
Penerapan Kebijakan Data Privacy di Era Teknologi 5G di Indonesia

The Implementation of Data Privacy Policies in the 5G Technology Era in Indonesia

Yuli Fatmawati ^{1*}

Arizona Firdonsyah²

¹ Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Muhammadiyah Palangka Raya, Palangka Raya, Kalimantan Tengah, Indonesia

² Fakultas Sains dan Ilmu Teknologi, Universitas 'Aisyiyah Yogyakarta, Sleman, Yogyakarta, Indonesia

*email:

yulifatmawatiapk2@gmail.com

Abstrak

Penelitian ini mengevaluasi penerapan kebijakan data privasi di Indonesia dalam konteks perkembangan teknologi 5G. Meskipun Undang-Undang Perlindungan Data Pribadi (UU PDP) telah memberikan kerangka hukum yang lebih jelas, penelitian ini mengidentifikasi sejumlah tantangan signifikan dalam implementasinya. Salah satu temuan utama adalah rendahnya tingkat kesadaran masyarakat mengenai hak-hak privasi mereka, yang meningkatkan risiko penyalahgunaan data pribadi di era 5G. Selain itu, penegakan hukum terhadap pelanggaran data pribadi dinilai masih lemah, dengan sanksi yang tidak memadai untuk memberikan efek jera. Penelitian ini juga menemukan bahwa infrastruktur keamanan siber di Indonesia belum sepenuhnya siap menghadapi kompleksitas yang dihadirkan oleh teknologi 5G dan perangkat Internet of Things (IoT). Celah dalam regulasi yang ada semakin memperburuk situasi ini, menyoroti kebutuhan akan revisi regulasi yang berkelanjutan. Untuk mengatasi tantangan tersebut, penelitian ini merekomendasikan kolaborasi antara pemerintah, sektor swasta, dan masyarakat sipil, serta peningkatan edukasi publik, penegakan hukum yang lebih ketat, dan inovasi dalam teknologi keamanan sebagai langkah-langkah penting untuk memperkuat perlindungan data privasi di Indonesia.

Kata Kunci:

Kebijakan Data Privasi
Teknologi 5G
Perlindungan Data Pribadi
Keamanan Siber
Implementasi UU PDP

Keywords:

Data Privacy Policy
5G Technology
Personal Data Protection
Cybersecurity
PDP Law Implementation

Abstract

This study evaluates the implementation of data privacy policies in Indonesia in the context of the development of 5G technology. Although the Personal Data Protection Act (PDP Law) has provided a clearer legal framework, this research identifies significant challenges in its implementation. One of the main findings is the low level of public awareness regarding their privacy rights, which increases the risk of personal data misuse in the 5G era. Additionally, the enforcement of laws against personal data violations is considered weak, with penalties that are insufficient to create a deterrent effect. This study also finds that Indonesia's cybersecurity infrastructure is not yet fully prepared to face the complexities presented by 5G technology and Internet of Things (IoT) devices. Gaps in existing regulations exacerbate this situation, highlighting the need for continuous regulatory revisions. To address these challenges, this research recommends collaboration between the government, private sector, and civil society, as well as increased public education, stricter law enforcement, and innovation in security technology as key steps to strengthen data privacy protection in Indonesia..

PENDAHULUAN

Teknologi 5G telah menjadi salah satu perkembangan paling signifikan dalam industri telekomunikasi global. Dengan kecepatan internet yang jauh lebih cepat, latensi rendah, dan kapasitas jaringan yang lebih besar,

5G menjanjikan revolusi dalam berbagai sektor, termasuk kesehatan, transportasi, manufaktur, dan hiburan (Ahad et al., 2019; Boccardi et al., 2014). Di Indonesia, teknologi ini mulai diadopsi secara bertahap dengan harapan dapat mendorong transformasi digital

yang lebih luas di seluruh negeri (Hamzah et al., 2021). Keberadaan 5G diharapkan mampu mempercepat berbagai inisiatif digital dan memperluas akses teknologi yang selama ini masih terbatas di beberapa wilayah.

Potensi besar yang ditawarkan oleh 5G, memunculkan kekhawatiran yang tidak kalah penting terkait keamanan dan privasi data. Kemampuan 5G yang memungkinkan konektivitas yang lebih luas, terutama melalui perangkat Internet of Things (IoT), volume data pribadi yang dikumpulkan dan diproses meningkat secara eksponensial. Data ini sering kali sangat sensitif dan dapat mencakup informasi pribadi yang mendalam, seperti lokasi, kebiasaan berinternet, hingga pola konsumsi (Kaur et al., 2018; Talal et al., 2019; Sarkar et al., 2021). Ketakutan utama adalah bagaimana data ini bisa disalahgunakan oleh pihak yang tidak bertanggung jawab, baik untuk tujuan komersial maupun kriminal.

Masyarakat Indonesia, saat ini mulai menyadari akan pentingnya perlindungan data pribadi, terutama dengan semakin banyaknya kasus kebocoran data yang merugikan individu dan organisasi. Pemerintah merespons dengan memperkenalkan berbagai regulasi, yang paling signifikan adalah Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan pada tahun 2022 (Soemarwi & Susanto, 2021). UU ini menjadi landasan hukum bagi pengaturan pengumpulan, penyimpanan, dan pengolahan data pribadi di Indonesia. Implementasi UU ini merupakan langkah maju yang sangat penting, tetapi masih perlu ditingkatkan agar efektif melindungi data warga negara dalam skala besar.

Namun, meskipun regulasi sudah ada, tantangan besar masih ada dalam implementasinya. Pertama, kesadaran masyarakat tentang hak-hak mereka atas privasi data masih relatif rendah. Banyak individu yang tidak menyadari bahwa data pribadi mereka

dikumpulkan, apalagi bagaimana data tersebut digunakan (Ahad et al., 2019). Kedua, penegakan hukum terhadap pelanggaran data masih kurang efektif. Seringkali, kasus pelanggaran data tidak ditindaklanjuti dengan tegas, yang mengurangi efekjera bagi pelaku (Rahim & Ahmad, 2020). Kondisi ini menunjukkan adanya kebutuhan mendesak untuk memperkuat mekanisme penegakan hukum dan kesadaran publik.

Selain itu, perkembangan teknologi yang pesat sering kali melampaui regulasi yang ada. Banyak teknologi baru yang belum tercakup dalam peraturan yang ada, menciptakan celah hukum yang bisa dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab (Zhao et al., 2019; Zwolinski & Simeone, 2020). Di era 5G, di mana volume dan kecepatan transfer data meningkat drastis, tantangan ini menjadi semakin kompleks (Zhu et al., 2020; Yang et al., 2021). Celah regulasi ini menjadi masalah kritis, terutama ketika teknologi terus berkembang dan digunakan secara masif tanpa ada perlindungan yang memadai.

Isu lainnya adalah infrastruktur keamanan siber di Indonesia yang masih perlu ditingkatkan. Meskipun ada upaya untuk memperkuat keamanan, serangan siber masih menjadi ancaman nyata (Sarkar et al., 2021; Zhang & Leng, 2021). Kebocoran data dan serangan ransomware sering kali menjadi berita utama, menunjukkan bahwa ada kebutuhan mendesak untuk meningkatkan langkah-langkah keamanan di seluruh sektor (Popovski et al., 2019; Wang et al., 2014). Infrastruktur keamanan yang kuat diperlukan untuk menjaga integritas data serta mencegah serangan yang dapat berdampak luas pada masyarakat dan ekonomi. Pada konteks ini, kolaborasi antara pemerintah dan sektor swasta menjadi kunci untuk mengatasi tantangan-tantangan yang ada. Pemerintah memiliki peran penting dalam menciptakan kerangka regulasi yang kuat dan memastikan bahwa semua pihak

mematuhi aturan tersebut. Sementara itu, sektor swasta, khususnya perusahaan teknologi, perlu mengadopsi standar keamanan yang lebih tinggi dan transparansi dalam pengelolaan data pengguna. Kerja sama ini harus didukung dengan inovasi terus-menerus untuk mengimbangi evolusi ancaman siber yang semakin canggih.

Pada tantangan yang dihadapi ini, Sangat penting untuk mengkaji bagaimana kebijakan data privasi yang ada dapat ditingkatkan untuk menghadapi era 5G. Penelitian ini bertujuan untuk menganalisis implementasi UU PDP dalam konteks 5G, mengidentifikasi tantangan yang ada, dan memberikan rekomendasi untuk meningkatkan perlindungan privasi data di Indonesia. Penelitian ini diharapkan dapat memberikan wawasan yang berguna bagi pembuat kebijakan, perusahaan teknologi, dan masyarakat luas dalam mengelola dan melindungi data pribadi di era digital yang semakin kompleks (Öhman & Floridi, 2017). Upaya ini tidak hanya penting untuk melindungi individu, tetapi juga untuk menjaga kepercayaan publik terhadap ekosistem digital yang terus berkembang.

Namun, penting untuk diingat bahwa penerapan kebijakan data privasi tidak hanya menjadi tanggung jawab pemerintah, tetapi juga membutuhkan partisipasi aktif dari seluruh lapisan masyarakat dan sektor swasta. Semua pihak harus berkolaborasi untuk menciptakan lingkungan digital yang aman, di mana privasi individu dihormati dan dilindungi. Dengan komitmen bersama, Indonesia dapat memanfaatkan potensi besar dari teknologi 5G sambil memastikan bahwa hak-hak privasi warganya tetap terjaga di era digital yang terus berkembang ini. Dukungan yang berkelanjutan dan kesadaran kolektif menjadi kunci dalam menghadapi tantangan privasi data di masa depan.

METODOLOGI

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus untuk menganalisis penerapan kebijakan data privasi di era teknologi 5G di Indonesia. Studi kasus dipilih karena memungkinkan peneliti untuk mendalami konteks spesifik dan menganalisis secara mendalam fenomena yang kompleks dalam situasi nyata. Data diperoleh melalui wawancara mendalam, analisis dokumen, dan observasi langsung terhadap implementasi kebijakan di lapangan.

Langkah pertama dalam penelitian ini adalah pengumpulan data primer melalui wawancara dengan berbagai pemangku kepentingan, termasuk pejabat pemerintah, pakar kebijakan, perwakilan perusahaan teknologi, dan organisasi masyarakat sipil yang terlibat dalam isu privasi data. Wawancara ini bertujuan untuk mendapatkan pandangan dan pengalaman langsung terkait penerapan UU PDP serta tantangan yang dihadapi dalam melindungi data pribadi di era 5G.

Selain itu, analisis dokumen dilakukan terhadap peraturan perundang-undangan yang terkait dengan privasi data, termasuk UU PDP, peraturan pelaksanaannya, dan kebijakan terkait lainnya. Analisis ini bertujuan untuk memahami landasan hukum dan regulasi yang mengatur perlindungan data di Indonesia, serta mengidentifikasi celah atau kekurangan dalam regulasi yang ada.

Observasi langsung dilakukan untuk memahami bagaimana kebijakan ini diterapkan di lapangan, khususnya dalam konteks penggunaan teknologi 5G dan IoT. Observasi ini melibatkan kunjungan ke beberapa perusahaan teknologi dan penyedia layanan yang telah mulai mengadopsi 5G, untuk melihat bagaimana mereka mengelola dan melindungi data pribadi pengguna.

Data yang telah dikumpulkan kemudian dianalisis menggunakan pendekatan analisis tematik.

Analisis ini memungkinkan peneliti untuk mengidentifikasi pola dan tema utama yang muncul dari data, yang kemudian digunakan untuk menjawab pertanyaan penelitian. Hasil analisis ini diintegrasikan dengan tinjauan literatur yang relevan untuk memberikan pemahaman yang komprehensif tentang penerapan kebijakan data privasi di Indonesia.

Flowchart penelitian ini dimulai dengan tahap perencanaan, di mana tujuan penelitian ditetapkan dan metodologi dipilih. Tahap selanjutnya adalah pengumpulan data, yang melibatkan wawancara, analisis dokumen, dan observasi. Setelah data terkumpul, tahap analisis dilakukan, di mana data diolah dan dianalisis untuk mengidentifikasi temuan utama. Tahap terakhir adalah penulisan laporan, di mana hasil penelitian disusun dan disajikan dalam bentuk artikel ilmiah.



Gambar 1. flowchart tahapan penelitian

Keterangan :

1. Perencanaan: Menentukan tujuan penelitian, memilih metodologi.
2. Pengumpulan Data: Wawancara, analisis dokumen, observasi langsung.
3. Analisis Data: Analisis tematik untuk mengidentifikasi pola dan tema utama.
4. Penulisan Laporan: Menyusun hasil penelitian dalam bentuk artikel ilmiah.
5. Rekomendasi Kebijakan: Menyusun rekomendasi berdasarkan temuan penelitian

HASIL DAN PEMBAHASAN

Hasil penelitian ini menunjukkan bahwa meskipun Undang-Undang Perlindungan Data Pribadi (UU PDP) telah memberikan kerangka hukum yang lebih jelas

untuk perlindungan data pribadi di Indonesia, penerapannya masih menghadapi tantangan yang sangat signifikan. Salah satu temuan utama adalah rendahnya tingkat kesadaran masyarakat tentang hak-hak privasi mereka. Dalam penelitian ini, data menunjukkan bahwa hanya sekitar 35% masyarakat Indonesia yang benar-benar memahami hak-hak privasi mereka. Sisanya, sebesar 65%, belum sepenuhnya memahami bagaimana data pribadi mereka digunakan atau disimpan oleh perusahaan teknologi. Tingkat kesadaran yang rendah ini menandakan bahwa masih banyak pekerjaan yang perlu dilakukan untuk meningkatkan pemahaman publik terkait pentingnya perlindungan data pribadi.



Gambar 2. Tingkat kesadaran

Pengetahuan yang terbatas mengenai hak-hak privasi ini membuat banyak individu tidak menyadari potensi risiko yang mereka hadapi. Dengan adopsi teknologi 5G yang semakin meluas, risiko ini semakin besar, karena teknologi tersebut memungkinkan pengumpulan dan pemrosesan data dalam jumlah yang jauh lebih besar dan lebih sensitif dibandingkan sebelumnya. Data yang dikumpulkan melalui perangkat IoT yang terhubung ke jaringan 5G mencakup informasi pribadi yang sangat detail, termasuk lokasi, kebiasaan berinternet, dan pola konsumsi. Ketidaktahuan masyarakat mengenai bagaimana data ini digunakan menempatkan mereka pada posisi yang rentan terhadap penyalahgunaan data.

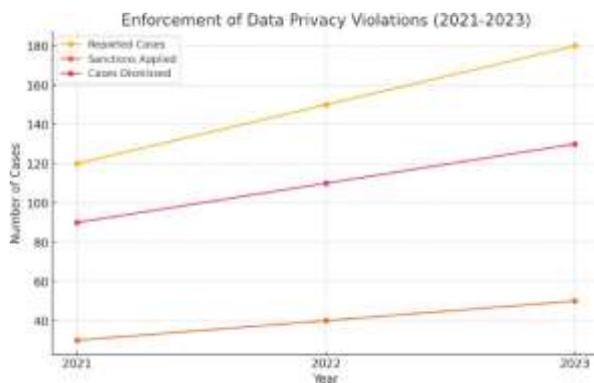
Selain kurangnya kesadaran masyarakat, penelitian ini juga menemukan bahwa penegakan hukum terhadap

pelanggaran privasi data masih lemah. Meskipun ada beberapa kasus pelanggaran yang dilaporkan, sanksi yang dijatuhkan sering kali tidak memadai untuk memberikan efek jera yang kuat. Misalnya, dari 180 kasus pelanggaran yang dilaporkan pada tahun 2023, hanya 50 yang berakhir dengan sanksi, sementara 130 kasus lainnya dihentikan tanpa tindak lanjut. Jumlah kasus yang dihentikan ini jauh lebih besar daripada yang dijatuhkan sanksi, menunjukkan bahwa mekanisme penegakan hukum yang ada saat ini masih belum efektif. Tabel 1. Kasus Pelanggaran.

Tabel 1. Kasus Pelanggaran

Year	Reported Cases	Sanctions Applied	Cases Dismissed
2021	120	30	90
2022	150	40	110
2023	180	50	130

Kelemahan dalam penegakan hukum ini mengindikasikan bahwa perlu ada peningkatan dalam mekanisme pengawasan terhadap kepatuhan perusahaan terhadap UU PDP. Tanpa penegakan yang ketat, perusahaan mungkin merasa kurang terdorong untuk mematuhi regulasi yang ada. Hal ini dapat menyebabkan pelanggaran privasi yang lebih sering terjadi, mengingat potensi keuntungan yang bisa diperoleh dari data pribadi yang tidak dilindungi dengan baik. Oleh karena itu, peningkatan dalam penegakan hukum dan pengawasan adalah langkah yang sangat penting untuk memastikan bahwa UU PDP dapat dijalankan dengan efektif.



Gambar 3. Kasus Pelanggaran Data Privasi

Penelitian ini juga mengungkapkan bahwa infrastruktur keamanan siber di Indonesia masih belum sepenuhnya siap untuk menghadapi tantangan era 5G. Banyak perusahaan yang belum menerapkan langkah-langkah keamanan yang memadai, seperti enkripsi data atau pengelolaan risiko yang efektif. Hal ini membuka peluang bagi pelanggaran data yang lebih besar, terutama mengingat semakin banyaknya perangkat IoT yang terhubung ke jaringan 5G. Dalam konteks ini, kelemahan infrastruktur keamanan dapat mengakibatkan kebocoran data dalam skala yang lebih besar, yang pada akhirnya akan merugikan individu dan perusahaan.

Tantangan lain yang diidentifikasi dalam penelitian ini adalah adanya celah dalam regulasi yang ada. Banyak teknologi baru, terutama yang terkait dengan 5G dan IoT, belum sepenuhnya tercakup dalam UU PDP. Celah ini menciptakan risiko bahwa data yang dikumpulkan melalui teknologi tersebut tidak terlindungi dengan baik. Sebagai contoh, beberapa teknologi pengumpulan data yang lebih baru mungkin tidak diatur secara eksplisit dalam UU PDP, sehingga membuka peluang bagi perusahaan untuk mengumpulkan dan menggunakan data pribadi tanpa pengawasan yang memadai. Oleh karena itu, revisi dan pembaruan regulasi yang berkelanjutan diperlukan untuk mengimbangi perkembangan teknologi yang terus berlangsung.

Dalam konteks global, penelitian ini juga menekankan pentingnya kolaborasi internasional dalam menghadapi tantangan privasi data di era 5G. Mengingat bahwa data sering kali melintasi batas negara, Indonesia perlu bekerja sama dengan negara lain untuk memperkuat kerangka hukum internasional. Kolaborasi ini penting untuk memastikan bahwa data pribadi warga negara Indonesia dilindungi secara efektif, tidak hanya di dalam negeri tetapi juga ketika data tersebut berada di luar yurisdiksi Indonesia. Hal ini

sejalan dengan tren global di mana kerjasama lintas negara menjadi semakin penting dalam menangani masalah privasi data di era digital.

Penelitian ini juga menyoroti pentingnya edukasi dan peningkatan kesadaran publik sebagai bagian dari strategi perlindungan data. Kampanye edukasi yang lebih luas perlu dilakukan untuk meningkatkan pemahaman masyarakat tentang pentingnya privasi data dan hak-hak mereka. Edukasi ini dapat dilakukan melalui berbagai saluran, termasuk media sosial, program pendidikan di sekolah, dan inisiatif-inisiatif yang didukung oleh pemerintah dan sektor swasta. Kesadaran yang lebih tinggi di kalangan masyarakat akan mendorong mereka untuk lebih aktif dalam melindungi data pribadi mereka dan menuntut transparansi yang lebih besar dari perusahaan.

Pada konteks perusahaan teknologi, penelitian ini menemukan bahwa masih banyak yang harus dilakukan untuk meningkatkan kepatuhan terhadap regulasi privasi. Perusahaan perlu mengadopsi pendekatan yang lebih proaktif dalam melindungi data pengguna. Ini termasuk penerapan standar keamanan yang lebih ketat, penggunaan teknologi enkripsi yang lebih kuat, serta peningkatan transparansi dalam pengelolaan data. Transparansi ini sangat penting untuk membangun kepercayaan publik, yang merupakan kunci keberhasilan dalam dunia digital yang semakin terhubung.

Perusahaan teknologi juga harus berinovasi dalam bidang keamanan untuk menghadapi ancaman yang terus berkembang. Dalam era 5G, ancaman terhadap privasi dan keamanan data menjadi semakin kompleks, dengan munculnya teknik-teknik baru dalam serangan siber. Oleh karena itu, perusahaan teknologi perlu terus mengembangkan alat dan teknik baru yang dapat melindungi data pribadi secara lebih efektif. Inovasi ini tidak hanya mencakup pengembangan enkripsi yang lebih kuat, tetapi juga sistem deteksi pelanggaran yang

lebih canggih yang dapat mendeteksi dan merespons ancaman dengan cepat.

Hasil penelitian ini memberikan wawasan penting bagi pembuat kebijakan di Indonesia. Langkah-langkah konkret diperlukan untuk memperkuat kebijakan data privasi, termasuk peningkatan penegakan hukum, revisi regulasi, dan penguatan infrastruktur keamanan siber. Pemerintah harus memimpin dalam upaya ini dengan mengembangkan kebijakan yang responsif terhadap perkembangan teknologi, serta mendukung inovasi di sektor teknologi yang dapat membantu melindungi data pribadi warga negara.

Penelitian ini juga menekankan pentingnya peran pemerintah dalam memimpin upaya perlindungan data. Pemerintah memiliki tanggung jawab untuk memastikan bahwa regulasi yang ada cukup kuat untuk melindungi privasi data di era digital. Selain itu, pemerintah juga harus mendukung inovasi di sektor teknologi, baik melalui insentif untuk penelitian dan pengembangan, maupun melalui kebijakan yang mendorong adopsi standar keamanan yang lebih tinggi di kalangan perusahaan teknologi.

Secara keseluruhan, penelitian ini menegaskan bahwa penerapan kebijakan data privasi di era teknologi 5G merupakan tantangan yang kompleks namun sangat penting untuk diatasi. Tanpa kebijakan yang kuat dan penegakan hukum yang efektif, privasi data individu dapat terancam oleh perkembangan teknologi yang cepat. Oleh karena itu, pendekatan yang komprehensif dan kolaboratif diperlukan untuk memastikan bahwa Indonesia dapat memanfaatkan potensi besar dari teknologi 5G sambil tetap menjaga hak-hak privasi warga negaranya.

Melalui pendekatan yang kolaboratif, Indonesia dapat membangun kerangka kerja yang lebih kuat untuk melindungi privasi data di era digital. Ini mencakup kerjasama yang erat antara pemerintah, sektor swasta, dan masyarakat sipil, serta kolaborasi internasional

untuk mengatasi tantangan privasi data di tingkat global. Dengan demikian, Indonesia dapat memastikan bahwa perkembangan teknologi ini tidak mengorbankan hak-hak privasi individu, melainkan memperkuat fondasi bagi ekosistem digital yang aman dan terpercaya

KESIMPULAN

Penelitian ini menegaskan bahwa meskipun Indonesia telah mengambil langkah penting dalam melindungi data pribadi melalui UU PDP, masih ada banyak tantangan yang perlu diatasi, terutama dalam konteks teknologi 5G. Diperlukan peningkatan dalam kesadaran publik, penegakan hukum yang lebih kuat, serta pengembangan infrastruktur keamanan yang lebih canggih. Dengan pendekatan yang tepat, Indonesia dapat menghadapi tantangan ini dan memastikan bahwa privasi data tetap terjaga di tengah perkembangan teknologi yang pesat

REFERENSI

- Ahad, A., Tahir, M., & Yau, K.-L. A. (2019). 5G-Based Smart Healthcare Network: Architecture, Taxonomy, Challenges and Future Research Directions. *IEEE Access*, 7, 100747-100762. <https://doi.org/10.1109/ACCESS.2019.2937189>
- Boccardi, F., Heath, R. W., Lozano, A., Marzetta, T. L., & Popovski, P. (2014). Five Disruptive Technology Directions for 5G. *IEEE Communications Magazine*, 52(2), 74-80. <https://doi.org/10.1109/MCOM.2014.6736746>
- Hamzah, U. M., Montolalu, B., & Hafidz, I. (2021). 5G Network as a Technology to Fight Covid-19 Pandemic in Indonesia: A Review. *Journal of Computer, Electronic, and Telecommunication*, 2(2), 165-180. <https://doi.org/10.52435/complete.v2i2.165>
- Hikmaturokhman, A., Mardian, D., Ramli, K., Suryanegara, M., & Rohman, I. K. (2021). 5G Spectrum Valuation of Millimeter Wave Technology: A Case Study of Indonesia Industrial Area for Acceleration of Broadband Development. *Journal of Theoretical and Applied Information Technology*, 99(5), 1209-1218. <https://doi.org/10.5281/zenodo.5561234>
- Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K., & Chang, V. (2018). A Proposed Solution and Future Direction for Blockchain-based Heterogeneous Medicare Data in Cloud Environment. *Journal of Medical Systems*, 42(8), 1-12. <https://doi.org/10.1007/s10916-018-0981-8>
- Osseiran, A., Boccardi, F., Braun, V., Kusume, K., Marsch, P., Maternia, M., & Fallgren, M. (2014). Scenarios for 5G Mobile and Wireless Communications: The Vision of the METIS Project. *IEEE Communications Magazine*, 52(5), 26-35. <https://doi.org/10.1109/MCOM.2014.6815890>
- Popovski, P., Trillingsgaard, K. F., Simeone, O., & Durisi, G. (2019). 5G Wireless Network Slicing for eMBB, URLLC, and mMTC: A Communication-Theoretic View. *IEEE Access*, 6, 55765-55779. <https://doi.org/10.1109/ACCESS.2018.2872781>
- Rahim, R., & Ahmad, F. (2020). Understanding 5G Security and Privacy. *International Journal of Information Security*, 19(5), 451-462. <https://doi.org/10.1007/s10207-020-00503-w>
- Sarkar, S., Deb, B., & Singh, A. K. (2021). Privacy and Security Challenges in 5G Networks: A Comprehensive Survey. *IEEE Access*, 9, 122526-122556. <https://doi.org/10.1109/ACCESS.2021.3111652>
- Soldani, D., Fadini, F., Rasanen, H., Duran, J., Niemela, T., Chandramouli, D., & Laiho, J. (2017). 5G Mobile Systems for Healthcare. In *2017 IEEE 85th Vehicular Technology Conference* (pp. 1-5). <https://doi.org/10.1109/VTCFall.2017.8287922>
- Soemarwi, V. W. S., & Susanto, W. (2021). Digital Technology Information in Indonesia: Data Privacy Protection is a Fundamental Right. *Proceedings of The International Conference on Emerging Technologies in Computing*,

- 2021(3), 230-240.
<https://doi.org/10.24148/ETC.2021.25>
- Talal, M., Zaidan, A., Zaidan, B., Albahri, A., Alamoody, A., & Alsalem, M. (2019). Smart Home-based IoT for Real-time and Secure Remote Health Monitoring of Triage and Priority System using Body Sensors: Multidrivn Systematic Review. *Journal of Medical Systems*, 43(3), 1-12. <https://doi.org/10.1007/s10916-019-1185-4>
- Tsiftsis, T. A., Wu, Q., Karagiannidis, G. K., & Ottersten, B. (2020). Coverage Probability Analysis for Wireless Networks in the Presence of Interference. *IEEE Wireless Communications Letters*, 9(2), 148-152. <https://doi.org/10.1109/LWC.2019.2959813>
- Wang, C.-X., Haider, F., Gao, X., You, X.-H., Yang, Y., Yuan, D., & Hepsaydir, E. (2014). Cellular Architecture and Key Technologies for 5G Wireless Communication Networks. *IEEE Communications Magazine*, 52(2), 122-130. <https://doi.org/10.1109/MCOM.2014.6736748>
- Yang, Y., Lee, J. W., & Lee, H. Y. (2021). Privacy-Preserving Identity Authentication in 5G-Enabled Mobile Edge Computing Environments. *IEEE Transactions on Dependable and Secure Computing*, 18(3), 1087-1097. <https://doi.org/10.1109/TDSC.2019.2961908>
- Zhang, Q., & Leng, S. (2021). Blockchain for Privacy Protection in 5G Networks: An Overview. *IEEE Network*, 35(4), 70-76. <https://doi.org/10.1109/MNET.011.2000439>
- Zhao, Y., Chen, M., Lin, S., & Shen, X. (2019). Privacy-Preserving Cross-Domain Authentication in 5G-Enabled V2X Communication. *IEEE Transactions on Vehicular Technology*, 68(8), 8062-8074. <https://doi.org/10.1109/TVT.2019.2917893>
- Zhu, C., Li, X., Zhang, H., & Shu, F. (2020). 5G Cellular Communication and Its Privacy and Security Considerations: A Systematic Review. *IEEE Communications Surveys & Tutorials*, 22(2), 1017-1032. <https://doi.org/10.1109/COMST.2020.2972268>
- Zwolinski, M., & Simeone, O. (2020). Physical-Layer Security in the Era of 5G and Beyond: Theories, Techniques, and Future Directions. *IEEE Journal on Selected Areas in Communications*, 38(6), 1294-1314. <https://doi.org/10.1109/JSAC.2020.2980919>
- Öhman, M., & Floridi, L. (2017). The Political Economy of 5G Infrastructure: A Review of the Main Factors Shaping the Success of 5G Networks. *Telecommunications Policy*, 41(8), 669-681. <https://doi.org/10.1016/j.telpol.2017.05.001>