi dapat direduksi menjadi satu skor saja atau bahwa individu sendirilah yang harus memikul tanggung jawab untuk mengelola sistem yang kompleks.

Masyarakat masih dapat mengambil langkah-langkah yang berarti untuk mengurangi paparan yang dapat dihindari, misalnya menggunakan kata sandi yang unik dan kuat untuk akun-akun penting, serta pertimbangkan untuk menggunakan pengelola kata sandi yang terpercaya (Kanta et al., 2023; Kennison et al., 2021; Renaud, 2020; Simon et al., 2025). Aktifkan autentikasi multi-faktor jika tersedia, terutama untuk akun email, keuangan, dan pekerjaan. Waspada pesan yang tidak terduga: daripada membuka tautan dalam pemberitahuan yang mengejutkan, kunjungi situs web atau aplikasi resmi organisasi tersebut secara mandiri. Jangan pernah mengungkapkan kode verifikasi sekali pakai sebagai tanggapan atas permintaan yang tidak diminta. Selalu perbarui perangkat dan aplikasi, tinjau izin untuk lokasi, kamera, mikrofon, kontak, dan foto, serta hapus akses yang tidak diperlukan. Sebelum memposting atau meneruskan materi, pertimbangkan apakah materi tersebut berisi informasi tentang orang lain atau detail yang dapat mengungkapkan lebih dari yang dimaksudkan.

Langkah-langkah perlindungan juga harus diintegrasikan ke dalam sistem sejak awal, bukan ditambahkan setelah masalah muncul. Dalam praktiknya, hal ini berarti mengevaluasi bagaimana suatu sistem dapat memengaruhi orang, membatasi aliran data yang tidak perlu, menetapkan tanggung jawab, dan memeriksa apakah mekanisme perlindungan berfungsi sesuai tujuan. Pertanyaan selanjutnya adalah bagaimana data pribadi memengaruhi keputusan-keputusan penting. Sistem otomatis atau berbasis data dapat memengaruhi akses terhadap layanan, peluang, atau dukungan. Oleh karena itu, tata kelola yang bertanggung jawab menuntut perhatian terhadap akurasi, konteks, keadilan, keterjelasan, serta jalur yang efektif untuk memperbaiki kesalahan. Privasi tidak hanya berkaitan dengan pencegahan akses

tanpa izin; hal ini juga menyangkut apakah informasi digunakan secara tepat serta apakah masyarakat dapat memahami dan mengajukan keberatan terhadap keputusan yang memengaruhi mereka.

Apabila ada dugaan bahwa akun telah diretas, segera ambil tindakan melalui saluran yang terpercaya. Ubah kata sandi dari perangkat yang dianggap aman, akhiri sesi aktif lainnya jika layanan tersebut menyediakan opsi tersebut, dan lindungi akun email yang digunakan untuk pemulihan kata sandi. Jika ada kemungkinan informasi keuangan terlibat, hubungi lembaga terkait menggunakan nomor yang terverifikasi atau aplikasi resmi. Catat insiden tersebut dan ikuti panduan pelaporan lokal yang berlaku. Tanggapan yang cepat dapat membatasi risiko lebih lanjut, namun tanggung jawab atas pelanggaran keamanan tidak boleh dilimpahkan kepada pihak yang terkena dampaknya.

Edukasi penting yang ditekankan kepada warga adalah mengenai konsekuensi hukum bagi pihak-pihak yang menyalahgunakan data pribadi. Menurut hukum yang berlaku, terdapat sanksi tegas baik secara administratif maupun pidana, yaitu sanksi administratif bagi Pengendali atau prosesor data (misalnya perusahaan atau instansi) yang gagal melindungi data masyarakat dapat dikenakan teguran tertulis, penghentian sementara kegiatan pemrosesan, hingga denda administratif paling tinggi 2% dari pendapatan tahunan (Pasal 57 UU PDP) (Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, 2022). Sanksi selanjutnya adalah sanksi pidana. UU PDP memuat sanksi pidana yang sangat berat bagi pelaku kejahatan data pribadi, diantaranya setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi orang lain untuk menguntungkan diri sendiri, dipidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (Pasal 67 ayat 1) (Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, 2022). Pasal 67 ayat 2 menyatakan bahwa setiap orang yang dengan sengaja dan melawan hukum mengungkapkan data pribadi yang bukan miliknya, dipidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp4.000.000.000,00 (Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, 2022). Selain itu, tindakan memalsukan data pribadi untuk keuntungan finansial (seperti mendaftarkan pinjaman online menggunakan KTP orang lain) diancam dengan pidana penjara maksimal 6 (enam) tahun dan denda hingga Rp6.000.000.000,00 (Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, 2022).

Perlindungan data pribadi paling baik dipahami sebagai tanggung jawab bersama yang berkelanjutan. Setiap individu dapat membuat pilihan yang sadar, mengamankan akun, dan mempertanyakan permintaan yang tidak terduga. Organisasi harus menyertakan mekanisme perlindungan dalam produknya, membatasi pengumpulan data, berkomunikasi dengan jelas, serta menggunakan informasi secara bertanggung jawab. Pemerintah dan badan pengatur menetapkan standar yang dapat ditegakkan serta mekanisme pertanggungjawaban. Tidak ada satu tindakan pun yang dapat

menghilangkan semua risiko, tetapi perlindungan yang terkoordinasi dapat mengurangi paparan yang tidak perlu dan meningkatkan kepercayaan. Pada intinya, perlindungan data bertujuan untuk menjaga kemampuan masyarakat untuk berpartisipasi dalam kehidupan modern tanpa menyerahkan kendali yang tidak wajar atas informasi mengenai diri mereka sendiri (Chen & Wang, 2026; Faisal, 2026; Kont & Soekörv, 2026; Mukherjee & Chang, 2025).

KESIMPULAN

Kegiatan pengabdian masyarakat berupa penyuluhan hukum di Celeban, Umbulharjo, Yogyakarta pada 7 Agustus 2026 yang dihadiri 11 warga telah terlaksana dengan baik. Kegiatan ini berhasil menjembatani kesenjangan pengetahuan (*knowledge gap*) antara teks undang-undang dan realitas pemahaman masyarakat. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menjadi dasar hukum yang kuat dan memberikan konsekuensi hukum yang tegas, berupa denda miliaran rupiah hingga kurungan penjara, bagi siapa saja yang menyalahgunakan data pribadi. Warga kini memiliki kesadaran preventif untuk tidak sembarangan membagikan dokumen kependudukan di ruang digital maupun kepada pihak yang tidak memiliki otoritas hukum yang sah.

UCAPAN TERIMA KASIH

Ucapan terima kasih pengabdian disampaikan kepada Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Universitas Widya Mataram (UWM) serta masyarakat di Celeban, Kecamatan Umbulharjo, Yogyakarta atas fasilitas dan kerjasamanya sehingga kegiatan pengabdian masyarakat ini berjalan dengan baik

DAFTAR PUSTAKA

- Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. In *Telematics and Informatics* (Vol. 34, Number 7, pp. 1038–1058). Elsevier Ltd. <https://doi.org/10.1016/j.tele.2017.04.013>
- Carbone, E., & Loewenstein, G. (2023). The drive to disclose. In *Consumer Psychology Review* (Vol. 6, Number 1, pp. 17–32). John Wiley and Sons Inc. <https://doi.org/10.1002/ARCP.1086>
- Chen, W., & Wang, Y. (2026). Data privacy as strategy: Corporate personal data protection system and M&A performance. *Finance Research Letters*, 112, 110821. <https://doi.org/10.1016/J.FRL.2026.110821>
- Economides, K. (2015). Legal Education. *International Encyclopedia of the Social & Behavioral Sciences: Second Edition*, 734–739. <https://doi.org/10.1016/B978-0-08-097086-8.92073-7>
- Faisal, K. (2026). Navigating the fine line: the complex reconciliation of data protection and freedom of expression in criminal conviction and offences data. *Digital Policy, Regulation and Governance*, 28(1), 17–34. <https://doi.org/10.1108/DPRG-10-2024-0260>

- Geradts, Z. (2023). Identity Theft. *Encyclopedia of Forensic Sciences: Volume 1-4, Third Edition*, 3, 213–217. <https://doi.org/10.1016/B978-0-12-823677-2.00264-6>
- Kanta, A., Coisel, I., & Scanlon, M. (2023). Harder, better, faster, stronger: Optimising the performance of context-based password cracking dictionaries. *Forensic Science International: Digital Investigation*, 44. <https://doi.org/10.1016/j.fsidi.2023.301507>
- Kennison, S. M., Jones, I. T., Spooner, V. H., & Chan-Tin, D. E. (2021). Who creates strong passwords when nudging fails. *Computers in Human Behavior Reports*, 4. <https://doi.org/10.1016/j.chbr.2021.100132>
- Kont, K. R., & Soekõrv, T. (2026). Policies and procedures as tools for ensuring data protection in rescue services: the case of Estonian Rescue Services Agency. *Transforming Government: People, Process and Policy*. <https://doi.org/10.1108/TG-10-2025-0329>
- Kotronoulas, G., Miguel, S., Dowling, M., Fernández-Ortega, P., Colomer-Lahiguera, S., Bağcıvan, G., Pape, E., Drury, A., Semple, C., Dieperink, K. B., & Papadopoulou, C. (2023). An Overview of the Fundamentals of Data Management, Analysis, and Interpretation in Quantitative Research. In *Seminars in Oncology Nursing* (Vol. 39, Number 2). Elsevier Inc. <https://doi.org/10.1016/j.soncn.2023.151398>
- Kropczynski, J., Akter, M., Asadi, A. R., Alzughbi, H., Park, J. K., Lipford, H. R., & Wisniewski, P. J. (2026). Growing Together for Digital Safety: Examining the Effects of Group Formation and Engagement in Building Privacy and Security Efficacy. *Proceedings of the ACM on Human-Computer Interaction*, 10(2 May). <https://doi.org/10.1145/3788054>
- Laurent, M., & Levallois-Barth, C. (2015). Privacy Management and Protection of Personal Data. *Digital Identity Management*, 137–205. <https://doi.org/10.1016/B978-1-78548-004-1.50004-3>
- Mallinson, D. J., & Hatemi, P. K. (2018). The effects of information and social conformity on opinion change. *PLoS ONE*, 13(5). <https://doi.org/10.1371/journal.pone.0196600>
- Meier, Y., & Krämer, N. C. (2024). The Privacy Calculus Revisited: An Empirical Investigation of Online Privacy Decisions on Between- and Within-Person Levels. *Communication Research*, 51(2), 178–202. <https://doi.org/10.1177/00936502221102101>
- Meier, Y., Schäwel, J., Kyewski, E., & Krämer, N. C. (2020). Applying Protection Motivation Theory to Predict Facebook Users' Withdrawal and Disclosure Intentions. *ACM International Conference Proceeding Series*, 21–29. <https://doi.org/10.1145/3400806.3400810>
- Mukherjee, A., & Chang, H. H. (2025). *Agentic AI: Autonomy, Accountability, and the Algorithmic Society*. <http://arxiv.org/abs/2502.00289>
- Ostendorf, S., Müller, S. M., & Brand, M. (2020). Neglecting Long-Term Risks: Self-Disclosure on Social Media and Its Relation to Individual Decision-Making Tendencies and Problematic Social-Networks-Use. *Frontiers in Psychology*, 11. <https://doi.org/10.3389/fpsyg.2020.543388>
- Paunov, Y., Wänke, M., & Vogel, T. (2019). Ethical defaults: which transparency components can increase the effectiveness of default nudges? *Social Influence*, 14(3–4), 104–116. <https://doi.org/10.1080/15534510.2019.1675755>

- Renaud, K. (2020). Strong passwords can't keep children safe. *Network Security*, 2020(3), 20. [https://doi.org/10.1016/S1353-4858\(20\)30033-7](https://doi.org/10.1016/S1353-4858(20)30033-7)
- Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. In *Sensors* (Vol. 23, Number 15). Multidisciplinary Digital Publishing Institute (MDPI). <https://doi.org/10.3390/s23156666>
- Simon, J., Watson, S. J., & van Sintemaartensdijk, I. (2025). Response-efficacy messages produce stronger passwords than self-efficacy messages ... for now: A longitudinal experimental study of the efficacy of coping message types on password creation behaviour. *Computers in Human Behavior Reports*, 17. <https://doi.org/10.1016/j.chbr.2025.100615>
- Soomro, Z. A., Ahmed, J., Shah, M. H., & Khoubati, K. (2019). Investigating identity fraud management practices in e-tail sector: a systematic review. *Journal of Enterprise Information Management*, 32(2), 301–324. <https://doi.org/10.1108/JEIM-06-2018-0110>
- Sulianta, F. (2025). *Masyarakat Digital: Tren, Tantangan, dan Perubahan di Era Teknologi*. Feri Sulianta.
- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, 1 (2024).
- Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, 1 (2022).
- Vrhovec, S., Bernik, I., & Markelj, B. (2023). Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign. *Computers and Security*, 125. <https://doi.org/10.1016/j.cose.2022.103038>
- Wang, Y. (2026). Predicting Users' Privacy Protection Behavior in Mobile Applications: An Empirical Study Using Machine Learning and Explainable AI. *IEEE Access*, 14, 77931–77943. <https://doi.org/10.1109/ACCESS.2026.3691944>
- Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2019). App Users Unwittingly in the Spotlight: A Model of Privacy Protection in Mobile Apps. *Journal of Consumer Affairs*, 53(3), 1056–1083. <https://doi.org/10.1111/joca.12218>
- Yan, W., Liu, Y. li, Mamaeva, V., Dong, F., Tao, G., Li, R., & Yang, H. (2026). Generative AI literacy: Scale development and its influence on privacy protection behaviors and information verification behaviors. *Telecommunications Policy*, 50(2), 103117. <https://doi.org/10.1016/J.TELPOL.2025.103117>