Konstruksi Sosial:
Jurnal Penelitian Ilmu Sosial
Vol. 5 No. 1 Januari Tahun 2025 | Hal. 7 – 16

Survey Mengenai Kebocoran Data di Era Digital

Fathania Aliefa Meshar[a, 1*], Syifa Khairul Bariiyah[a, 2], Dadi Mulyadi [a, 3], Ilfah Nurhasbiyah[a,4], Wanda Azhar Nurmalasari [a,5], Sabrina An Nissa Fitria [a,6]

[a] Universitas Pendidikan Indonesia, Indonesia
[1] fathaniaaliefam@upi.edu*
*korespondensi penulis

Informasi artikel
Received: 5 Januari 2025;
Revised: 16 Januari 2025;
Accepted: 28 Januari 2025.

Kata-kata kunci:
Kebocoran Data;
Privasi;
Era Digital.

ABSTRAK

Pada era digital saat ini salah satu ancaman yang paling signifikan adalah kebocoran data, hal ini tentunya menimbulkan kekhawatiran yang mendalam bagi masyarakat umum. Penelitian ini berfokus untuk memahami mengenai apa itu kebocoran data yang saat ini sering terjadi, khususnya di media digital serta untuk mengetahui pandangan masyarakat mengenai kebocoran data. Studi ini menerapkan pendekatan kuantitatif dan deskriptif. Untuk mengumpulkan data, kuesioner disebarkan kepada responden melalui Google Forms. Hasil penelitian menunjukkan bahwa mayoritas responden mengalami kebocoran data pada nomor handphone yang seringkali mendapatkan panggilan dari orang asing yang mencurigakan. Berdasarkan hasil survei, di Indonesia saat ini mengenai kebocoran data masih belum ditanggapi dengan serius oleh pemerintah karena masih banyak orang yang mengalami kebocoran data diakibatkan oleh sistem yang kurang memadai. Penelitian ini diharapkan dapat menjadi sumber wawasan baru serta meningkatkan kepedulian dan kesadaran pada keamanan privasi dan data.

Keywords:
Data Leakage;
Privacy;
Digital Era.

ABSTRACT

Analyzing a survey on data leakage in the digital era. *In today's digital era, one of the most significant threats is data leakage, which certainly raises deep concerns for the general public. This research focuses on understanding what data leakage is, which is currently happening frequently, especially in digital media and to find out the public's views on data leakage.The method applied in This study uses a descriptive methodology and a quantitative approach. Respondents are given a questionnaire via Google Forms as part of the data gathering method. The findings indicated that the vast majority of participants had data leakage on cell phone numbers that often get calls from suspicious strangers. Based on the survey result, in Indonesia at this time data leaks are still not taken seriously by the government due to the fact that many people still experience data leaks due to an inadequate system. This study is anticipated to serve as a source of new insights and increase awareness of privacy and data security.*

How to Cite : Meshar, F. A., Bariiyah, S. K., Mulyadi, D., Nurhasbiyah, I., Nurmalasari, W. A., & Fitria, S. A. N. (2025). Survey Mengenai Kebocoran Data di Era Digital. *Konstruksi Sosial : Jurnal Penelitian Ilmu Sosial*, *5*(1), 7–16. https://doi.org/10.56393/konstruksisosial.v5i1.2808

Pendahuluan

Era digital telah membawa kemajuan teknologi informasi yang tak terduga, namun demikian, perkembangan ini tentu membawa resiko yang besar bagi keamanan dan privasi data. Salah satu ancaman yang paling signifikan adalah kebocoran data, yang merajuk pada akses yang tidak sah atau tidak diizinkan terhadap data rahasia. Belakangan ini, dunia maya digemparkan oleh insiden kebocoran data pribadi berskala besar yang melibatkan 2,9 miliar data individu dari tiga negara berbeda. Menurut penelitian Hootsuite, 64% penduduk Indonesia, atau lebih dari separuh populasi, terhubung ke internet. (Hootsuite, 2020) (Setiawan & Najicha, 2022). Karena data warga Indonesia memiliki potensi kebocoran data yang besar, pihak ilegal seringkali dapat mengaksesnya.

Kebocoran ini menimbulkan kekhawatiran yang mendalam di antara masyarakat dan pemerintah di ketiga negara tersebut, mengingat potensi risiko pemanfaatan data oleh pihak yang tidak berwenang. Tidak ada aturan yang jelas yang bertanggung jawab atas perlindungan data pribadi di Indonesia, namun tentu saja selalu ada masalah kebocoran data, sehingga menyusun kebijakan perlindungan data pribadi akan menjadi langkah yang tepat (Firmansyah Putri & Fahrozi, 2021). Setiap orang berhak atas perlindungan pribadi, keluarga, kehormatan, martabat, dan harta benda yang dikuasainya, serta rasa aman dan perlindungan dari orang lain, menurut Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (Niffari, 2020). Indonesia bisa dikatakan tertinggal jauh dalam hal perlindungan data pribadi warganya, ini sangat menonjol dibandingkan dengan negara lain seperti Thailand, yang memiliki mengadopsi Konvensi Perlindungan Data Pribadi (PDPA) dan Malaysia, yang menjadi negara pertama yang menetapkan undang-undang untuk menjaga keamanan data pribadi (Delpiero, Reynaldi, Ningdiah, & Muthmainnah, 2021).

Kebocoran data merupakan masalah yang terjadi di seluruh dunia, berkaitan dengan informasi rahasia seperti nama, alamat, nomor, dan informasi keuangan penting lainnya yang bisa diakses secara ilegal di internet. Hal ini dapat terjadi akibat serangan siber, kesalahan yang dilakukan oleh pihak internal, atau bahkan karena kehilangan perangkat fisik (UMA, 2023). Keamanan informasi dan privasi adalah isu yang kian krusial di zaman digital saat ini.

Pada masa digital sekarang ini, perlindungan informasi dan keamanan data menjadi hal yang semakin signifikan. Pelanggaran Pelanggaran data terkait erat dengan data. Ketika data sengaja dikirim ke Internet atau ke situs web yang tidak aman, peretas dapat mengakses informasi pribadi Anda dengan cepat. dan melakukan pelanggaran data. Banyak faktor yang dapat menyebabkan pelanggaran data. Berdasarkan beberapa literatur, penulis mengkategorikan faktor-faktor tersebut menjadi tiga penyebab utama pelanggaran data: kesalahan manusia, serangan malware (perangkat lunak berbahaya), dan manipulasi psikologis melalui rekayasa sosial. Semakin majunya teknologi semakin memudahkan pekerjaan masyarakat. Namun di saat yang sama, ancaman terhadap keamanan pengguna teknologi juga semakin meningkat. Berdasarkan fenomena diatas, penulis akan meneliti bagaimana pandangan masyarakat terhadap kebocoran data. Artikel ini bertujuan untuk mengetahui pandangan masyarakat terhadap kebocoran data serta mengetahui jenis apa saja yang dialami masyarakat dalam kebocoran data.

Beberapa penelitian terdahulu telah membahas faktor-faktor penyebab kebocoran data serta dampaknya terhadap individu maupun organisasi. (Zwilling et al., 2022) menyoroti pentingnya kesadaran masyarakat terhadap keamanan siber dalam mencegah serangan siber. (Adristi & Ramadhani, 2024) menganalisis bagaimana kebocoran data berdampak pada PDNS 2—Pusat Data Nasional Sementara Surabaya, menggunakan metode matriks budaya keamanan siber dan dimensi budaya nasional Hofstede. Penelitian ini bertujuan untuk meningkatkan pemahaman tentang komponen yang mempengaruhi terjadinya kebocoran data dalam sistem penyimpanan informasi berskala nasional. Sementara itu, (Milafebina, Lesmana, & Syailendra, 2023) menekankan bahwa kebocoran data pelanggan dalam e-commerce merupakan isu krusial yang dapat mempengaruhi kepercayaan konsumen

terhadap layanan digital. Penelitian-penelitian ini menunjukkan bahwa kebocoran data merupakan permasalahan kompleks yang membutuhkan pendekatan multidimensi, termasuk regulasi ketat, edukasi masyarakat, dan adopsi teknologi keamanan informasi yang lebih baik

Kebaruan ilmiah dalam artikel ini terletak pada analisis persepsi masyarakat Indonesia terhadap kebocoran data, yang belum banyak dibahas dalam penelitian sebelumnya. Berbeda dari studi sebelumnya yang lebih berfokus pada regulasi atau aspek teknis perlindungan data, kajian ini menyoroti bagaimana individu memahami, menghadapi, dan merespons ancaman kebocoran informasi pribadi di era digital. Selain itu, studi ini juga akan mengidentifikasi jenis kebocoran data yang paling sering dialami oleh masyarakat serta faktor-faktor yang memengaruhinya.

Dengan demikian, tujuan penelitian ini adalah untuk menganalisis persepsi masyarakat terhadap kebocoran data, mengeksplorasi faktor-faktor yang berkontribusi terhadap insiden tersebut, serta merumuskan tindakan yang dapat meningkatkan kesadaran dan keamanan informasi pribadi. Dengan memahami bagaimana masyarakat merespons ancaman ini, diharapkan penelitian ini dapat memberikan kontribusi bagi pengembangan kebijakan perlindungan data yang lebih efektif serta strategi mitigasi risiko yang lebih baik di Indonesia.

Metode

Dalam upaya mendapatkan data dan informasi untuk penelitian ini menerapkan metode kuantitatif dengan menggunakan kuisioner. Angket, juga sering disebut sebagai Kuesioner adalah metode untuk mengumpulkan informasi atau data dengan menggunakan formulir tanya jawab yang dimaksudkan untuk seseorang atau sekelompok orang dalam suatu organisasi untuk mendapatkan tanggapan atau informasi yang dapat dianalisis oleh pihak yang bertanggung jawab untuk mencapai tujuan tertentu (Cahyo, Martini, & Riana, 2019). Menurut Sugiyono (2023), data kuantitatif mengacu pada data yang telah dikuantifikasi atau diberi skor. Sedangkan menurut Kamus Besar Bahasa Indonesia, besaran didasarkan pada jumlah atau porsi energi yang tidak dapat dibagi lagi. Penggunaan metode survei bertujuan untuk memperoleh data dan informasi terkait pembobolan data di Indonesia dari warga negara Indonesia.

Hasil dan pembahasan

Berdasarkan hasil survei kuesioner/angket didapat data seberapa sering masyarakat mengalami kebocoran data pribadi di era digital. Dibawah ini disajikan tabel, diagram, dan deskripsi mengenai pendapat responden dalam menanggapi kebocoran data.

Tabel 1. Pengalaman Kebocoran Data Pribadi

Mengalami Kebocoran Data Pribadi	
Pernah	Tidak Pernah
7	33
17,5%	82,5%

Menurut Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, setiap individu berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya. Selain itu, setiap individu berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk melakukan atau tidak melakukan apa yang dianggap sebagai hak asasi manusia. (Hansen Samin, 2023). Undang-Undang No. 24 Tahun 2013, yang mengubah Undang-Undang No. 23 Tahun 2006 tentang pengelolaan data penduduk (juga dikenal sebagai UU Administrasi), pengertian data pribadi merujuk kepada informasi pribadi individu yang disimpan, dirawat, dan akurat, serta memiliki sifat rahasia. Konfirmasi harus bersifat wajib dilindungi, nyata dan unik serta dapat diidentifikasi langsung atau tidak langsung sesuai dengan ketentuan hukum. Berdasarkan tabel di atas, terdapat hasil dari responden terhadap kebocoran data pribadi. Sebagian besar

responden tidak pernah mengalami kebocoran data pribadi yaitu 33 dari 40 orang (Gunadi, Subiran, Lee, Gunawan, & Baretta, 2023).

Gambar 1. Jenis data pribadi yang mengalami kebocoran

Di era digital ini, pengguna media sosial Indonesia kerap mempublikasikan secara terbuka alamat rumah, tanggal lahir, nomor telepon, dan hubungan dengan orang-orang terdekatnya di platform media sosial. Hal ini menunjukkan bahwa masih terdapat permasalahan besar mengenai kesadaran akan privasi dan perlindungan data pribadi di Indonesia. Berdasarkan diagram diatas, diketahui jenis data pribadi responden yang mengalami kebocoran data. Sebagian besarnya yaitu 82,5% responden tidak pernah mengalami kebocoran data pribadi dan 17,5% responden lainnya pernah mengalami kebocoran data seperti, identitas diri; nomor *handphone*; data akun; Instagram; Email, *password*; dan KIP (Gunadi et al., 2023).

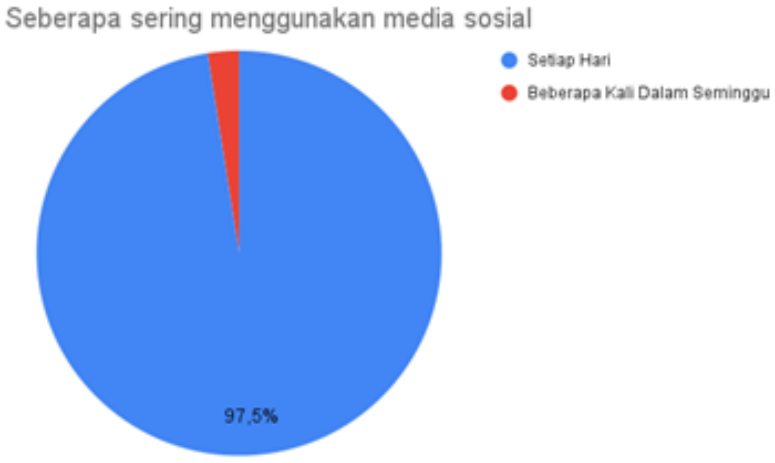
Gambar 2. Jenis Sosial Media yang pernah terkena hack

Era perkembangan media sosial saat ini berkaitan dengan berbagai permasalahan terkait keamanan informasi dan privasi. Media sosial dianggap sebagai salah satu sumber dari kebocoran data pribadi. Dimana fungsi awal media sosial untuk mempermudah penggunanya dalam berinteraksi secara sosial menggunakan teknologi internet menjadi metode distribusi informasi. Sebelumnya, itu berfungsi untuk menyebarkan informasi yang bisa diakses oleh banyak pengguna situs jejaring sosial seperti WhatsApp, Instagram, Facebook, dan lainnya. Namun, berdasarkan diagram diatas, diketahui jenis media sosial responden yang pernah terkena *hack.* Sebagian besar responden tidak pernah terkena *hack*

yaitu sebesar 72,5%. Kemudian, responden lainnya pernah terkena hack pada media sosial mereka, yaitu 20% di Instagram; 5% di Facebook; dan 2,5% di Twitter (Vidiana, Ruhtiani, & Afrilies, 2023).

Gambar 3. Cara Mengatasi data pribadi yang bocor

Berbagai bagian kehidupan dipengaruhi oleh kemajuan teknologi. Salah satu contoh dampak kemajuan teknologi adalah proses pengelolaan data yang sebagian besar digital. Beberapa peraturan hukum mengatur proteksi data pribadi di lembaga pemerintah dan swasta, tetapi aturan ini tidak cukup untuk melindungi data pribadi. (Tambunan, 2014). Peraturan mengenai Peraturan Nomor 20 Tahun 2016 dari Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi Dalam Sistem Elektronik menetapkan bagaimana data pribadi dikumpulkan, diproses, dan digunakan dalam sistem elektronik, serta bagaimana melaporkan pelanggaran data. Berdasarkan diagram diatas, diketahui bagaimana cara responden mengatasi data pribadi yang bocor. Yaitu dengan cara 30% responden akan memulihkan kembali data yang mereka simpan di email; 15% responden akan melaporkan ke pihak yang berwajib; 12,5% responden tidak akan menyebarkan data-data pribadi mereka; 7,5% responden akan meminta bantuan kepada orang terdekat; 7,5% responden tidak memahami hal yang harus mereka lakukan; dan responden lainnya mempunyai cara tersendiri dalam mengatasi kebocoran data pribadi mereka (Milafebina et al., 2023).



Gambar 4. Seberapa Sering penggunaan media sosial

Semakin banyak pengguna internet yang menggunakan media sosial menunjukkan bahwa masyarakat semakin melek media, atau literasi digital (Harahap & Adeni, 2020). Dari 262 juta

penduduk Indonesia, 106 juta menggunakan media sosial. Kegiatan berinteraksi di media sosial di Indonesia mayoritas dilakukan oleh generasi digital, yaitu 62% memakai smartphone, 16% memakai komputer, dan 6% memakai Tab. Grafik di atas menunjukkan seberapa sering responden menggunakan media sosial. Sebagian besar responden memakai media sosial setiap hari, 97,5% dan 2,5% hanya menggunakan media sosial beberapa kali dalam seminggu (Supratman, 2018). karena banyaknya pihak yang menggunakan media elektronik untuk berkomunikasi dan bertransaksi terjadinya pencurian data pribadi (Rumlus & Hartadi, 2020).

Gambar 5. Keseriusan pelaporan dayta

Upaya membangun hubungan yang jelas antara bisnis dan pelanggan telekomunikasi membutuhkan perlindungan legal terhadap informasi pribadi. Hal ini juga dapat mendorong pengumpul data untuk melindungi data pribadi lebih baik. (Satrio & Widiatno, 2020). Berdasarkan diagram diatas, kami dapat melihat tanggapan responden tentang apakah pelaporan kebocoran data di Indonesia telah direspon dengan serius atau tidak. Setengah dari mereka menyatakan bahwa belum ada respon yang signifikan terhadap kebocoran data di Indonesia, 22,5 persen menyatakan bahwa respon yang signifikan telah diterima, 15% menyatakan bahwa respons yang signifikan telah diterima, dan 12,5 persen menyatakan pendapat yang berbeda (Gunadi et al., 2023).

Gambar 6. Kebocoran data harus mendapatkan tanggapan serius

Salah satu komponen yang sangat penting untuk dijaga adalah data pribadi. Mengamankan informasi pribadi Anda bisa mencegah resiko pelecehan seksual, melindungi individu yang tidak bersalah dari potensi pencemaran nama baik, dan memberikan Anda kekuasaan untuk mengatur informasi pribadi Anda. Berdasarkan diagram diatas, diketahui pendapat para responden tentang mengapa kebocoran data perlu mendapatkan tanggapan yang serius. 42,5% responden menyatakan bahwa kebocoran data perlu mendapatkan tanggapan yang serius karena itu mencakup privasi data; 22,5% responden menyatakan bahwa kebocoran data perlu mendapatkan tanggapan yang serius karena ini sangat penting menyangkut hal pribadi; 17,5% responden menyatakan bahwa kebocoran data perlu mendapatkan tanggapan yang serius karena berbahaya dan bisa disalahgunakan; dan 17,5% responden lainnya menyatakan pendapat lain (Gunadi et al., 2023).

Gambar 7. Keamanan data media sosial

Di tengah-tengah revolusi industri 4.0 dan pandemi COVID-19, semakin banyak perusahaan berkonsentrasi pada perdagangan elektronik dan penggunaan teknologi yang mengumpulkan data pribadi. E-commerce adalah salah satu contohnya (Glenn Wijaya, 2020). Di media sosial, keamanan sistem informasi sangat penting, tetapi pemilik dan pengelola sistem seringkali tidak memperhatikan masalah ini. Berdasarkan diagram diatas, diketahui platform online apa yang sering responden gunakan dan apakah keamanan datanya terjamin. 7,7% responden sering menggunakan Instagram dan keamanan datanya terjamin; 5,1% responden sering menggunakan Shopee dan keamanannya terjamin; dan responden lain dengan pendapat mereka masing-masing (Yel & Nasution, 2022).

Gambar 8. Metode pengelolaan password

Salah satu penyebab pembobolan data di Internet adalah lemahnya kata sandi pengguna. Hal ini dikarenakan manusia mempunyai kemampuan yang terbatas dalam mengingat sesuatu yang unik dan panjang, seperti password. Pastikan Anda menggunakan kata sandi dan PIN yang tidak mudah ditebak, dan jangan gunakan tanggal lahir untuk PIN (Maya Safitri, Sefri Larasati, & Rizki Hari, 2020). Berdasarkan diagram diatas, diketahui seberapa sering responden memperbaharui password dan tips atau metode responden dalam mengelola password yang aman. 33,3% responden jarang memperbaharui password mereka; 25,6% responden juga jarang memperbaharui password, tetapi mereka menggunakan password yang susah; dan responden lain yang mempunyai pendapat masing-masing.

Tabel 2. Hasil Jawaban responden

Pertanyaan	Hasil persentase jawaban				
	Sering	Jarang	Tidak pernah	Ya	Tidak
Seberapa sering anda menerima email, pesan, atau telepon yang mencurigakan terkait dengan pencurian data?	12,5%	12,5%	75,0%		
Seberapa sering anda mendengar berita tentang kebocoran data dalam satu tahun terakhir?	60,0%	12,5%	27,5%		
Apakah anda menggunakan fitur keamanan tambahan? (Misalnya autentikasi dua faktor) untuk melindungi akun media sosial anda?				72,5%	27,5%

Studi tahun 2019 dilakukan oleh We Are Social, perusahaan media, dan Hootsuite tentang tren pengguna internet Indonesia. Hasilnya menunjukkan peningkatan 20 persen dalam jumlah pengguna internet dibandingkan dengan data tahun 2018. Ternyata, laporan media menyatakan bahwa 150 juta orang di Indonesia menggunakan media sosial. Berita tentang pencurian data pribadi untuk 87 juta pengguna Facebook pada tahun yang sama oleh Cambridge Analytica 2018 menjadi perbincangan hangat di dunia maya. Pemahaman yang buruk tentang keamanan digital kemudian menyebabkan berbagai masalah keamanan. Pengguna layanan digital terus melakukan kesalahan keamanan seperti menggunakan kata sandi yang tidak kuat dan menyebarkan informasi terlalu banyak (Syahputri, Harahap, Siregar, & Tommy, 2023).

Fitur autentikasi dua faktor adalah cara verifikasi identitas pengguna melalui dua tahap. Sebagai contoh, ketika pengguna akan masuk ke akun Facebook mereka, setelah memasukkan kata sandi seperti biasa, mereka akan diminta untuk memasukkan kode unik yang telah dikirim melalui pesan teks ke nomor yang terkait. Dari tabel diatas dapat kita lihat bahwa 60% responden mengatakan bahwa mereka sering mendengar soal kebocoran data dalam setahun terakhir ini dan 12,5% dari mereka sering mendapat email atau pesan yang mencurigakan dari handphone mereka salah satunya dari aplikasi atau media sosial yang mereka pakai seperti instagram, facebook, dan sebagainya. Namun ternyata kebanyakan orang sadar akan pentingnya keamanan siber di handphone mereka 72,5% responden mengatakan mereka menggunakan fitur keamanan tambahan untuk melindungi akun media sosial mereka.

Simpulan

Berdasarkan pembahasan diatas dapat disimpulkan bahwa kebocoran data di Indonesia marak terjadi dan belum ditanggapi dengan serius oleh pemerintah karena masih banyak orang yang mengalami kebocoran data diakibatkan oleh system yang kurang memadai. Berdasarkan hasil temuan

menunjukkan bahwa sebagian besar responden mengalami kebocoran data berupa nomor telepon yang sering kali mendapatkan panggilan dari orang tak dikenal, meskipun sebagian besar orang sudah mengetahui cara menanganinya, tidak bisa dibantah bahwa masih terdapat seseorang yang belum memahami pelanggaran data atau tidak berpendidikan mengenai hal tersebut.

Referensi

Adristi, F. I., & Ramadhani, E. (2024). Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya. *Selekta Manajemen: Jurnal Mahasiswa Bisnis & Manajemen*, *2*(6), 196–212. Retrieved from https://journal.uii.ac.id/selma/article/view/35529

Cahyo, K. N., Martini, & Riana, E. (2019). Perancangan sistem informasi pengelolaan kuesioner pelatihan pada PT Brainmatics Cipta Informatika. *Journal of Information System Research (JOSH)*, *1*(1), 45–53. Retrieved from http://ejurnal.seminar-id.com/index.php/josh/article/view/44

Delpiero, M., Reynaldi, F. A., Ningdiah, I. U., & Muthmainnah, N. (2021). Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data. *Padjadjaran Law Review*, *9*(1), 1–22. Retrieved from http://jurnal.fh.unpad.ac.id/index.php/plr/article/view/509

Firmansyah Putri, D. D., & Fahrozi, M. H. (2021). Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com). *Borneo Law Review*, *5*(1), 46–68. https://doi.org/10.35334/bolrev.v5i1.2014

Glenn Wijaya. (2020). Dalam konflik tentang akses data rekam jejak para calon anggota legislatif ke publik. *Law Review*, *XIX*(3), 326–361.

Gunadi, C. G., Subiran, D., Lee, E. P., Gunawan, L. A., & Baretta, N. (2023). Perlindungan Hukum Atas Kebocoran Data Pribadi. *Proceeding of Conference on Law and Social Studies*, *4*(1), 1–14.

Hansen Samin, H. (2023). Perlindungan Hukum Terhadap Kebocoran Data Pribadi Oleh Pengendali Data Melalui Pendekatan Hukum Progresif. *Jurnal Sains Student Research*, *1*(2), 1–15. Retrieved from https://doi.org/10.61722/jssr.v1i3.386

Harahap, M. A., & Adeni, S. (2020). Tren Penggunaan Media Sosial Selama Pandemi Di Indonesia. *Jurnal Professional FIS UNIVED*, *7*(2), 13–23.

Maya Safitri, E., Sefri Larasati, A., & Rizki Hari, S. (2020). Analisis Keamanan Sistem Informasi E-Banking Di Era Industri 4.0: Studi Literatur. *Jurnal Ilmiah Teknologi Informasi Dan Robotika*, *2*(1), 12–16. https://doi.org/10.33005/jifti.v2i1.25

Milafebina, R., Lesmana, I. P., & Syailendra, M. R. (2023). Perlindungan Data Pribadi terhadap Kebocoran Data Pelanggan E-commerence di Indonesia. *Jurnal Tana Man*, *4*(1), 158–169. Retrieved from https://ojs.staialfurqan.ac.id/jtm/

Niffari, H. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain. *Jurnal Hukum Dan Bisnis (Selisik)*, *6*(1), 1–14. https://doi.org/10.35814/selisik.v6i1.1699

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik. *Jurnal HAM*, *11*(2), 285. https://doi.org/10.30641/ham.2020.11.285-299

Setiawan, H. B., & Najicha, F. U. (2022). Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data. *Jurnal Kewarganegaraan*, *6*(1), 976–982.

Supratman, L. P. (2018). Penggunaan Media Sosial oleh *Digital Native*. *Jurnal ILMU KOMUNIKASI*, *15*(1), 47–60. https://doi.org/10.24002/jik.v15i1.1243

Syahputri, N. I., Harahap, H., Siregar, R., & Tommy, T. (2023). Penyuluhan Pentingnya Two Factor Authentication dan Aplikasinya Di Era Keamanan Digital. *Jurnal Pengabdian Masyarakat Bangsa*, *1*(6), 768–773. https://doi.org/10.59837/jpmba.v1i6.256

Tambunan, L. (2014). Jurnal Hukum, *37*(2), 24.

Vidiana, V. O., Ruhtiani, M., & Afrilies, M. H. (2023). Kesadaran Hukum Terhadap Perlindungan Data Pribadi Media Sosial (Studi Mahasiswa Hukum Banyumas). *Lontar Merah*, *6*(1), 609–618. Retrieved from https://databoks.katadata.co.id/datapublish/2022/06/

Yel, M. B., & Nasution, M. K. M. (2022). Keamanan Informasi Data Pribadi Pada Media Sosial. *Jurnal Informatika Kaputama (JIK)*, *6*(1), 92–101. https://doi.org/10.59697/jik.v6i1.144

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems, 62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269