KAMPUS AKADEMIK PUBLISHER
Jurnal Ilmiah Penelitian Mahasiswa
Vol.3, No.2 April 2025
e-ISSN: 3025-5465; p-ISSN: 3025-7964, Hal 129-140
DOI: https://doi.org/10.61722/jipm.v3i2.787

ANALISIS KRIMINOLOGI TERHADAP PENCURIAN DATA PRIBADI DI ERA DIGITAL: STUDI KASUS KEBOCORAN DATA PENGGUNA APLIKASI MYPERTAMINA TAHUN 2023

Irvin Atara
01051220060@student.uph.edu
Universitas Pelita Harapan
Sharron Syallomeita
01051220052@student.uph.edu
Universitas Pelita Harapan
Raffi Aqil Baihaqi Haksoro
01051220199@student.uph.edu
Universitas Pelita Harapan

Abstract *This study analyzes the data breach of MyPertamina users in May 2023, with a focus on the criminological implications of cybercrime in Indonesia. The incident highlights systemic vulnerabilities in personal data management, which represent not only a technical failure but also a reflection of the weaknesses in national cybersecurity policies. This data breach is identified as a broader threat to the country's digital sovereignty and national economic stability, with over 44 million lines of sensitive data exposed. The research employs classical criminological theories, such as cyber space theory and routine activity theory, to analyze the contributing factors, motivations of the perpetrators, and the existing system vulnerabilities. Findings emphasize that although investigative efforts have been made, the government's response has been delayed and ineffective in addressing the evolving cyber threats. The study also provides recommendations to strengthen personal data protection policies and enhance cybersecurity infrastructure through a situational approach and regulatory reinforcement. Overall, this research contributes significantly to understanding the dynamics of cybercrime in Indonesia and urges the development of more adaptive policies to safeguard citizens' data in the digital era.*
Keywords*: cybercrime, data breach, MyPertamina, personal data protection, criminological theory, cybersecurity, digital policy.*

Abstrak Penelitian ini menganalisis kebocoran data pengguna aplikasi MyPertamina yang terjadi pada Mei 2023, dengan fokus pada implikasi kriminologis dalam konteks kejahatan siber di Indonesia. Insiden ini menunjukkan kerentanan sistemik dalam pengelolaan data pribadi, yang tidak hanya merupakan kegagalan teknis, tetapi juga refleksi dari kelemahan kebijakan keamanan siber di tingkat nasional. Kebocoran data ini diidentifikasi sebagai ancaman yang lebih luas terhadap kedaulatan digital negara dan stabilitas ekonomi nasional, dengan lebih dari 44 juta baris data sensitif yang terekspos. Penelitian ini menggunakan teori kriminologi klasik seperti teori ruang siber dan teori aktivitas rutin untuk menganalisis faktor-faktor penyebab, motivasi pelaku, serta kerentanan sistem yang ada. Hasil penelitian menekankan bahwa meskipun upaya investigasi telah dilakukan, respons pemerintah masih terlambat dan tidak cukup efektif dalam menghadapi ancaman siber yang terus berkembang. Penelitian ini juga memberikan rekomendasi untuk memperkuat kebijakan perlindungan data pribadi, serta meningkatkan infrastruktur keamanan siber melalui pendekatan situasional dan penguatan regulasi. Secara keseluruhan, studi ini memberikan kontribusi penting dalam memahami dinamika kejahatan siber di Indonesia dan mendorong pengembangan kebijakan yang lebih adaptif untuk melindungi data pribadi warga negara di era digital.
Kata Kunci: kejahatan siber, kebocoran data, MyPertamina, perlindungan data pribadi, teori kriminologi, keamanan siber, kebijakan digital.

PENDAHULUAN

Dalam dekade terakhir, fenomena kejahatan siber telah berkembang pesat menjadi ancaman yang melampaui batas-batas konvensional, baik secara teknis maupun geopolitik. Kejahatan siber kini telah menjadi masalah global yang mengancam bukan

Received Januari 30, 2024; Revised Februari 28, 2025; Maret 15, 2025
* Irvin Atara, 01051220060@student.uph.edu

hanya sektor teknologi, tetapi juga fondasi ekonomi dan keamanan nasional. Dalam era digital yang semakin kompleks, ancaman ini bukan hanya berbicara tentang serangan terhadap data atau sistem komputer, tetapi juga mengacu pada potensi ketidakstabilan geopolitik dan sosial yang ditimbulkan oleh eksploitasi digital. Kejahatan siber telah menjadi instrumen yang digunakan dalam perang asimetris antar negara, meruntuhkan struktur-struktur keamanan yang selama ini dianggap tangguh.

Menurut laporan yang dikeluarkan oleh Cybersecurity Ventures, diperkirakan kerugian akibat kejahatan siber akan mencapai angka yang mencengangkan, yakni USD 10,5 triliun per tahun pada 2025 (Chin, 2025). Angka ini lebih dari sekadar angka *statistic*, yang merupakan cerminan dari kerentanannya sistemik yang dapat merusak kestabilan perekonomian global. Proyeksi kerugian ini mencerminkan betapa besar dan kompleksnya ancaman yang dihadapi dunia digital. Yang lebih memprihatinkan adalah tren pertumbuhan yang sangat cepat, dengan estimasi pertumbuhan tahunan sebesar 15% (Pichurov, 2025), yang menunjukkan betapa kejahatan siber telah berkembang menjadi ekonomi bayangan yang mampu menyaingi GDP negara-negara besar.

Indonesia, sebagai negara dengan populasi terbesar di Asia Tenggara, tak luput dari ancaman ini. Data dari Badan Siber dan Sandi Negara (BSSN) menunjukkan lonjakan yang mengkhawatirkan dalam jumlah serangan siber. Sepanjang tahun 2022, tercatat 976.429.996 insiden serangan siber (Kristianti, 2023). Angka ini menunjukkan masih masifnya aktivitas kejahatan siber, yang tidak hanya mengindikasikan masalah teknis, tetapi juga mencerminkan kelemahan dalam arsitektur keamanan siber nasional Indonesia yang perlu segera dievaluasi dan diperbaiki.

Tabel 1: Tren Kejahatan Siber di Indonesia (2018-2022)

Tahun	Jumlah Serangan	Peningkatan (%)
2018	232.447.974	-
2019	290.000.000	24,9%
2020	189.937.542	-34,8%
2021	1.637.973.022	762,1%
2022	976.429.996	-40,3%

(Hasil diolah dari BSSN Tahun 2018-2022)

Melalui tabel di atas, jelas terlihat betapa tajamnya jumlah serangan siber yang terjadi di Indonesia. Tidak hanya sebagai angka, tetapi ini adalah indikator adanya kelemahan struktural dalam sistem keamanan siber nasional. Tren ini harus dipahami sebagai bagian dari gejala yang lebih besar dan memerlukan respons yang lebih komprehensif dan berkelanjutan.

Salah satu insiden yang menyoroti betapa seriusnya ancaman ini adalah kebocoran data MyPertamina pada Mei 2023, yang mengungkapkan kerentanannya infrastruktur digital Indonesia. Sekitar 21 juta data pengguna terekspos dalam insiden ini (ManageEngine, 2025), yang bukan hanya menunjukkan kegagalan teknis dalam perlindungan data, tetapi juga menunjukkan ketidaksiapan institusional dalam menghadapi ancaman siber yang semakin canggih. Kebocoran ini membuka celah bagi eksploitasi oleh aktor-aktor yang berniat jahat, baik domestik maupun internasional.

Bjorka, sosok misterius yang mengklaim bertanggung jawab atas kebocoran data tersebut, berhasil mengunggah 44.237.264 baris data dengan total ukuran mencapai 30GB (Septiani, 2022). Hal ini bukan sekadar pelanggaran data, tetapi juga sebuah serangan terhadap kedaulatan digital Indonesia yang membutuhkan respons lintas sektoral dan segera.

Penelitian ini berfokus pada insiden kebocoran data MyPertamina dan menganalisisnya dalam konteks kejahatan siber kontemporer. Penelitian ini tidak hanya bertujuan untuk mengungkap pola-pola baru dalam kejahatan siber, tetapi juga untuk mengidentifikasi kelemahan dalam sistem keamanan siber Indonesia dan merumuskan strategi mitigasi yang lebih efektif dan adaptif.

Rumusan masalah dalam penelitian ini difokuskan pada tiga pertanyaan utama terkait dengan kebocoran data MyPertamina pada Mei 2023. Pertama, penelitian ini akan mengidentifikasi karakteristik dan modus operandi kejahatan siber dalam insiden tersebut, serta menganalisis bagaimana hal ini mencerminkan evolusi ancaman siber di Indonesia. Kedua, penelitian akan mengeksplorasi sejauh mana kebijakan dan kerangka hukum Indonesia dapat merespons ancaman siber yang terus berkembang. Ketiga, penelitian akan menganalisis implikasi jangka panjang insiden ini terhadap kepercayaan publik dan stabilitas ekonomi digital nasional.

Tujuan penelitian ini adalah untuk menganalisis faktor-faktor penyebab kebocoran data MyPertamina, termasuk kelemahan teknis dan kebijakan yang tidak memadai. Penelitian ini juga akan mengevaluasi efektivitas respons institusional terhadap insiden tersebut dan mengidentifikasi area yang perlu perbaikan. Selain itu, penelitian ini bertujuan untuk merumuskan rekomendasi kebijakan untuk memperkuat ketahanan siber Indonesia dalam menghadapi ancaman yang semakin kompleks. Dengan pemahaman lebih mendalam tentang kejahatan siber dan kelemahan kebijakan yang ada, diharapkan penelitian ini dapat membantu mengembangkan langkah-langkah pencegahan yang lebih efektif dan adaptif di masa depan.

Keamanan siber kini telah menjadi isu geopolitik yang menghubungkan teknologi, ekonomi, dan politik. Sebagai bagian dari ancaman transnasional, kejahatan siber memiliki potensi untuk menggoyahkan fondasi kestabilan global. Dalam konteks ini, kasus MyPertamina tidak hanya dapat dilihat sebagai sebuah insiden terisolasi, tetapi juga sebagai sebuah alarm yang menandakan adanya kerentanan yang lebih besar dalam ekosistem digital Indonesia. Oleh karena itu, analisis kriminologi terhadap insiden ini memiliki urgensi yang sangat tinggi, tidak hanya untuk merespons ancaman yang ada, tetapi juga untuk merumuskan kebijakan yang lebih adaptif. Di tingkat internasional, kasus ini memberikan gambaran tentang tantangan yang dihadapi oleh negara-negara berkembang dalam membangun ketahanan siber. Dengan sifatnya yang transnasional, kejahatan siber memerlukan kolaborasi global untuk menghadapinya. Penelitian ini, dengan fokus pada kasus MyPertamina, memiliki potensi untuk memberikan kontribusi dalam diskursus global mengenai tata kelola keamanan siber, serta memperkuat pemahaman akan pentingnya kolaborasi internasional dalam memerangi ancaman siber lintas batas.

Kejahatan siber kini lebih dari sekadar ancaman teknologi, yang menjadi instrumen dalam perang asimetris yang dapat meruntuhkan stabilitas politik, ekonomi, dan sosial di berbagai negara. Indonesia, sebagai salah satu episentrum serangan siber di Asia Tenggara, harus segera menanggapi tantangan ini dengan respons yang lebih strategis, holistik, dan berbasis data. Kasus MyPertamina harus dijadikan pelajaran berharga untuk menyusun kebijakan yang dapat memperkuat ketahanan siber nasional, serta untuk membuka ruang bagi pembaruan dan reformasi dalam pengelolaan infrastruktur kritis digital negara. Dengan pemahaman yang mendalam dan langkah-langkah yang tepat, Indonesia dapat menjaga kedaulatan digitalnya di tengah ancaman siber global yang terus berkembang.

TINJAUAN PUSTAKA

Keberadaan kejahatan siber dalam konteks global dan nasional kini semakin mengemuka sebagai salah satu tantangan utama dalam era digital. Kejahatan ini tidak hanya mengancam keamanan dunia maya, tetapi juga stabilitas ekonomi global dan kedaulatan negara. Di tengah dinamika yang berkembang pesat, teori-teori kriminologi perlu beradaptasi untuk memahami fenomena kejahatan yang beroperasi di ruang maya, yang berbeda secara substansial dengan kejahatan tradisional. Transformasi ini tidak hanya mencakup pengembangan teori, tetapi juga penerapan teori yang relevan dalam menjelaskan pola dan motivasi pelaku kejahatan di dunia maya.

Teori-teori kriminologi yang sebelumnya diterapkan dalam dunia fisik kini telah menemukan relevansinya dalam dunia maya. Salah satu kontribusi besar dalam hal ini adalah teori ruang siber yang diajukan oleh Djanggih & Qamar (2018), yang menggambarkan ruang siber sebagai "tempat tanpa tempat". Dalam konteks ini, dunia maya tidak terikat oleh batas geografis atau waktu, menciptakan lingkungan yang sangat menguntungkan bagi pelaku kejahatan. Anonimitas yang diberikan oleh dunia maya memungkinkan pelaku kejahatan untuk beroperasi tanpa takut terdeteksi. Hal ini disebabkan oleh tidak adanya pengawasan fisik yang ketat, yang seharusnya ada dalam ruang fisik. Sebagai contoh, dalam studi Djanggih dan Qamar (2018), mereka juga menegaskan bahwa dunia maya memberi kesempatan besar bagi aktor-aktor kriminal untuk beroperasi tanpa adanya penghalang geografis atau hukum yang ketat, yang semakin mempersulit penegakan hukum.

Di sisi lain, teori aktivitas rutin yang dikembangkan oleh Cohen & Felson (1979) juga telah beradaptasi dengan keadaan dunia maya. Teori ini menjelaskan bahwa kejahatan terjadi ketika ada konvergensi antara pelaku yang termotivasi, target yang rentan, dan tidak adanya penjaga yang efektif. Dalam konteks dunia maya, konvergensi ini terjadi melalui akses mudah terhadap data pribadi dan kelemahan sistem keamanan yang ada. Anshori (2021) mengungkapkan bahwa kondisi-kondisi ini menciptakan "keadaan ideal" untuk terjadinya kejahatan siber, terutama dalam hal pencurian data pribadi, yang menjadi salah satu modus operandi yang paling sering ditemui dalam kejahatan dunia maya.

Pencurian data pribadi merupakan fenomena yang semakin mendapat perhatian serius dalam diskursus keamanan siber global. Reynolds (2023) mengungkapkan bahwa pencurian identitas, salah satu bentuk pencurian data pribadi, mempengaruhi hampir 1 dari 10 orang dewasa setiap tahunnya, menandakan skala masalah ini. Lebih dari sekadar memperoleh informasi pribadi, pencurian data kini berfungsi sebagai alat untuk eksploitasi dan monetisasi dalam ekonomi digital bawah tanah. Dalam hal ini, pelaku pencurian identitas sering kali memiliki keterampilan teknis tinggi, yang memungkinkan mereka untuk menutupi jejak mereka dan menghindari deteksi. Daripada itu, pelaku kejahatan ini memiliki kemampuan untuk mengantisipasi risiko dan mengeksploitasi celah-celah dalam sistem keamanan yang ada (Reynolds, 2023). Fenomena ini semakin mempertegas betapa canggihnya modus operandi dalam kejahatan siber yang tidak hanya menargetkan individu, tetapi juga entitas-entitas besar, termasuk institusi pemerintah dan perusahaan swasta.

Di Indonesia, pengembangan kerangka hukum mengenai perlindungan data pribadi telah menunjukkan kemajuan yang signifikan, meskipun masih menghadapi tantangan besar dalam hal implementasi dan penegakan hukum. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menjadi langkah penting dalam upaya melindungi hak privasi warga negara di era digital (Tan et al., 2023). Undang-undang ini mencakup berbagai aspek dalam perlindungan data pribadi, dari pengumpulan hingga penggunaan data, dan mengatur hak-hak individu terhadap data pribadi mereka. Namun, sebagaimana diungkapkan oleh (Parihin, 2023), meskipun UU Perlindungan Data Pribadi memberikan dasar hukum yang cukup komprehensif, efektivitasnya dalam menghadapi ancaman siber yang terus berkembang masih perlu diuji. Penegakan hukum yang lemah, kurangnya pengawasan yang memadai, serta kesadaran masyarakat yang rendah menjadi beberapa faktor yang menghambat keberhasilan implementasi UU tersebut.

Studi-studi terdahulu mengenai kebocoran data juga memberikan gambaran yang mempertegas betapa seriusnya ancaman ini. Penelitian yang dilakukan oleh Hammouchi *et al.* (2019) menunjukkan adanya tren peningkatan jumlah dan skala kebocoran data, terutama dalam sektor kesehatan di Amerika Serikat, yang mungkin mencerminkan potensi risiko yang sama di Indonesia. Kebocoran data yang melibatkan informasi sensitif, seperti data medis dan data pribadi lainnya, dapat berujung pada penyalahgunaan data yang merugikan individu dan masyarakat. Hammouchi et al. (2019) menganalisis lebih dari 9.000 kasus kebocoran data sejak tahun 2005 dan menemukan adanya pergeseran dalam pola peretasan data. Penelitian ini menunjukkan adaptabilitas pelaku kejahatan siber, yang terus berinovasi dan mengembangkan metode baru dalam mengeksploitasi celah-celah yang ada dalam sistem digital.

Dalam konteks Indonesia, kebocoran data yang terjadi pada aplikasi MyPertamina pada tahun 2023 menjadi contoh terbaru dan sangat signifikan dari ancaman kejahatan siber yang dihadapi. Kasus ini menggambarkan bagaimana data pribadi pengguna, yang berjumlah sekitar 21 juta orang, dapat terekspos ke pihak yang tidak bertanggung jawab, menimbulkan kerugian besar baik dari segi kepercayaan masyarakat maupun dari sisi ekonomi. Selain itu, insiden ini juga membuka celah bagi pelaku kejahatan siber untuk

mengeksploitasi kelemahan yang ada dalam pengelolaan dan perlindungan data di Indonesia. Oleh karena itu, penting untuk memahami konteks yang lebih luas dari kebocoran data ini dan merumuskan langkah-langkah kebijakan yang lebih efektif untuk memperkuat sistem perlindungan data pribadi di Indonesia.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus untuk menganalisis fenomena pencurian data pribadi di dunia maya, dengan fokus utama pada insiden kebocoran data yang terjadi pada aplikasi MyPertamina pada tahun 2023. Metode deskriptif-analitis dipilih untuk memungkinkan peneliti menggambarkan dan menganalisis dengan rinci fakta-fakta yang terkait dengan kebocoran data ini, serta untuk memahami implikasi dari insiden tersebut dalam perspektif kriminologi.

Studi ini menggunakan data sekunder yang diperoleh dari berbagai sumber seperti dokumen resmi, artikel berita, jurnal akademik, dan laporan terkait keamanan siber. Penggunaan data sekunder memungkinkan triangulasi sumber untuk memastikan validitas temuan yang lebih akurat dan komprehensif. Pengumpulan data dilakukan melalui studi pustaka, analisis dokumen, dan penelusuran daring, yang memungkinkan peneliti untuk mengakses informasi terkini mengenai kasus MyPertamina dan tren kejahatan siber lainnya.

Metode analisis konten kualitatif digunakan untuk menganalisis data yang terkumpul. Tahapan analisis ini melibatkan pengkodean, penyajian data, dan penarikan kesimpulan yang memungkinkan peneliti untuk menghasilkan interpretasi mendalam terhadap temuan yang ada. Dengan demikian, penelitian ini tidak hanya akan memberikan wawasan yang mendalam tentang kejahatan siber di Indonesia, tetapi juga memberikan rekomendasi kebijakan untuk memperkuat ketahanan siber negara. Melalui pendekatan ini, diharapkan penelitian ini dapat memberikan sumbangan penting bagi pengembangan kebijakan keamanan siber yang lebih efektif dan responsif, serta mengarah pada langkah-langkah yang lebih komprehensif dalam menghadapi ancaman kejahatan siber yang semakin canggih dan merugikan.

HASIL DAN PEMBAHASAN

Analisis Kasus MyPertamina

Pada 10 November 2022, Indonesia diguncang oleh insiden kebocoran data berskala besar yang melibatkan aplikasi MyPertamina. Seorang hacker yang mengaku bernama Bjorka mengklaim berhasil mengakses dan membocorkan lebih dari 44 juta data pengguna aplikasi tersebut (Damar, 2022). Klaim ini pertama kali muncul melalui unggahan di forum breached.to, sebuah platform yang sering digunakan oleh para peretas untuk memperdagangkan data yang dicuri (Antara, 2022). Insiden ini bukan hanya memperlihatkan kerentanan mendalam dalam infrastruktur digital nasional, tetapi juga mengungkapkan betapa rapuhnya perlindungan data pribadi warga negara di era digital. Kejadian ini memperlihatkan bagaimana ancaman kejahatan siber kini telah melampaui

batas konvensional dan bertransformasi menjadi ancaman terhadap kedaulatan digital nasional.

Skala kebocoran data yang terjadi pada MyPertamina sangat mengkhawatirkan. Data yang bocor melibatkan lebih dari 44 juta baris data, dengan total ukuran mencapai 30 gigabyte dalam keadaan tidak terkompresi (Antara, 2022). Data ini termasuk informasi sensitif, seperti nomor induk kependudukan (NIK), nomor pokok wajib pajak (NPWP), nomor telepon, dan data transaksi BBM, yang berpotensi disalahgunakan untuk berbagai kejahatan, mulai dari pencurian identitas hingga penipuan keuangan.

Tabel 2: Jenis Data yang Bocor dan Potensi Penyalahgunaan

Jenis Data	Potensi Penyalahgunaan
Nama Lengkap	Pencurian identitas, penipuan
Email	Phishing, spam
NIK	Pemalsuan dokumen, pembukaan rekening palsu
NPWP	Penipuan pajak, pencucian uang
Nomor Telepon	Social engineering, penipuan via SMS
Alamat	Stalking, pengiriman barang ilegal
Tanggal Lahir	Pencurian identitas, penipuan
Jenis Kelamin	Profiling untuk kejahatan yang ditargetkan
Data Penghasilan	Pemerasan, penargetan korban berdasarkan status ekonomi
Data Transaksi BBM	Analisis pola konsumsi untuk kejahatan ekonomi

Bocornya data pribadi ini bukan hanya ancaman langsung bagi individu, tetapi juga berpotensi menimbulkan ketidakstabilan ekonomi digital nasional. Sebab, data sensitif yang mengalir bebas di dunia maya memberikan peluang besar bagi pelaku kejahatan siber untuk mengeksploitasi dan memanipulasi informasi yang dapat merugikan korban secara jangka panjang.

Tanggapan terhadap insiden kebocoran data ini terkesan reaktif dan tidak memadai. PT Pertamina (Persero) dan Telkom segera melakukan investigasi untuk memverifikasi keamanan data MyPertamina, namun langkah-langkah yang diambil masih terlalu lambat dan reaktif setelah insiden tersebut terjadi (Putri, 2022). Kementerian Komunikasi dan Informatika (Kominfo) juga turut serta dalam penyelidikan dan memberikan peringatan kepada penyedia aplikasi untuk mematuhi standar keamanan data nasional (Septiani, 2022). Meskipun demikian, respons ini terlambat diambil mengingat besarnya kerusakan yang telah terjadi dan urgensi dalam menjaga data sensitif pengguna.

Faktor Kriminogenik

Motivasi di balik serangan siber yang dilakukan oleh Bjorka menunjukkan kompleksitas yang lebih dalam daripada sekadar keuntungan finansial. Berdasarkan analisis, tindakan Bjorka dapat dipahami sebagai bentuk protes terhadap lemahnya sistem keamanan siber nasional dan ketidaktransparanannya dalam pengelolaan data warga (Putri & Hidayat, 2022). Hal ini sesuai dengan teori kriminologi yang diungkapkan oleh Garcia (2015), yang menekankan bahwa dunia maya menyediakan ruang baru bagi ekspresi ketidakpuasan sosial dan politik yang seringkali melampaui motif keuntungan pribadi. Dalam konteks ini, pelaku kejahatan siber seperti Bjorka mungkin beroperasi

dengan agenda yang lebih luas, yakni untuk menunjukkan kelemahan dan ketidakberdayaan negara dalam menjaga kedaulatan digital.

Keberhasilan Bjorka dalam mengakses data MyPertamina dapat dijelaskan dengan teori *Routine Activity Theory* yang dikembangkan oleh Cohen dan Felson (1979). Menurut teori ini, kejahatan terjadi akibat konvergensi antara tiga elemen: pelaku yang termotivasi, target yang menarik, dan ketiadaan penjaga yang efektif. Dalam konteks kejahatan siber ini, data sensitif yang tidak terlindungi dengan baik menjadi target yang sangat menarik bagi pelaku. Ketiadaan pengamanan yang memadai, serta lemahnya sistem keamanan di sektor-sektor strategis, menciptakan peluang bagi pelaku untuk melakukan serangan yang berpotensi merusak. Keberhasilan serangan ini menunjukkan kerentanannya sistemik yang harus segera diatasi dengan peningkatan sistem pertahanan yang lebih efektif.

Salah satu faktor yang memperburuk situasi adalah ketimpangan sosial dan ekonomi yang masih luas di Indonesia. Kesenjangan digital yang ada memperparah kurangnya kesadaran masyarakat mengenai pentingnya keamanan data pribadi (Latifa, 2024). Terlebih lagi, tingkat literasi digital yang rendah di kalangan sebagian besar masyarakat Indonesia menjadikan mereka sasaran empuk bagi pelaku kejahatan siber. Ketidakmerataan akses terhadap pendidikan digital dan infrastruktur teknologi yang memadai semakin memperburuk situasi ini, sehingga meningkatkan kerentanannya terhadap eksploitasi.

Implikasi Kriminologis

Dampak dari kebocoran data MyPertamina sangat luas dan multidimensional. Selain potensi kerugian finansial langsung, yang dapat timbul dari penipuan dan pencurian identitas, korban juga menghadapi dampak jangka panjang berupa pelanggaran privasi yang lebih mendalam. Lebih jauh lagi, penyalahgunaan data pribadi untuk tujuan kriminal di masa depan dapat menciptakan trauma berkepanjangan bagi korban. Penelitian Deliema *et al.* (2021) menunjukkan bahwa korban pencurian identitas sering kali mengalami dampak psikologis yang signifikan, termasuk stres, kecemasan, dan hilangnya rasa aman.

Penegakan hukum dalam kasus kebocoran data ini menghadapi tantangan besar. Kejahatan siber memiliki sifat transnasional yang mempersulit investigasi dan penuntutan pelaku. Di samping itu, keterbatasan sumber daya yang dimiliki oleh aparat penegak hukum, terutama dalam bidang forensik digital, menjadi penghalang besar dalam proses penyelidikan dan penuntutan yang efektif (Rizky *et al.*, 2024). Tidak hanya itu, kerangka hukum yang ada, seperti UU Perlindungan Data Pribadi yang baru disahkan, masih perlu diuji efektivitasnya dalam menghadapi kejahatan siber yang terus berkembang (Soleh & Tjenreng, 2025).

Tabel 3: Perbandingan Kasus Kebocoran Data di Indonesia (2020-2023)

Tahun	Kasus	Jumlah Data Bocor	Jenis Data	Dampak
2020	Tokopedia	91 juta	Email, nama, nomor telepon	Potensi phishing massal

2021	BPJS Kesehatan	279 juta	NIK, data kesehatan	Risiko penyalahgunaan data medis
2022	MyPertamina	44 juta	NIK, NPWP, data transaksi	Ancaman keamanan ekonomi
2023	Dukcapil	337 juta	Data kependudukan	Risiko pencurian identitas skala besar

(Hasil diolah dari Tokopedia, BPJS Kesehatan, MyPertamina, Dukcapil Tahun 2020-2023)

Kasus kebocoran data MyPertamina menandai pergeseran signifikan dalam pola kejahatan siber di Indonesia. Kejahatan siber yang sebelumnya didominasi oleh aksi sporadis dan skala kecil kini bergeser menjadi serangan terorganisir yang menargetkan infrastruktur kritis nasional. Pola ini mencerminkan evolusi kemampuan pelaku kejahatan siber dan semakin meningkatnya nilai strategis data dalam lanskap geopolitik yang semakin kompetitif (Soleh & Tjenreng, 2025). Hal ini menandakan bahwa kejahatan siber kini bukan hanya ancaman terhadap individu, tetapi juga terhadap kestabilan nasional dan internasional.

Strategi Pencegahan dan Mitigasi

Strategi pencegahan kejahatan situasional menjadi sangat penting dalam konteks keamanan siber. Dengan mengidentifikasi dan menghilangkan peluang bagi terjadinya kejahatan, seperti memperkuat protokol autentikasi, menerapkan enkripsi *end-to-end*, dan melakukan audit keamanan secara berkala, Indonesia dapat mengurangi peluang bagi pelaku untuk melakukan kejahatan siber. Implementasi prinsip *"security by design"* dalam setiap aplikasi dan sistem informasi akan memperkuat pertahanan terhadap serangan yang mungkin terjadi.

Strategi pencegahan kejahatan situasional harus menjadi prioritas utama dalam memperkuat keamanan siber di Indonesia. Dengan mengidentifikasi dan menghilangkan peluang yang dapat dimanfaatkan oleh pelaku kejahatan siber, langkah-langkah preventif dapat diambil untuk memperkecil ruang gerak mereka. Misalnya, memperkuat protokol autentikasi dan menerapkan enkripsi *end-to-end* pada setiap saluran komunikasi akan mengurangi kemungkinan akses yang tidak sah. Selain itu, audit keamanan secara berkala juga penting untuk memastikan bahwa setiap sistem yang digunakan tetap aman dan tidak ada celah yang dapat dimanfaatkan. Prinsip *"security by design"* dalam pengembangan aplikasi dan sistem informasi perlu diterapkan sejak awal untuk memastikan bahwa dari tahap desain, keamanan sudah menjadi bagian integral, sehingga setiap sistem yang diluncurkan sudah siap untuk menghadapi serangan siber.

Selain itu, peningkatan keamanan siber harus dipandang sebagai agenda nasional yang melibatkan berbagai elemen di masyarakat. Investasi dalam teknologi keamanan canggih dan pengembangan kapasitas untuk mendeteksi serangan siber lebih awal menjadi hal yang mutlak dilakukan. Kapabilitas respons yang cepat terhadap ancaman juga harus menjadi fokus, dengan memanfaatkan kecerdasan buatan dan sistem analitik

untuk mengidentifikasi potensi serangan sebelum dampaknya dirasakan. Kolaborasi antara sektor publik dan privat dalam berbagi informasi mengenai ancaman siber juga sangat penting untuk menciptakan ekosistem yang lebih tangguh. Pembentukan tim khusus yang terdiri dari ahli keamanan siber, kriminolog, dan pembuat kebijakan akan membantu merumuskan kebijakan dan respons yang lebih komprehensif dan adaptif dalam menghadapi ancaman yang semakin kompleks.

Namun, dalam menghadapi tantangan ini, literasi digital yang kuat di kalangan masyarakat juga tak kalah penting. Program edukasi publik yang menyeluruh, baik di sektor formal maupun informal, harus digalakkan untuk meningkatkan pemahaman tentang pentingnya perlindungan data pribadi dan langkah-langkah pencegahan kejahatan siber. Kampanye kesadaran yang berkelanjutan akan membantu menciptakan budaya keamanan siber yang lebih baik, sehingga masyarakat lebih waspada dan siap menghadapi ancaman. Selain itu, penguatan regulasi di bidang keamanan siber dan perlindungan data pribadi juga harus diperkuat. Implementasi yang efektif dari Undang-Undang Perlindungan Data Pribadi, serta pembentukan lembaga pengawas independen yang memiliki kewenangan untuk mengawasi dan menindak pelanggaran, akan memastikan bahwa kebijakan berjalan sesuai dengan tujuan dan dapat beradaptasi dengan cepat terhadap dinamika teknologi dan ancaman siber yang terus berkembang.

KESIMPULAN

Penelitian ini telah mengungkapkan temuan penting mengenai kebocoran data pengguna aplikasi MyPertamina pada tahun 2023, yang lebih dari sekadar kegagalan teknis. Insiden ini mencerminkan kerentanan sistemik dalam pengelolaan data pribadi di Indonesia, di mana faktor-faktor kriminogenik seperti motivasi pelaku, kerentanan sistem, dan ketimpangan sosial-ekonomi turut berkontribusi terhadap terjadinya kebocoran data berskala besar. Penelitian ini juga menunjukkan bahwa meskipun upaya investigasi dan penindakan telah dilakukan oleh pemerintah dan lembaga terkait, masih ada kekurangan dalam implementasi kebijakan keamanan siber yang efektif, serta respons yang belum cukup cepat dan adaptif terhadap ancaman siber yang terus berkembang. Kejadian ini menyoroti perlunya perbaikan signifikan dalam manajemen data dan kebijakan keamanan nasional.

Secara teoretis, penelitian ini memperkaya pemahaman tentang penerapan teori kriminologi klasik, seperti teori ruang siber dan teori aktivitas rutin, dalam menjelaskan fenomena kejahatan siber. Pendekatan-pendekatan tersebut memberikan kerangka analitis yang berguna untuk memahami kompleksitas kejahatan di dunia maya. Praktiknya, penelitian ini menekankan pentingnya penguatan infrastruktur keamanan siber nasional, termasuk penerapan pendekatan situasional, peningkatan kesadaran publik, dan penguatan regulasi, serta implementasi efektif UU Perlindungan Data Pribadi. Langkah-langkah ini, termasuk pembentukan lembaga pengawas independen, menjadi krusial dalam memperkuat ketahanan siber nasional, yang pada gilirannya akan melindungi kepentingan warga negara di era digital yang semakin terhubung ini.

DAFTAR REFERENSI

Anshori, A. (2021). CYBER CRIME IN A CRIMINOLOGY PERSPECTIVE. *INTERNATIONAL JOURNAL OF SOCIAL, POLICY AND LAW*, *2*(3 SE-), 120–125. https://doi.org/10.8888/ijospl.v2i3.107

Antara. (2022, November 10). Pakar Siber Bilang Bjorka Bocorkan 44 Juta Data MyPertamina. *Tempo.Co*. https://www.tempo.co/hukum/pakar-siber-bilang-bjorka-bocorkan-44-juta-data-mypertamina-258656

Chin, K. (2025, January 5). *The impact of cybercrime on the economy*. UpGuard.Com. https://www.upguard.com/blog/the-impact-of-cybercrime-on-the-economy

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach (1979). In *Classics in environmental criminology* (pp. 203–232).

Damar, A. M. (2022, November 10). Bjorka Muncul Lagi, Klaim Bobol 44 Juta Data MyPertamina. *Liputan6.Com*. https://www.liputan6.com/tekno/read/5121753/bjorka-muncul-lagi-klaim-bobol-44-juta-data-mypertamina

Deliema, M., Langton, L., & Brunes, D. (2021). *WI21-11: Consequences and Response to Identity Theft Victimization among Older Americans*.

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta*, *13*(1), 10–23. https://doi.org/10.15294/pandecta.v13i1.14020

Garcia, S. (2015). *Can Cyberactivism Effectuate Global Political Change?*

Hammouchi, H., Cherqi, O., Mezzour, G., Ghogho, M., & Koutbi, M. El. (2019). Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time. *Procedia Comput. Sci.*, *151*, 1004–1009. https://doi.org/10.1016/j.procs.2019.04.141

Kristianti, L. (2023, January 19). BSSN ungkap serangan keamanan siber di 2022 turun dibanding 2021. *Antaranews.Com*. https://www.antaranews.com/berita/3356178/bssn-ungkap-serangan-keamanan-siber-di-2022-turun-dibanding-2021

Latifa, N. R. (2024). *Mencegah Data Breach: Strategi untuk Hindari Kebocoran Data*. SiberMate. https://sibermate.com/hrmi/mencegah-data-breach-strategi-untuk-hindari-kebocoran-data

ManageEngine. (2025, January 15). *6+ Tren Cybersecurity 2025 di Indonesia yang Wajib Anda Ketahui*. Blogs.Manageengine.Com. https://blogs.manageengine.com/indonesia/2025/01/15/tren-cybersecurity-di-indonesia-yang-wajib-anda-ketahui.html

Parihin, N. mardiana. (2023). Urgensi Perlindungan Data Pribadi Dalam Perpektif Hak Asasi Manusia. *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia*, *5*(1 SE-Artikel). https://doi.org/10.52005/rechten.v5i1.108

Pichurov, T. (2025, January 29). *The top 37 cyber crime statistics you need to know in 2025*. SpyHunter.Com; EnigmaSoftware Ltd. https://www.spyhunter.com/shm/cyber-crime-statistics/

Putri, R. S. (2022, November 10). 44 Juta Data My Pertamina Diduga Dibobol Bjorka, Pertamina Gelar Investigasi. *Tempo.Co*. https://www.tempo.co/ekonomi/44-juta-data-my-pertamina-diduga-dibobol-bjorka-pertamina-gelar-investigasi-258926

Putri, R. S., & Hidayat, A. A. N. (2022). *Ekonom Usul Aplikasi MyPertamina Terkoneksi dengan Data Kemensos agar Subsidi Tepat Sasaran*. https://www.tempo.co/ekonomi/ekonom-usul-aplikasi-mypertamina-terkoneksi-dengan-data-kemensos-agar-subsidi-tepat-sasaran-329630

Reynolds, D. (2023). Identity theft. In *Oxford Research Encyclopedia of Criminology and Criminal Justice*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190264079.013.797

Rizky, L. R. N., Maulidia, S., Kusniatin, N. T., Alfarizi, R., Klaping, C. R., Hidayatullah, Q., Manurung, D. A., Akbar, T. F., Satria, M., & Putra, A. H. (2024). EDUKASI PELAJAR TENTANG KEAMANAN CYBER DAN PERLINDUNGAN DATA PRIBADI. *AJP*, *3*(2), 60–64. http://jurnal.portalpublikasi.id/index.php/AJP/article/view/1549

Septiani, L. (2022, November 11). Ahli IT Sebut Data Aplikasi MyPertamina yang Dibocorkan Bjorka Valid. *Katadata.Co.Id*. https://katadata.co.id/digital/teknologi/636dcfe83c9b3/ahli-it-sebut-data-aplikasi-mypertamina-yang-dibocorkan-bjorka-valid

Soleh, M., & Tjenreng, Z. (2025). Strategi Pencegahan Kebocoran Data Pelayanan Publik Di Era Digital. *Jurnal Kajian Pemerintah: Journal of Government, Social and Politics*, *11*(1), 1–10.

Tan, S., Alexander, C., & Tantimin, T. (2023). An Academic Analysis of Data Privacy Frameworks in Indonesia. *Barelang Journal of Legal Studies*, *1*(1), 72–89.