



Landasan Hukum Keamanan Perlindungan Data Pribadi Dalam Mendukung Ketahanan Nasional

Rivan Achmad Purwantono

Universitas Islam Sultan Agung, Indonesia

Email: rivantono@gmail.com

**Correspondence: Rivan Achmad Purwantono*

Article Info:

Submitted:

17-02-2025

Final Revised:

24-04-2025

Accepted:

28-04-2025

Published:

28-04-2025

ABSTRAK

Perkembangan pesat teknologi informasi dan internet telah mendorong perubahan besar dalam masyarakat dan ekonomi digital. Namun, perkembangan ini juga membawa potensi risiko besar, termasuk kejahatan siber, peretasan data pribadi, dan ancaman terhadap kedaulatan negara. Penelitian ini bertujuan untuk menganalisis efektivitas implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi di Indonesia dalam menghadapi ancaman kejahatan siber. Metode yang digunakan adalah penelitian yuridis normatif dengan pendekatan kualitatif, menganalisis data sekunder yang bersumber dari peraturan perundang-undangan dan literatur terkait. Hasil penelitian menunjukkan bahwa meskipun sudah ada regulasi yang mengatur perlindungan data pribadi, implementasinya masih belum optimal. Pengawasan dan penegakan hukum yang lemah serta terbatasnya edukasi kepada masyarakat menyebabkan maraknya pelanggaran data pribadi. Penelitian ini mengungkapkan perlunya perbaikan sistem pengawasan, peningkatan kerjasama antar lembaga pemerintah, serta penguatan kebijakan perlindungan data yang lebih komprehensif. Implikasi dari penelitian ini adalah pentingnya kebijakan yang lebih efektif dalam mengatasi kejahatan siber, melindungi data pribadi, dan menjaga ketahanan nasional dalam menghadapi ancaman global yang terus berkembang.

Kata kunci: Kejahatan Siber, Perlindungan Data.

ABSTRACT

The rapid development of information technology and the internet has driven significant changes in society and the digital economy. However, this advancement also brings major risks, including cybercrimes, data breaches, and threats to national sovereignty. This study aims to analyze the effectiveness of the implementation of Law Number 27 of 2022 on Personal Data Protection in Indonesia in addressing cybercrime threats. The method used is a juridical-normative approach with a qualitative analysis of secondary data sourced from relevant laws and literature. The results indicate that although regulations on personal data protection are in place, their implementation remains suboptimal. Weak enforcement, limited public education, and inadequate monitoring have led to frequent data breaches. This study reveals the need for improved monitoring systems, enhanced inter-agency collaboration, and stronger policies for comprehensive data protection. The implications of this study highlight the need for more effective policies to tackle cybercrime, protect personal data, and safeguard national resilience against the growing global threats.

Keywords: Cyber Crime, Data Protection.

PENDAHULUAN

Saat ini, perhatian terhadap perlindungan data pribadi semakin meningkat di tingkat nasional, regional, dan internasional. Dunia telah memasuki era ekonomi digital dengan hadirnya teknologi digital, internet, *big data*, *Artificial Intelligence*, 5G (Afonasova et al., 2019). Ekonomi digital diperkirakan mencapai pertumbuhan tahunan dua (2) digit di seluruh Dunia (*World Economic Forum*, 2015). Ekonomi Digital sebagai ‘struktur yang kompleks’ (Bukht dan Heeks, 2017) sepakat dengan para ahli sebagai penggunaan alat – alat digital pada ekonomi digital. Pentingnya ekonomi digital menurut Bank Dunia East (2015) menyumbang 15,5% dari Produk Domestik Bruto Global. Di Indonesia sendiri ekonomi internet Indonesia diperkirakan akan mencapai 146\$ pada tahun 2025 dan 330\$ miliar pada tahun 2030.

Sebagaimana ditulis *Lon Fuller* dalam *The Morality of Law* (Edwin, 1965) menceritakan penguasa muda yang mencoba mereformasi hukum negara berhadapan dengan ketidakpuasan masyarakat yang menjadikan pengabaian undang – undang (aturan hukum) untuk membatalkan kewenangan penguasa. Karena ketika memerintah tapi tidak dapat melakukan tindakan hanya akan menimbulkan kebingungan, ketakutan dan kekacauan. Pemerintah harus dapat menyesuaikan aturan hukum dengan perkembangan yang terjadi pada masyarakatnya sesuai dengan adagium “*ubi societas ibi ius*” ungkapan *Cicero Arthadana* (2023) yang terkenal bahwa “*dimana ada masyarakat disitu ada hukum*”.

Organisasi internasional dan regional telah mengeluarkan rekomendasi bagi anggotanya (*member state*) seperti ASEAN / Perhimpunan Bangsa – Bangsa Asia Tenggara yang mengeluarkan Kerangka Perlindungan Data Pribadi yang diadopsi Menteri dan Teknologi Informasi (termasuk Indonesia). Peraturan yang dikembangkan sebagai bagian dari perlindungan data pribadi diharapkan berkembang secara eksponensial mengikuti peningkatan produksi dan agregasi data. Hal ini bisa terjadi karena adanya: a) kaburnya perbedaan realitas dan virtualitas; b) perbedaan antara manusia, mesin dan alam; c) pembalikan kelangkaan informasi menjadi keberlimpahan informasi; d) pergeseran keutamaan benda, properti fisik, dan relasi oposisi biner menjadi keutamaan interaksi proses dan jaringan (Floridi, 2015). Hal ini membawa perlindungan dan perspektif hukum melampaui berbagai dimensi dan perkembangan masyarakat yang kita hadapi saat ini.

Kehebohan Kasus pembobolan data pribadi telah terjadi di banyak negara, misalnya pada tahun 2018 di Inggris terdapat kasus peretasan data sekitar 420.000 staf dan pelanggan di website *British Airways*. Terakhir, *British Airways* didenda oleh Kantor Komisaris Informasi Inggris (ICO) sebesar 20 juta pound karena gagal memberikan perlindungan terhadap data pribadi (*British Airways Menyelesaikan Korban Pelanggaran Data 2018*, Reuters, 2018) Kasus besar juga pernah terjadi di India pada awal tahun 2018, yaitu peretasan database ID terbesar di dunia, *Aadhaar*, berupa informasi lebih dari 1,1 miliar warga India termasuk nama, alamat, foto, nomor telepon, dan email. serta data biometrik seperti sidik jari dan pemindaian iris mata. Basis data juga berisi informasi tentang rekening bank yang terhubung dengan 12 digit unik (15 Pelanggaran Data Terbesar Abad 21 | *CSO Online*)

Data dari Konferensi PBB tentang Perdagangan dan Pembangunan menunjukkan bahwa data pribadi tidak dilindungi di sepertiga negara di dunia terjadi meskipun sudah terdapat perkembangan (Data dan Privasi Tidak Dilindungi di Sepertiga Negara, meskipun Ada Kemajuan | UNCTAD). 137 dari 194 negara telah menerapkan undang-undang untuk menjamin perlindungan data dan privasi. Sebanyak 61 persen negara-negara Afrika dan 57 persen negara-negara Asia telah mengadopsi undang-undang tersebut (Perlindungan Data dan Legislasi Privasi Seluruh Dunia | UNCTAD). Sementara di negara-negara kurang berkembang hanya 48 persen yang mengadopsinya, Indonesia termasuk telah mengadopsi undang-undang ini pada tahun 2022.

Tiongkok sendiri sebagai salah satu negara maju pada tanggal 10 September 2018, Komite Tetap Kongres Rakyat Nasional ke-13 (NPCSC) telah memasukkan Undang – Undang Perlindungan Data Pribadi sebagai bagian dari Prolegnasnya dan sudah menjadi konsensus di antara pemimpin Tiongkok. Penelitian empiris yang ada di Tiongkok telah memberikan perhatian terhadap perlindungan data yang semakin meningkat salah satu contohnya adalah pada topik tertentu seperti *Great Firewall Tiongkok*, sistem pendaftaran nama asli dan undang – undang Keamanan Siber (Lee & Liu, 2016).

Urgensi Undang – Undang Perlindungan Data Pribadi juga dirasakan Pemerintahan Malaysia yakni dengan pengesahan Undang – Undang Perlindungan Data Pribadi Malaysia pada tahun 2010 (Munir dan Asemi, 2021). Nilai, sensitivitas dan bahaya informasi pribadi seperti data keuangan meningkat secara luar biasa. Data dari JP Morgan Chase & Co, Bank Multinasional dan jasa keuangan terbesar yang berkantor di New York, Amerika Serikat mengatakan lebih dari 76 juta rumah tangga dan 7 juta usaha kecil dicuri oleh para peretas (*hacker*).

Ibaratnya dunia sekarang ini telah mengalami konektivitas dan arus data global yang belum pernah terjadi sebelumnya akibat akses, penggunaan, dan pertukaran data lintas batas untuk mendorong pertumbuhan ekonomi sehingga memungkinkan perusahaan global, skala usaha kecil, dan wirausaha berpartisipasi dalam satu pasar global yang saling terhubung. Aliran data (termasuk biaya transaksi dan kendala jarak) mempersingkat penyebaran ide / aliran data global yang meningkatkan Produk Domestik Bruto Global setara dengan \$2,8 Triliun (Manyika et al., 2016).

Pengungkapan seorang tokoh terkenal Edward Snowden mengenai program pengawasan kontra-terorisme Amerika Serikat dan pelanggaran data *Cambridge Analytica* menimbulkan kekhawatiran yang semakin besar terkait perlindungan data pribadi (Sargsyan, 2016). Beberapa negara berusaha untuk melakukan lokalisasi data (pengumpulan, pemrosesan, dan penyimpanan data warga negara atau penduduk) dalam batas wilayah suatu negara (Burman & Sharma, 2021). Hal ini seperti juga dilakukan oleh Pemerintah Indonesia melalui Peraturan pemerintah Nomor 82 Tahun 2012 mengenai Penyelenggaraan Sistem dan Transaksi Elektronik sebagai aturan pelaksana Undang – Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik. Dorongan terhadap hal ini dilakukan untuk mencegah Badan Intelijen Asing yang berusaha untuk memata-matai server suatu negara, dan pentingnya mendorong pembangunan ekonomi dengan juga menjaga informasi pribadi, memudahkan penegakan hukum dan mengendalikan arus informasi. Ini merupakan konseptualisasi perlindungan data sebagai tindakan sekuritisasi melalui kebijakan publik di bawah suatu sistem politik pemerintahan yang mencakup perlindungan data pribadi, militer, ekonomi dan politik yang saling berkaitan. Dari sudut keamanan negara memiliki kewenangan untuk secara berdaulat dalam politik melindungi pembelian dan arus perlintasan data (keluar masuk batasan wilayahnya) dengan kerangka perlindungan data yang tepat. Sebab badan – badan intelijen asing yang terlibat juga mengawasi dan menyusup masuk ke dalam jaringan komputer negara – negara yang menjadi saingannya, sehingga serangan siber antar negara dampaknya terasa signifikan (*Council on Foreign Relations*, 2023).

Pengelolaan risiko keamanan yang berorientasi pada pengendalian bahaya atau sumber bahaya berkembang sejalan dengan adanya *International Standart Organization (ISO)* atau melalui Manajemen Risiko yang berlandaskan pada dampak ketidakpastian terhadap tujuan (ISO 31000, 2009). Hal ini dapat berdampak pada Ketahanan dan Ketangguhan yang sifatnya formal maupun operasional sebagai suatu sistem yang memberikan respon dan publik dari guncangan. Ataupun sebuah kemampuan di setiap tingkat yang relevan untuk mendeteksi, mencegah dan jika perlu menangani dan memulihkan tantangan yang mengganggu, (Adey &

Anderson, 2011). Pada tahun 2009, *Resilient Nation* memfokuskan adaptasi pada kapasitas individu, komunitas atau sistem yang beradaptasi guna mempertahankan tingkat fungsi, struktur dan identitas yang dapat diterima (Edwards, 2009). Akademi Ilmu Pengetahuan Nasional Amerika Serikat juga mengembangkan gagasan ketahanan sebagai kemampuan untuk mempersiapkan dan merencanakan, menyerap, memulihkan dan beradaptasi terhadap kejadian buruk (Academies et al., 2012). Ketahanan digambarkan juga sebagai kapasitas untuk beradaptasi terhadap perubahan kondisi tanpa kehilangan bentuk dan fungsi secara besar – besaran (Park et al., 2013).

Oleh karena pentingnya hal ini maka perlindungan data dari perspektif hukum (perlindungan data pribadi) dapat meningkatkan ekonomi digital (dan pertumbuhan ekonomi nasional), keamanan (dan ketahanan data) sebagai bagian yang kritical karena ekonomi digital menganggap keamanan data (dan khususnya data) sebagai industri minyak baru abad dua puluh satu yang menggerakkan ekonomi digital global.

Peningkatan penggunaan teknologi digital dan data besar dalam era digitalisasi ini telah menimbulkan berbagai tantangan terkait dengan perlindungan data pribadi (Aswandi et al., 2020). Kasus pencurian data yang semakin marak, seperti yang terjadi di Indonesia dan negara lainnya, menunjukkan adanya kelemahan dalam pengamanan data pribadi. Meskipun sudah ada regulasi seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, penerapan kebijakan ini belum optimal dalam memberikan perlindungan yang maksimal terhadap data pribadi masyarakat. Oleh karena itu, penting untuk mengevaluasi efektivitas perlindungan data pribadi dalam menghadapi ancaman kejahatan siber, yang semakin berkembang dengan adanya teknologi informasi yang lebih canggih.

Selain itu, masih terdapat banyak kekurangan dalam sistem perlindungan data pribadi yang ada, baik dari segi hukum, teknologi, maupun tata kelola. Meskipun sudah ada perangkat hukum yang diatur oleh pemerintah, namun implementasi pengawasan dan penegakan hukum terhadap pencurian data pribadi masih sangat lemah, sehingga menyebabkan kerugian besar bagi korban dan menurunnya kepercayaan masyarakat terhadap pengelolaan data pribadi.

Penelitian ini sangat penting mengingat tingginya angka pencurian data pribadi di Indonesia dan dunia yang menunjukkan bahwa perlindungan data pribadi belum memadai. Keamanan data pribadi tidak hanya menjadi tanggung jawab individu atau perusahaan, tetapi juga menjadi masalah yang harus ditangani oleh negara. Perlindungan data pribadi yang efektif sangat krusial untuk mendukung ketahanan nasional, di mana ancaman dari serangan siber dapat merusak stabilitas sosial dan ekonomi. Dengan meningkatnya serangan siber, perlindungan data pribadi harus menjadi prioritas dalam kebijakan negara agar dapat menjaga integritas dan keamanan data masyarakat.

Penelitian oleh Dewi (2018) mengungkapkan bahwa meskipun beberapa negara sudah mengadopsi peraturan perlindungan data pribadi, implementasi kebijakan tersebut masih sangat bervariasi. Di sisi lain, penelitian oleh Pratama & Suradi (2016) menunjukkan bahwa pengawasan dan penegakan hukum terhadap kebocoran data pribadi di Indonesia masih sangat lemah, yang mengarah pada semakin maraknya pelanggaran data. Penelitian oleh Sargsyan (2016) juga mencatat pentingnya perlindungan data pribadi dalam konteks global, terutama terhadap ancaman siber yang dapat merusak integritas data negara. Temuan ini menunjukkan bahwa meskipun perlindungan data telah diatur dalam berbagai peraturan, implementasi yang efektif dan pengawasan yang ketat masih menjadi tantangan besar.

Meskipun penelitian sebelumnya telah mengkaji perlindungan data pribadi dalam berbagai sektor, penelitian tentang implementasi Undang-Undang Perlindungan Data Pribadi di Indonesia, khususnya dalam mengatasi ancaman kejahatan siber, masih terbatas. Selain itu, penelitian yang lebih mendalam tentang pengaruh regulasi ini terhadap ketahanan nasional juga

masih minim. Oleh karena itu, penelitian ini berusaha untuk mengisi kekosongan tersebut dengan fokus pada efektivitas kebijakan perlindungan data pribadi dalam menghadapi ancaman siber di Indonesia.

Penelitian ini menawarkan kebaruan dengan mengkaji implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam konteks Indonesia, serta bagaimana kebijakan ini dapat meningkatkan ketahanan nasional terhadap ancaman siber. Penelitian ini juga menghubungkan perlindungan data pribadi dengan dampaknya terhadap sistem pemerintahan dan ekonomi digital, yang belum banyak dibahas dalam literatur yang ada.

Tujuan penelitian ini adalah untuk menganalisis implementasi Undang-Undang Perlindungan Data Pribadi di Indonesia dalam konteks ketahanan nasional serta mengevaluasi efektivitas kebijakan tersebut dalam menghadapi ancaman kejahatan siber. Penelitian ini juga bertujuan untuk memberikan rekomendasi bagi pemerintah dalam meningkatkan sistem perlindungan data pribadi di Indonesia.

Manfaat dari penelitian ini adalah memberikan kontribusi dalam pengembangan kebijakan perlindungan data pribadi yang lebih efektif di Indonesia, khususnya untuk menghadapi ancaman kejahatan siber. Penelitian ini juga memberikan wawasan bagi pemerintah dan lembaga terkait dalam merancang strategi pengamanan data pribadi yang dapat memperkuat ketahanan nasional, serta meningkatkan kepercayaan masyarakat terhadap pengelolaan data pribadi di era digital.

METODE PENELITIAN,

Metode yang digunakan dalam penelitian ini adalah penelitian hukum yuridis normatif, yaitu penelitian yang mengkaji hukum berdasarkan dokumen-dokumen hukum yang ada, baik berupa peraturan perundang-undangan, keputusan pengadilan, maupun literatur hukum lainnya. Penelitian ini bersifat deskriptif, yang bertujuan untuk menggambarkan secara rinci mengenai penerapan kebijakan perlindungan data pribadi di Indonesia dan dampaknya terhadap ketahanan nasional, khususnya dalam menghadapi ancaman serangan siber. Data yang digunakan dalam penelitian ini adalah data sekunder, yang diperoleh dari berbagai sumber seperti peraturan perundang-undangan, jurnal, artikel, serta laporan resmi terkait perlindungan data pribadi dan serangan siber di Indonesia. Selain itu, analisis yang dilakukan menggunakan pendekatan kualitatif untuk menilai efektivitas implementasi Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022 dan dampaknya terhadap keamanan data serta ketahanan nasional. Dalam hal ini, penelitian ini menganalisis literatur yang relevan serta perbandingan dengan kebijakan serupa di negara lain. Pendekatan ini memungkinkan peneliti untuk memberikan analisis komprehensif terkait tantangan, hambatan, dan rekomendasi untuk meningkatkan perlindungan data pribadi di Indonesia sebagai bagian dari upaya memperkuat ketahanan nasional terhadap ancaman kejahatan siber.

HASIL DAN PEMBAHASAN

Melonjaknya jumlah data yang disimpan dalam sistem digital akan menciptakan etika interaksi baru, sehingga penyimpanan banyak data dari pengguna akan meningkatkan efektivitas operasional bisnis, terutama untuk hal-hal yang berkaitan dengan sistem perdagangan (Hisbulloh, 2021). Perkembangan perlindungan data pribadi tidak terlepas dari perkembangan teknologi informasi dan komunikasi, termasuk internet. Meningkatnya jumlah pengguna internet, fleksibilitas akses internet, dan keterjangkauan penggunaan internet menjadi faktor pendorong meningkatnya penggunaan internet di berbagai bidang, seperti

komunikasi, hiburan, dan lain-lain. Namun perlu diingat bahwa sektor bisnis merupakan sektor yang paling maju dalam memajukan internet.

Perkembangan teknologi informasi dan komunikasi saat ini, khususnya yang dibawa oleh internet telah menciptakan perdagangan bebas dalam peradaban manusia. Perdagangan bebas dihasilkan dari proses perdagangan yang tidak terbatas tanpa mengenal batasan ruang dan waktu. Dengan kata lain, wajar jika dikatakan bahwa perdagangan bebas merupakan hasil dari perkembangan teknologi. Dalam waktu dekat, perkembangan teknologi ini akan menjadi cikal bakal munculnya e-commerce yang semakin populer di kalangan masyarakat..

Perdagangan elektronik atau online commerce yang memungkinkan pertukaran barang atau jasa secara elektronik, khususnya melalui internet, semakin populer di kalangan masyarakat. Kondisi ini terutama disebabkan karena sistem perdagangan elektronik tidak mengharuskan penjual dan pembeli bertemu langsung (tatap muka). Perdagangan online dilakukan melalui korespondensi elektronik, seperti email, fax, dan platform elektronik lainnya (Enoma, 2020). Demikian pula pembayaran juga dilakukan melalui sistem online, sehingga sistem tersebut lebih efisien dan memakan waktu lebih sedikit. Interaksi masyarakat dalam media elektronik melalui sistem digital kini telah merambah seluruh lini sektor kehidupan, seperti industri pariwisata, perdagangan (e-commerce), industri keuangan (e-Payment), transportasi, dan sektor pemerintahan (e-commerce) (Bukht & Heeks, 2017). pemerintah) (Alibeigi et al., 2021). Interaksi ini mencakup beberapa ruang lingkup antara lain penyimpanan, pengolahan, pengumpulan, pengiriman dan produksi dari dan ke industri atau masyarakat secara efektif dan cepat (Dewi, 2015).

Instrumen hukum modern untuk perlindungan data pribadi harus memenuhi tiga kriteria berikut: (1) berfungsi sebagai jembatan antara individu dan masyarakat ekonomi; (2) bersifat internasional; dan (3) mendorong masyarakat untuk mengambil bagian dalam masyarakat ekonomi digital (Dewi & Gumelar, 2018). Indonesia baru-baru ini telah menerbitkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai penegakan hukum yang memenuhi prinsip kepastian hukum terhadap segala pelanggaran terkait data pribadi (Azizah et al., 2024; Bahtiar, 2024). Lahirnya undang-undang ini antara lain disebabkan oleh banyaknya kejadian pelanggaran data pribadi dan belum adanya undang-undang yang memenuhi prinsip kepastian hukum tentang perlindungan data, yang jelas merugikan banyak pihak, seperti yang dialami salah satu e-commerce besar (Pradana, 2015).

Peretasan Tokopedia pada tahun 2020 sempat menghebohkan masyarakat karena peretasan tersebut diduga membocorkan data pribadi 91.000.000 pengguna akun untuk dijual di dark web (Wibowo et al., 2024). Web gelap mengacu pada bagian dari web dalam internet tempat data yang dicuri dari jaringan perusahaan, seperti informasi pribadi pelanggan, catatan kesehatan, dan sebagainya, dijual untuk mendapatkan keuntungan. Data pribadi pengguna akun Tokopedia yang berisi email, nomor telepon, alamat rumah, dan privasi lainnya dibocorkan ke pihak ketiga. Di bidang transportasi online, data pribadi pengguna seperti nomor telepon disalahgunakan untuk mengirimkan pesan pribadi yang tidak ada hubungannya dengan penggunaan layanan transportasi online tersebut (Pratama & Suradi, 2016). Di Indonesia, sering terjadi kebocoran data pribadi seperti yang terjadi pada sistem perbankan, dimana data pribadi nasabah sering kali dikirimkan ke sesama card center lainnya. Praktik ini memungkinkan pegawai bank memberikan informasi nasabah kartu kredit kepada pihak ketiga sebagai cara untuk mendapatkan keuntungan ekonomi melalui kebocoran data (Rosadi, 2017). Tokopedia tidak mau bertanggung jawab atas kebocoran data pribadi karena Tokopedia telah menetapkan syarat dan ketentuan yang dianggap telah dipahami dan disetujui oleh konsumen saat mendaftar dan/atau menggunakan situs www.tokopedia.com.

Peretasan data PDNS 2 (Pusat Data Nasional Sementara) yang terjadi pada bulan Juni 2024 merupakan krisis siber nasional, karena akibat dari peretasan ini data masyarakat, Kementerian/Lembaga menjadi hilang/dicuri sehingga pelayanan publik terganggu. Peristiwa ini menjadi evaluasi bagi pemerintah untuk meningkatkan manajemen krisis siber nasional dan saat ini instansi seperti Kemenkominfo dan Badan Siber dan Sandi Negara (BSSN) berupaya untuk melakukan pemulihan seperti sebelumnya dan pencegahan agar tidak berulang kembali kejadian tersebut.

Pelaku kejahatan siber ini adalah *sindikata criminal* yang bernama Brain Chipper yang mengaku meretas dan melakukan serangan ransomware *Lockbit 3.0* pada PDNS 2 (Kompas, 3 Juli 2024) untuk kemudian merilis kunci enkripsi yang telah menggembok data pemerintah, dimana sebelumnya pelaku meminta tebusan sebesar 8 juta dollar AS atau sekitar 130 Milyar.

Berdasarkan hasil Survei Penetrasi dan Perilaku Pengguna Internet Indonesia tahun 2019 sampai tahun 2020 oleh Asosiasi Pengguna Jasa Internet Indonesia (API) bahwa 73,7 persen atau sekitar 196,71 juta jiwa dari penduduk Indonesia menggunakan internet. diantaranya terdapat 12,2 persen sering menggunakan media sosial.

Negara mempunyai kewajiban untuk memenuhi (*fulfill*), menyediakan (*provide*), melayani (*service*) dan melindungi (*protect*) warga negaranya dalam konteks ancaman kejahatan siber, sehingga peran Negara sebagai pelindung dituntut hadir untuk memberikan perlindungan hukum. Menurut Setiono perlindungan hukum adalah tindakan atau upaya untuk Melindungi masyarakat dari perbuatan sewenang-wenang oleh penguasa yang tidak sesuai dengan aturan hukum. Perlindungan hukum negara juga diatur dalam pembukaan. UUD 1945 alinea IV yaitu "...Pemerintah Negara Indonesia yang melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia...".

Pemerintah saat ini sudah menerbitkan Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (selanjutnya disebut UU PDP) dengan tujuan memberikan pelindungan data pribadi sebagai salah satu hak asasi manusia yang merupakan bagian dari pelindungan diri pribadi untuk memberikan keamanan atas data pribadi berdasarkan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, namun cita-cita itu belum terwujud terbukti kejadian peretasan data pada PDNS 2 yang menjadi perhatian kita bersama.

Menurut Mansur, 2005, sebagaimana dikutip dari Ervan Yudi Widyarto dan Dita Kusuma Hapsari Politeknik Jakarta Internasional, Jakarta, salah satu modus operan di terhadap kejahatan-kejahatan para penjahat digital disebut *Unauthorized Access to Computer System and Service*, yaitu melakukan suatu kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Modus kriminalitas yang dilakukan adalah pencurian data-data account penting. Pelaku biasanya adalah seorang cracker dengan cara menjebak orang lain untuk tidak sadar bersedia memberikan data-data *account*-nya. Modus operandi cracker ini sangat berbeda dengan tindak kejahatan konvensional. Hal yang paling mencolok dari perbedaan tersebut antara lain adalah terletak pada tempat kejahatan perkara karena dalam kejahatan ini yang diserang adalah jaringan komputer atau internet.

Menurut Rommy Roosyana, 2019, sebagaimana dikutip dari Ririn Aswandi, dkk, Sistem keamanan data pribadi pengakses dunia maya pernah menjadi sorotan. Digital Forensic Indonesia (DFI) menduga ada sekitar 7.5 miliar data pribadi pengguna internet di seluruh dunia diretas pihak ketiga dalam 15 tahun terakhir. Ratusan juta di antaranya milik pengakses asal Indonesia. Sumber kebocoran data di seluruh sektor tersebut berasal dari peretasan pihak luar (*malicious outsider*) dan pihak dalam (*malicious insider*), kebocoran data yang tak disengaja

akibat sistem tak aman (*accidental loss*), *hacktivist*, gawai atau ponsel yang raib, perangkat pemeras (*ransomware*), dan beragam sumber yang tidak dapat diketahui.

Peretasan data pengguna bisa terjadi jika sistem perlindungan data dalam situs tersebut tidak ketat akibatnya, data pribadi bisa diperjualbelikan. Jaminan perlindungan data sudah diatur dalam Pasal 15 ayat (1) dan ayat (3) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Teknologi Elektronik (selanjutnya disebut UU ITE) yang mengharuskan setiap penyelenggara sistem elektronik untuk menjaga keamanan platform, namun ketentuan penjagaan keamanan tersebut tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik. Frasa ini menegaskan bahwa pengguna sistem elektronik harus ikut bertanggung jawab dalam menjaga keamanan data, sehingga jangan sampai akibat kelalaiannya menjadi pintu masuk serangan siber yang lebih besar dan masif yang berakibat cakupan kerusakannya meluas di tingkat nasional.

Berdasarkan data Bareskrim Polri, laporan mengenai pencurian data pribadi cukup meningkat selama empat tahun terakhir. Pada tahun 2017 terdapat 47 kasus, kemudian tahun 2018 meningkat menjadi 88 kasus, dan lonjakan kasus terjadi pada tahun 2019 sampai tahun 2020 yakni hingga 182 kasus.

E-commerce atau perdagangan elektronik saat ini menjadi salah satu bentuk perdagangan yang semakin populer di Indonesia. Penggunaan internet dan teknologi digital yang semakin meluas membuat kegiatan perdagangan elektronik semakin mudah dan nyaman. Namun, perkembangan perdagangan elektronik juga membawa risiko terhadap keamanan dan privasi data pribadi pelanggan. Perilaku masyarakat yang senang membeli produk *e-commerce* dengan harga murah serta kualitas rendah berisiko terhadap keamanan privasi data pribadinya, mengingat pada saat aktivasi produk customer diminta menyetujui persyaratan-persyaratan tertentu, namun tidak ada jaminan perlindungan atas data pribadinya.

Secara empiris pelanggaran hukum data pribadi pelanggan *e-commerce* sudah banyak. Pelanggaran ini dapat berupa pengumpulan data pribadi tanpa izin, penggunaan data pribadi secara tidak sah, penyebaran data pribadi tanpa persetujuan, atau bahkan kebocoran data pribadi karena tidak adanya tindakan keamanan yang memadai. Untuk itu diperlukan perlindungan hukum dan penegakan hukum yang tegas terhadap pelanggaran yang dilakukan oleh pelaku kejahatan *e-commerce*. Pemerintah perlu meningkatkan pengawasan dan pengendalian terhadap pengumpulan, pengolahan, dan penggunaan data pribadi pelanggan *e-commerce* sebagai bentuk perlindungan hukum.

Bahan hukum utama yang digunakan adalah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik, dan lainnya peraturan perundang-undangan yang berkaitan dengan objek penelitian ini.

Sebelum ditetapkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Indonesia telah menetapkan beberapa peraturan untuk melindungi data pribadi konsumen. Namun pengaturan hukum tersebut tetap berlaku sebagian, sebagaimana diatur dalam Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, dan Surat Edaran Otoritas Jasa

Keuangan Nomor 14/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen.

Misalnya, pada 17 April 2020, seorang peretas internasional yang dikenal dengan nama ‘*Why So Dank*’ berhasil meretas Tokopedia dan membocorkan data pribadi akun pengguna. Peretasan Tokopedia awalnya beredar di Twitter, seperti dilansir @underthebreach yang menuliskan data pribadi 15 juta pengguna Tokopedia telah diretas. Menurut @underthebreach, email, kata sandi, dan nama pengguna pengguna bocor ke pihak ketiga. Penelusuran lebih lanjut menemukan jumlah akun pengguna Tokopedia yang diretas melonjak menjadi 91 juta akun dan 7 juta akun *merchant*. Setahun sebelumnya, Tokopedia melaporkan bahwa platformnya memiliki sekitar 91 juta pengguna (Kronologi Lengkap 91 Juta Akun Tokopedia Bocor Dan Dijual, CNN Indonesia, 2022). Artinya, hampir seluruh akun pengguna Tokopedia bocor ke pihak ketiga termasuk informasi pribadinya. Peretas menjual informasi pribadi yang bocor di Web Gelap, termasuk nama lengkap pengguna, lokasi, tanggal lahir, nomor telepon, jenis kelamin, dan alamat email. Data tersebut dijual kepada pihak ketiga seharga \$5.000 atau Rp. 75.000.000.00 (tujuh puluh empat juta rupiah).

Masifnya penggunaan internet di satu sisi memberikan kontribusi pada perubahan sosial, dan kemajuan peradaban manusia tapi disisi lain memiliki risiko yang sangat besar, karena internet bisa digunakan sebagai wadah atau sarana untuk melakukan perbuatan melawan hukum seperti merusak situs web, pencurian data pribadi pada jaringan sosial, dan penipuan yang disebut deception / Muslihat yang ditujukan untuk mencari dan mendapatkan keuntungan pribadi.

Kita menyadari bahwa perlindungan data pribadi tidak sepenuhnya diserahkan kepada pemerintah semata, akan tetapi setiap anggota masyarakat juga harus dengan cermat dan cerdas ikut mengamankan keamanan data pribadinya dengan memilih dan memilah dengan bijak pemakaian internet, mulai dari chatting, milis, browsing, ditambah aplikasi canggih seperti video conference yang sudah mulai digunakan di seluruh dunia.

Dampak kejahatan siber menyentuh sendi kehidupan suatu bangsa, mulai dari terganggunya pelayanan publik, hilangnya kesempatan berbisnis maupun terganggunya ketertiban masyarakat. Menurut penulis kejahatan siber tidak semata-mata tindak kejahatan biasa akan tetapi bisa dikategorikan sebagai gerakan separatis yang dapat menyerang dan mengganggu kedaulatan suatu negara. Setiap perbuatan yang mengganggu negara berarti mengganggu rakyat, setiap pihak yang menjadi musuh negara berarti musuh rakyat. Hal ini sejalan yang disampaikan oleh John Locke bahwa negara adalah suatu perjanjian masyarakat untuk mendirikan suatu negara, pembentukan ini disebut dengan pactum unionis. Komitmen rakyat ini menjadikan negara dan rakyat secara bersama-sama menjaga keamanan dalam konteks pengamanan data baik yang bersifat individu atau kelembagaan, karena hal ini merupakan bagian dari Ketahanan Nasional.

Menurut Satjipto Raharjo, perlindungan hukum adalah memberikan pengayoman kepada hak asasi manusia yang dirugikan orang lain dan perlindungan tersebut diberikan kepada masyarakat agar mereka dapat menikmati semua hak-hak yang diberikan oleh hukum atau dengan kata lain perlindungan hukum adalah berbagai upaya hukum yang harus diberikan oleh aparat penegak hukum untuk memberikan rasa aman, baik secara pikiran maupun fisik dari gangguan dan berbagai ancaman dari pihak manapun. Keberadaan Kemenkominfo dan BSSN punya tanggung jawab besar untuk menjaga ketahanan nasional data dengan melakukan tata kelola sistem yang lebih baik serta meningkatkan literasi dan edukasi bagi pengakses data di level pengguna.

Pemerintah, masyarakat dan pelaku usaha harus saling bekerja sama agar e-commerce dapat memberikan manfaat bagi masyarakat dengan tetap menjaga keamanan dan privasi data

pribadi pelanggan serta tetap memberikan perlindungan bagi masyarakat yang mengkonsumsi barang/jasa e-commerce dari pelaku kejahatan siber dengan tipu muslihat menawarkan produk murah dengan harga terjangkau.

Kita menyadari kemajuan teknologi informasi menjadikan kehidupan menjadi mudah, transaksi keuangan, perdagangan maupun interaksi sosial dapat dilakukan dengan efektif dan efisien dengan teknologi informasi. Kemudahan itu tidak lepas dari risiko kejahatan dari orang-orang yang akan mengambil keuntungan. Kejahatan siber senantiasa mengintai kita, maka kecerdasan dan kewaspadaan setiap insan untuk melindungi datanya menjadi suatu kewajiban.

Kejahatan siber bukan lagi permasalahan regional akan tetapi sudah menjadi isu global, beberapa negara maju menghadapi ancaman yang sama dengan modus operandi yang beragam baik untuk kepentingan politik, pertahanan dan finansial. Perlindungan data tidak sepenuhnya diserahkan kepada negara/pemerintah akan tetapi kecerdasan dan kebijaksanaan masing-masing pribadi dalam menggunakan perangkat *chatting*, *milis*, *browsing*, persetujuan lisensi pada perangkat aplikasi dan *video conference* menjadi hal yang harus diwaspadai mengingat aktivitas ini menjadi pintu masuk kejahatan siber. Hal ini mempengaruhi ketahanan nasional Indonesia.

KESIMPULAN.

Perkembangan internet yang kini mendasari ekonomi digital telah menjadi aspek krusial dalam kehidupan manusia dan masyarakat, mendorong perubahan sosial serta kemajuan peradaban, namun di sisi lain membawa potensi risiko yang besar karena sering dijadikan sarana kejahatan, termasuk peretasan data pribadi yang tidak hanya merupakan kejahatan kriminal biasa tetapi juga dapat mengancam kedaulatan negara sehingga membutuhkan perhatian serius dari pemerintah seperti Kemenkominfo dan BSSN. Kejahatan siber dan peretasan ini tidak mengenal batas yurisdiksi atau sekat negara, sehingga dapat menargetkan individu atau negara manapun, menuntut penanganan lintas kementerian serta kerjasama regional dan global. Di samping itu, UUD 1945 telah memberikan perlindungan hukum kepada rakyat sesuai dengan amanat Pembukaan UUD 1945 alinea IV, meskipun masih diperlukan pengembangan kerangka kebijakan yang komprehensif mengenai perlindungan data untuk menghadapi tantangan era digital yang semakin kompleks.

Saran untuk penelitian selanjutnya adalah untuk memperluas kajian mengenai pengaruh kebijakan perlindungan data pribadi terhadap penguatan ketahanan siber di Indonesia, dengan mempertimbangkan tantangan yang dihadapi di tingkat internasional. Penelitian lebih lanjut sebaiknya melibatkan analisis mendalam mengenai efektivitas implementasi Undang-Undang Perlindungan Data Pribadi di Indonesia dalam menghadapi ancaman peretasan lintas negara. Selain itu, penelitian juga dapat mengkaji kerjasama antara pemerintah Indonesia dengan negara-negara lain dalam penanganan kejahatan siber secara global, serta mengeksplorasi integrasi teknologi baru dalam memperkuat perlindungan data pribadi. Pendekatan yang lebih komprehensif dalam mengkaji kebijakan ini diharapkan dapat memberikan rekomendasi yang lebih tepat untuk meningkatkan ketahanan nasional terhadap ancaman dunia maya yang semakin berkembang.

DAFTAR PUSTAKA.

- Academies, N., Policy, Affairs, G., Science, C. on, Policy, P., & Hazards, C. on I. N. R. to. (2012). *Disaster resilience: A national imperative*. National Academies Press.
- Adey, P., & Anderson, B. (2011). Event and anticipation: UK civil contingencies and the space—Times of decision. *Environment and Planning A*, 43(12), 2878–2899.
- Afonasova, M. A., Panfilova, E. E., Galichkina, M. A., & Ślusarczyk, B. (2019). *Digitalization*

- in economy and innovation: The effect on social and economic processes. *Polish Journal of Management Studies*, 19(2), 22–32. <https://doi.org/10.17512/pjms.2019.19.2.02>
- Alibeigi, A., Munir, A. B., & Asemi, A. (2021). Compliance with Malaysian Personal Data Protection Act 2010 by banking and financial institutions, a legal survey on privacy policies. *International Review of Law, Computers & Technology*, 35(3), 365–394.
- Arthadana, M. G. (2023). Reconstruction of Customary Criminal Law Based on Balinese Hindu Local Wisdom. *Law Doctoral Community Service Journal*, 2(1), 61–66.
- Aswandi, R., Muchin, P. R. N., & Sultan, M. (2020). Perlindungan data dan informasi pribadi melalui Indonesian Data Protection System (IDPS). *Jurnal Legislatif*, 167–190.
- Azizah, R., Anggraeni, R., & Mustika, Y. S. B. (2024). Peran Perlindungan Konsumen dalam Era Digitalisasi Perbankan Bagi Konsumen. *OPTIMAL Jurnal Ekonomi Dan Manajemen*, 4(2), 221–233.
- Bahtiar, N. (2024). Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah. *Development Policy and Management Review (DPMR)*, 85–100.
- Bukht, R., & Heeks, R. (2017). Defining, conceptualising and measuring the digital economy. *Development Informatics Working Paper*, 68.
- Burman, A., & Sharma, U. (2021). *How would data localization benefit India?* Carnegie India New Delhi.
- Dewi, S., & Gumelar, G. (2018). Perlindungan Privasi dan Data Pribadi Dalam Era Ekonomi Digital di Indonesia. *Jurnal Vej*, 4(1), 88–110.
- East, M., & Africa, N. (2015). World Bank Group. URL: <https://www.worldbank.org/en/region/mena> [Accessed 2023-04-24] *JOURNAL OF MEDICAL INTERNET RESEARCH*.
- Enoma, B. (2020). Data breach in the travel sector and strategies for risk mitigation. *Journal of Data Protection & Privacy*, 3(4), 418–426.
- Floridi, L. (2015). *The onlife manifesto: Being human in a hyperconnected era*. Springer nature.
- Lee, J.-A., & Liu, C.-Y. (2016). Real-name registration rules and the fading digital anonymity in China. *Wash. Int'l LJ*, 25, 1.
- Manyika, J., Pinkus, G., & Ramaswamy, S. (2016). *The US economy: An agenda for inclusive growth*. McKinsey Global Institute.
- Park, J., Seager, T. P., Rao, P. S. C., Convertino, M., & Linkov, I. (2013). Integrating risk and resilience approaches to catastrophe management in engineering systems. *Risk Analysis*, 33(3), 356–367. <https://doi.org/10.1111/j.1539-6924.2012.01885.x>
- Pradana, M. (2015). Klasifikasi bisnis e-commerce di Indonesia. *Modus*, 27(2), 163–174.
- Sargsyan, T. (2016). Data localization and the role of infrastructure for surveillance, privacy, and security. *International Journal of Communication*, 10, 17.
- Wibowo, A., Alawiyah, W., & Azriadi. (2024). The importance of personal data protection in Indonesia's economic development. *Cogent Social Sciences*, 10(1), 2306751.



Imam Aziz, Ima Mayasari

Implementasi Meritokrasi dalam Pengembangan Kompetensi Penyidik Polri untuk Meningkatkan Kepercayaan Publik

(<https://creativecommons.org/licenses/by-sa/4.0/>).