Jurnal Manajemen dan Pendidikan Agama Islam
Volume 3, Nomor 3, Mei 2025
e-ISSN: 3031-8394; p-ISSN: 3031-8416, Hal. 396-404
DOI: https://doi.org/10.61132/jmpai.v3i3.1150
Available Online at: https://journal.aripafi.or.id/index.php/jmpai

Pentingnya Perlindungan dan Keamanan Data Privasi di Era Digital

Abelia Mita Baqis [1]*, Muhammad Irwan Padli Nasution [2]
[1,2] Universitas Islam Negeri Sumatera Utara, Indonesia
Email: abeliamitabaqis7@gmail.com *

Abstract, *Along with the rapid development of the digital era, data privacy is now one of the most valuable assets for individuals and organisations. The increase in the use of information and communication technology also has the impact of increasing the potential for data breaches. Personal data, which includes information such as names, addresses, phone numbers, and financial data, is often a target for irresponsible parties. Data breaches can result in financial loss, reputation, and even threats to individual safety. Therefore, it is important to understand and implement effective protection measures to safeguard data privacy in this digital era. This paper reviews the urgency of personal data protection and security, the various challenges that arise, and the efforts that can be made to maintain the confidentiality of personal information. Using a qualitative approach, data is obtained from various literature sources and relevant case studies. The findings of this study indicate the need to raise awareness of the importance of safeguarding personal data, both at the individual and institutional levels, in order to prevent misuse of information. In addition, this research also suggests a number of strategies that can be implemented to strengthen the privacy data security system.*

Keywords: *data, breaches, protection, security*

Abstrak, Seiring dengan pesatnya perkembangan era digital, data privasi kini menjadi salah satu aset yang sangat bernilai bagi individu maupun organisasi. Peningkatan penggunaan teknologi informasi dan komunikasi turut membawa dampak berupa meningkatnya potensi pelanggaran data. Salah satunya Data pribadi, yang mencakup informasi seperti nama, alamat, nomor telepon, dan data keuangan, sering kali menjadi target bagi pihak-pihak yang tidak bertanggung jawab. Pelanggaran data dapat mengakibatkan kerugian finansial, reputasi, dan bahkan ancaman terhadap keselamatan individu. Oleh karena itu, penting untuk memahami dan menerapkan langkah-langkah perlindungan yang efektif untuk menjaga data privasi di era digital ini.Tulisan ini mengulas urgensi perlindungan dan keamanan data pribadi, berbagai tantangan yang muncul, serta upaya yang dapat dilakukan untuk menjaga kerahasiaan informasi pribadi. Menggunakan pendekatan kualitatif, data diperoleh dari beragam sumber literatur dan studi kasus yang relevan. Temuan dari penelitian ini menunjukkan perlunya peningkatan kesadaran akan pentingnya menjaga data pribadi, baik di tingkat individu maupun institusi, guna mencegah terjadinya penyalahgunaan informasi. Selain itu, penelitian ini juga menyarankan sejumlah strategi yang dapat diterapkan guna memperkuat sistem keamanan data privasi.

Kata Kunci: data, keamanan, Pelanggaran, Perlindungan

1. PENDAHULUAN

Perkembangan teknologi digital telah membawa banyak perubahan positif dalam kehidupan manusia. Saat ini, hampir semua aktivitas dapat dilakukan secara online, mulai dari berkomunikasi, bekerja, belajar, berbelanja, hingga mengakses layanan kesehatan. Namun, di balik semua kemudahan ini, ada satu hal penting yang perlu kita waspadai, yaitu perlindungan dan keamanan data pribadi. Data pribadi adalah segala informasi yang dapat digunakan untuk mengidentifikasi seseorang, seperti nama, alamat, nomor telepon, alamat email, informasi keuangan, dan bahkan kebiasaan saat menggunakan internet.

Received: April 19, 2025; Revised: Mei 04, 2025; Accepted: Mei 19, 2025; Published: Mei 22, 2025

Di era digital ini, data pribadi menjadi sangat berharga. Bagi perusahaan, data ini bisa dimanfaatkan untuk mengenal konsumen lebih dekat. Namun, jika tidak dijaga dengan baik, data tersebut bisa menjadi celah yang membahayakan. Misalnya, insiden kebocoran data pengguna platform media sosial dan e-commerce yang mengakibatkan jutaan data pribadi terekspos ke publik, menjadi bukti nyata bahwa keamanan data belum sepenuhnya terjamin. contoh kebocoran data pribadi baru-baru ini telah menjadi masalah yang parah. Beberapa di antaranya terdiri dari:

1. Kasus Tokopedia (2020): Pada awal 2020, platform e-commerce besar di Indonesia, Tokopedia, dilaporkan mengalami pelanggaran keamanan yang mengakibatkan informasi pribadi dari jutaan pengguna bocor. Data yang dikompromikan meliputi nama, alamat, nomor telepon, alamat email, dan kata sandi terenkripsi.
2. Kasus Bukalapak (2021): Bukalapak, platform e-commerce lainnya di Indonesia, juga dilaporkan mengalami pelanggaran data pada tahun 2021. Lebih dari 13 juta akun pengguna dilaporkan terdampak, dengan data seperti nama pengguna, alamat email, nomor telepon, dan kata sandi bocor.
3. Kasus TokoTalk (2021): Pada tahun 2021, aplikasi pesan instan asal Indonesia, TokoTalk, juga dilaporkan mengalami kebocoran data. Lebih dari 91 juta akun pengguna terdampak, dan informasi yang bocor termasuk nama, nomor telepon, alamat email, dan salinan kartu identitas.

Kebocoran data pribadi bukan lagi persoalan sepele. Dampak dari insiden seperti ini bisa sangat merugikan, baik secara individu maupun kolektif. Mulai dari kerugian finansial, penyalahgunaan identitas, hingga pemanfaatan data untuk tindakan kriminal—semuanya menjadi ancaman nyata di era digital saat ini. Data pribadi yang semestinya bersifat rahasia dapat digunakan tanpa izin oleh pihak-pihak tidak bertanggung jawab untuk kepentingan tertentu yang merugikan pemilik data.

Oleh karena itu, peran aktif dari semua pihak sangat dibutuhkan. Pemerintah harus mengambil langkah tegas melalui kebijakan dan regulasi yang mengatur perlindungan data secara menyeluruh. Di sisi lain, perusahaan dan penyedia layanan digital harus memastikan sistem keamanan mereka mampu melindungi data konsumen dengan optimal. Tidak kalah penting, individu sebagai pengguna juga perlu meningkatkan literasi digital serta menerapkan kebiasaan aman saat menggunakan layanan berbasis internet. Upaya pencegahan bisa dimulai dari hal-hal sederhana, seperti tidak sembarangan memberikan informasi pribadi, menggunakan kata sandi yang kuat, hingga mengaktifkan fitur keamanan tambahan seperti

verifikasi dua langkah. Edukasi berkelanjutan mengenai pentingnya menjaga privasi juga perlu ditingkatkan, baik melalui media, pendidikan formal, maupun kampanye publik.

Selain itu, mengikuti berita dan perkembangan terbaru mengenai insiden kebocoran data maupun tren keamanan siber sangat penting agar kita selalu siap menghadapi risiko yang terus berkembang. Di tengah meningkatnya serangan siber dan eksploitasi data, sikap waspada menjadi kunci utama dalam menjaga privasi.Dengan meningkatnya ancaman terhadap keamanan informasi pribadi, kita tidak bisa lagi memandang remeh isu perlindungan data. Privasi digital adalah hak setiap individu yang harus dilindungi bersama. Perlindungan data bukan sekadar urusan teknis atau teknologi informasi, melainkan tanggung jawab kolektif antara pemerintah, sektor swasta, dan masyarakat luas. Hanya dengan kesadaran bersama dan tindakan nyata, ekosistem digital yang aman dan terpercaya dapat terwujud.

2. METODE PENELITIAN

Metode Penelitian yang digunakan dalam penulisan ini adalah literature review dimana penulis menggunakan jumal, artikel, tesis, buku, laporan penelitian, artikel akademis, serta sumber-sumber online yang terpercaya yang berhubungan dalam penulisannya. Proses pengumpulan data dimulai dengan identifikasi kata kunci yang terkait dengan perlindungan data pribadi, kemudian dilakukan pencarian literatur menggunakan database akademik seperti Google Scholar, PubMed, dan Acedemia. Setiap sumber yang ditemukan dievaluasi berdasarkan relevansi, keandalan, dan kualitas informasi yang disajikan. Analisis literatur dilakukan secaramendalam untuk mengidentifikasi tema-tema utama, tantangan, serta solusi yang diusulkan dalam konteks perlindungan data pribadi.

3. HASIL DAN PEMBAHASAN

Di era digital yang terus berkembang, data privasi telah menjadi salah satu aset paling berharga bagi individu dan organisasi. Salah satunya adalah Informasi pribadi, seperti nama, alamat, nomor telepon, dan data keuangan, sering kali menjadi sasaran bagi pihak-pihak yang tidak bertanggung jawab. Salah satu penyebab utama dari rentannya perlindungan data pribadi di Indonesia adalah rendahnya tingkat kesadaran masyarakat mengenai pentingnya menjaga privasi di dunia digital. Banyak individu masih menggunakan kata sandi yang lemah, membagikan informasi pribadi di media sosial tanpa pertimbangan, dan tidak memahami bahaya dari mengakses situs atau aplikasi yang tidak terpercaya. Di sisi lain, banyak perusahaan juga belum mengadopsi teknologi keamanan yang memadai seperti enkripsi data end-to-end, sistem autentikasi multi-faktor, serta sistem pemantauan aktivitas mencurigakan

secara real-time. Hal ini diperparah dengan kurangnya kebijakan internal dan audit keamanan siber yang rutin.

Menurut Fitriani dan Nurhadi (2021), lemahnya sistem perlindungan data tidak hanya disebabkan oleh aspek teknis, tetapi juga akibat rendahnya budaya perlindungan privasi baik di tingkat organisasi maupun individu. Dalam konteks ini, perlindungan data pribadi tidak hanya menjadi urusan teknis yang bergantung pada kecanggihan sistem, tetapi juga menyangkut tanggung jawab moral dan sosial dari seluruh elemen masyarakat. Pemerintah memiliki peran sentral dalam menetapkan regulasi yang adil dan menindak pelanggaran, sementara perusahaan wajib menjamin keamanan data pengguna melalui investasi dalam sistem keamanan dan sumber daya manusia yang andal. Sementara itu, individu sebagai pemilik data juga harus memahami hak dan kewajibannya dalam menjaga informasi pribadinya sendiri. Seperti dikatakan oleh Solove (2021), perlindungan privasi bukan hanya sekadar menyembunyikan informasi, melainkan upaya untuk mengontrol bagaimana data tersebut digunakan dan disebarluaskan.

Masukkan Disini Yang Mau Ditambahi Kata Pembukanya

1. Tantangan Perlindungan Data Pribadi

a. Kurangnya kesadaran pengguna

Banyak pengguna internet yang belum menyadari betapa pentingnya melindungi data pribadi mereka. Ketidaktahuan ini sering kali disebabkan oleh kurangnya edukasi yang memadai mengenai isu-isu privasi dan keamanan data. Sebagian besar pengguna tidak memahami bagaimana data pribadi mereka dapat disalahgunakan atau dieksploitasi oleh pihak yang tidak bertanggung jawab.

Kurangnya pemahaman tentang risiko kebocoran data pribadi juga diperburuk oleh kompleksitas teknologi yang ada. Banyak pengguna merasa kesulitan untuk mengikuti perkembangan teknologi keamanan dan praktik perlindungan data yang baik. Mereka sering kali mengabaikan langkah-langkah keamanan dasar, seperti menggunakan kata sandi yang kuat, memperbarui perangkat lunak secara teratur, atau mengaktifkan autentikasi dua faktor. Selain itu, pengguna cenderung tidak membaca kebijakan privasi atau syarat dan ketentuan yang ditetapkan oleh aplikasi dan layanan online, sehingga mereka tidak menyadari bagaimana data mereka dikumpulkan, disimpan, dan digunakan.

Ketiadaan kesadaran ini menciptakan celah yang dapat dimanfaatkan oleh penjahat siber. Tanpa pengetahuan yang cukup tentang cara melindungi data pribadi, pengguna menjadi target yang mudah bagi berbagai bentuk serangan siber, seperti *phishing, malware, dan ransomware*. Oleh karena itu, sangat penting untuk meningkatkan

kesadaran dan pemahaman pengguna melalui program edukasi dan kampanye publik yang efektif. Dengan pengetahuan yang lebih baik, pengguna dapat mengambil langkah proaktif untuk melindungi data pribadi mereka.

b. Kelemahan Regulasi

Regulasi yang berkaitan dengan perlindungan data pribadi masih berbeda-beda di berbagai negara dan belum sepenuhnya mampu menangani masalah yang bersifat global. Beberapa negara telah memiliki undang-undang yang ketat, seperti *General Data Protection Regulation (GDPR)* di Uni Eropa, sementara negara lain masih dalam proses pengembangan regulasi atau bahkan tidak memiliki kerangka hukum yang memadai untuk mengatasi isu ini. Perbedaan dalam tingkat kematangan regulasi ini menciptakan tantangan bagi perusahaan multinasional yang harus mematuhi berbagai peraturan yang berbeda di setiap negara tempat mereka beroperasi.

Ketidaksesuaian regulasi ini juga memengaruhi efektivitas perlindungan data di tingkat global. Sebagai contoh, perusahaan yang beroperasi di negara dengan regulasi yang longgar mungkin tidak menerapkan standar keamanan yang sama ketatnya seperti yang diwajibkan di negara dengan regulasi yang lebih ketat. Hal ini dapat menyebabkan kebocoran data atau penyalahgunaan informasi di negara-negara dengan regulasi yang kurang memadai, meskipun data tersebut berasal dari individu di negara yang memiliki regulasi yang ketat. Selain itu, perbedaan regulasi juga menyulitkan kerja sama internasional dalam penegakan hukum terkait pelanggaran data pribadi.

Lebih lanjut, regulasi yang ada sering kali tidak dapat mengikuti perkembangan teknologi yang sangat cepat. Inovasi teknologi seperti kecerdasan buatan, *big data, dan Internet of Things (IoT)* menghadirkan tantangan baru dalam perlindungan data pribadi yang mungkin belum sepenuhnya dipertimbangkan oleh regulasi saat ini. Ini menciptakan kebutuhan mendesak untuk terus memperbarui dan menyesuaikan regulasi agar tetap relevan dan efektif dalam melindungi data pribadi. Tanpa adanya regulasi yang fleksibel dan menyeluruh, upaya untuk melindungi data pribadi akan selalu tertinggal dari perkembangan ancaman dan teknologi baru.

c. Ancaman dari *Cybercrime*

Cybercrime, seperti *hacking*, *phishing*, dan *malware*, terus mengalami perkembangan pesat dan menjadi ancaman yang signifikan bagi keamanan informasi pribadi. Pelaku kejahatan siber kini semakin mahir dalam memanfaatkan celah keamanan sistem untuk mengakses dan mencuri data penting. Salah satu bentuk kejahatan siber yang paling merugikan, seiring dengan kemudahan akses informasi di era digital, adalah

pencurian data pribadi. Informasi yang dicuri bisa mencakup identitas pribadi, informasi rekening bank, hingga data kartu kredit (Hamid & Djollong, 2019; Doutel et al., 2023).

Para pelaku umumnya menggunakan teknik-teknik canggih untuk menipu pengguna dan menembus sistem keamanan, dengan tujuan utama memperoleh keuntungan finansial atau informasi sensitif. Sebagai contoh, *phishing* adalah metode penipuan yang dirancang untuk membuat seseorang secara tidak sadar memberikan informasi pribadi dengan menyamar sebagai pihak yang terpercaya. Sementara itu, *hacking* dan *malware* digunakan untuk merusak sistem, mencuri data, atau mengenkripsi informasi pengguna guna meminta tebusan (*ransomware*).

Tidak hanya mengandalkan cara konvensional, pelaku *cybercrime* juga telah mulai menerapkan teknologi mutakhir untuk melancarkan serangan. Penggunaan kecerdasan buatan (AI) dan pembelajaran mesin (*machine learning*) memungkinkan serangan menjadi lebih spesifik dan sulit untuk dikenali. Selain itu, teknologi *deepfake*, yang dapat menghasilkan video atau audio palsu dengan tingkat kemiripan tinggi, juga berpotensi digunakan dalam tindakan penipuan dan pencurian identitas. Serangan seperti *Distributed Denial of Service (DDoS)* yang semakin canggih dapat mengganggu layanan daring secara signifikan, bahkan menghentikan operasional bisnis, sehingga memperbesar risiko kebocoran informasi pribadi.

2. Solusi Untuk Perlindungan Data Pribadi

a. Peningkatan Edukasi dan Kesadaran

Salah satu langkah penting untuk melindungi data pribadi adalah meningkatkan edukasi dan kesadaran masyarakat tentang perlindungan data. Program edukasi dapat dilakukan melalui kampanye publik, seminar, dan pelatihan. Kampanye di media sosial, televisi, dan internet dapat menjangkau banyak orang dan menyebarkan informasi tentang pentingnya melindungi data pribadi, seperti penggunaan kata sandi yang kuat dan mengaktifkan autentikasi dua faktor.

Seminar di sekolah, universitas, dan komunitas lokal juga dapat meningkatkan kesadaran sejak dini. Pelatihan khusus untuk karyawan yang menangani data sensitif dapat membantu mereka mengenali dan mencegah ancaman siber. Dengan pengetahuan yang lebih baik, individu dapat lebih proaktif dalam melindungi data mereka dan mengurangi risiko kebocoran.

Selain itu, penting untuk mengintegrasikan edukasi tentang keamanan data ke dalam kurikulum pendidikan formal. Kolaborasi antara organisasi non-pemerintah dan sektor swasta dalam menyelenggarakan *workshop* dan program sertifikasi juga dapat

meningkatkan pemahaman tentang perlindungan data. Partisipasi aktif dari berbagai pihak dapat menciptakan lingkungan yang lebih aman terhadap ancaman siber. *Cybercrime*, yang merupakan kejahatan yang dilakukan dengan teknologi digital, menjadi fokus penelitian ini untuk menjelaskan tindak pidana dan sanksinya dalam Undang-Undang Informasi dan Transaksi Elektronik (Dm & Hasibuan, 2022).

b. Penerapan Teknologi Keamanan

Penerapan teknologi keamanan canggih seperti enkripsi data, autentikasi multi-faktor (MFA), dan sistem deteksi intrusi (IDS) sangat penting untuk melindungi data pribadi dari ancaman *cybercrime*. Enkripsi data mengubah informasi sensitif menjadi format yang tidak dapat dibaca tanpa kunci yang tepat, sehingga meskipun data dicuri, penjahat siber tidak dapat memanfaatkannya. Enkripsi end-to-end dalam komunikasi online memastikan hanya pengirim dan penerima yang sah yang dapat mengakses data. Sementara itu, MFA menambahkan lapisan keamanan dengan meminta pengguna memberikan dua atau lebih bukti identitas sebelum mengakses akun atau data sensitif, menggabungkan kata sandi, perangkat yang dimiliki, dan biometrik.

Selain itu, IDS dan sistem pencegahan intrusi (IPS) berperan penting dalam mendeteksi dan menghentikan serangan siber. Pemantauan keamanan yang berkelanjutan dan audit reguler juga sangat penting untuk mengidentifikasi kerentanan baru dan memastikan kebijakan keamanan diikuti. Terakhir, integrasi teknologi keamanan dengan pendidikan dan kesadaran pengguna sangat krusial, karena meskipun teknologi memberikan perlindungan, faktor manusia sering menjadi titik lemah. Oleh karena itu, melatih pengguna tentang praktik keamanan yang baik akan menciptakan lingkungan yang lebih aman terhadap ancaman.

4. KESIMPULAN

Perlindungan dan keamanan data pribadi di era digital merupakan isu yang sangat penting dan mendesak. Dengan pesatnya perkembangan teknologi informasi dan komunikasi, data pribadi menjadi salah satu aset paling berharga yang sering kali menjadi target bagi pihak-pihak yang tidak bertanggung jawab. Insiden kebocoran data yang terjadi di berbagai platform menunjukkan bahwa keamanan data masih rentan dan dapat mengakibatkan kerugian finansial, reputasi, serta ancaman terhadap keselamatan individu. Oleh karena itu, diperlukan upaya kolaboratif dari pemerintah, perusahaan, dan individu untuk meningkatkan kesadaran dan literasi digital mengenai pentingnya perlindungan data.

Tantangan yang dihadapi dalam perlindungan data pribadi meliputi rendahnya kesadaran pengguna, kelemahan regulasi, dan ancaman dari cybercrime yang semakin canggih. Untuk mengatasi masalah ini, langkah-langkah seperti peningkatan edukasi dan kesadaran masyarakat, penerapan teknologi keamanan yang canggih, serta pengawasan dan audit reguler sangat diperlukan. Edukasi yang berkelanjutan dan integrasi keamanan data dalam kurikulum pendidikan formal juga akan membantu menciptakan lingkungan yang lebih aman.

Dengan menggabungkan teknologi yang efektif dan kesadaran pengguna yang tinggi, kita dapat membangun ekosistem digital yang lebih aman dan terpercaya. Perlindungan data bukan hanya tanggung jawab teknis, tetapi juga merupakan tanggung jawab kolektif yang melibatkan semua elemen masyarakat. Hanya dengan kesadaran bersama dan tindakan nyata, kita dapat melindungi privasi digital sebagai hak setiap individu di era yang semakin terhubung ini.

DAFTAR PUSTAKA

CNN. “10 Kasus Kebocoran Data 2022." https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah, 2022.

Disemadi, Hari Sutra, et al. "Perlindungan Data Pribadi di Era Digital: Mengapa Kita Perlu Peduli.?" Sang Sewagati Journal 1.2 (2023): 66-90.

Fitriani, E., & Nurhadi, W. (2021). "Perlindungan Data Pribadi di Era Digital: Studi Kasus Indonesia." *Jurnal Hukum dan Teknologi*, 5(2), 123–134.

Hanifan N, 2020, "Perlindungan Data Pribadi Sebagai Bagian Hak Asasi Manusia Atas Perlindungan Diri pribadi Suatu Tinjauan Komparatif Dengan Peraturan Perundang undangan di Negara Lain", Selisik, Vol.6 No.1. Hal 2685-6816

Indriani, Masitoh. "Perlindungan Privasi Dan Data Pribadi Konsumen Daring Pada Online Marketplace System." Justitia Jurnal Hukum 1.2 (2017).

Mahuli, Jenda Ingan. "Perlindungan Hukum Terhadap Data Pribadi dalam Era Digital." All Fields of Science Journal Liaison Academia and Sosiety 3.4 (2023): 188-194.

Putri, Adelia, et al. "Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering)." Jurnal Pengabdian Nasional (JPN) Indonesia 6.1 (2025): 38-52.

Solove, D. J. (2021). *Understanding Privacy*. Harvard University Press.

Suari, Kadek Rima Anggen, and I. Made Sarjana. "Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia." Jurnal Analisis Hukum 6.1 (2023): 132-142.

Suharyanti, Ni Putu Noni, and Ni Komang Sutrisni. "Urgensi perlindungan data pribadi dalam menjamin hak privasi masyarakat." Prosiding Seminar Nasional Fakultas Hukum Universitas Mahasaraswati Denpasar 2020. Vol. 1. No. 1. 2021.

Suwito, A., & Ramadhan, F. (2022). "Tantangan Keamanan Siber dan Perlindungan Data Pribadi di Indonesia." *Jurnal Keamanan Informasi*, 8(1), 45-60.

Yamin, Ahmad Fachri, et al. "Perlindungan Data Pribadi Dalam Era Digital: Tantangan Dan Solusi." Meraja journal 7.2 (2024): 138-155.

Yuniarti, Siti. "Perlindungan hukum data pribadi di Indonesia." Business Economic, Communication, and Social Sciences Journal (BECOSS) 1.1 (2019): 147-154.

Zahwani, Syfa Tasya, and Muhammad Irwan Padli Nasution. "Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi Di Era Digital." Journal of Sharia Economics Scholar (JoSES) 2.2 (2024).