

Lindungi Diri dengan Keamanan Digital melalui Menjaga Rekam Jejak

Almasari Aksenta¹, Mulyanto², Istia Budi³, Masna Wati⁴

^{1,2}Politeknik Negeri Samarinda, ³Universitas Mulia, ⁴Universitas Mulawarman
¹a.aksenta@polnes.ac.id, ²mulyanto@polnes.ac.id, ³istiabudi@universitasmulia.ac.id,
⁴masnawat@ft.unmul.ac.id

Abstrak

Pengambilan data pribadi untuk meretas sebuah situs ataupun sekedar dalam hal untuk proses rekrutmen karyawan, seseorang memerlukan data pribadi yang diperlukan dengan melihat rekam jejak digitalnya. Hal ini bisa berdampak buruk/merugikan bagi pengguna jika mengetahui cara menjaganya. Pemahaman tentang digital safety dapat membantu seseorang dalam mengamankan data dirinya atau rekam jejak digitalnya. Penelitian ini menggunakan studi literatur dan bertujuan sebagai literasi tambahan pengetahuan masyarakat dalam melindungi rekam jejak digitalnya dengan pemahaman digital safety (keamanan digital). Penelitian ini menggunakan analisis kualitatif deskriptif. Sumber penelitian berasal dari literatur ilmiah dan sumber pustaka lainnya. Literatur diambil kisaran 5 tahun terakhir dari saat ini. Tujuan penelitian ini adalah untuk memberikan literasi tentang cara melindungi diri dengan pengetahuan keamanan digital melalui pemeliharaan jejak digital. Manfaat penelitian ini diharapkan dapat menjadi tambahan pengetahuan bagi masyarakat dalam menghadapi era digital ini dan sebagai pelengkap karya ilmiah akademis di bidang keamanan digital. Temuan artikel ini ialah berbagai cara menjaga rekam jejak digital melalui keamanan digital. Semua hal yang dikutip merupakan bagian dari banyak literatur terkait keamanan digital agar diharapkan menjadi literasi bentuk perlindungan dan pengamanan sebuah rekam jejak digital. Sebagai saran, melalui berbagai literatur yang ada, diharapkan dapat menjadi inspirasi dan literasi pengetahuan dalam melindungi data pribadi di era digital ini. Menjaga rekam jejak sangat penting dalam menanggulangi segala bentuk kejahatan di dunia maya.

Kata kunci: Keamanan Digital, Literasi Digital, Rekam Jejak Digital, Pelindungan Privasi

1. Pendahuluan

Tanpa disadari, apa yang dilakukan menggunakan internet atau berada di dunia maya meninggalkan sebuah riwayat. Riwayat ini adalah data yang menjadi identitas pribadi. Identitas tersebut dapat digunakan oleh suatu pihak untuk tujuan tertentu. Identitas digital dapat dipahami sebagai bentuk representasi individu dalam lingkungan digital yang tersusun atas berbagai data atau atribut unik untuk membedakan satu entitas dengan entitas lainnya (Robles-Carrillo, 2024). Data tersebut mencakup informasi seperti nomor identitas, nomor telepon, alamat email, serta elemen autentikasi yang terhubung dengan sistem identifikasi tertentu (Sedlmeir et al., 2021). Selain itu, identitas digital juga menggambarkan kumpulan informasi atau klaim mengenai individu yang dimanfaatkan dalam berbagai aktivitas dan layanan berbasis digital (Comb & Martin, 2024).

Di sebagian besar negara maju, identitas digital kini diwajibkan bagi individu untuk mengakses layanan pemerintah dengan mudah dan diwajibkan untuk sebagian besar transaksi di sektor swasta. Penggunaan identitas digital sangat dibutuhkan saat ini, misalnya verifikasi email memerlukan nomor pon-

sel, pembayaran *online* memerlukan verifikasi nomor ponsel dan sebagainya. Maka, identitas digital ini harus dijaga dengan ketat (Sullivan & Tyson, 2023).

Hal ini dapat berdampak di masa depan. Media sosial, panggilan internet, belanja, penggunaan aplikasi, permainan daring, atau email dicatat dalam basis data dan dapat dilihat dan digunakan oleh orang lain kapan pun mereka mau. Oleh karena itu, apa yang diinginkan, ditulis, dan diunggah di dunia digital bisa sangat penting dan terkadang berbahaya bagi manusia. Jejak digital muncul sebagai hasil dari penggunaan berbagai *platform* digital, seperti aplikasi pesan, media sosial, email, situs web, dan layanan *cloud*. Setiap aktivitas pengguna, mulai dari berinteraksi hingga berbagi informasi, akan menghasilkan data yang menggambarkan aspek kehidupan pribadi seseorang (Porwal et al., 2025). Oleh karena itu, jejak digital dapat dipahami sebagai kumpulan data yang terbentuk dari aktivitas seperti posting, komunikasi, dan pertukaran informasi di dunia maya (Gholve, 2025).

Perkembangan media sosial sejak awal 2000-an telah mengubah pembentukan identitas digital serta distribusi pengetahuan global. Analisis data Scopus (2001–2025) menunjukkan bahwa produksi penge-

tahuan tidak merata dan cenderung didominasi oleh negara, institusi, dan kelompok tertentu. Meskipun akses informasi semakin luas melalui media sosial dan mesin pencari seperti Google, ketimpangan epistemik tetap terjadi dalam produksi, kontrol, dan penyebaran informasi (Purnama, 2026).

Data jejak digital dari media sosial mampu memberikan gambaran yang lebih komprehensif mengenai perilaku dan kesejahteraan remaja dibandingkan pendekatan konvensional yang hanya mengukur durasi penggunaan. Namun, rendahnya kesadaran generasi muda terhadap risiko jangka panjang jejak digital menjadi perhatian penting, mengingat sifatnya yang permanen dan berpotensi memengaruhi reputasi, peluang sosial, serta kondisi psikologis di masa depan. Oleh karena itu, diperlukan peningkatan literasi digital dan kesadaran etis agar pemanfaatan media sosial dapat mendorong perilaku yang positif dan bertanggung jawab (Sultan et al., 2023).

Transaksi identitas ini dapat menjadi masalah jika ada orang yang tidak menyukainya atau sengaja mencemarkan nama baik mereka. Karena banyaknya kasus di dunia maya, identitas digital ini harus dilindungi. Hal ini juga berdampak pada menjaga privasi Anda sendiri. Aktivitas berselancar di dunia maya telah menjadi identitas bagi para penggunanya. Dari apa pun yang diposting atau dibagikan, mengunjungi situs apa pun, mengunduh, menonton, atau mengomentari apa pun dengan pengguna lain. Aktivitas berselancar di dunia maya dapat mengakibatkan semua aktivitas ini memiliki rekam jejak digital. Adjei et al., (2020) Salah satu tantangan mendasar yang dihadapi pengguna beberapa *platform* media sosial adalah bagaimana melindungi privasi pribadi dan seberapa banyak pengguna dapat mengungkapkan diri mereka secara daring. Pengungkapan diri ini memicu rekam jejak digital. Sama seperti orang yang meninggalkan jejak di lapangan ketika sedang berada di lingkungan fisik pasti meninggalkan berbagai jejak dari apa yang mereka lakukan di *platform* digital. Jejak yang ditinggalkan di lingkungan digital juga dapat menimbulkan berbagai macam persepsi (Karabatak & Alanoglu, 2022).

Pengaturan data pribadi memiliki peran penting dalam membantu individu untuk mengontrol sekaligus memahami jejak digital yang mereka hasilkan (Kaku, 2024). Pentingnya mengelola jejak digital untuk menghindari dan mengurangi eksploitasi oleh peretas atau penjahat di internet (kejahatan siber). Jejak digital membantu masyarakat memahami bagaimana jejak digital dapat memengaruhi privasi daring mereka. Oleh karena itu, sebagai masyarakat, kita juga perlu mengetahui beberapa cara untuk melindungi diri dari kejahatan siber (keamanan digital) (Jamal & Zain, 2022). Keamanan internet berkaitan dengan aktivitas-aktivitas berikut, termasuk memahami dan melindungi privasi daring, menghindari perundungan siber, paparan konten kekerasan, cara berinteraksi dengan orang asing dar-

Tabel 1. Gap Penelitian

Penelitian Terdahulu	Fokus & Kontribusi	Gap Penelitian
Porwal et al, 2025	Menunjukkan kekhawatiran terhadap privasi dan kesadaran dalam mengelola jejak digital.	Lebih fokus pada kekhawatiran, tidak menunjukkan strategi keamanan digital dalam pengelolaan jejak digital
Zezulka 2016	Menunjukkan pembahasan jejak digital dalam perspektif hukum.	Tidak membahas praktek keamanan keseharian secara umum
Ketipov, 2024	Ancaman jejak digital yang diintegrasikan dengan kepribadian dan perilaku pengguna.	Tidak ada fungsi teknis literasi keamanan dalam menghadapi ancaman jejak digital.

ing, dan menggunakan bahasa yang santun saat beraktivitas daring. Hal lain yang perlu dipertimbangkan dalam keamanan digital adalah melindungi informasi pribadi, mencegah serangan siber, mengamankan transaksi keuangan, dan menjaga reputasi daring (jejak digital) (Shanmugapriya & Priya, 2024).

Adapun penelitian sebelumnya yang berkaitan dengan keamanan jejak digital ini ialah yang pertama dari Porwal et al (2025), Pada penelitian ini memberikan riset bahwa ada kekhawatiran terhadap privasi dan kesadaran dalam mengelola jejak digital. Penelitian dilakukan dengan metode kuantitatif dan memberikan sedikit literatur tentang keamanan jejak digital (Porwal et al., 2025). Kedua riset Zezulka (2016), penelitian dari kesamaan pada penelitian ini ialah merupakan studi literatur yang menjelaskan pengamanan digital dan perlindungan data pribadi hanya saja pada perbedaannya penulis mengaitkan dengan aturan hukum perundang-undangan dengan objek masyarakat kalangan uni eropa (Zezulka, 2016). Lalu, yang ketiga pada riset Ketipov et al (2024), pada penelitian ini juga memberikan studi literatur mengenai keamanan digital pada rekam jejak digital namun pada perbedaannya, penelitian ini mengaitkan pada kepribadian penggunaannya. Ciri-ciri kepribadian individu pengguna dapat menunjukkan perilakunya dalam melakukan aktivitas keamanan cyber yang mana pada akhirnya meninggalkan jejak digital di internet (Ketipov et al., 2024).

Analisis kritis penelitian ini terhadap penelitian terdahulu dapat diuraikan pada Tabel 1 sebagai berikut:

Dari artikel sebelumnya lebih banyak ditemukan bentuk literatur yang dihubungkan dengan kasus tertentu dan banyak ditemukan dalam bentuk penerapan pengabdian masyarakat, maka artikel ini memberikan literatur tentang keamanan jejak dgital secara umum saja. Pertanyaan penelitian dari artikel ini ialah bagaimana bentuk secara umum dan tren literasi dari sebuah keamanan digital dan jejak digital

serta bagaimana hubungannya dalam menjaga rekam jejak?

Keterbaruan yang didapat dari artikel ini ialah pengembangan literasi keamanan digital yang tidak hanya sekedar berorientasi pada perangkat dan pencegahan serangan cyber tetapi juga pengelolaan jejak digital secara berkelanjutan. Literasi mengintegrasikan aspek keamanan akun, perlindungan data pribadi, pengaturan privasi, pengendalian jejak digital serta reputasi diri dalam suatu kebersihan jejak digital. Kontribusi artikel ini yang membedakan dari penelitian sebelumnya ialah keamanan digital tidak hanya dipahami dengan upaya perlindungan terhadap ancaman cyber tetapi juga strategi terhadap pengelolaan identitas, privasi, dan reputasi secara berkelanjutan dalam upaya sebuah kebersihan rekam jejak digital. Pengelolaan tersebut dapat menjadi panduan masyarakat untuk memahami, mengendalikan dan mengurangi resiko ancaman dari aktivitas digital.

Tujuan penelitian ini adalah untuk memberikan literasi tentang cara melindungi diri dengan pengetahuan keamanan digital melalui pemeliharaan jejak digital. Manfaat penelitian ini diharapkan dapat menjadi tambahan pengetahuan bagi masyarakat dalam menghadapi era digital ini dan sebagai pelengkap karya ilmiah akademis di bidang keamanan digital.

2. Metode

Penelitian ini menggunakan analisis kualitatif deskriptif. Sumber penelitian berasal dari literatur ilmiah dan sumber pustaka lainnya. Kriteria literatur yang diambil dengan menggunakan teknik inklusi yang mana mengambil sumber pustaka kisaran 5 tahun terakhir dari saat ini dan bentuk eksklusi yaitu dengan melihat tren terkini cara perlindungan keamanan jejak digital. Kata kunci yang digunakan ialah sebagai berikut keamanan digital, literasi digital, rekam jejak digital, dan perlindungan privasi.

3. Hasil dan Pembahasan

3.1 Keamanan Digital

Keamanan digital adalah mempelajari cara menjaga privasi dan melindungi diri dari predator saat terhubung di era digital baru ini. Keamanan digital dikenal sebagai keamanan internet, keamanan media, keamanan daring, keamanan elektronik, atau keamanan siber (Sadiku et al, 2021). Riset keamanan digital digunakan untuk merujuk pada riset tentang kondisi keamanan, privasi, keselamatan, dan otonomi seseorang atau suatu kelompok, yang berkaitan dengan jejak digital mereka. Meskipun terdapat beragam definisi keamanan, penulis menggunakannya untuk merujuk pada saat teknologi melayani, memungkinkan, atau memberdayakan suatu aktivitas, alih-alih menjadi sumber bahaya (misalnya, vektor pelecehan, pengawasan) (Bellini et al., 2023).

Pada aspek keamanan digital, unsur yang dilihat adalah kemampuan mengatur siapa saja yang dapat melihat timeline pengguna, Kemampuan melaporkan penyalahgunaan di jejaring sosial, kemampuan menonaktifkan opsi menampilkan posisi geografis, pemahaman data pribadi, kemampuan menggunakan aplikasi untuk mencari dan menghapus perangkat digital yang dimiliki, kemampuan membedakan email yang mengandung virus/spam/malware, kebiasaan membuat password, dan kemampuan melakukan backup data ke beberapa tempat (Nisa et al., 2023). Diskusi tentang tren terbaru pada ancaman dunia cyber merupakan bentuk kewaspadaan dalam menjaga keamanan digital. Beberapa panduan praktis dan mencegah insiden keamanan digital ialah penggunaan kata sandi yang kuat, autentifikasi faktor dan enkripsi data. Bentuk pencegahan tersebut biasanya juga terjadi pada kasus phishing dan malware (Taufik Syastra et al., 2022).

Penguatan literasi keamanan digital menjadi kebutuhan mendesak seiring cepatnya pertumbuhan teknologi dan paparan resiko digital yang kompleks. Berikut beberapa cara mendasar dalam menjaga keamanan digital ialah mengelola ijin akses aplikasi yang terpasang pada gadget, mengelola privasi pada akun media sosial dan mengaktifasi autentifikasi dua atau tiga faktor. Selain itu, penghapusan riwayat pencarian dan non aktivasi pelacakan lokasi pada foto dan unggahan tertentu (Bate & Prasetyo, 2025).

3.2 Jejak Digital

Jejak digital merupakan akumulasi data yang muncul dari aktivitas serta interaksi individu dalam ruang digital yang dapat dilacak dan dianalisis lebih lanjut (Prabhakar & Kumar, 2022). Data ini terbentuk melalui berbagai aktivitas daring, termasuk penggunaan media sosial, penelusuran internet, dan komunikasi digital, yang menggambarkan perilaku serta eksistensi individu di dunia maya (Sugiarto & Arif, 2024). Jejak digital merefleksikan eksistensi individu dalam dunia daring serta mencakup beragam aktivitas yang dilakukan melalui internet. Setiap bentuk interaksi dan aktivitas pengguna akan menghasilkan data digital yang dapat dianalisis untuk menggambarkan perilaku serta aktivitas *online* individu ((Zarate et al., 2022); (Weiler et al., 2024)). Aktivitas tersebut meliputi penggunaan media sosial, penelusuran informasi, komunikasi digital, hingga transaksi secara *online* (Ketipov et al., 2024).

Jejak digital diklasifikasikan lebih lanjut menjadi dua kategori, yaitu jejak digital pasif dan jejak digital aktif. Jejak digital aktif ialah dengan berbagi berbagai informasi yang ditinggalkan pada media sosial dan aplikasi lainnya. Jejak digital pasif ialah pengguna tanpa sadar meninggalkan aktivitas berselancar di internet seperti histori pencarian, sandi, Alamat IP dan sebagainya (Niyu & Gerungan, 2022). Jejak Digital Pasif adalah jejak yang dibuat ketika

data dikumpulkan tentang beberapa aktivitas daring. Misalnya, dalam aktivitas daring setiap kali pengguna menjelajahi situs web mana pun, situs web tersebut dapat melacak lokasi geografisnya melalui alamat IP pengguna. Ini dapat dilacak melalui konten yang diposting daring atau aktivitas seperti komentar, suka, berbagi gambar, dll. Lebih lanjut, jejak digital aktif adalah ketika pengguna bersedia melepaskan data pribadi mereka dengan tujuan berbagi informasi tentang diri mereka sendiri. Dalam aktivitas daring, pengguna membuat profil media sosial, membagikan status, serta memposting berbagai konten yang secara tidak langsung membentuk jejak digital aktif, yaitu data yang secara sengaja dihasilkan melalui aktivitas *online* (Sedlmeir et al., 2021).

3.3 Perlindungan Data Pribadi dalam Keamanan Digital

Memahami keamanan digital dapat dimulai dari pengetahuan dan kemudian menerapkannya. Dimulai dengan melindungi data sendiri. Membangun kapabilitas Indonesia terkait keamanan data sangat dibutuhkan. Dalam hal ini, negara bertanggung jawab membangun sistem keamanan siber untuk menyediakan perlindungan data yang aman dan demokratis bagi warga negara Indonesia. Perlindungan data merupakan peraturan perundang-undangan yang bertujuan untuk memberikan perlindungan terhadap data pribadi yang dimiliki seseorang (Aji, 2022).

Ada beberapa upaya untuk melindungi data. Ketika seseorang ingin memasuki suatu situs, biasanya mereka akan melakukan login atau mendaftar akun terlebih dahulu. Akun yang dibuat harus memiliki kata sandi yang kuat dan sesuai dengan pedoman keamanan situs tersebut. Sebelum menjelajah, ada baiknya untuk benar-benar memeriksa secara detail situs yang akan dituju, apakah situs tersebut resmi atau palsu. Dengan begitu, dapat meminimalisir penyebaran virus komputer. Menutup iklan yang tidak pantas lebih baik daripada hanya melihat-lihat, hal ini juga dapat mencegah malware. Setiap pengguna internet dan media sosial harus melakukan segala upaya yang memungkinkan untuk mencegah kejahatan siber, yaitu melindungi komputer dari virus, menjaga privasi, menjaga keamanan akun, menghindari hoaks, dan selalu memperbarui informasi atau meninjau kebenaran konten media sosial, serta menyebarkan informasi yang positif (Fitriani & Pakpahan, 2020).

Keamanan siber adalah teknologi yang dirancang untuk melindungi data dan sistem informasi yang tersimpan di komputer. Keamanan siber juga merupakan bagian dari keamanan digital. Terdapat 5 fungsi utama dalam kerangka kerja keamanan, seperti yang ditunjukkan pada Gambar 1 (Perwej et al., 2021):



Gambar 1. Lima Fungsi Utama Kerangka Kerja Keamanan Siber

1. Identifikasi: Untuk mengelola risiko keamanan siber terhadap sistem, aset, data, dan kemampuan, perusahaan harus terlebih dahulu memahami lingkungan mereka.
2. Deteksi: Organisasi harus menerapkan prosedur yang diperlukan untuk mendeteksi insiden keamanan siber secepat mungkin.
3. Melindungi: Organisasi harus membuat dan menerapkan kontrol yang tepat untuk membatasi atau menahan konsekuensi dari potensi insiden keamanan siber.
4. Respons: Dunia bisnis harus mampu membuat rencana reaksi untuk mengurangi dampak serangan siber.
5. Pemulihan: Bisnis harus merancang dan menerapkan strategi yang efektif untuk memulihkan kemampuan atau layanan yang dirugikan oleh insiden keamanan siber.

3.4 Menjaga Rekam Jejak Digital

Keamanan digital adalah pemahaman bahwa seseorang harus melindungi data pribadi dan perangkat digitalnya saat berada di lingkungan digital. Hal ini biasanya digunakan untuk manajemen data digital dan banyak forum berbasis daring. Selain itu, data atau perangkat pribadi ini juga dapat mendorong peretasan, penipuan, pencurian, pelanggaran data, dan kejahatan siber lainnya yang terus meningkat karena penggunaan perangkat digital semakin umum dan dapat digunakan untuk menipu orang lain (Ridwan B, 2024). Jadi, baik data maupun perangkat bersifat pribadi. Tidak semua orang dapat dengan mudah menggunakannya. Penelitian (McDonald et al., 2023) menunjukkan bahwa terdapat individu yang memiliki sikap positif dalam berbagi data jejak digital untuk tujuan penelitian dan kepentingan publik. Dengan mengintegrasikan preferensi tersebut ke dalam model penelitian yang etis dan bertanggung jawab, dapat menciptakan kerangka kerja berbagi data yang lebih adil dan seimbang, yang pada akhirnya dapat membantu orang membuat pilihan yang lebih baik tentang data jejak digital pribadi mereka. Bijaksana dalam berbagi informasi sangat diperlukan, tetapi jika benar-benar bersifat pribadi, seperti identitas pribadi berupa nomor penduduk, tidaklah tepat untuk dipublikasikan.

Penelitian (Soni, 2024) menyimpulkan bahwa remaja sering menghasilkan jejak digital yang permanen tanpa memahami risikonya, sehingga rentan terhadap cyberbullying, pencurian identitas, dan penyalahgunaan data. Oleh karena itu, menjaga rekam jejak digital sangat penting melalui peningkatan literasi digital, kesadaran privasi, dan penggunaan media sosial yang bijak.

Pengguna media sosial terkadang tidak menyadari meninggalkan jejak digital setiap melakukan aktivitas virtualnya. Setiap orang dapat melacak informasi dengan mudah melalui media sosial. Sikap yang harus diterapkan ialah menyaring dalam mendapatkan dan berbagi informasi yang didapatkan. Jejak digital sangat berpengaruh dalam membangun jaringan sosial yang kuat dan reputasi. Reputasi pribadi yang baik mencerminkan karakter dan profesional. Namun tidak hanya reputasi melainkan menciptakan peluang dan membangun relasi dalam hal tujuan pribadi maupun profesional sangat diperlukan. Edukasi tentang jejak digital masih diperlukan dalam berselancar di dunia maya. Pengetahuan terhadap pentingnya etika dalam penggunaan media sosial dan membatasi diri untuk tidak membagikan data pribadi kedalam media sosial dengan membatasinya dengan privasi. Pembuatan password secara berkala dapat menghindarkan diri dari kebocoran data, dan paling penting ialah pengguna media sosial memahami bahwa segala informasi yang di akses akan meninggalkan jejak digital (Razak et al., 2024). Berikut beberapa cara keamanan digital untuk menghindari dampak negatif jejak digital. Kegiatan edukasi dalam memahami penggunaan media sosial dan membuat privasi pribadi. Pemahaman bahwa segala yang diakses pasti akan meninggalkan jejak digital. Menghindari kebocoran data ialah dengan membuat password secara berkala. Pengguna juga harus mampu membatasi diri dalam membagikan informasi pribadi hal ini dilakukan untuk menjaga privasi (Widnyani et al., 2022).

Cara lain untuk mengurangi dampak negatif jejak digital adalah dengan memeriksa data pribadi di mesin pencari secara berkala. Pengguna menerapkan pengaturan privasi pada setiap unggahan di media sosial atau situs web pribadi. Pengguna menghapus data yang kurang penting dan memilih pertemanan di media sosial. (Levy & Gafni, 2021). Menghapus foto dari perangkat digital, menghapus ulasan daring, menghapus informasi dari situs web organisasi, mengurangi konfirmasi permintaan pertemanan yang tidak dikenal dan/atau menghapus teman di jejaring sosial, menghapus data pelanggan yang tidak relevan, dan sebagainya. Ini adalah beberapa cara untuk menjaga keamanan pribadi dan kebersihan jejak digital Anda saat berinteraksi atau pernah berinteraksi di dunia maya. Ada baiknya seseorang memiliki pengetahuan tentang manajemen risiko di dunia maya, memahami peraturan terkait situs tertentu (pemblokiran, kata sandi, dll.) agar pengguna

merasa aman dan nyaman saat berselancar di dunia maya.

4. Kesimpulan

Keamanan digital merupakan cara melindungi diri dan menjaga privasi baik melalui perangkat elektronik maupun jaringan internet. Penguatan literasi keamanan digital didasari dengan panduan praktis dan cara mencegah agar meningkatkan kewaspadaan dalam dunia cyber. Pengelolaan izin perangkat digital, pengelolaan akun web atau media sosial, dan cara menjaga privasi data pribadi. Aktivitas yang dilakukan di dunia maya dapat dilacak melalui internet. Aktivitas tersebut mengidentifikasi perilaku dan kegiatan penggunaannya yang disebut jejak digital. Informasi apapun yang dibagikan di internet dikatakan jejak digital aktif, namun yang pasif jika aktivitas tersebut merupakan kegiatan berselancar di internet. Jejak digital aktif dapat dibuktikan dengan melihat data-data pribadi seperti aktivitas keseharian, posting gambar, video dan artikel lainnya di situs web atau media sosial. Pada jejak digital pasif dibuktikan dengan riwayat pencarian, Lokasi pengguna yang mengakses web tersebut, dan berbagai riwayat aktivitas mengakses situs internet.

Keamanan digital dapat dimulai dengan melindungi data pribadi terlebih dahulu. Melindungi data pribadi dimulai dengan melindungi akun untuk login dengan sandi yang kuat. Berdasarkan kerangka kerja keamanan, Perusahaan harus memahami lingkungannya dengan mengidentifikasi aset data yang ada, lalu mendeteksi insiden dari keamanan cyber dan membuat prosedur penanganan secepat mungkin. Perusahaan menerapkan control untuk melindungi dari potensi insiden. Selanjutnya organisasi dapat merespon dengan mengurangi dampak negative adanya serangan cyber dan menerapkan strategi pemulihan layanan yang terjadi akibat adanya insiden dari keamanan cyber.

Individu harus sadar dan mengurangi dampak negatif dari jejak digital dengan harus lebih bijak dalam membagikan data pribadinya. Sikap yang harus diterapkan ialah menyaring informasi dan berbagi postingan positif. Jejak digital yang baik membuat reputasi pribadi menjadi baik. Edukasi etika dalam penggunaan teknologi digital juga sangat penting. Keamanan digital lain untuk mengurangi dampak jejak digital negatif ialah pengelolaan pengaturan pada privasi akun, update password berkala, memeriksa data pribadi di mesin pencari, menghapus data kurang penting, apapun pengetahuan yang terkait dengan manajemen resiko serta peraturan kebijakan situs-situs di internet.

Temuan artikel ini ialah berbagai cara menjaga rekam jejak digital melalui keamanan digital. Semua hal yang dikutip merupakan bagian dari banyak literatur terkait keamanan digital agar diharapkan menjadi literasi bentuk perlindungan dan pengamanan sebuah

rekam jejak digital.

Sebagai saran, melalui berbagai literatur yang ada, diharapkan dapat menjadi inspirasi dan literasi pengetahuan dalam melindungi data pribadi di era digital ini. Menjaga rekam jejak sangat penting dalam menanggulangi segala bentuk kejahatan di dunia maya.

Daftar Pustaka

- Adjei, J. K., Adams, S., Mensah, I. K., Tobbin, P. E., & Odei-Appiah, S. (2020): *Digital identity management on social media: Exploring the factors that influence personal information disclosure on social media*, Sustainability (Switzerland), 12(23), 1–17. <https://doi.org/10.3390/sul2239994>
- Aji, M. P. (2022): *Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]*, Jurnal Politika Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 13(2), 222–238. <https://doi.org/10.22212/jp.v13i2.3299>
- Bate, A. P., & Prasetyo, K. (2025): *Pengamanan Jejak Digital Jejak Digital: Pelatihan dan Edukasi Keamanan Data Pribadi bagi Siswa SMAN 1 Cimarga, Kabupaten Lebak, Provinsi Banten*, Jurnal Abdi Masyarakat Indonesia (JAMSI), 5(5). <https://doi.org/10.54082/jamsi.2055>
- Bellini, R., Tseng, E., Warford, N., Daffalla, A., Matthews, T., Consolvo, S., Woelfer, J. P., Kelley, P. G., Mazurek, M. L., Cuomo, D., Dell, N., & Ristenpart, T. (2023): *SoK: Safer Digital-Safety Research Involving At-Risk Users*, <http://arxiv.org/abs/2309.00735>
- Comb, M., & Martin, A. (2024): *Mining digital identity insights: patent analysis using NLP*, EURASIP Journal on Information Security, 2024(1), 21. <https://doi.org/10.1186/s13635-024-00172-5>
- Fitriani, Y., & Pakpahan, R. (2020): *Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace*, Jurnal Nusantara Bina Sarana Bina Informatika, 20(1). <https://doi.org/10.31294/jc.v19i2>
- Gholve, S. S. (2025): *Data Privacy while using Social Media Platforms*, International Journal of Scientific Research in Modern Science and Technology, 4(10), 27–33. <https://doi.org/10.59828/ijrmst.v4i10.385>
- Jamal, N., & Zain, J. M. (2022): *A Review on Nature, Cybercrime and Best Practices of Digital Footprints*, International Conference on Cyber Resilience, ICCR 2022. <https://doi.org/10.1109/ICCR56254.2022.9995834>
- Kaku, S. (2024): *Navigating the Digital Landscape: Understanding and Managing Your Digital Footprint*, Global Media Journal, 22, 68. <https://doi.org/10.36648/1550-7521.22.68.429>
- Karabatak, S., & Alanoglu, M. (2022): *Faculty Members' Digital Footprint Experiences and Digital Footprint Awareness*, Educational Academic Research, 1(44), 31–41. <https://doi.org/10.54614/AUJKEF.2022.891924>
- Ketipov, R., Schnalle, R., Doukovska, L., & Dehez, D. (2024): *Managing Cybersecurity: Digital Footprint Threats*, Cybernetics and Information Technologies, 24(3), 151–162. <https://doi.org/10.2478/cait-2024-0030>
- Levy, Y., & Gafni, R. (2021): *Introducing the concept of cybersecurity footprint*, Information and Computer Security, 29(5), 724–736. <https://doi.org/10.1108/ICS-04-2020-0054>
- McDonald, R., Skatova, A., & Maple, C. (2023): *Attitudes towards Sharing Digital Footprint Data: a Discrete Choice Experiment*, International Journal of Population Data Science, 8(3). <https://doi.org/10.23889/ijpds.v8i3.2287>
- Nisa, U., Lusi, C., Nisak, C., & Fatia, D. (2023): *Literasi Digital Lansia Pada Aspek Digital Skill Dan Digital Safety*, Jurnal Komunikasi Global, 12(1), 2023.
- Niyu, & Gerungan, A. (2022): *Literasi Digital: Mengenal Cyber Risk Dan Aman Dalam Bermedia Digital*, Prosiding PKM-CSR, 5, 2655–3570.
- Perwej, Dr. Y., Qamar Abbas, S., Pratap Dixit, J., Akhtar, Dr. N., & Kumar Jaiswal, A. (2021): *A Systematic Literature Review on the Cyber Security*, International Journal of Scientific Research and Management, 9(12), 669–710. <https://doi.org/10.18535/ijssrm/v9i12.ec04>
- Porwal, P. D., Kasera, N., Khan, L., & Kumawat, P. (2025): *A Study on Digital Footprints and Concerns About Privacy and Security on Social Media*, Idealistic Journal of Advanced Research in Progressive Spectrums (IJARPS), 4.
- Prabhakar, A., & Kumar, R. (2022): *Digital footprints: How Big Really It Is?* In Interactive Learning Environments (Vol. 31, Number 2, pp. 50–53). Routledge. <https://doi.org/10.1080/10494820.2020.1814821>
- Purnama, D. H. (2026): *The virtual identity and global epistemic inequality on social media: a reflective bibliometric analysis*, In Cogent Social Sciences (Vol. 12, Number 1). Cogent OA. <https://doi.org/10.1080/23311886.2026.2629632>
- Razak, F. R., Muammar, Kencana, N. W., Fadlil, & Herman. (2024): *Membangun Jejak Digital Positif: Cara Memanfaatkan Media Sosial Secara Produktif*, Jurnal Pengabdian Informatika, 2(4).
- Ridwan B, M. (2024): *Instagram as a Tool for Implementation of Social Crm (Customer Relationship Management) Study on Tourism in Lamongan Regency (Wisata Bahari Lamongan and Maharani Zoo)*, Jurnal Ekonomi & Ekonomi Syariah,

- 7(1), 970–980. <https://doi.org/10.36778/jesya.v7i1.1505>
- Robles-Carrillo, M. (2024): *Digital identity: an approach to its nature, concept, and functionalities*, International Journal of Law and Information Technology, 32. <https://doi.org/10.1093/ijlit/eaee019>
- Sadiku et al. (2021): *Digital safety*, International Journal of Scientific Advances, 2(5), 22–23. <https://doi.org/10.51542/ijscia.v2i5.21>
- Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021): *Digital Identities and Verifiable Credentials*, Business and Information Systems Engineering, 63(5), 603–613. <https://doi.org/10.1007/s12599-021-00722-y>
- Shanmugapriya & Priya, K. (2024): *Digital Safety*, <https://www.researchgate.net/publication/379038589>
- Soni, M. N. (2024): *Digital footprints of the young: privacy concerns and awareness among teen social media users*, Scienxt International Journal of Cyber Security, 1(1), 1–7.
- Sugiarto, E., & Arif, M. F. (2024): *Digital Footprints: Unpacking Cultural Identity Through English-Language Practices On Social Media*, English Review: Journal of English Education, 12(3), 983–992. <https://doi.org/10.25134/erjee.v12i3.10321>
- Sullivan, C., & Tyson, S. (2023): *A global digital identity for all: the next evolution*, Policy Design and Practice, 6(4), 433–445. <https://doi.org/10.1080/25741292.2023.2267867>
- Sultan, M., Scholz, C., & van den Bos, W. (2023): *Leaving traces behind: Using social media digital trace data to study adolescent wellbeing*, Computers in Human Behavior Reports, 10, 100281. <https://doi.org/10.1016/j.chbr.2023.100281>
- Taufik Syastra, M., Soleh Fajari, M., Novarini, R., Karim Harahap, A., Khaerullah, A., Kurniawan, R., Maulid, E., Irfayanti, Y., & Kurnia Wijayanti, E. (2022): *Digital Safety Tips untuk Generasi Milenial*, Bernas: Jurnal Pengabdian Kepada Masyarakat, 3(4), 1120–1124. <https://doi.org/10.31949/jb.v3i4.3974>
- Weiler, M., Jansen, N., & Hinz, O. (2024): *Can We Measure the Structural Dimension of Social Capital with Digital Footprint Data?—An Assessment of the Convergent Validity of an Indicator Extracted from Digital Footprint Data*, Schmalenbach Journal of Business Research, 76(2), 159–195. <https://doi.org/10.1007/s41471-024-00180-8>
- Widnyani, N. M., Reganata, G. P., Rettobjaan, F. V. C., Richadinata, K. R. P., & Aristayudha, A. A. N. B. (2022): *Digital Footprint: Dasar-Dasar Komunikasi Dengan Privasi di Media Sosial*, Jurnal Pengabdian Kepada Masyarakat Nusantara (JPKMN), 3(2), 942–947.
- Zarate, D., Stavropoulos, V., Ball, M., de Sena Collier, G., & Jacobson, N. C. (2022): *Exploring the digital footprint of depression: a PRISMA systematic literature review of the empirical evidence*, BMC Psychiatry, 22(1). <https://doi.org/10.1186/s12888-022-04013-y>
- Zezulka, O. (2016): *The Digital Footprint And Principles Of Personality Protection In The European Union*, <https://ssrn.com/abstract=2896864>

Halaman ini sengaja dikosongkan