

Perlindungan Hukum Terhadap Data Pribadi Remaja di Media Sosial: Tinjauan UU ITE dan UU Perlindungan Data Pribadi di SMP 3 Muhammadiyah Samarinda

Insan Nur Rahmanda Putra¹, Bayu Pramana Putra², Reynathan maulana resi³, lukman⁴, muhammad Rizky Safardianur⁵ Ade Putra Amanda⁶, Abdurrahman Fauzan⁷, Sunariyo⁸

Fakultas Hukum, Universitas Muhammadiyah Kalimantan Timur

Corresponding Author: insanputra@gmail.com

Published: Desember, 2025

ABSTRAK

Pelaksanaan kegiatan pengabdian kepada siswa/i di SMK Negeri 1 Samarinda ini merupakan implementasi dari Tri Dharma Perguruan Tinggi yang bertujuan untuk meningkatkan pemahaman generasi muda mengenai perlindungan hukum dan pencegahan kejahatan siber di era digital. Permasalahan utama yang dihadapi saat ini adalah masih rendahnya literasi digital di kalangan pelajar, sehingga banyak dari mereka belum memahami bentuk-bentuk kejahatan siber seperti penipuan online, pencurian data pribadi, dan penyebaran konten ilegal. Padahal, aktivitas digital telah menjadi bagian penting dalam kehidupan sehari-hari. Untuk menjawab permasalahan tersebut, kegiatan sosialisasi dilaksanakan di SMK Negeri 1 Samarinda dengan melibatkan 27 siswa/i sebagai peserta melalui metode ceramah normatif-yuridis dan diskusi interaktif. Kegiatan ini berlandaskan pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas UU ITE, yang mengatur tanggung jawab hukum bagi pengguna internet serta perlindungan terhadap korban kejahatan siber. Dalam konteks ini, negara hukum sebagaimana diatur dalam Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menjadi dasar bahwa setiap warga negara memiliki hak atas perlindungan hukum dan kewajiban untuk menaati ketentuan hukum dalam ruang digital. Hasil kegiatan menunjukkan bahwa peserta mulai memahami pentingnya menjaga keamanan digital pribadi, mengenali bentuk-bentuk kejahatan siber, serta mengetahui prosedur hukum dalam melaporkan tindak pidana siber. Diskusi juga menekankan perlunya kolaborasi antara sekolah, keluarga, dan aparat penegak hukum untuk memperkuat literasi hukum digital, agar generasi muda tidak hanya menjadi pengguna teknologi yang cerdas, tetapi juga warga negara yang patuh hukum dan berperan aktif dalam menciptakan ruang digital yang aman dan bertanggung jawab.

Keywords: Perlindungan Hukum, Kejahatan Siber, Undang-Undang ITE, Literasi Digital

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Attribution 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 dalam beberapa tahun terakhir telah membawa perubahan besar dalam pola hidup masyarakat modern. Internet tidak lagi dipandang sekadar sebagai instrumen komunikasi, tetapi telah menjadi ruang baru yang memfasilitasi berbagai aktivitas penting, seperti transaksi ekonomi, layanan publik, pendidikan, hingga pengelolaan data pribadi. Revolusi digital ini secara perlahan menggantikan banyak proses konvensional dan membuka peluang baru bagi efisiensi serta inovasi. Namun, di balik berbagai kemudahan tersebut, terdapat konsekuensi yang tidak dapat dihindari, yakni meningkatnya ancaman dan kejahatan yang terjadi di dunia maya.

Kejahatan siber tidak hanya terjadi pada individu, tetapi juga menasar lembaga pemerintah, perusahaan, hingga infrastruktur penting negara. Serangan berupa pencurian data, peretasan, pemalsuan identitas digital, manipulasi informasi, dan penipuan online kini menjadi fenomena yang semakin sering ditemukan. Kerugian yang ditimbulkan pun tidak hanya bersifat material, melainkan

juga menyangkut aspek keamanan, reputasi, dan kepercayaan publik terhadap sistem digital. Kondisi ini menunjukkan bahwa ruang siber memiliki karakteristik yang kompleks dan membutuhkan pengaturan hukum yang jelas agar tidak menjadi arena yang rawan penyalahgunaan. Dalam konteks penyebaran informasi digital, ajaran agama telah memberikan pedoman penting tentang kehati-hatian dalam menerima dan menyebarkan berita. Hal ini termaktub dalam firman Allah SWT pada QS. Al-Hujurat ayat 6:

﴿يَا أَيُّهَا الَّذِينَ آمَنُوا إِن جَاءَكُمْ فَاسِقٌ بِنَبَأٍ، فَتَبَيَّنُوا أَن تُصِيبُوا قَوْمًا بِجَهَالٍ، فَإِنَّكُمْ عَلَىٰ مَا فَعَلْتُمْ تَوَّابِينَ﴾

"Wahai orang-orang yang beriman, apabila datang kepadamu seorang fasik membawa suatu berita, maka telitilah kebenarannya, agar kamu tidak menimpakan suatu musibah kepada suatu kaum tanpa mengetahui keadaannya yang menyebabkan kamu menyesal atas perbuatanmu itu." Ayat ini memiliki relevansi kuat dalam konteks hukum siber, terutama terkait fenomena hoaks, ujaran kebencian, dan penyebaran informasi yang tidak terverifikasi di ruang digital. Nilai moral yang terkandung dalam ayat tersebut menegaskan pentingnya verifikasi, etika, dan tanggung jawab dalam berkomunikasi di dunia maya.

Di Indonesia, upaya untuk merespons dinamika tersebut salah satunya diwujudkan melalui lahirnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Regulasi ini menjadi dasar hukum utama dalam mengatur aktivitas di dunia digital, termasuk transaksi elektronik, perlindungan data, serta sanksi bagi pelanggaran hukum siber. Walaupun keberadaan UU ITE memberikan arah bagi penegakan hukum, implementasinya masih menghadapi berbagai permasalahan. Tantangan tersebut antara lain disebabkan oleh perkembangan teknologi yang lebih cepat dibandingkan proses pembaruan regulasi, keterbatasan kompetensi aparat penegak hukum dalam menghadapi kasus siber yang semakin kompleks, serta masih lemahnya mekanisme perlindungan data pribadi di tingkat nasional.

Di sisi lain, tingkat literasi digital masyarakat Indonesia belum merata. Banyak pengguna internet yang belum memahami batasan hukum, etika digital, dan cara melindungi diri dari ancaman siber. Hal ini menyebabkan tingginya jumlah korban kejahatan digital, sekaligus meningkatkan peluang terjadinya pelanggaran hukum oleh individu yang tidak menyadari konsekuensi dari tindakannya. Kondisi ini menegaskan bahwa pembentukan hukum siber tidak cukup hanya melalui regulasi yang bersifat represif, tetapi juga harus didukung oleh pendekatan preventif melalui edukasi, peningkatan kesadaran, dan penguatan sistem keamanan digital.

Perkembangan hukum siber di Indonesia tidak dapat dilepaskan dari pergeseran cara masyarakat berinteraksi di dunia digital yang semakin masif. Dengan jumlah pengguna internet yang terus meningkat setiap tahun, kompleksitas permasalahan yang timbul dalam ruang siber pun ikut bertambah. Hal ini menuntut adanya kebijakan hukum yang adaptif, komprehensif, dan responsif terhadap perubahan teknologi. Namun, realitas menunjukkan bahwa perkembangan hukum siber berjalan lebih lambat dibandingkan percepatan inovasi digital. Akibatnya, banyak celah hukum yang dimanfaatkan oleh pelaku kejahatan siber, sementara masyarakat dan aparat penegak hukum kerap berada dalam posisi sulit menghadapi fenomena baru yang belum terwadahi secara jelas dalam regulasi.

UU ITE sebagai regulasi utama sebenarnya telah mengalami beberapa kali revisi untuk memperbaiki sejumlah ketentuan yang dinilai multitafsir. Meski begitu, sejumlah pasal masih menimbulkan perdebatan, seperti mengenai pencemaran nama baik, penyebaran kebencian, dan pelanggaran privasi. Selain itu, banyak kasus siber baru yang belum memiliki dasar hukum yang memadai, seperti deepfake, pencurian identitas digital menggunakan AI, manipulasi data biometrik, hingga eksploitasi anak melalui platform digital. Perkembangan teknologi kecerdasan buatan (AI) dan Internet of Things (IoT) semakin memperluas potensi kerentanan yang belum sepenuhnya dipahami oleh pembuat kebijakan.

Salah satu isu besar dalam hukum siber Indonesia adalah lemahnya kerangka perlindungan data pribadi. Sebelum hadirnya Undang-Undang Pelindungan Data Pribadi (UU PDP) pada 2022, Indonesia hanya mengandalkan sejumlah pasal tersebar dalam UU ITE dan beberapa peraturan sektoral. Hal ini menyebabkan banyak kasus kebocoran data tidak dapat ditangani secara efektif. Kasus kebocoran data besar seperti BPJS Kesehatan, Polri, bahkan data SIM card, menunjukkan bahwa infrastruktur keamanan digital lembaga publik dan swasta masih rentan. Kondisi ini

menimbulkan kekhawatiran masyarakat karena data pribadi dapat digunakan untuk penipuan, pencurian identitas, hingga pemerasan.

Selain aspek regulasi, tantangan besar lain adalah kapasitas penegak hukum. Kejahatan siber membutuhkan kemampuan digital forensik, analisis jaringan, dan rekonstruksi rekam jejak elektronik yang sangat teknis. Namun, tidak semua aparat memiliki kualifikasi tersebut. Hal ini mengakibatkan beberapa kasus siber sulit ditangani atau memerlukan waktu lama. Di sisi lain, kerja sama internasional juga menjadi kebutuhan mendesak karena banyak kejahatan siber dilakukan lintas negara, sehingga melibatkan yurisdiksi yang berbeda. Tanpa koordinasi yang baik, pelaku kejahatan sering memanfaatkan celah ini untuk menghindari penegakan hukum.

Masyarakat sebagai pengguna internet pun memegang peran penting dalam terciptanya ruang digital yang aman dan sehat. Namun, rendahnya literasi digital membuat banyak masyarakat tidak menyadari bahaya dunia maya, seperti phishing, malware, rekayasa sosial, atau penyebaran informasi palsu. Fenomena hoaks, misinformasi, dan disinformasi yang menyebar dengan cepat melalui media sosial menjadi bukti lemahnya kontrol informasi pada tingkat individu. Padahal, dalam perspektif ajaran agama sebagaimana termuat dalam QS. Al-Hujurat ayat 6, kehati-hatian dalam menerima dan menyebarkan informasi merupakan kewajiban moral untuk mencegah terjadinya mudarat bagi orang lain. Nilai-nilai tersebut relevan untuk dijadikan dasar etika digital dalam membentuk masyarakat yang lebih kritis dan bertanggung jawab.

Dari sini dapat dipahami bahwa penguatan hukum siber di Indonesia harus dilakukan secara holistik. Hukum tidak boleh bersifat reaksioner semata, tetapi harus mampu mengantisipasi risiko-risiko masa depan. Hal ini menuntut pembuat kebijakan untuk selalu mengikuti perkembangan teknologi serta menjalin kolaborasi dengan para ahli, akademisi, dan pelaku industri digital. Harmonisasi kebijakan antar lembaga juga menjadi keharusan, mengingat keamanan siber tidak dapat diselesaikan oleh satu institusi saja.

Selain pembaruan regulasi, peningkatan kapasitas aparat penegak hukum juga merupakan prioritas penting. Program pelatihan teknis, pengadaan perangkat digital forensik, dan kerja sama internasional perlu diperkuat. Pada saat yang sama, edukasi kepada masyarakat mengenai etika digital, keamanan online, dan cara mengenali ancaman siber harus disosialisasikan secara lebih luas melalui sekolah, perguruan tinggi, lembaga pemerintah, dan platform digital lainnya. Pada akhirnya, pengaturan hukum siber yang efektif harus mencerminkan keseimbangan antara perlindungan hak asasi manusia, inovasi teknologi, dan kepastian hukum. Dengan memperkuat regulasi, meningkatkan kapasitas penegakan hukum, serta mendorong literasi digital masyarakat, Indonesia dapat membangun ekosistem digital yang lebih aman, inklusif, dan terpercaya. Penelitian ini diharapkan dapat memberikan masukan strategis dalam perumusan kebijakan di masa depan agar hukum siber di Indonesia tidak hanya menjadi instrumen represif, tetapi juga fondasi bagi pembangunan ruang digital yang sehat dan berkeadilan.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis perkembangan hukum siber di Indonesia dengan berfokus pada efektivitas regulasi yang telah berlaku, tantangan yang dihadapi dalam penerapannya, serta kebutuhan pembaruan kebijakan di masa mendatang. Penelitian ini menggunakan pendekatan analitis berbasis data untuk memberikan gambaran komprehensif mengenai kondisi aktual sistem hukum siber di Indonesia. Diharapkan, kajian ini dapat menjadi kontribusi dalam penguatan regulasi, peningkatan kapasitas penegak hukum, serta mendorong terciptanya ekosistem digital yang aman dan bertanggung jawab.

METODE

Metode pelaksanaan dalam kegiatan ini disusun untuk memastikan penyampaian materi hukum siber dapat dipahami secara optimal oleh peserta. Pendekatan yang digunakan menggabungkan metode presentasi, diskusi interaktif, dan sesi tanya jawab. Secara keseluruhan, metode ini dirancang agar peserta tidak hanya menerima penjelasan secara teoritis, tetapi juga dapat terlibat aktif dalam proses pembelajaran. Pertama, kegiatan diawali dengan penyampaian materi melalui presentasi menggunakan media PowerPoint (PPT). Materi yang disusun mencakup konsep dasar hukum siber, jenis-jenis kejahatan siber, regulasi yang berlaku di Indonesia, serta contoh kasus yang relevan. Penggunaan PPT bertujuan membantu peserta memahami alur pembahasan melalui

tampilan visual yang sistematis, sehingga informasi dapat tersampaikan secara lebih jelas dan terstruktur.

Selanjutnya, setelah pemaparan materi selesai, kegiatan dilanjutkan dengan sesi diskusi kelompok. Pada tahap ini, peserta diberikan kesempatan untuk menanggapi, mengkritisi, maupun menambahkan perspektif berdasarkan pemahaman masing-masing. Diskusi ini diharapkan dapat mendorong kemampuan analisis peserta serta membuka ruang bagi pertukaran pandangan terkait isu-isu hukum siber yang sedang berkembang. Tahap terakhir adalah sesi tanya jawab antara pemateri dan peserta. Melalui sesi ini, peserta dapat mengajukan pertanyaan mengenai hal-hal yang belum dipahami atau ingin digali lebih dalam. Sesi tanya jawab juga berfungsi sebagai evaluasi informal untuk melihat tingkat pemahaman peserta terhadap materi yang disampaikan. Dengan menggabungkan ketiga tahapan tersebut presentasi, diskusi, dan tanya jawab metode pelaksanaan ini diharapkan mampu memberikan pemahaman yang menyeluruh, meningkatkan keterlibatan peserta, serta memperkuat kemampuan analitis mereka terhadap isu-isu hukum siber.

HASIL DAN PEMBAHASAN

Pelaksanaan kegiatan penyampaian materi mengenai hukum siber menghasilkan beberapa temuan penting terkait tingkat pemahaman peserta, respons terhadap isu-isu digital, serta dinamika diskusi yang berkembang selama kegiatan berlangsung. Secara umum, kegiatan ini memberikan gambaran bahwa topik hukum siber masih menjadi isu yang menarik sekaligus membutuhkan penjelasan yang komprehensif karena berkaitan langsung dengan kehidupan digital masyarakat saat ini. Pada tahap pemaparan materi menggunakan media PowerPoint (PPT), peserta terlihat mampu mengikuti alur penyampaian dengan baik. Tampilan visual berupa rangkuman konsep hukum siber, contoh kasus, serta regulasi terkait (khususnya UU ITE) membantu peserta memahami kerangka dasar hukum yang mengatur aktivitas di dunia maya. Banyak peserta yang baru mengetahui bahwa beberapa tindakan yang sering dianggap sepele, seperti menyebarkan informasi tanpa verifikasi atau mengambil konten orang lain tanpa izin, memiliki konsekuensi hukum.

Hal ini menunjukkan bahwa penggunaan media presentasi efektif dalam memperkenalkan konsep dan aturan dasar hukum siber. Pada sesi diskusi, peserta menunjukkan antusiasme yang cukup tinggi. Beberapa isu yang paling banyak dibahas antara lain penyebaran hoaks, keamanan data pribadi, serta persoalan multitafsir dalam penerapan UU ITE. Peserta memberikan beragam pandangan berdasarkan pengalaman pribadi maupun pengamatan terhadap fenomena digital yang sering terjadi di masyarakat. Diskusi juga menyoroti adanya kesenjangan literasi digital, khususnya terkait pemahaman masyarakat umum mengenai batasan etika dan hukum dalam menggunakan media sosial. Temuan ini menguatkan bahwa salah satu masalah utama dalam penegakan hukum siber bukan hanya regulasinya, tetapi juga tingkat kesadaran masyarakat terhadap risiko di ruang digital.

Sementara itu, pada sesi tanya jawab, peserta mengajukan pertanyaan yang menggambarkan keingintahuan mendalam tentang implikasi hukum dari aktivitas digital yang sehari-hari mereka lakukan. Beberapa pertanyaan berfokus pada mekanisme pelaporan kejahatan siber, perlindungan data pribadi, serta bagaimana seseorang dapat melindungi diri dari ancaman digital seperti phishing, peretasan akun, dan penyalahgunaan informasi. Pertanyaan-pertanyaan tersebut menunjukkan bahwa peserta memiliki ketertarikan untuk memahami aspek praktis dari hukum siber, tidak hanya teorinya.



Gambar 1

Pengaturan mengenai aktivitas digital di Indonesia memiliki fondasi hukum yang cukup jelas melalui beberapa peraturan perundang-undangan yang saling melengkapi. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahan dalam Undang-Undang Nomor 19 Tahun 2016 menjadi dasar utama dalam mengatur perilaku masyarakat di ruang siber. Regulasi ini mencakup berbagai aspek, seperti transaksi elektronik, penyebaran informasi, pelanggaran privasi, hingga sanksi pidana bagi tindakan yang berdampak merugikan individu maupun kelompok.

Selain itu, kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memperkuat struktur hukum siber di Indonesia. UU PDP memberikan landasan hukum yang lebih komprehensif terkait pengumpulan, penyimpanan, pemrosesan, dan penyebaran data pribadi. Regulasi ini menegaskan bahwa setiap individu berhak atas perlindungan data yang melekat pada dirinya sebagai bagian dari hak privasi yang harus dihormati. Dengan demikian, kombinasi antara UU ITE dan UU PDP menjadi kerangka hukum penting dalam menanggapi tantangan yang muncul akibat semakin berkembangnya teknologi digital. Dalam konteks hukum siber, data pribadi dipahami sebagai setiap informasi yang dapat mengidentifikasi seseorang, baik secara langsung maupun tidak langsung. Secara umum, data pribadi terbagi menjadi dua kategori utama:

1. Data pribadi umum, seperti nama, alamat, nomor telepon, jenis kelamin, dan informasi dasar lainnya.
2. Data pribadi sensitif, seperti data biometrik, data kesehatan, rekam jejak keuangan, informasi agama, dan data yang menyangkut kondisi spesifik seseorang yang berpotensi menimbulkan diskriminasi.



Gambar 2

Data pribadi bukan hanya sekedar identitas, tetapi juga aset digital yang memiliki nilai tinggi. Dalam era transformasi digital, data pribadi menjadi bagian penting dalam berbagai aktivitas, mulai dari penggunaan media sosial, transaksi perbankan, hingga pendaftaran layanan publik berbasis online. Karena itu, keberadaan regulasi yang melindungi data pribadi sangat diperlukan untuk memastikan bahwa pengelolaan data dilakukan secara etis dan bertanggung jawab. Penyalahgunaan data pribadi dapat menimbulkan dampak yang signifikan bagi individu maupun masyarakat, beberapa risiko utama yang disorot antara lain:

a. Pencurian Identitas (Identity Theft)

Penyalahgunaan data pribadi dapat digunakan untuk membuat akun palsu, mengakses layanan keuangan tanpa izin, atau melakukan tindakan kriminal atas nama korban. Hal ini dapat menyebabkan kerugian finansial maupun reputasi.

b. Serangan Siber (Cyber Attack)

Data pribadi yang bocor dapat dimanfaatkan untuk melakukan serangan seperti phishing, peretasan akun, dan penyebaran malware. Pelaku dapat dengan mudah menargetkan korban menggunakan informasi pribadi yang telah didapatkan sebelumnya.

c. Eksploitasi dan Pemerasan Digital

Data sensitif seperti foto pribadi, riwayat kesehatan, atau informasi keuangan dapat digunakan untuk memeras korban. Penyebaran data tanpa izin (doxxing) juga menjadi ancaman serius yang dapat membahayakan keselamatan pribadi.

d. Gangguan Psikologis dan Sosial

Dampak penyalahgunaan data pribadi tidak hanya bersifat material. Korban sering mengalami tekanan psikologis, rasa takut, dan kehilangan rasa aman. Dalam beberapa kasus, tindakan ini juga berdampak pada hubungan sosial, reputasi, dan karier seseorang.

e. Penyalahgunaan oleh Pihak Korporasi atau Lembaga

Selain kejahatan individual, penyalahgunaan data pribadi juga dapat terjadi pada skala yang lebih besar, misalnya oleh perusahaan atau institusi yang tidak mengelola data pengguna secara benar. Kebocoran data massal berpotensi menimbulkan kerugian kolektif dan mengganggu kepercayaan publik terhadap layanan digital.

KESIMPULAN

Kegiatan sosialisasi mengenai hukum siber dan perlindungan data pribadi yang dilaksanakan di SMP 3 Muhammadiyah Samarinda memberikan gambaran nyata bahwa edukasi mengenai keamanan digital sangat dibutuhkan sejak tingkat pendidikan menengah. Melalui penyampaian materi berbasis presentasi dan sesi diskusi interaktif, peserta khususnya para siswa menunjukkan ketertarikan serta pemahaman yang semakin baik tentang pentingnya menjaga jejak digital, melindungi informasi pribadi, dan bersikap bijak dalam menggunakan media sosial. Materi terkait dasar hukum siber, termasuk UU ITE dan UU Perlindungan Data Pribadi, memberikan pemahaman awal kepada siswa bahwa aktivitas digital memiliki konsekuensi hukum yang harus dipahami dan dihormati. Sosialisasi ini juga menunjukkan bahwa sebagian besar siswa belum sepenuhnya menyadari jenis data apa saja yang termasuk data pribadi dan bagaimana data tersebut dapat disalahgunakan apabila tidak dijaga dengan baik. Melalui studi kasus sederhana dan contoh konkret, para peserta dapat melihat risiko nyata seperti penipuan online, pencurian identitas, peretasan akun, hingga penyebaran informasi palsu.

Hasil diskusi dan tanya jawab memperlihatkan bahwa siswa membutuhkan pedoman praktis untuk melindungi diri di dunia maya, seperti penggunaan kata sandi yang kuat, verifikasi dua langkah, kehati-hatian dalam menerima informasi, serta kebiasaan tidak membagikan data pribadi secara sembarangan. Respon positif dari peserta menunjukkan bahwa sosialisasi ini berperan penting dalam meningkatkan kesadaran digital (digital awareness) di lingkungan sekolah.

Secara keseluruhan, kegiatan sosialisasi ini membuktikan bahwa penguatan literasi digital harus dimulai dari tingkat pelajar. Sosialisasi hukum siber di SMP 3 Muhammadiyah Samarinda menjadi langkah preventif yang penting untuk meminimalkan risiko penyalahgunaan data pribadi dan mendorong terciptanya budaya digital yang aman, bertanggung jawab, dan sesuai dengan norma hukum yang berlaku. Ke depan, kegiatan serupa diharapkan dapat dilakukan secara berkelanjutan, baik melalui pelatihan lanjutan maupun kerja sama antara sekolah dan pihak terkait untuk membangun ekosistem digital yang lebih sehat.

REFERENSI

- Ardiansyah, F. (2020). "Tinjauan Yuridis Terhadap Penyalahgunaan Informasi Elektronik." *Jurnal Komunikasi dan Hukum*, 8(4), 302–315.
- Halim, S. (2022). "Penguatan Regulasi Perlindungan Data Pribadi sebagai Upaya Pencegahan Cyber Crime." *Jurnal Legislasi Nasional*, 19(1), 67–78.
- Lestari, N. (2019). "Dampak Kebocoran Data dan Tantangan Perlindungan Privasi di Era Digital." *Jurnal Transformasi Digital*, 5(1), 44–55.
- Nasution, B. J. (2018). *Hukum dan Regulasi Teknologi Informasi di Indonesia*. Bandung: Refika Aditama.
- Prawiro, R., Jamhur, A. I., Ariandi, V., & Afira, R. (2025). Literasi Keamanan Digital Edukasi Perlindungan Data Pribadi bagi Remaja di Era Media Sosial pada organisasi Pemuda dan Karang Taruna Nagari Sungai Pinang. *Jurnal Pesona Nusantara*, 1(2), 7-15.
- Putra, I. G. (2020). "Analisis Pengaturan Perlindungan Data Pribadi di Indonesia dalam Perspektif Cyber Law." *Jurnal Hukum & Teknologi*, 12(2), 115–128.
- Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2025). Keamanan online dalam media sosial: pentingnya perlindungan data pribadi di era digital (Studi Kasus Desa Pematang Jering). *Jurnal Pengabdian Nasional (JPN) Indonesia*, 6(1), 38-52.
- Rahardjo, M. (2020). *Keamanan Data di Era Digital*. Yogyakarta: CV Andi Offset.
- Santoso, R. & Wijaya, A. (2021). "Implementasi UU ITE dalam Penegakan Hukum Kejahatan Siber." *Jurnal Ilmu Hukum Indonesia*, 7(3), 201–214.
- Saragih, L. K., Budhijanto, D., & Somawijaya, S. (2020). Perlindungan hukum data pribadi terhadap penyalahgunaan data pribadi pada platform media sosial berdasarkan undang-undang republik indonesia nomor 19 tahun 2016 tentang perubahan atas undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elek. *Jurnal Hukum De'rechtstaat*, 6(2), 125-142.
- Satrio, M. B., & Widiatno, M. W. (2020). Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook Di Indonesia). *JCA of Law*, 1(1).
- Shafira, A., & Narwastuty, D. (2025). Perlindungan Data Pribadi Pelaku Cyberbullying Di Bawah Umur Dihubungkan Dengan Tindakan Doxing Oleh Pengguna Media Sosial Menurut UU PDP. *Unes Journal of Swara Justisia*, 9(1), 37-44.
- Sembiring, R. (2019). *Hukum Siber (Cyber Law): Aspek Hukum Teknologi Informasi*. Jakarta: PT Grasindo.
- Setiawan, S., & Fatmawati, N. (2024). Urgensi Perlindungan Identitas Anak Melalui Media Sosial. *AKADEMIK: Jurnal Mahasiswa Humanis*, 4(3), 700-712.
- Sutadi, E. (2017). *Cyber Crime: Ancaman dan Penanggulangannya*. Jakarta: PT Elex Media Komputindo.
- Sutarno, R. S. (2022). Analisis Perlindungan Hukum Terhadap Kekerasan Seksual Pada Remaja Berbasis Gender Di Media Sosial. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, 9(6), 2120-2128.
- Syafuddin, K. (2023). Peningkatan literasi keamanan digital dan perlindungan data pribadi bagi siswa di SMPN 154 Jakarta. *Eastasouth Journal of Impactive Community Services*, 1(03), 122-133.
- Telaumbanua, T. H. (2024). Perlindungan hukum bagi pengguna media sosial terhadap penyalahgunaan data pribadi terkait hak privasi menurut hukum positif. *Lex Privatum*, 13(1).
- Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas UU No. 11 Tahun 2008 tentang ITE.
- Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.