PORTOFOLIO
Jurnal Manajemen dan Bisnis
Vol 3. No. 3 Juli 2024

Menganalisis Penanganan Kebocoran Data Pengguna Facebook Dalam Konteks Manajemen Sekuriti

Muzakki Sudirman[1], Milda Handayani[2], Achmad Fauzi[3], Faysa Firli Devianti[4], Nabila Alifiyah Gunawan[5], Ayu Diah Puspita[6], Muhammad Nafis Makruf [7], Arif Musyaffa[8]

[1)s/d8)] **Fakultas Ekonomi dan Bisnis Universitas Bhayangkara Jakarta Raya**

email: muzakky27@gmail.com[1], milda.handayani@ubharajaya.ac.id[2], achmad.fauzi@dsn.ubharajaya.ac.id[3], deviantifaysa@gmail.com[4], nabilagunawan163@gmail.com[5], pitaa334@gmail.com[6], muhammadnafis50100@gmail.com[7], arifmusyaffa2004@gmail.com[8]

Article History
Received: 16/6/2024
Revised: 27/6/2024
Accepted: 11/07/2024

***Keywords:* Facebook, cyber security, security management**

Abstract: *The misuse of information technology for cyber crimes such as online gambling, pornography, carding, phishing, and hacking increases the risk of leaking users' personal data, as seen in the case of Facebook, due to the lack of privacy protection by technology companies. Risks and security threats from social media and sharing personal information online are also on the rise, while the lack of codified regulations for personal data protection in Indonesia poses a problem. The research aims to understand how Facebook addresses user data leaks and the obstacles faced in cyber security in Indonesia. The analysis employs qualitative techniques and literature studies, gathering data and information from online articles, journals, and books. The research findings conclude that Facebook has secured data to protect user privacy. However, with the rapid advancement of technology, increasingly complex cyber crimes pose a growing threat to data security. Awareness of cyber security among the Indonesian public remains limited.*

PENDAHULUAN

Evolusi teknologi informasi sudah mengindikasikan efek menguntungkan pada kemajuan manusia, terutama dalam bidang komputer dan internet. Meskipun memberikan manfaat dan kenyamanan, kedua teknologi tersebut juga memiliki potensi negatif yang mampu mengancam eksistensi dan tradisi manusia. Seiring dengan kemajuan teknologi informasi, konsep tentang batasan-batasan baik fisik maupun virtual, harga, entitas, pola pikir, rutinitas kerja, dan tingkah laku sosial bertransformasi semakin penting. Pengetahuan dipandang sebagai "kekuasaan," yang memberikan kemampuan untuk mengontrol nasib manusia secara menyeluruh.

Semakin besar ketergantungan individu pada teknologi informasi, semakin tinggi risiko yang harus dihadapi. Adopsi teknologi informasi saat ini merupakan permasalahan ganda karena,

selain mempercepat kemajuan peradaban manusia, kesejahteraan, dan aspek lainnya, teknologi informasi juga dapat dimanfaatkan untuk melakukan tindakan kriminal dan ilegal. Konsep "Kejahatan dunia maya" merujuk pada beragam kegiatan ilegal yang dapat dilakukan dengan memanfaatkan kemajuan teknologi informasi, mulai dari perjudian online, pornografi, carding (penipuan kartu kredit), phishing (penipuan internet banking), hacking, cracking, hingga penyebaran malware seperti virus, worm, trojan, atau bot. Selain itu, kejahatan transnasional seperti transaksi obat-obatan terlarang, sindikat, kekerasan politik, pencucian uang, eksploitasi manusia, dan ekonomi bawah tanah juga semakin marak dengan dukungan dari teknologi informasi.

Kemajuan teknologi informasi telah memudahkan berbagai jenis kejahatan dilakukan dengan cepat dan efisien. Di bidang cybercrime, terutama dalam pengelolaan data dan informasi, risiko tindak pidana meningkat karena perlindungan data pribadi semakin rentan dengan perkembangan teknologi (Muhamad Hasan Rumlus, 2020). Privasi individu semakin terancam akibat kemajuan teknologi informasi dan komunikasi, sehingga data pribadi rentan untuk disalahgunakan.

Contoh nyata dari penyalahgunaan data pribadi berlangsung di tahun 2018 melalui pelanggaran informasi pengguna akun Facebook secara global. Indonesia sendiri memiliki lebih dari 1 juta pengguna Facebook yang terdampak oleh insiden tersebut, mencapai sekitar 1,26% dari total data yang disalahgunakan. Mengingat ada 130.000.000 (seratus tiga puluh juta) anggota Facebook di Indonesia, atau 6% dari seluruh pengguna Facebook di seluruh dunia, ini adalah angka yang signifikan.

Selain pelanggaran data, Facebook juga menghadapi berbagai masalah lain, salah satunya adalah peningkatan konten yang bersifat negatif. Dimana facebook digunakan untuk menyebarkan berita palsu dan terlibat aktivitas penipuan. Berguna untuk menentukan apakah masyarakat yang memiliki pengetahuan atau mempublikasikan bahaya yang dapat mempengaruhi pengguna yang dapat menerima penggunaan Facebook, sebab sangat penting untuk mengetahui tingkat penerimaan suatu teknologi, termasuk Facebook. Hal ini bisa jadi disebabkan oleh kurangnya keamanan informasi, tata kelola, dan manajemen risiko TI, sampai tak mampu memastikan bahwa data pribadi detail pribadisetiap pengguna akan tersimpan dengan aman dan tidak diberitahukan kepada pihak lain.

Penyelenggara harus mematuhi aturan kerahasiaan data dan segera memberitahukan pelanggaran kerahasiaan data menurut Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 (Permenkominfo No. 20 Tahun 2016) mengenai Perlindungan Data Pribadi dalam Sistem Elektronik. Facebook dinilai gagal melindungi data pribadi penggunanya, yang bisa berujung pada sanksi pidana atas kebocoran data. Persoalannya bermula dari kebiasaan Facebook memantau aktivitas online pengguna, menyimpan data kunjungan pengguna ke situs web, serta mencatat semua tindakan pengguna secara terperinci, yang sulit dihapus. Meskipun media sosial memudahkan komunikasi, penggunaan Facebook juga membawa risiko besar bagi privasi dan keamanan pengguna. Pengguna sering kali membagikan informasi pribadi di platform sosial tersebut, meningkatkan risiko keamanan data mereka yang rentan terhadap ancaman dan bahaya yang dapat timbul secara tidak terduga. Keamanan informasi menjadi salah satu ancaman utama akibat dari praktik tersebut.

Agar perusahaan telekomunikasi dan klien mereka memiliki hubungan hukum yang jelas, maka perlindungan data pribadi harus dijaga. Ada beragam aturan yang berkaitan langsung pada preservasi detail pribadi, bermula dari yang lazim (lex generalis) sampai yang spesifik (lex

specialis). Akan tetapi, mampu diamati bahwa dalam peraturan yang berlaku saat ini terkait topik ini di Indonesia, belum ada satu peraturan yang mengkodifikasi seluruhnya, sehingga belum mencapai standar internasional untuk perlindungan data pribadi. (Satrio, 2020). Menurut Audun J. (2007), Definisi keamanan secara luas adalah tidak adanya bahaya. Ancaman keamanan, di sisi lain, digambarkan sebagai keadaan, peristiwa, atau kondisi apa pun yang berpotensi membahayakan jaringan atau data. Keadaan ini dapat mencakup kerusakan, kehilangan, perubahan, atau penyalahgunaan data (Edy Soesanto, 2023).

Tujuan dari penulisan artikel ini, untuk menganalisis pengaruh kebocoran data pada pengguna Facebook. Rumusan masalah dapat diambil dari informasi yang telah dijelaskan sebelumnya; 1) Bagaimana pihak facebook mencegah masalah kebocoran data para penggunanya? 2) Hambatan apa dalam melaksanakan keamanan cyber di Indonesia?

KAJIAN TEORITIK

Internet Of Things

Internet of Things adalah jenis teknologi canggih yang, di permukaan, dimaksudkan untuk menghubungkan banyak perangkat dan sistem yang berbeda di seluruh dunia sehingga mereka dapat bertukar data dan tetap berkomunikasi satu sama lain. Perangkat dan sistem ini mencakup sensor dan perangkat lunak yang dirancang untuk digunakan untuk komunikasi, pengumpulan data, berbagi data, dan pertukaran data melalui perangkat lain yang terhubung ke internet dan mendukung proses kerja tanpa memerlukan kabel atau jaringan nirkabel.

Internet of Things memiliki hubungan yang kuat dengan konsep mesin-ke-mesin. Perangkat cerdasadalah sebutan umum untuk semua perangkat yang memiliki kemampuan komunikasi mesin-ke-mesin. Perangkat cerdas seperti ini dinantikan sebagai alat pendukung bagi tenaga kerja manusia dalam menangani berbagai tantangan atau tugas yang timbul (Arief Selay, 2022).

Big Data

Istilah "big data" merujuk pada dataset yang sangat besar dengan struktur yang lebih kompleks dan beragam yang dieksplorasi untuk menghasilkan solusi atau simpulan. Big Data sangat bermanfaat untuk meningkatkan efisiensi operasional perusahaan. Persaingan di masa depan akan semakin ketat, dengan memanfaatkan teknologi canggih dan memungkinkan penggunaan big data untuk memajukan tujuan perusahaan. Namun, ada sejumlah kekurangan pada big data, termasuk masalah pengumpulan, penyimpanan, pemrosesan, dan visualisasi data. Karena perangkat big data sekarang sering digunakan dalam sistem perusahaan, keamanan sistem tidak bisa lagi hanya mengandalkan langkah-langkah keamanan konvensional, melainkan harus diperkuat dengan adanya ancaman terhadap data, terutama data yang penting dan sensitif seperti informasi pribadi pelanggan, yang jika disusupi, bisa sangat berbahaya bagi bisnis karena dapat menyebabkan kehilangan reputasi di pasar.

Kumpulan data yang lebih besar (volume), keragaman yang lebih besar, termasuk data yang terorganisir, semi-terstruktur, dan tidak terstruktur (variasi), lebih cepat dari sebelumnya (kecepatan), keakuratan data, dan nilai dalam data adalah aspek-aspek yang dianggap sebagai big data. Big Data tidak terorganisir dan sangat besar, ini bukan hanya tentang ukuran, berbagai sifat dan dimensi, termasuk ukuran, memiliki pengaruh yang signifikan terhadap penelitian produksi dan ilmiah. Data tidak dikelola saat dikumpulkan.

Informasi dikumpulkan dan diorganisir untuk menemukan hubungan dan contoh yang

tampak meragukan pada awalnya, namun kemudian terbukti menguntungkan bagi bisnis. Keamanan dan perlindungan data, serta kemampuan untuk memulihkan data dengan solusi yang sesuai, merupakan persyaratan mendasar untuk pembuatan alat pengujian Big Data. Data sensitif dapat hilang, oleh karena itu sebelum ditumpuk di cloud, data tersebut diacak untuk mencegah degradasi data (Dimas Prayoga, 2022).

Kejahatan Cyber

Semua tindak pelanggaran yang mengarah pada komputer, jaringan komputer, dan penggunanya, serta pelanggaran konvensional yang memanfaatkan atau didukung oleh perangkat komputer, dianggap sebagai pelanggaran terkait dengan komputer. Tindak pidana ini terbagi menjadi dua golongan: kejahatan yang didefinisikan secara luas dan kejahatan dalam pengertian yang lebih spesifik. Dalam konteks yang lebih spesifik, kejahatan siber mengacu pada pelanggaran terhadap sistem komputer, sementara dalam definisi yang lebih luas, kejahatan siber mencakup pelanggaran terhadap jaringan atau sistem komputer dan pelanggaran yang melibatkan penggunaan fasilitas komputer.

Masalah kejahatan siber menjadi suatu tantangan yang kompleks untuk diatasi. Ini disebabkan oleh kenyataan bahwa kejahatan di dunia maya merupakan jenis kejahatan yang unik yang dapat terjadi tanpa adanya interaksi fisik antara korban dan pelaku karena terjadi di dunia yang dikecualikan dari aturan-aturan hukum. Dengan demikian, dapat disimpulkan bahwa siapa pun, dari berbagai negara yang memiliki akses ke internet, bisa terjerumus kejahatan siber, sebagai korban, atau bahkan sekadar sebagai saksi (Sari, 2018).

Perilaku dan kebiasaan manusia berubah seiring dengan kemajuan peradaban. Keinginan masyarakat untuk bebas dari kekangan budaya telah menyebabkan pergeseran budaya hukum, yang memandang hukum sebagai kumpulan aturan dalam bentuk pasal-pasal yang sama sekali tidak dapat menghukum atau membuat jera para penjahat untuk mengulangi kejahatan mereka. Kejahatan jalanan dan tindakan main hakim sendiri meningkat karena adanya persepsi bahwa hukum itu keras untuk beberapa kelompok dan tumpul untuk kelompok lainnya.

Karena meningkatnya ketidakpercayaan terhadap sistem hukum, aparat penegak hukum dianggap lebih cepat menanggapi kejadian-kejadian yang melanggar hukum. Karena TI (informasi dan teknologi) digunakan dengan cara-cara baru untuk melakukan kejahatan, maka diperlukan ketentuan hukum yang dapat memberikan keyakinan kepada masyarakat jika mereka menjadi korban kejahatan berbasis TI. Sasaran perlindungan hukum haruslah sistem keamanan data masyarakat. Aplikasi Peduli Lindungi disebut-sebut memuat 3,2 miliar data pengguna, termasuk alamat surat elektronik, nomor panggilan, tempat kelahiran, tanggal lahir (DOB), identitas perangkat, kondisi Covid-19, latar belakang registrasi dan penelusuran kontak, riwayat vaksinasi, dan konten lainnya. Menurut laporan di media CNBC Indonesia, Bjorka melakukan pembobolan data pribadi terhadap data-data tersebut (Beridiansyah, 2023).

AI (*Artificial Intelligence*)

Kecerdasan Buatan (AI) adalah gabungan ilmu yang berfokus pada otomatisasi tugas-tugas yang biasanya memerlukan tingkat kapabilitas manusia. Kerjasama antara manusia dan hewan tenaga kerja dapat digunakan untuk menghasilkan keputusan yang tidak selalu berdampak negatif terhadap kepentingan personal. Teknologi AI terbaru mencakup sistem yang mampu secara otomatis mengadaptasi tampilan layar sesuai dengan kebutuhan yang sedang dialami oleh pengguna saat itu. Pendekatan metodologi yang diterapkan dalam riset ini adalah pemantauan. Di

samping itu, pendekatan analisis metodologis menggunakan metode observasi sehingga dapat diterapkan.

Penelitian kualitatif deskriptif difokuskan pada menyusun karakteristik atau ciri-ciri dari penelitian yang sedang di analisis dalam prosedur akumulasi informasi. Riset ini memanfaatkan tinjauan tulisan sistematik dari sumber jurnal yang ada. Aspek-aspek seperti tanggal publikasi, lokasi tempat penelitian dilaksanakan, dan spesifikasi desain data berdasarkan aplikasi kecerdasan buatan dalam eksperimen turut dipertimbangkan ketika mengevaluasi kembali isi jurnal tersebut.

Tujuan dari kecerdasan buatan, salah satu cabang dari ilmu komputer, adalah untuk mengembangkan kecerdasan dengan proses berpikir dan perilaku yang mirip dengan manusia. Kecerdasan buatan (AI) memiliki potensi untuk mengubah nilai dan karakter siswa, mempertajam pikiran mereka, dan membuka mata mereka. AI memiliki aplikasi di sejumlah disiplin ilmu, termasuk ekonomi, kesehatan, dan pertanian (Wahyudi, 2023).

Tujuan dari bidang ilmu komputer kecerdasan buatan (AI) adalah untuk membangun mesin yang mampu melakukan beban pekerjaan diselesaikan oleh manusia, seperti penyelesaian masalah, menentukan kepastian, dan adaptasi situasional. Kecerdasan Buatan adalah sistem perangkat lunak yang dapat bertindak atau memutuskan sendiri tanpa memerlukan interaksi manusia. AI membantu masyarakat dalam berbagai hal, termasuk menyederhanakan pekerjaan dan mempercepat prosedur perusahaan. AI dapat membantu dalam menentukan kepastian secara cekatan serta akurasinya terjaga dan menyelesaikan masalah yang rumit.

AI sangat bermanfaat dalam berbagai industri, termasuk produksi, transportasi, dan perawatan kesehatan. Kekhawatiran tentang masa depan tenaga kerja dan bagaimana AI dapat memengaruhi pekerjaan juga muncul karena kemajuan AI. Walaupun mayoritas pakar meyakini bahwa kecerdasan buatan (AI) akan membuka kesempatan kerja baru dan mendukung manusia dalam menjalankan beban pekerjaan yang rumit dan repetitif, sebagian individu merasa cemas bahwa AI bakal menyingkirkan pekerjaan manusia (Ishak Farid, 2023).

Facebook

Facebook adalah sebuah media sosial yang memberikan kesempatan bagi pengguna untuk berinteraksi dan terkoneksi dengan orang lain. Berbagai layanan yang disediakan oleh Facebook, seperti arsip gambar dan rekaman, laman obrolan, tulisan memo, program laman, jawaban komersial, permainan, serta platform komunitas, menjadikan platform ini lengkap. Dengan Facebook, pengguna dapat membentuk hubungan pertemanan yang luas di dunia maya.

Sejalan dengan Robert McDrie, manajemen mengacu pada metode untuk mencapai tujuan. Dengan demikian, memberikan keamanan adalah tujuan akhir dari manajemen keamanan, yang juga merupakan proses untuk mencapainya. Manajemen keamanan adalah proses mengambil tindakan pencegahan yang diperlukan untuk menjaga keselamatan dan mencegah korban untuk menghindari kejadian yang berpotensi fatal dan memastikan bahwa kejadian tersebut ditangani secara efektif dan cepat. Manusia, sebagai makhluk yang unik, umumnya memiliki dua tujuan hidup utama, bisa memasak dan merasa cukup percaya diri untuk mempertahankan diri agar dapat bertahan hidup (Hadiman, 2008) (Edy Soesanto F. K., 2023).

Peretasan adalah tindakan membobol komputer, sistem, atau jaringan tanpa persetujuan pengguna (Ramadhan A, 2022). Kejahatan siber didefinisikan sebagai tindakan ilegal yang dilakukan melalui media virtual yang dimungkinkan oleh teknologi siber (Ramailis, 2020). Lebih lanjut, kejahatan siber dapat dipahami sebagai serangan terhadap korban yang memanfaatkan berbagai sumber daya, termasuk komputer, internet, teknologi, dan lain sebagainya (Habibi &

Liviani, 2020). Kejahatan siber mencakup, namun tidak terbatas pada, peretasan akun media sosial, pengambilan saldo akun korban secara diam-diam, dan pembobolan informasi penting tentang korban (Saputra, 2022) (Nurul Khasanah, 2023).

Kejahatan siber dapat secara signifikan memengaruhi individu dan bisnis. Kerugian finansial, kerusakan reputasi, dan penderitaan psikologis dapat diakibatkan oleh kejahatan siber seperti penipuan, pencurian identitas, dan pembobolan data. Bisnis juga rentan terhadap kejahatan siber, yang dapat mengakibatkan kerugian uang, baik serangan ransomware maupun pencurian data. Organisasi pemerintah juga dapat menjatuhkan denda pada bisnis. Jika mereka mengabaikan hukum yang berkaitan dengan perlindungan data (Nugroho & Chandrawulan, 2022).

METODOLOGI PENELITIAN

Teknik yang mana diterapkan pada riset ini merupakan pendekatan berbasis kualitatif dan penelitian warisan. Sasaran dari pendekatan ini adalah untuk memperoleh wawasan dari studi yang telah dilakukan. Sebab studi ini terkait dengan mengevaluasi suatu teori dan koneksi antar sebuah variabel dengan yang lainnya, yang bersumber dari buku dan jurnal daring.

Tabel 1 - Penelitian Terdahulu

No	(Nama Penulis)	Judul Penelitian	Hasil Penelitian
1	Nabila Aulia Agustin dan Refania Meilani Firdos (2024)	Ancaman Cybercrime di Indonesia dan Pentingnya Pemahaman akan Fenomena Kejahatan Digital	Berbagai serangan siber, seperti serangan DDoS, serangan malware, dan pencurian data, dapat memengaruhi suatu negara. Penegakan hukum yang tidak memadai, serangan tingkat lanjut, dan ketidaksetaraan dalam masyarakat. Oleh karena itu, dalam lingkup keamanan siber, ada kebutuhan untuk meningkatkan kesadaran, keahlian, dan upaya terkoordinasi yang kuat.
2	Putri Hasian Silalahi, Fiorella Angella Dameria (2023)	Perlindungan Data Pribadi Mengenai Kebocoran Data Dalam Lingkup Cyber Crime Sebagai Kejahatan Transnasional	Karena jangkauan jaringan yang luas dan kemampuannya untuk melampaui batas-batas internasional, kejahatan siber-juga dikenal sebagai kejahatan transnasional-yang menyebabkan kerugian material dan tidak berwujud yang signifikan dapat terjadi.

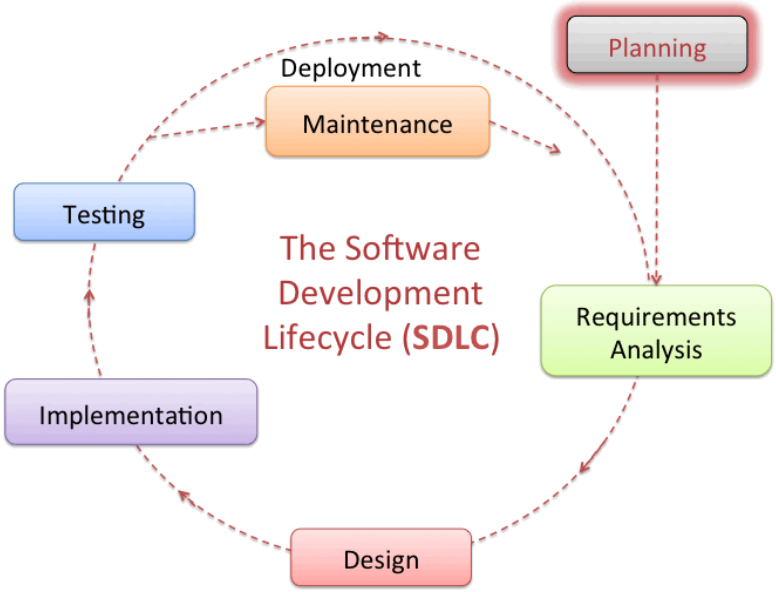
3	Muhamad Hasan Rumlus, Hanif Hartadi (2020)	Kebijakan penanggulangan pencurian data pribadi dalam media elektronik	Menetapkan peraturan yang tepat untuk melindungi informasi pribadi setiap warga negara sangatlah penting, seperti halnya membuat peraturan yang ketat dan mencakup semua hal untuk mengatasi pencurian identitas melalui media elektronik di Indonesia. dengan melindungi data pribadi dan menghapus informasi elektronik.
4	M. Habibullah Arief, Khoirunnisa' Afandi, Emha Diambang Ramadhany, Stivaniyanti (2023)	Pengaruh Kesadaran Risiko TI Terhadap Kepercayaan Pengguna Fecebook	Kebahagiaan yang lebih rendah dari pengguna yang kembali ke Facebook adalah bukti bahwa komponen risiko dari kesadaran TI mempengaruhi perilaku pengguna. Kenyamanan dan keuntungan yang dinikmati konsumen dianggap lebih besar daripada potensi kekhawatiran, sehingga nilai ini masih cukup rendah.
5	Natasya Salsabila Nainggolana, Irwan Padli Nasution (2023)	Pentingnya Keamanan Big Data Dalam Lembaga Pemerintahan Di Era Digital	Keamanan big data menjadi amat vital di zaman digital, khususnya bagi organisasi pemerintah yang perlu menjaga informasi pribadi penduduknya. Melindungi big data memerlukan pengamanan setiap komponen yang membentuk big data.
6	Muhammad Bayu Satria, Meh Wih Widiatno (2020)	Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook di Indonesia)	Terdapat sejumlah ketentuan undang-undang yang berkaitan melalui perlindungan data pribadi, termasuk ketentuan umum (lex generalis) dan khusus (lex specialis). Namun, regulasi yang sekarang berfungsi terkait proteksi informasi pribadi di Indonesia belum sepenuhnya terkodifikasi sesuai dengan standar internasional untuk perlindungan data pribadi.

7	Yustika Citra Mahendra, Ni Komang Desy Setiawati Arya Pinatih (2023)	Strategi Penanganan Keamanan Siber (Cyber Security) di Indonesia	Hanya beberapa undang-undang, termasuk UU ITE, yang berlaku di Indonesia; edukasi lebih lanjut juga diperlukan mengenai kejahatan dunia maya dan tanggapan yang tepat. Peran pemerintah juga diperlukan untuk mengatasi masalah ini dan meningkatkan kesadaran masyarakat di kalangan pengguna internet.
8	Wen Lung Shiau, Xiaoqun Wang, Fei Zheng (2023)	What are the Trend and Core Knowledge of Information Security? A citation and Co-citation Analysis (Apa tren dan pengetahuan inti keamanan informasi? Analisis kutipan dan kutipan bersama)	Karena serangan dan ancaman menyertai pertumbuhan teknologi baru seperti blockchain, 5G, loT, kecerdasan buatan, dan kecerdasan buatan, ISec menarik lebih banyak perhatian dari kalangan akademisi dan bisnis. Perusahaan dapat mengalami kerugian yang tidak dapat dipulihkan akibat kebocoran informasi dan pelanggaran keamanan lainnya yang mengakibatkan kerugian pada keuangan, reputasi, dan area lainnya. Oleh karena itu, ISec telah menarik perhatian industri dan akademisi.
9	Beryl A. Ehondor, Silk Ugwu Ogbu (2020)	Personal Data Protection and Facebook Privacy Infringements in Nigeria	Kontroversi Facebook-Cambridge Analytica menyingkap contoh-contoh pelanggaran kepercayaan dan privasi data pribadi. Facebook bertanggung jawab atas pelanggaran privasi ini, dan negara-negara harus fokus untuk melindungi data warga negara. Meskipun mereka belum membuat banyak kemajuan, negara-negara lain seperti Nigeria juga bekerja untuk melindungi data online penduduk mereka.

10	Ankit Kumar Jain, Somya Ranjan Sahoo, Jyoti Kaubiyal (2021)	Online Social Networks Security and Privacy: Comprehensive Review and Analysis	Pengguna media sosial harus lebih waspada terhadap potensi bahaya, serangan, dan masalah privasi lainnya seiring dengan meningkatnya penggunaan platform ini. Namun, ketidaktahuan pengguna akan masalah keamanan dan privasi memungkinkan terjadinya berbagai peretasan berbasis media sosial.
11.	Achmad Fauzi, Rido Akbar, Adela Rizkha, Safira Tamiya Putri, Intan Fadhilah, Nadia Putri Iskandar, I Gusti Ngurah Agung (2023)	Keamanan Cyber dan Peretasan Etis: Pentingnya Melindungi Data Pengguna	Pembobolan data bisa merusak kepercayaan pengguna dan berdampak serius pada keuangan perusahaan. Dalam situasi seperti ini, perusahaan harus memikirkan untuk menerapkan langkah-langkah keamanan mendasar seperti enkripsi data, deteksi penyusupan, sistem autentikasi, pemeliharaan dan pembaruan sistem operasi dan platform bisnis, serta pemfilteran paket. Semua ini dilakukan untuk memastikan ketersediaan, kerahasiaan, dan integritas data.
12.	Dian Rahmawati, Muhammad Darriel Aqmal Aksana, Siti Mukaromah (2023)	Privasi dan Keamanan Data di Media Sosial: Dampak Negatif dan Strategi Pencegahan Data Privacy and Security in Social Media: Negative Impact and Prevention Strategies	Temuan penelitian menunjukkan tingkat kesadaran privasi pengguna yang buruk, dengan banyak orang mendapatkan berita atau iklan yang dapat menyebabkan kebocoran data, serta kurangnya fokus pada keamanan dan privasi data. Selain itu, tidak sering mengganti kata sandi, membiarkan akun media sosial terlihat oleh publik, dan tidak menerapkan pengaturan privasi yang memadai.
13.	Rifqi Galuh Putra Ahmad Fauzi Ery Teguh Prasetyo Salza Rio Pratama Indah Deya Ramadhan Febriyanti Febriyanti Siti Nurlela (2023)	Pentingnya Manajemen Keamanan di Era Digitalisasi	Temuan penelitian ini menjelaskan bahwa, di era digitalisasi saat ini, manajemen keamanan merupakan prasyarat penting bagi bisnis atau organisasi. Perusahaan dan organisasi dapat melindungi data dan teknologi mereka dari serangan siber dan mengurangi potensi risiko keamanan melalui implementasi pengelolaan proteksi

			yang terpadu, mengendalikan risiko dengan akurat, dan menerbitkan strategi pengamanan.
14.	Amina Hassan, Kareem Ahmed (2023)	Cybersecurity's Impact on Customer Experience: An Analysis of Data Breaches and Trust Erosion (Dampak Keamanan Siber terhadap Pengalaman Pelanggan: Analisis Pelanggaran Data dan Erosi Kepercayaan)	Metode dan strategi yang digunakan untuk mencapai keseimbangan antara kegunaan dan keamanan siber dikaji dalam penelitian ini. Makalah ini dimulai dengan ringkasan mendalam tentang perkembangan keamanan siber dan semakin pentingnya antarmuka yang ramah pengguna dalam ekosistem digital modern. Kemudian menjelaskan mengapa antarmuka yang ramah pengguna sangat penting untuk mengoptimalkan pengalaman pelanggan dan melindungi data sensitif.
15.	Jinli, Wei Xiao, Chong Zhang (2023)	Data Security Crisis in Universities: Identification of Key Factors Affecting Data Breach Incidents (Krisis Keamanan Data di Universitas: Identifikasi Faktor-Faktor Utama Yang Mempengaruhi Insiden Pelanggaran Data)	Selain memperjelas pemahaman kami tentang pelanggaran data dan menawarkan rekomendasi praktis untuk universitas dan institusi lain yang ingin memperkuat keamanan informasi dan mengungkapkan kerentanan kepada publik dalam menghadapi frekuensi pelanggaran data yang semakin meningkat, temuan estimasi dan ketahanan ini juga menjelaskan mekanisme yang mendasari yang memengaruhi keamanan data universitas.
16.	Edy Soesanto, Alifah Jiddal Masyruroh, Ganis Aliefiani Mulya Putri, Srirahayu Putri Maharan (2023)	Peranan Manajemen Sekuriti Dalam Mengamankan Dan Memecahkan Masalah PT SK Keris Indonesia	Bisnis harus menerapkan ilmu manajemen keamanan untuk memastikan keamanan mereka sendiri. Risiko negatif bisa meningkat karena tindakan bisnis yang tidak memasukkan keamanan ke dalam proses mereka.

KERANGKA KONSEPTUAL (*KONSEPTUAL FRAMEWORK*)



HASIL DAN PEMBAHASAN

Bagaimana Pihak Facebook Mencegah Masalah Kebocoran Data Para Penggunanya

Berdasarkan topik permasalahan yang dibahas, seperti yang diketahui setiap sosial media memiliki kelemahan dalam menyimpan data privasi dan keamanan penggunanya. Berikut termasuk cara pencegahan perlindungan data privasi pengguna Facebook :

1. Memanfaatkan kata sandi yang sulit ditebak dengan menggabungkan kapital, non-kapital, nomor, dan lambang juga bisa merubahnya secara rutin.
2. Menyusun pembatasan berhubungan dengan publikasi konten, menetapkan pengaturan privasi, dan membatasi jangkauan data pengguna dari pihak ketiga.
3. Selalu waspada dalam membagikan informasi krusial seperti tanggal kelahiran, tempat tinggal.
4. Memahami peraturan secara cermat mengenai berbagi data diri.
5. Memprioritaskan pemahaman dan pengetahuan pengguna akan pentingnya melindungi privasi serta keamanan informasi.
6. Meneliti kegiatan dan jejak profil apabila ada kecurigaan aktivitas mergukan atau pun entri tak valid.
7. Memakai perangkat lunak yang resmi dan kredibel (hindari aplikasi yang informal atau telah dimodifikasi).
8. Menjaga kewaspadaan saat mengeklik tautan dan mengunduh berkas.

9. Dengan penerapan langkah-langkah pencegahan ini diharapkan bisa meningkatkan keamanan dan juga privasi data bagi pengguna platform media sosial (Dian Rahmawati, 2023).

Selain langkah-langkah pencegahan yang telah disebutkan di atas, Facebook juga menyediakan fitur autentikasi dua faktor untuk meningkatkan keamanan akun daring sebagai tindakan pencegahan terhadap kejahatan dunia maya. 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.

Hal-Hal Yang Dapat Dilakukan Pengguna Facebook Indonesia Jika SudahTerjadi Kebocoran Data

1. Pengguna Facebook di Indonesia berhak meminta pembersihan informasi pribadi mereka yang sudah dieksploitasi oleh entitas Facebook Indonesia, asalkan penghapusan itu telah diresmikan oleh lembaga peradilan dalam keputusan terkait pelanggaran privasi.
2. Facebook Indonesia harus menghilangkan informasi pribadi yang telah dicemarkan nama baiknya berdasarkan permohonan pengguna Facebook di Indonesia yang merasa dirugikan akibat eksploitasi informasi pribadi oleh entitas Facebook Indonesia, juga harus mengklarifikasi proses penghapusan informasi pribadi yang bersangkutan (Satrio, 2020).

Hambatan dalam Melaksanakan Keamanan Siber Di Indonesia

Kendala utama dalam penegakan proteksi siber di Indonesia akhir-akhir ini mengikutsertakan sejumlah elemen kritis. Taraf keaksaraan publik Indonesia tentang proteksi digital masih tidak memadai, sehingga pengetahuan tentang urgensi proteksi digital bagi pengguna jejaring sosial masih terkendala. Kendati demikian, SKKNI telah mendefinisikan SPI dalam kapasitas norma proteksi informasi di lingkungan kerja Indonesia, upaya penyebaran edukassi terkait terbatas. Kekurangan program publisitas yang mendalam dan kesulitan dalam memperbarui elemen keahlian dalam SKKNI memblokir penyebaran informasi, terkhusus mempertimbangkan evolusi teknologi yang pesat.

Kurangnya polisi yang khusus dalam hal proteksi informasi menjadi hambatan, khususnya sebab UU ITE tidak detail menjelaskan berbagai macam risiko siber di periode teknologi di zaman modern. Kurangnya penempatan polisi dan aset yang adekuat untuk menjalankan proteksi digital menjadi problematika penting. Di samping sumber daya alam, kurangnya tenaga kerja yang berpengalaman dalam proteksi siber menjadi rintangan yang signifikan. Diakibatkan pengendalian ahli proteksi digital luar negri, menghambat alih teknologi yang mendukung penegakan proteksi digital.

Hanya ada sekitar 500 orang tenaga ahli proteksi digital di Indonesia di tahun 2015 yang telah terakreditasi oleh ISO270001, CEH, CISA. Indonesia memerlukan lebih banyak dari 1000 spesialis proteksi digital di luar teknikal officiers di tahun 2016. Kurangnya data berkaitan dengan jumlah profesional yang telah dibina \ menghasilkan evaluasi terkait memadai SDM proteksi siber menjadi kurang bisa diandalkan. Hambatan lain dalam perkembangan polisi proteksi siber adalah sifat bahaya siber yang multidimensi, membutuhkan envolvement yang cukup banyak.

Teknologi senantiasa diperbaharui berjalan dengan peningkatan jenis penyerangan siber. Kendala eksekusi proteksi siber di Indonesia, sesuai fondasi-fondasi Global Cybersecurity Index (2017), tampak pada yang pertama pilar capacity building, di mana edukasi proteksi informasi, publisitas SKKNI area Proteksi Informasi dan Auditor TI masih terkendala. Prosedur pembaruan elemen keahlian dalam SKKNI membutuhkan durasi yang panjang, sementara evolusi teknologi informasi dan jenis risiko siber berlanjut dengan cepat. Pendidikan masyarakat luas, terutama dalam hal edukasi konten unggulan, proteksi siber, pemahaman tentang pluralitas, dan anti-teror, belum diimplementasikan secara terorganisir, terutama pada usia dini, meskipun pengguna internet di Indonesia usia 9 hingga 15 tahun cukup tinggi, mencapai 27.5%.

Jumlah hukum dan peraturan untuk proteksi siber belum seluruhnya dapat memfasilitasi beragam jenis risiko siber, sementara laju evolusi teknologi terus bertambah seiring dengan kenaikan tidank pidana siber. Kegentingan verifikasi RUU Proteksi Data dan Informasi Pribadi menjadi vital untuk memberikan jaminan legal terkait proteksi data pribadi. Pilar ketiga, yakni susunan organisasi, juga menghadapi kendala, seperti; ambiguitas deadline transisi penyatuann tugas Direktorat Proteksi Informasi dan Lembaga Sandi Negara menjadi Badan Siber dan Sandi Negara (BSSN) sebagai entitas baru. Dibutuhkan kegentingan dalam membangun sistem ekologi ranah siber Indonesia yang resisten, serta memulai rencana strategis dan petunjuk penanganan proteksi siber.

SIMPULAN

Berdasarkan hasil yang sudah dibuat maka dapat disimpulkan bahwa dari penelitian yang sudah dilakukan dapat disimpulkan bahwa facebook telah melakukan pengamanan data untuk menjaga data privasi penggunanya. Namun dengan perkembangan teknologi yang makin pesat, kejahatan cyber juga makin banyak dan kompleks yang dapat mengancam keamanan data. Indonesia juga masih kurang minimnya pengetahuan tentang keamanan cyber di masyarakat umum.

DAFTAR PUSTAKA

Achmad Fauzi, R. A (2023). "Keamanan Cyber dan Peretasan Etis: Pentingnya Melindungi Data Pengguna," *Jurnal Ilmu Multidisiplin*, Vol. 2, No. 1

Amina Hassan, K. A (2023). "Cybersecurity's Impact on Customer Experience: An Analysis of Data Breaches and Trust Erosion,"*Orient Review*, Vol. 15 No. 9.

Jain, Ankit Kumar et al (2021). "Online social networks security and privacy: comprehensive review and analysis." *Complex & Intelligent Systems* 7 (2021): 2157 - 2177.

Arief Selay, G. D (2022). "Internet of Things," *Jurnal Karimah Tauhid*, Vol. 1 No. 6.

Beridiansyah (2023). *Kejahatan Siber Ancaman dan Permasalahannya: Tinjauan Yuridis pada Upaya Pencegahan dan Pemberantasannya di Indonesia.* Banda Aceh: Syiah Kuala University Press.

Beryl Ehondor, S. U (2020). "Personal Data Protection and Facebook Privacy Infringements in Nigeria," *Journal of Leadership, Accountability and Ethics*, Vol. 17 No. 2

Dian Rahmawati, M. D. (2023). "Privasi dan Keamanan Data di Media Sosial: Dampak Negatif dan Strategi Pencegahan," *Prosiding Seminar Nasional Teknologi dan Sistem Informasi (SITASI*, Vol. 3 No. 1.

Prayoga, Dimas, et. al. (2022). "Risiko Keamanan Data Pribadi Pelanggan Dalam Penggunaan Big Data," *Jurnal Komputasi dan Teknologi Informasi*, Vol. 5 No. 3

Soesanto, Edy, et al. (2023). "Peranan Manajemen Sekuriti Dalam Mengamankan Dan Memecahkan Masalah PT. SK Keris Indonesia," *Jurnal Manajemen Riset Inovasi* Vol.1 No. 3

Soesanto, Edy, et.al (2023). "Pengaruh Sistem Pengamanan Objek Vital, File dan Cyber Terhadap Manajemen Sekuriti Pada PT Freeport Indonesia," *Jurnal of Research dan Publication Innovation*, Vol. 1 No. 2.

Farid, Ishak (2023). "Pemanfaatan Artificial Intelligence Dalam Pertahanan Siber," *Nusantara Jurnal Ilmu Sosial*, Vol. 6, No. 7

Jin Li, W. X. (2023). "Data Security Crisis in Universities: Identification of Key Factors Affecting Data Breach Incidents," *Journal Humanities and Social Science*, Vol. 10 No. 27

Arief, Habibullah, et.al (2023). "Pengaruh Kesadaran Risiko TI Terjadap Kepercayaan Pengguna Facebook," *Jurnal Minfo Polgan*, Vol. 12 No. 1.

Rumlus, Muhamad Hasan, H. H. (2020). "Kebijakan Penanggulangan Pencurian Data Pribadi," *Unnes Law Review*, Vol. 4 No. 3.

Nabila Aulia Agustin, R. M. (2024). "Studi Literatur: Ancaman Cybercrime di Indonesia dan Pentingnya," *Jurnal Jamastika*, Vol. 3 No. 1

Nainggolan, Natasya, I. P. (2023). "Pentingnya Keamanan Big Data Dalam Lembaga Salsabila Pemerintahan di Era Digital. *JSIT (Jurnal Sains dan Teknologi)*, Vol. 3 No. 2.

Khasanah, Nurul dan T. Sutarbi. (2023). "Analisis Kejahatan Cybercrime Pada Peretasan dan Penyadapan Aplikasi Whatsapp," *Blantika: Multidisciplinary Jornal*, Vol. 2 No. 1

Putri Hasian Silalahi, F. A. (2023). "Perlindungan Data Pribadi Mengenai Kebocoran Data Dalam Lingkup Cyber Crime Sebagai Kejahatan Transnasional," *Jurnal Wajah Hukum*, Vol. 7 No. 2

Putra, Rifqi Galuh, et.al (2023). "Pentingnya Manajemen Security di Era Digitalisasi," *Jurnal Ilmu Multidisiplin*, Vol. 2 No. 1

Sari, N. W (2018). "Kejahatan Cyber Dalam Perkembangan Teknologi Informasi Berbasis Komputer," *Jurnal Ilmu Hukum Satya Dharma*, Vol. 3 No. 2

Satrio, W. (2020). "Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook di Indonesia)," *Jurnal Wajah Hukum*, Vol. 7 No. 2.

Wahyudi, T. (2023). "Studi Kasus Pengembangan dan Penggunaan Artificial Intelligence (AI) Sebagai Penunjang Kegiatan Masyarakat Indonesia," *IJSE*, Vol.9 No.1

Wen-Lung Shiau, X. W. (2023). "What are The Trend and Core Knowledge of Information Security? a Citation and Co-Citation Analysis," *Journal Information and Management*, Vol. 60 No. 3

Mahendra, Yustika Citra, N. K. (2023). "Strategi Penanganan Keamanan Siber (Cyber Security) di Indonesia," *JRPP*, Vol 6 No. 4.