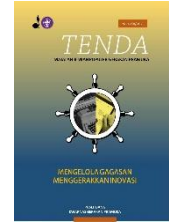


ANALISIS IMPLEMENTASI DASA DARMA PRAMUKA TERHADAP ASAS PELINDUNGAN DATA PRIBADI: STUDI RISIKO PELINDUNGAN DATA PRIBADI DI INDONESIA



Tegar Islami Putra ^{1*}; Martitah ²

¹ Universitas Negeri Semarang

² Universitas Negeri Semarang

*Korespondensi: tegarislami44@students.unnes.ac.id

Abstrak

Artikel ini bertujuan untuk memberikan hasil analisis komprehensif atas implementasi dasa darma pramuka terhadap asas perlindungan data pribadi dengan melakukan studi terhadap risiko perlindungan data pribadi yang ada di Indonesia. Pelindungan data pribadi dinilai sejalan dengan nilai dasa darma pramuka, akan tetapi perlu dilakukan kajian komprehensif untuk memberikan validasi akan hal tersebut. Penelitian ini menggunakan pendekatan kualitatif dengan tinjauan literatur dan analisis data sekunder dari artikel jurnal, laporan pemerintah, dan publikasi industri terkait perlindungan data pribadi serta peran gerakan Pramuka dalam pendidikan masyarakat. Hasil penelitian menunjukkan bahwa terdapat beberapa risiko yang dapat terjadi dalam hal terjadi kegagalan perlindungan data pribadi di lingkungan masyarakat, tiga diantaranya berkaitan dengan penjatuhan sanksi yang berlaku, operasional pengendali data pribadi menjadi tidak efisien, serta meningkatnya kasus penipuan digital terhadap kelompok rentan. Kegagalan perlindungan data pribadi dapat menimbulkan risiko seperti sanksi hukum, operasional yang tidak efisien, dan meningkatnya penipuan digital terhadap kelompok rentan. Implementasi dan irisan nilai Dasa Darma Pramuka dengan asas perlindungan data pribadi dapat menjadi upaya mengurangi risiko tersebut. Asas perlindungan data pribadi meliputi perlindungan, kepastian hukum, kemanfaatan, kehati-hatian, keseimbangan, pertanggungjawaban, dan kerahasiaan. Pelanggaran terhadap asas-asas tersebut memiliki risiko yang berbeda, sementara penerapan nilai Dasa Darma Pramuka mendukung implementasi asas ini secara lebih efektif.

Kata Kunci: Implementasi; Dasa Darma Pramuka; Asas; Pelindungan Data Pribadi; Indonesia

Abstract

This article aims to provide the results of a comprehensive analysis of the implementation of the scout dasa darma towards the principle of personal data protection by conducting a study of existing personal data protection risks in Indonesia. Personal data protection is considered to be in line with the values of the dasa darma scout, but it is necessary to conduct a comprehensive study to provide validation of this. This research uses a qualitative approach with a literature review and secondary data analysis of journal articles, government reports, and industry publications related to personal data protection and the role of the Scout movement in public education. The results show that there are several risks that can occur in the event of a failure of personal data protection in the community, three of which are related to the imposition of applicable sanctions, inefficient operations of personal data controllers, and increased cases of digital fraud against rentan groups. Failure to protect personal data can lead to risks such as legal sanctions, inefficient operations, and increased digital fraud against vulnerable groups. The implementation and intersection of the values of the Dasa Darma Pramuka with the principles of personal data protection can be an effort to reduce these risks. The principles of personal data protection include protection, legal certainty, expediency, prudence, balance, accountability, and confidentiality. Violations of these principles have different risks, while the application of the values of the Scout Charter supports the implementation of these principles more effectively.

Keywords: Implementation; Dasa Darma Pramuka; Principles; Personal Data Protection; Indonesia

1. PENDAHULUAN

Perkembangan teknologi yang pesat telah menyebabkan meningkatnya urgensi dalam pengelolaan informasi dan data dalam berbagai aspek kehidupan individu.(Anand et al., 2020) Ketersediaan berbagai bentuk teknologi media yang semakin meningkat telah memberikan banyak pilihan bagi individu untuk mendapatkan informasi yang mereka inginkan. Namun, hal ini juga menimbulkan potensi penyalahgunaan data pribadi yang dapat melanggar hak-hak pemilik data.(Anand et al., 2020) Selain itu, dimensi internasional dari pelanggaran data menekankan sifat tantangan perlindungan data yang saling berhubungan. Kasus-kasus seperti yang melibatkan Amazon, WhatsApp, Google, dan Instagram menunjukkan reaksi dan dampak global dari pelanggaran data, menggarisbawahi perlunya kerangka kerja peraturan yang selaras dan upaya kolaboratif lintas batas.(Putra et al., 2024: 89)

Di Indonesia, kurangnya pengaturan yang komprehensif dan konvergen untuk perlindungan data pribadi telah berkontribusi pada meningkatnya urgensi masalah ini. Berdasarkan data tahun 2021, kebocoran data pribadi telah mencapai 279 juta warga negara Indonesia (Neta et al., 2022). Perlindungan data pada dasarnya dapat berhubungan secara khusus dengan privasi sebagaimana dikemukakan oleh Allan Westin yang untuk pertama kalinya mendefinisikan privasi sebagai hak individu, kelompok atau institusi untuk menentukan apakah informasi tentang dirinya akan dikomunikasikan atau tidak kepada pihak lain sehingga definisi yang dikemukakan oleh Westin ini disebut sebagai privasi informasi karena menyangkut informasi pribadi (Putra & Fibrianti, 2024: 2). Pelindungan data pribadi dinilai sejalan dengan nilai-nilai Dasa Darma Pramuka, seperti tanggung jawab, kepercayaan, dan kepedulian terhadap sesama. Prinsip dalam Dasa Darma, seperti taat aturan, jujur, dan bertanggung jawab, menjadi panduan moral untuk menjaga privasi dan mencegah penyalahgunaan data. Pelindungan data pribadi sejalan dengan Dasa Darma karena keduanya menekankan tanggung jawab, kepercayaan, dan etika dalam menjaga hak dan privasi orang lain. Prinsip Dasa Darma mendukung perilaku yang jujur, disiplin, dan peduli, yang esensial dalam melindungi data pribadi. Akan tetapi, perlu dilakukan analisis untuk memberi validasi atas hal tersebut.

Penelitian serupa pernah dilakukan oleh Andri Pranata sebagaimana dipublikasikan pada Journal of Law and Nation. Penelitian ini mengkaji implementasi prinsip kehati-hatian dalam perlindungan data pribadi di Indonesia berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Pranata et al., 2024). Sedangkan penelitian yang diusulkan bertujuan untuk menganalisis risiko kegagalan perlindungan data pribadi di masyarakat dan mengeksplorasi implementasi Dasa Dharma Pramuka sebagai upaya mengurangi risiko kegagalan perlindungan data pribadi. Sehingga dinilai terdapat *novelty* penelitian, bahwa penelitian ini bertujuan untuk menilai bagaimana pengimplementasian nilai pada dasa darma pramuka terhadap asas pelindungan data pribadi berdasarkan UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Pertanyaan penelitian pertama berfokus pada risiko kegagalan perlindungan data pribadi di masyarakat, sedangkan pertanyaan penelitian kedua mengkaji implementasi Dasa Dharma Pramuka dalam kaitannya dengan prinsip-prinsip perlindungan data pribadi.

Penelitian ini penting karena bertujuan untuk mengatasi keterbatasan penelitian sebelumnya, yang terutama berfokus pada aspek hukum perlindungan data pribadi di Indonesia. Penelitian yang diusulkan ini berusaha untuk memberikan pemahaman yang lebih komprehensif tentang masalah ini dengan memasukkan prinsip-prinsip Dasa Dharma Pramuka, yang dapat menawarkan pendekatan unik untuk meningkatkan perlindungan data pribadi dalam konteks Indonesia.

Berdasarkan latar belakang sebagaimana yang telah dijelaskan, penulis menarik 2 rumusan masalah, yakni:

1. Bagaimana dampak kegagalan perlindungan data pribadi di Indonesia?
2. Bagaimana implementasi dasa darma pramuka terhadap asas perlindungan data pribadi berdasarkan risiko perlindungan data pribadi di Indonesia?

2. METODE

Penelitian ini menggunakan pendekatan kualitatif, dengan menggunakan tinjauan literatur yang relevan dan analisis sumber data sekunder. Sumber data utama meliputi artikel jurnal akademik, laporan pemerintah, dan publikasi industri yang membahas masalah perlindungan data pribadi dan peran gerakan Pramuka dalam pendidikan masyarakat. Penelitian ini menggunakan metodologi penelitian kualitatif, yang mengacu pada tinjauan komprehensif terhadap literatur yang relevan dan analisis mendalam terhadap sumber data sekunder. Sumber data primer meliputi artikel jurnal ilmiah, laporan pemerintah, dan publikasi industri yang menyelidiki isu-isu penting seputar perlindungan data pribadi dan peran strategis gerakan Kepanduan dalam pendidikan masyarakat dan pembangunan kesadaran. Dengan mengkaji beragam sumber ini, penelitian ini bertujuan untuk mendapatkan pemahaman holistik tentang lanskap saat ini, tantangan, dan potensi gerakan Pramuka untuk memainkan peran penting dalam menumbuhkan kesadaran dan tindakan kolektif tentang perlindungan data pribadi di masyarakat Indonesia (Putri & Elmina Martha, 2022).

3. PEMBAHASAN

A. Dampak Kegagalan Pelindungan Data Pribadi di Indonesia

Meningkatnya penggunaan teknologi digital dalam beberapa dekade terakhir telah menyebabkan maraknya pengumpulan data pribadi oleh pemerintah (Anand et al., 2020). Permasalahan keamanan data pribadi telah cukup banyak terjadi di berbagai negara, yang mana hal tersebut sudah seharusnya pemerintah juga turun tangan dan mengatur (Waspiyah et al., 2023). Hal ini telah meningkatkan urgensi untuk langkah-langkah perlindungan data pribadi yang kuat, karena penyalahgunaan data pribadi dapat melanggar hak-hak pemilik data (Neta et al., 2022). Prevalensi pelanggaran data pelanggaran data, baik di dalam negeri di Indonesia maupun di luar negeri menggarisbawahi pentingnya mengintegrasikan langkah-langkah perlindungan data yang kuat ke dalam kerangka hukum yang ada (Putra & Fibrianti, 2024b). Namun, di Indonesia, peraturan yang ada tentang perlindungan data pribadi masih terfragmentasi dan gagal memberikan perlindungan yang optimal dan efektif (Anand et al., 2020). Berikut beberapa risiko yang menjadi dampak dalam hal terjadi kegagalan perlindungan data pribadi masyarakat oleh pengendali data pribadi.

a. Dijatuhinya Sanksi Atas Pelanggaran Yang dilakukan Terhadap Regulasi Yang Berlaku

Penggunaan teknologi informasi dan komunikasi yang masif di Indonesia, terutama di kalangan generasi muda, telah meningkatkan risiko kejahatan siber dan potensi penyalahgunaan data pribadi. Terdapat kebutuhan mendesak untuk meningkatkan kesadaran tentang bahaya dunia maya dan pentingnya untuk lebih berhati-hati saat menggunakan perangkat pribadi dan mengakses berbagai situs internet (Abror et al., 2021).

Seperti yang disoroti dalam literatur, kurangnya peraturan perlindungan data pribadi yang komprehensif dan konvergen di Indonesia telah menyebabkan maraknya kebocoran data pribadi. Data dari tahun 2021 menunjukkan bahwa pelanggaran data pribadi telah memengaruhi 279 juta warga negara Indonesia, menggarisbawahi kebutuhan mendesak akan langkah-langkah efektif untuk melindungi data pribadi (Neta et al., 2022). Kegagalan perlindungan data pribadi merupakan risiko yang dirasakan oleh subjek data pribadi. Dampak

terpenting kegagalan perlindungan data pribadi adalah pencurian identitas yang menyebabkan kerugian finansial, pemerasan menggunakan informasi sensitif, dan kerusakan reputasi yang berdampak pada kehidupan sosial dan profesional subjek data. Hal ini dapat melanggar regulasi yang berlaku. Pelanggaran terhadap regulasi yang berlaku inilah yang dapat berujung kepada pemberian sanksi kepada pengendali data pribadi atau prosesor data pribadi yang memberikan dampak kepada berkurangnya kepercayaan publik.

b. Operasional Pengendali Data Pribadi yang Tidak Efisien

Kegagalan perlindungan data pribadi dapat mengakibatkan operasionalisasi perlindungan data menjadi tidak efektif karena organisasi harus mengalihkan sumber daya untuk penyelesaian insiden, perbaikan kelemahan sistem, dan pemenuhan persyaratan hukum. Kegiatan investigasi, perbaikan dampak, dan komunikasi dengan regulator mengganggu operasi sehari-hari seperti pemantauan perlindungan data dan perumusan serta implementasi kebijakan. Selain itu, dengan biaya yang harus dikeluarkan untuk melatih kembali karyawan, membeli teknologi baru, dan membayar denda, organisasi seringkali mengalami pengeluaran tambahan yang membebani anggaran mereka.

Kegagalan perlindungan data pribadi dapat menyebabkan operasional pengendali data pribadi menjadi tidak efisien karena memicu gangguan operasional, biaya tambahan, dan kerugian reputasi. Insiden pelanggaran data sering memaksa perusahaan menghentikan atau memperlambat operasinya untuk menangani masalah tersebut, disertai biaya besar untuk investigasi, pemulihan, serta pembayaran denda atau kompensasi. Selain itu, kehilangan kepercayaan pelanggan dapat mengurangi bisnis, sementara pengawasan regulasi yang lebih ketat menambah kompleksitas dan beban kerja. Semua faktor ini mengakibatkan alokasi sumber daya yang tidak optimal dan menurunkan efisiensi operasional pengendali data pribadi.

c. Meningkatnya Kasus Penipuan Digital dengan Target Kelompok Rentan

Faktor penting lainnya yang menggarisbawahi urgensi keterlibatan gerakan Pramuka dalam perlindungan data pribadi adalah meningkatnya penipuan digital yang menargetkan kelompok-kelompok rentan, seperti orang tua dan mereka yang memiliki literasi digital yang terbatas. Orang-orang ini sangat rentan terhadap penipuan dan pelanggaran data, sehingga menyoroti perlunya edukasi yang komprehensif dan upaya peningkatan kesadaran untuk memberdayakan masyarakat.

Kegagalan perlindungan data pribadi dapat meningkatkan kasus penipuan digital terhadap kelompok rentan karena data yang bocor, seperti informasi pribadi, kontak, atau keuangan, memberikan celah bagi pelaku kejahatan untuk menyusun strategi penipuan yang lebih meyakinkan. Kelompok rentan, seperti lansia, anak-anak, atau individu dengan literasi digital rendah, sering kali tidak memiliki kemampuan atau pengetahuan yang cukup untuk mengenali modus penipuan, sehingga lebih mudah menjadi target. Dengan akses ke data sensitif, pelaku dapat melakukan *phishing*, pencurian identitas, atau manipulasi psikologis, yang semakin memperburuk risiko dan kerugian bagi kelompok ini.

B. Implementasi Dasa Darma Pramuka Terhadap Asas Pelindungan Data Pribadi Sebagai Upaya Mengurangi Risiko Kegagalan Pelindungan Data Pribadi

Terdapat 8 asas yang terkandung dalam eksekusi UU Nomor 27 Tahun 2022 sebagai pelaksanaan upaya pelindungan data pribadi. Hal ini sebagaimana dijelaskan dalam Pasal 3 UU Nomor 27 Tahun 2022. Terdapat beberapa hal kaitan antara Dasa Darma dan Asas yang terkandung dalam pelaksanaan UU Nomor 27 Tahun 2022 tersebut, berikut penjelasan hal tersebut.

a. Pelindungan

Asas pelindungan data pribadi menekankan pentingnya melindungi data individu dari kebocoran, penyalahgunaan, atau akses tidak sah. Dalam kaitannya dengan Dasa Darma Pramuka, prinsip "Takwa kepada Tuhan Yang Maha Esa dan Suci dalam pikiran, perkataan, dan perbuatan" relevan karena mengajarkan kita untuk bertindak bertanggung jawab secara moral, termasuk dalam menjaga data pribadi orang lain. Gerakan Pramuka dapat membantu meningkatkan kesadaran masyarakat akan pentingnya perlindungan data melalui sosialisasi, lokakarya, atau kegiatan edukatif yang melibatkan kelompok rentan, sekaligus membangun kolaborasi dengan berbagai pihak untuk mewujudkan kesadaran digital yang lebih baik.

Jika asas perlindungan tidak berjalan, risiko yang muncul adalah kebocoran data pribadi yang dapat digunakan untuk kejahatan seperti penipuan, pencurian identitas, atau eksploitasi finansial. Selain itu, individu dapat kehilangan rasa aman dalam menggunakan layanan digital, yang pada akhirnya menurunkan kepercayaan publik terhadap sistem yang ada.

b. Kepastian Hukum

Kepastian hukum dalam pengelolaan data pribadi bertujuan untuk menghindari risiko operasional akibat ketidakpatuhan atau ketidakjelasan regulasi. Kehadiran UU Nomor 27 Tahun 2022 pada dasarnya memperjelas dan mengatur data pribadi secara spesifik, yang sebelumnya hanya diatur secara umum dalam berbagai peraturan (Pradana & Saragih, 2024). Hal ini selaras dengan Dasa Darma yang mengajarkan kita untuk menjadi "Patriot yang sopan dan kesatria," di mana kehadiran aturan yang menimbulkan ketaatan pada peraturan dan hukum menjadi bentuk penghormatan terhadap hak individu dan tanggung jawab kolektif.

Ketidakjelasan atau pelanggaran asas kepastian hukum dapat menyebabkan ketidakpastian regulasi, yang membuka celah untuk tindakan penyalahgunaan data oleh pihak yang tidak bertanggung jawab. Akibatnya, masyarakat kehilangan kepercayaan pada penegakan hukum, dan pengendali data dapat menghadapi tuntutan hukum yang membahayakan reputasi dan operasional mereka.

c. Kepentingan Umum

Asas ini berfokus pada perlindungan kelompok rentan, seperti anak-anak atau lansia, dari ancaman penipuan digital yang dapat terjadi akibat kebocoran data pribadi. Dalam Dasa Darma, prinsip "Cinta alam dan kasih sayang sesama manusia" menanamkan kepedulian terhadap kesejahteraan orang lain, termasuk dalam melindungi sesama subjek data pribadi dari risiko digital. Pramuka dapat melaksanakan simulasi pelanggaran data pribadi sebagai langkah edukasi praktis, yang tidak hanya mengajarkan keterampilan mitigasi tetapi juga meningkatkan kesadaran akan pentingnya menjaga privasi untuk kepentingan bersama.

Jika kepentingan umum diabaikan, kelompok rentan seperti anak-anak, lansia, atau masyarakat kurang teredukasi menjadi target utama serangan digital. Ketidaksiapan

melindungi kelompok ini dapat memperburuk ketidakadilan sosial dan memperbesar risiko penyalahgunaan data untuk kepentingan yang merugikan masyarakat luas.

d. Kemanfaatan

Pengelolaan data pribadi yang baik membawa manfaat besar bagi individu dan organisasi, baik dalam mendukung efisiensi operasional maupun menghindari sanksi hukum. Dalam Dasa Darma, prinsip "Rajin, terampil, dan gembira" mencerminkan semangat untuk bekerja keras dan cermat dalam menjalankan tanggung jawab, termasuk dalam menjaga manfaat dari data pribadi. Gerakan Pramuka dapat menyelenggarakan kegiatan simulasi yang mempersiapkan masyarakat dalam mengelola dan melindungi data, memastikan manfaat optimal dapat diraih tanpa risiko yang merugikan.

Tidak diterapkannya asas kemanfaatan dapat mengakibatkan pengelolaan data pribadi yang tidak efisien atau tidak efektif. Data yang dikelola dengan buruk tidak hanya mengurangi nilai manfaatnya, tetapi juga meningkatkan risiko kebocoran, ketidaksesuaian penggunaan data, atau pelanggaran hak privasi individu.

e. Kehati-hatian

Asas kehati-hatian menekankan pentingnya pengelolaan data pribadi dengan cermat agar terhindar dari insiden kebocoran atau pelanggaran. Prinsip "Hemat, cermat, dan bersahaja" dalam Dasa Darma mengajarkan pentingnya bertindak hati-hati dan efisien dalam menggunakan sumber daya, termasuk dalam menjaga data pribadi. Pramuka dapat memfasilitasi kegiatan pelatihan yang membangun kesadaran masyarakat tentang pentingnya kehati-hatian, dengan menyimulasikan potensi pelanggaran data dan cara-cara mengatasinya.

Jika kehati-hatian tidak diterapkan, risiko operasional seperti kebocoran data, manipulasi data, atau serangan siber meningkat. Kurangnya pengawasan dan pengelolaan yang hati-hati dapat membuat data pribadi rentan terhadap akses tidak sah dan menimbulkan kerugian finansial maupun reputasi. Dengan menerapkan asas kehati-hatian ini, diharapkan bahwa semua pihak yang terlibat dalam pemrosesan dan pengawasan data pribadi dapat mencegah potensi kerugian yang mungkin ditimbulkan terhadap individu, sehingga melindungi hak-hak privasi (Pranata et al., 2024: 728).

f. Keseimbangan

Keseimbangan antara perlindungan privasi individu dan kepentingan umum sangat penting agar hak-hak individu tetap terlindungi tanpa mengabaikan kebutuhan kolektif. Prinsip "Patuh dan suka bermusyawarah" dalam Dasa Darma relevan di sini, disebabkan oleh musyawarah membantu mencapai solusi yang adil dan berimbang. Dalam kegiatan Pramuka, pelatihan atau diskusi tentang pentingnya keseimbangan ini dapat menjadi media untuk mengajarkan cara menjaga harmoni antara kepentingan pribadi dan kepentingan umum, terutama adalah hal upaya perlindungan data pribadi yang pada dasarnya akan membutuhkan keterlibatan berbagai pihak terkait.

Ketidakseimbangan antara perlindungan privasi individu dan kepentingan umum dapat menyebabkan konflik antara hak individu dan kebutuhan kolektif. Terlalu fokus pada salah satu sisi tanpa mempertimbangkan yang lain dapat memicu pelanggaran privasi atau menghambat kebijakan yang bermanfaat bagi masyarakat luas.

g. Pertanggungjawaban

Asas pertanggungjawaban memastikan bahwa setiap pihak yang mengelola data pribadi bertindak transparan dan bertanggung jawab atas segala aktivitas yang dilakukan. Prinsip

"Bertanggung jawab dan dapat dipercaya" dalam Dasa Darma mengajarkan pentingnya memegang kepercayaan yang diberikan oleh orang lain, termasuk dalam hal menjaga data pribadi mereka. Gerakan Pramuka dapat mengadakan kegiatan yang mendorong individu untuk memahami konsekuensi dari setiap tindakan terkait data pribadi, sehingga tumbuh budaya tanggung jawab yang kuat di kalangan masyarakat.

Jika asas pertanggungjawaban tidak diterapkan, tidak ada pihak yang secara jelas bertanggung jawab atas pengelolaan data pribadi. Hal ini dapat memicu ketidakjelasan dalam menangani insiden kebocoran data, mengaburkan transparansi, dan menyebabkan ketidakpercayaan publik terhadap pengendali data maupun pemerintah.

h. Kerahasiaan

Asas kerahasiaan menekankan bahwa data pribadi harus dijaga dan dilindungi agar tidak disalahgunakan atau diakses oleh pihak yang tidak berwenang. Prinsip ini berfokus pada tanggung jawab pengendali data untuk menjamin keamanan informasi, termasuk dengan menggunakan teknologi dan kebijakan yang memadai. Pelanggaran asas ini dapat menyebabkan dampak buruk seperti pencurian identitas, penipuan, atau penyalahgunaan data. Asas kerahasiaan memiliki hubungan dengan Dasa Darma ke-8, yaitu "Disiplin, berani, dan setia." Melaksanakan prinsip kerahasiaan memerlukan kedisiplinan yang tinggi dalam menerapkan protokol keamanan data, keberanian untuk melaporkan pelanggaran, dan kesetiaan pada tugas menjaga amanah data pribadi yang dipercayakan kepada pengendali.

Jika asas kerahasiaan tidak diterapkan dengan benar, risiko utamanya adalah kebocoran data pribadi yang dapat diakses oleh pihak yang tidak berwenang. Hal ini membuka peluang bagi tindakan kejahatan seperti pencurian identitas, penyalahgunaan data untuk kepentingan komersial tanpa persetujuan, atau bahkan ancaman terhadap keselamatan individu. Selain itu, pelanggaran asas kerahasiaan dapat menurunkan kepercayaan masyarakat terhadap institusi yang mengelola data mereka, sehingga berdampak negatif pada hubungan antara pengendali data dan subjek data.

4. KESIMPULAN

Terdapat beberapa risiko yang dapat terjadi dalam hal terjadi kegagalan perlindungan data pribadi di lingkungan masyarakat. Hal ini di antaranya dapat dijatuhinya sanksi atas pelanggaran yang dilakukan terhadap regulasi yang berlaku, terjadinya operasional yang tidak efisien, dan meningkatnya kasus penipuan digital dengan target kelompok rentan. Selain itu, ditemukan beberapa bentuk implementasi dan irisan antara Dasa Darma Pramuka terhadap asas perlindungan data pribadi sebagai upaya yang dapat mengurangi risiko kegagalan perlindungan data pribadi. Hal ini dapat ditinjau dari asas perlindungan data pribadi itu sendiri yang terdiri atas asas perlindungan, kepastian hukum, kepentingan umum, kemanfaatan, kehati-hatian, keseimbangan, pertanggungjawaban, kepentingan umum, dan kerahasiaan. Setiap pelanggaran terhadap asas-asas tersebut memiliki masing-masing risiko yang berbeda. Masing-masing eksekusi asas perlindungan tersebut juga memiliki keterkaitan dengan nilai pada dasa darma pramuka dalam implementasinya.

5. UCAPAN TERIMA KASIH

Kami mengucapkan terima kasih kepada seluruh mitra, terutama Universitas Negeri Semarang, atas kontribusi yang sangat berharga dalam proses penyempurnaan naskah kami. Saran dan masukan yang diberikan telah sangat membantu kami dalam meningkatkan kualitas publikasi ini dan memastikan bahwa

hasil penelitian kami memenuhi standar akademik yang tinggi. Kami berharap kerja sama yang baik ini dapat terus terjalin untuk mendukung pengembangan ilmu pengetahuan.

REFERENSI

Buku dan Jurnal

- Abror, M. Y., Pratiwi, M., Yusa, M. Y., Musdalifah, F. S., & Murti, K. (2021). Raising The Awareness Of Privacy On The Use Of Internet Technology Among Adolescents. *Abdimas: Jurnal Pengabdian Masyarakat Universitas Merdeka Malang*, 6(4), 640–655. <https://doi.org/10.26905/abdimas.v6i4.5697>
- Anand, G., Hernoko, A. Y., & Dharmadji, A. G. (2020). The Urgency Of Enacting Personal Data Protection Law As A Patronage From The Development Of Communication And Information Technology In Indonesia. *Perspektif*, 25(1), 54. <https://doi.org/10.30742/perspektif.v25i1.750>
- Neta, Y., Awanisa, A., & Melisa, M. (2022). The Urgency of Establishing Independent Supervisory Authority for Personal Data Protection in Indonesia. *Constitutionale*, 3(1), 19–38. <https://doi.org/10.25041/constitutionale.v3i1.2535>
- Pradana, M. A. E., & Saragih, H. (2024). Prinsip Akuntabilitas dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR dan Akibat Hukumnya. *Innovative Journal of Social Science Research*, 4(4), 3412–3425.
- Pranata, A., Juono, A. A., Binarida, & Yulianigrum, A. V. (2024). Implementasi Asas Kehati-Hatian Dalam Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Di Era Digital 5.0 Andri. *Journal of Law and Nation (JOLN)*, 3(3), 721–730.
- Putra, T. I., & Fibrianti, N. (2024). Data Protection Impact Assessment Indicators In Protecting Consumer E-Commerce Platforms. *The Indonesian Journal of International Clinical Legal Education*, 6(1), 1–22: 11.
- Putra, T. I., & Fibrianti, N. (2024). Threats and Legal Protection of Personal Data Combined in E-Commerce Transactions Based on Personal Data Protection Law in Indonesia. *Lambung Mangkurat Law Journal*, 9(1), 64–74. <https://doi.org/10.32801/lamlaj.v9i1.438>.
- Putra, T. I., Islam, A. J., & Rahman, A. M. A. (2024). Integrating Islamic Laws into Indonesian Data Protection Laws: An Analysis of Regulatory Landscape and Ethical Considerations. *Contemporary Issues on Interfaith Law & Society*, 4(1), 85–118.
- Putri, E. P., & Elmina Martha, A. (2022). The Importance of Enacting Indonesian Data Protection Law as a Legal Responsibility for Data Leakage. *Varia Justicia*, 17(3), 287–303. <https://doi.org/10.31603/variajusticia.v17i3.6231>.
- Waspiah, W., Sekar, N., Lies, A., Putra, T. I., Wida, S., & Widyaning, S. (2023). Model Perlindungan Hukum Data Pribadi di Era Digital Guna Menjamin Hak Warga Negara Atas Perlindungan Data Pribadi. *Syntax Literate: Jurnal Ilmiah Indonesia*, 8(9), 5165–5179.

Peraturan Perundang-undangan

- Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik
- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945
- Undang-Undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi