KAJIAN STRATEGIS
INDONESIA DARURAT RUANG DIGITAL
KEBOCORAN DATA INDONESIA

PENGURUS PUSAT
PERHIMPUNAN MAHASISWA INFORMATIKA DAN KOMPUTER
NASIONAL REPUBLIK INDONESIA
PERIODE 2024 - 2026

PENDAHULUAN

Kebocoran data masyarakat yang terjadi pada Komisi Pemilihan Umum (KPU) pada 2020 dimana 2,3 juta data warga tersebar. Pada Mei 2020 kebocoran data terjadi lagi pada BPJS Kesehatan yang menyebabkan sebanyak 279 juta data pribadi masyarakat tersebar. Bahkan, pada awal tahun 2022 publik di sambut dengan kasus kebocoran data Bank Indonesia. Rentetan kasus yang terjadi seharusnya menjadi alarm darurat bagi semua pihak dalam melakukan perlindungan data pribadi masyarakat.

Pencurian, penjualan, dan penyalahgunaan data pribadi masyarakat merupakan pelanggaran hukum. Kasus kebocoran data yang seringkali menyebabkan berbagai data tersebar kemudian berpotensi disalahgunan oleh pihak yang memiliki kepentingan. Hal itu terjadi akibat banyaknya data pribadi yang tersebar dan dimiliki oleh instansi publik maupun swasta Dari beberapa kasus yang terjadi, data tersebut diretas kemudian diperjualbelikan di situs raidforum. Namun, hal yang bisa dilakukan oleh pemerintah kerap kali hanya memblokir situs dan belum menindak tegas terkait pelanggaran atas kebocoran data. Padahal seharusnya kita dapat menghentikan kasus serupa terjadi dengan melakukan upaya preventif, salah satunya regulasi hukum yang kuat.

Serangan dan kejahatan siber meningkat di tiap tahunnya, sebagai salah satu dampak dari kebocoran data pribadi masyarakat. Berdasarkan data BSSN (Badan Sandi dan Siber Nasional) pada periode Januari-Mei 2021 jumlah kasus serangan mencapai 448 juta, dimana peretasan akun di dominasi oleh sektor pemerintah yakni 16.233 akun. Untuk kejahatan siber sendiri, Kepolisian mencatat sebanyak 3.500 laporan kasus kejahatan siber sampai akhir Maret 2021. Bentuk kejahatan siber yang sering terjadi adalah tindakan provokatif, penipuan online, pornografi, akses ilegal, perjudian, peretasan, gangguan sistem, hingga penyadapan. (Media Indonesia, 2021)

Kondisi absennya regulasi kuat terkait perlindungan data pribadi dan maraknya kasus kebocoran data yang menyebabkan tingginya kasus serangan dan kejahatan siber seharusnya menjadi alarm darurat bagi pemerintah untuk mengambil peran utama dalam merespon dan menindaklanjuti terkait perlindungan data pribadi masyarakat dengan mengintegrasikan seluruh stakeholder terkait termasuk masyarakat untuk meningkatkan kesadaran terkait perlindungan data pribadi. Hal ini dikuatkan oleh laporan Majalah Tempo (2021) bahwa “Lemahnya regulasi yang ada dan tidak adanya sanksi yang tegas terkait perlindungan data pribadi memicu kebocoran data pribadi”

Faktor kedua terkait dengans istem keamanan data yang belum dibangun dengan baik. Kasus kebocoran data yang kerap kali terjadi mengindikasikan sistem keamanan data yang belum dibangun dengan baik. Hal tersebut terjadi pada instansi baik publik maupun privat yang memiliki bank data, tidak mempunyai server yang cukup baik untuk melindungi data tersebut yang bermuara pada tidak adanya regulasi jelas yang mengatur tentang standar sistem keamanan data yang harus diterapkan pada instansi pemilik bank data. Sistem keamanan data mencakup server atau domain yang digunakan dalam sistem penyimpanan data maupun sumber daya manusia yang membuat dan menjalankannya. Server atau domain yang ada saat ini masih dianggap lemah, terlebih sumber daya manusia yang membangun dan menjalankan sistem keamanan data belum mempunyai kualitas dan kesadaran terkait perlindungan data pribadi, baik secara personal maupun penguatan SDM secara kelembagaan, baik ditingkat instansi pemilik data maupun BSSN (Badan Sandi dan Siber Nasional) yang saat ini dianggap masih lemah dalam mengawasi hal seperti sistem keamanan data.

Di era digital, kemajuan teknologi yang pesat dan menjamurnya internet telah mengubah cara kita hidup, bekerja, dan berinteraksi. Meskipun perkembangan ini telah membawa banyak manfaat, seperti peningkatan akses terhadap informasi, peningkatan komunikasi, dan peluang ekonomi baru,

perkembangan tersebut juga menimbulkan tantangan yang signifikan, khususnya dalam bidang perlindungan data pribadi. Salah satu negara yang menghadapi tantangan ini adalah Indonesia, negara yang telah mengalami lonjakan digitalisasi namun pada saat yang sama juga menghadapi permasalahan penting terkait privasi dan keamanan data. Artikel ini menggali kompleksitas kebocoran data di Indonesia, menggarisbawahi kebutuhan mendesak akan peraturan pemerintah yang kuat dan pemberlakuan RUU Perlindungan Data Pribadi untuk melindungi informasi pribadi individu.

Lanskap digital di Indonesia, yang ditandai dengan basis pengguna internet yang besar dan berkembangnya sektor fintech, menghadirkan lahan subur bagi kejahatan dunia maya, termasuk pelanggaran data yang membahayakan privasi dan keamanan pribadi. Meskipun terdapat risiko yang nyata, kerangka peraturan di negara ini untuk perlindungan data masih belum berkembang dan tertinggal dari standar internasional. Ketidakcukupan ini tidak hanya memaparkan masyarakat pada potensi kerugian namun juga melemahkan kepercayaan terhadap platform digital, yang sangat penting bagi kelanjutan pertumbuhan ekonomi digital. Artikel ini meninjau undang-undang yang ada dan menyoroti kesenjangan antara langkah-langkah perlindungan data di Indonesia dan negara-negara lain, serta menganjurkan pendekatan komprehensif untuk meningkatkan keamanan dan privasi data.

Pentingnya literasi digital dalam memitigasi risiko kejahatan dunia maya tidak dapat dilebih-lebihkan. Seiring berkembangnya teknologi, taktik yang digunakan pelaku kejahatan siber juga ikut berkembang, sehingga pengguna internet harus dibekali dengan pengetahuan dan keterampilan untuk melindungi informasi pribadi mereka. Artikel ini berpendapat bahwa peningkatan literasi digital merupakan komponen penting dari strategi yang lebih luas untuk mencegah pelanggaran data dan memastikan lingkungan online yang lebih aman bagi seluruh masyarakat Indonesia.

Lebih lanjut, artikel ini mengeksplorasi berbagai aspek permasalahan ini, termasuk dampak kejahatan dunia maya terhadap perlindungan data pribadi, peran kepercayaan dan keamanan dalam penggunaan layanan fintech, serta tantangan yang ditimbulkan oleh Internet of Things (IoT) dalam hal keamanan. , etika, privasi, dan hukum. Laporan ini juga mengkaji perlunya undang-undang yang spesifik dan komprehensif untuk melindungi data pribadi, tidak hanya di Indonesia tetapi juga di negara-negara berkembang lainnya yang menghadapi tantangan serupa.

Kurangnya peraturan perlindungan data yang efektif di Indonesia telah menyebabkan banyak insiden kebocoran data, yang menyoroti kerentanan informasi pribadi di dunia digital. Pelanggaran ini tidak hanya melanggar hak privasi individu namun juga menimbulkan ancaman terhadap keamanan nasional. Artikel ini menekankan pentingnya mengadopsi perlindungan data yang spesifik dan komprehensif.

Perlindungan Hukum Data Pribadi di Indonesia

Perlindungan hukum atas data pribadi di Indonesia merupakan isu penting yang mendapat perhatian besar dalam beberapa tahun terakhir, terutama setelah banyaknya pelanggaran data tingkat tinggi yang mengungkap kerentanan infrastruktur digital di negara ini. Meskipun pertumbuhan ekonomi digital pesat dan ketergantungan terhadap teknologi dalam kehidupan sehari-hari meningkat, kerangka hukum di Indonesia untuk perlindungan data masih belum berkembang, sehingga menimbulkan risiko besar terhadap privasi dan keamanan informasi pribadi warga negara.

Peraturan yang ada, meskipun memberikan perlindungan pada tingkat dasar, masih belum mampu mengatasi kompleksitas dan tantangan yang ditimbulkan oleh era digital. Peraturan perundang-undangan utama yang mengatur perlindungan data pribadi di Indonesia adalah Undang-

Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diubah dengan Undang-Undang Nomor 19 Tahun 2016. Namun undang-undang tersebut dikritik karena kurangnya perlindungan data pribadi. kekhususan dan kelengkapan dalam menangani perlindungan data pribadi. Aturan-aturan tersebut tidak sepenuhnya mencakup prinsip-prinsip yang diperlukan untuk perlindungan data yang efektif, seperti persetujuan, minimalisasi data, dan hak-hak subjek data, yang penting untuk menjaga informasi pribadi di dunia digital.

Tidak adanya undang-undang perlindungan data pribadi yang spesifik dan komprehensif telah menyebabkan pendekatan privasi data yang terfragmentasi, dengan berbagai sektor dan lembaga menerapkan peraturan mereka sendiri. Situasi ini mengakibatkan inkonsistensi dan kesenjangan dalam perlindungan, sehingga data pribadi rentan terhadap penyalahgunaan dan akses tidak sah. Kebutuhan akan kerangka hukum yang terpadu dan kuat merupakan hal yang nyata, seperti yang disoroti oleh banyak akademisi dan pakar yang menyerukan diberlakukannya Rancangan Undangundang Perlindungan Data Pribadi (RUU Perlindungan Data Pribadi).

Kajian keamanan data di dunia digital menjadi perhatian semua ilmuan dan praktisi informasi dan komunikasi. Penelitian yang dilakukan oleh Siti Yuniarti (2019) berjudul "Perlindungan Hukum Data Pribadi di Indonesia" menganalisis perkembangan teknologi informasi dan komunikasi (TIK) yang memengaruhi kebutuhan untuk melindungi data pribadi di Indonesia. Yuniarti memulai dengan menguraikan bagaimana perkembangan TIK telah memudahkan pengumpulan, pengelolaan, dan penyimpanan data pribadi, yang secara simultan meningkatkan risiko terhadap privasi individu. Privasi, yang diakui sebagai hak asasi manusia, memerlukan perlindungan hukum yang kuat untuk mencegah pelanggaran. Penulis menekankan bahwa Indonesia, sebagai negara hukum, memiliki fondasi konstitusional untuk melindungi hak asasi manusia, termasuk privasi, namun masih membutuhkan undang-undang yang lebih spesifik dan komprehensif untuk mengatasi isu data pribadi secara efektif.

Yuniarti menggunakan metodologi penelitian yuridis normatif untuk menjelaskan bahwa perlindungan data pribadi di Indonesia saat ini terutama diatur melalui peraturan sektoral, dan belum ada undang-undang yang spesifik dan komprehensif. Studi ini mengeksplorasi berbagai sumber, termasuk perundang-undangan yang ada, rekomendasi dari organisasi internasional, dan praktik dari negara lain, untuk menilai bagaimana perlindungan data pribadi dapat diperkuat di Indonesia. Analisis tersebut menunjukkan bahwa perlindungan data pribadi di Indonesia perlu bertransformasi dari pendekatan sektoral menjadi lebih holistik, melalui pembentukan undang-undang yang menyeluruh.

Akbari, Zaman, Anwar, dan Fadlian (2021) mengkaji kebocoran data BPJS Kesehatan di Indonesia dan implikasinya terhadap pertanggungjawaban pidana menurut UU ITE. Mereka membahas bagaimana kebocoran data tersebut mencerminkan kelemahan dalam perlindungan data pribadi dan kebutuhan mendesak untuk tindakan hukum yang tegas.

Akbari, dkk. (2021) menjelaskan bahwa kasus kebocoran data BPJS menyoroti kerentanan sistem informasi Indonesia terhadap serangan siber dan penyalahgunaan data. Mereka menggunakan metode penelitian hukum normatif untuk mengevaluasi penerapan UU ITE dalam kasus ini, menunjukkan bahwa undang-undang saat ini memberikan ruang bagi korban kebocoran data untuk menuntut kompensasi. Namun, studi ini menemukan bahwa implementasi hukum sering kali tidak konsisten, dan mekanisme penegakan hukum belum sepenuhnya efektif dalam melindungi data pribadi warga.

RUU Perlindungan Data Pribadi yang diusulkan, yang telah masuk dalam jalur legislatif selama beberapa tahun, bertujuan untuk mengatasi kekurangan ini dengan menetapkan definisi yang jelas tentang data pribadi, menetapkan hak-hak subjek data, dan menguraikan kewajiban pengontrol dan

pemroses data. Hal ini juga berupaya untuk memperkenalkan mekanisme penegakan hukum dan hukuman atas pelanggaran, yang saat ini kurang atau tidak cukup berdasarkan undang-undang yang ada. RUU ini mengikuti standar internasional, seperti Peraturan Perlindungan Data Umum (GDPR) Uni Eropa, yang mewakili pendekatan komprehensif terhadap perlindungan data yang memprioritaskan hak dan privasi individu.

Kajian ini juga menyoroti peran penting pemerintah dalam mencegah kebocoran data, bukan hanya melalui pengesahan hukum tetapi juga melalui pengawasan yang lebih baik dan pengembangan infrastruktur teknologi informasi yang aman. Penulis berargumen bahwa, sementara undang-undang seperti UU ITE penting, pemerintah juga harus memprioritaskan investasi dalam keamanan siber untuk mencegah kejadian serupa di masa depan.

Disahkannya RUU Perlindungan Data Pribadi akan menandai langkah maju yang signifikan dalam upaya Indonesia untuk melindungi data pribadi. Hal ini tidak hanya akan meningkatkan perlindungan hukum bagi individu namun juga membangun kepercayaan terhadap layanan digital, yang penting bagi kelanjutan pertumbuhan ekonomi digital.

Perlindungan Data Pribadi sebagai Hak Asasi Manusia

Dalam karyanya, Hanifan Nifari (2021) meninjau perlindungan data pribadi di Indonesia dari perspektif hak asasi manusia. Nifari menggali kedalaman konsep privasi sebagai hak fundamental yang dilindungi oleh konstitusi dan hukum internasional, menekankan bahwa ini termasuk perlindungan terhadap data pribadi. Penelitian ini menyajikan analisis komparatif antara regulasi perlindungan data pribadi di Indonesia dan GDPR Uni Eropa, menyoroti kesenjangan dalam kerangka hukum dan praktik pengawasan. Nifari berargumen bahwa Indonesia perlu mengadopsi prinsip-prinsip dan standar internasional seperti yang terkandung dalam GDPR untuk memperkuat perlindungan data pribadi.

Nifari (2021) menyarankan reformasi hukum yang signifikan di Indonesia untuk memastikan bahwa hak atas privasi dan perlindungan data pribadi dihormati dan dijamin, menyarankan bahwa hal ini harus mencakup hak untuk mengakses dan memperbaiki data pribadi, serta mekanisme untuk pengawasan dan penegakan hukum yang efektif.

Hanifan Nifari (2021) juga membahas kerangka kerja perlindungan data pribadi di Indonesia, menyoroti perlunya pendekatan yang lebih holistik dan terpadu dalam melindungi informasi pribadi warga. Penelitian ini mengkritisi kerangka hukum saat ini sebagai tidak mencukupi untuk mengatasi tantangan yang muncul dari perkembangan teknologi digital yang cepat.

Nifari menekankan pentingnya mengadopsi standar internasional seperti GDPR, yang mencakup aspek-aspek seperti hak subjek data, tanggung jawab pengendali dan pemroses data, serta mekanisme penegakan yang efektif. Analisis ini menunjukkan bahwa Indonesia memerlukan undang-undang yang tidak hanya mengatur pengumpulan dan penggunaan data tetapi juga memberikan perlindungan terhadap hak privasi individu dan memfasilitasi tata kelola data yang bertanggung jawab Nifari (2021).

Nifari menyarankan bahwa reformasi hukum di Indonesia harus mencakup pembentukan lembaga pengawas independen, peningkatan kesadaran publik tentang hak-hak mereka terkait data pribadi, dan pengembangan infrastruktur teknologi informasi yang aman untuk mencegah kebocoran dan penyalahgunaan data Nifari (2021).

Hisbulloh (2021) menyoroti pentingnya pengesahan RUU Perlindungan Data Pribadi di Indonesia. Dalam era digital saat ini, kebocoran data pribadi menjadi masalah serius karena penggunaan teknologi yang luas. Meskipun sudah ada peraturan perundang-undangan yang mengatur

perlindungan data pribadi, masih terdapat kekurangan dalam implementasi yang efektif untuk memberikan perlindungan yang memadai.

Hisbulloh (2021) menekankan bahwa dengan adanya undang-undang yang spesifik dan komprehensif, Indonesia dapat memberikan kerangka kerja yang kuat untuk perlindungan data pribadi, mencegah kebocoran data, dan menjamin keamanan informasi pribadi warga negara. Hal ini tidak hanya penting untuk melindungi privasi individu, tetapi juga untuk membangun kepercayaan publik dalam penggunaan teknologi digital dan mendukung pertumbuhan ekonomi digital di Indonesia. Kesimpulannya, RUU Perlindungan Data Pribadi merupakan langkah krusial yang harus segera diambil untuk memperkuat perlindungan data pribadi di Indonesia.

Mutiara dan Maulana (2020), mengeksplorasi bagaimana perlindungan data pribadi di Indonesia terkait erat dengan hak asasi manusia. Penulis mengidentifikasi bahwa Indonesia belum memiliki undang-undang spesifik yang mengatur tentang perlindungan data pribadi. Melalui analisis komparatif, artikel ini menyoroti bagaimana negara lain, terutama di Eropa, telah memasukkan perlindungan data pribadi ke dalam kerangka hukum mereka, mengacu pada regulasi seperti GDPR yang memberikan perlindungan menyeluruh dan terperinci terhadap data pribadi. Penelitian ini menunjukkan bahwa perlindungan data pribadi di Indonesia masih bersifat fragmentaris dan tidak menyeluruh, menekankan kebutuhan mendesak untuk undang-undang khusus yang dapat menjamin hak privasi warga negara.

Wahyudi Djafar (2019), menggambarkan lanskap yang berubah cepat dari pengelolaan data di era digital. Djafar menguraikan bagaimana revolusi data, ditandai dengan kemajuan teknologi seperti Big Data, artificial intelligence, dan Internet of Things, telah menciptakan kapasitas baru untuk mengumpulkan, menyimpan, dan menganalisis data pada skala yang belum pernah ada sebelumnya. Dengan peningkatan kapasitas ini, muncul risiko yang signifikan terhadap privasi dan perlindungan data pribadi, memicu kebutuhan mendesak untuk pembaruan regulasi yang ada. Artikel ini mendiskusikan bagaimana kerangka hukum saat ini di Indonesia belum cukup untuk mengatasi tantangan yang ditimbulkan oleh dinamika digital baru, menekankan pentingnya mengadopsi pendekatan hukum yang lebih komprehensif dan dinamis yang sejalan dengan standar internasional.

Artikel tersebut menggambarkan kebutuhan mendesak untuk pembaruan hukum yang komprehensif di Indonesia dalam mengatasi tantangan perlindungan data pribadi di era digital. Mereka menyoroti bagaimana kebocoran data dan penyalahgunaan informasi pribadi telah menjadi lebih umum, menimbulkan ancaman serius terhadap privasi dan keamanan individu. Dengan merujuk pada model internasional seperti GDPR, kedua artikel menyarankan bahwa Indonesia harus mengambil langkah proaktif untuk memperbarui kerangka hukumnya, memastikan bahwa perlindungan data pribadi diperlakukan sebagai prioritas utama dan diintegrasikan ke dalam hak asasi manusia.

Literatur secara keseluruhan menunjukkan perlunya respons yang cepat dan efektif dari pemerintah dan lembaga legislatif di Indonesia untuk mengatasi kelemahan dalam regulasi perlindungan data pribadi. Peningkatan kesadaran publik dan kebutuhan untuk keamanan data yang lebih baik harus diiringi dengan tindakan legislatif yang kuat untuk menciptakan lingkungan digital yang aman dan terpercaya. Pembaruan hukum harus mencakup penyediaan hak untuk mengakses dan memperbaiki data pribadi, memperkuat transparansi dan akuntabilitas bagi pengolah data, dan memastikan bahwa pengumpulan dan penggunaan data pribadi dilakukan dengan cara yang adil dan legal.

Tanpa komitmen kuat untuk memperbarui dan memperkuat kerangka hukum perlindungan data pribadi, Indonesia akan terus menghadapi tantangan dalam menjaga privasi dan keamanan data warganya. Diperlukan langkah-langkah legislatif yang berani dan inovatif untuk menyesuaikan dengan kemajuan teknologi dan memenuhi standar internasional dalam perlindungan data pribadi.

Isu keamanan data menjadi hal paling rentan bagi warga di negeri berkembang dimana tingkat literasi digital masyarakat masih relative rendah. Hal ini membuat baik lembaga pemerintah, swasta atau bahkan individu di negara berkembang menjadi sangat rentan dengan keamanan data dan penyalahgunaan data mereka dalam aktivitas di dunia digital. Untuk itu kebijakan keamanan data menjadi penting dalam kajian kebijakan tata kelolanya.

Salah satu isu penting yang menjadi perhatian para peneliti adalah masalah etika dan tata kelola. Penelitian Tovi dan Mutama (2013) menunjukkan bahwa negara-negara berkembang menghadapi tantangan tambahan dibandingkan negara-negara maju dalam mengatasi masalah etika dan tata kelola terkait dengan perlindungan data. Negaranegara berkembang bergulat dengan tantangan tersendiri dalam mengelola permasalahan etika dan tata kelola terkait perlindungan data, yang membedakan mereka dengan negara-negara maju.

Kondisi ini dipengaruhi setidaknya lima hal. Pertama, negara-negara berkembang sering kali tidak memiliki kerangka peraturan yang kuat untuk mengatur perlindungan data, sehingga menimbulkan dilema etika. Tidak adanya pedoman yang ketat membuat individu dan organisasi rentan terhadap pelanggaran privasi dan penyalahgunaan data (Tovi dan Mutama, 2013).

Faktor kedua adalah pesatnya integrasi teknologi baru yang menimbulkan dilema etika, khususnya terkait privasi data. Seiring dengan kemajuan teknologi, risiko yang terkait dengan kecerdasan buatan dan inovasi berbasis data menjadi semakin besar, sehingga memerlukan pertimbangan etis dalam penerapannya (Dhirani, et. al, 2023).

Faktor ketiga terkait praktik berbagi data yang etis di negara-negara berkembang menghadapi tantangan terkait dengan meminimalkan dampak buruk. Studi Kaewkungwal et al., (2023) menyoroti pentingnya membangun praktik yang memprioritaskan nilai berbagi data sambil meminimalkan dampak buruk, dan menekankan perlunya pertimbangan etis.

Faktor keempat Pelanggaran privasi tidak hanya mengganggu kepercayaan tetapi juga membahayakan keamanan. Mengadopsi pendekatan etis terhadap perlindungan privasi data menjadi penting untuk menjaga kepercayaan dalam interaksi digital dan menjaga informasi sensitive (Lee et al., 2016). Faktor terakhir adalah pembuat kebijakan di negara-negara berkembang menghadapi tantangan dalam menyeimbangkan manfaat dan risiko yang terkait dengan akses dan pembagian data. Untuk mencapai keseimbangan yang tepat, sangat penting untuk mengatur maksimalisasi pemanfaata data sekaligus memitigasi potensi risiko (Borgesius et al., 2015).

Masalah kedua yang dihadapi negara berkembang dalam keamanan data adalah peraturan perundang-undangan dan internet yang tidak sesuai. Kesenjangan peraturan dan undang-undang yang tidak sesuai berkontribusi terhadap ancaman perlindungan data, yang menunjukkan perlunya kerangka hukum yang lebih kuat di negara-negara berkembang (Tovi dan Mutama, 2013). Dalam konteks perlindungan data, negara-negara berkembang bergulat dengan tantangan yang berasal dari kesenjangan peraturan dan peraturan perundang-undangan yang tidak tepat. Beberapa penelitian menyoroti peran penting kerangka hukum dalam menjaga data dan mengatasi ancaman yang muncul di kawasan ini.

Isu pertama terkait dengan sifat internet yang bersifat lintas batas menekankan pentingnya peraturan perlindungan data yang kuat. Perundang-undangan yang tidak tepat mungkin gagal mengatasi aspek transnasional dari ancaman siber, sehingga menekankan perlunya kerangka hukum komprehensif yang melampaui batas-batas negara (Walters, 2022).

Isu kedua merupakan kesenjangan peraturan yang seringkali menimbulkan tantangan etika dan tata kelola. Negara-negara berkembang menghadapi tantangan tambahan dibandingkan dengan negara-negara maju, sehingga memerlukan struktur hukum yang mampu mengatasi permasalahan spesifik ini dan mendorong praktik data yang etis (Karale, 2021).

Isu ketiga adalah menyeimbangkan akses dan privasi. Kajian terhadap akses data kesehatan dan privasi menggarisbawahi pentingnya menyeimbangkan langkah-langkah hukum. Undang-undang yang dirancang secara tidak tepat dapat merusak keseimbangan antara akses terhadap data untuk kepentingan publik dan menjamin hak privasi individu (Lane dan Schur,2010).

Isu terakhir terkait peraturan perundang-undangan dan internet yang tidak tepat adalah perlunya evolusi hukum. Seiring kemajuan teknologi, kerangka hukum harus berkembang. Perundang-undangan yang tidak tepat mungkin tidak bisa mengimbangi inovasi teknologi, sehingga menimbulkan kesenjangan dalam perlindungan data. Evolusi hukum yang berkelanjutan sangat penting untuk mengatasi ancaman yang muncul dan memastikan keamanan data yang komprehensif di negara-negara berkembang.

Masalah ketiga yang dihadapi negara berkembang dalam keamanan data digital adalah Kesenjangan Regulasi di Fintech. Sektor fintech di negara-negara berkembang mengalami kesenjangan peraturan yang menyebabkan terganggunya privasi data dan meningkatnya penipuan keuangan, sehingga menekankan pentingnya peraturan yang efektif (Jafri, et al.,2024). Kesenjangan peraturan di sektor Fintech menimbulkan tantangan besar terhadap keamanan digital. Meskipun inovasi Fintech menawarkan peluang yang sangat besar, perkembangan lanskap telah mengungkap kerentanan yang memerlukan kerangka peraturan yang komprehensif. Beberapa penelitian membahas tiga isu penting terkait Kesenjangan Regulasi di Fintech.

Pertama, evolusi fintech yang cepat mengakibatkan kesenjangan data, sehingga menghambat pemantauan yang efektif. Studi Marqués et al. (2023) menekankan perlunya langkah-langkah regulasi untuk mengatasi tantangan besar dalam memantau aktivitas Fintech dan mengatasi potensi kesenjangan data.

Kedua, arbitrase peraturan, dimana perusahaan mengeksploitasi perbedaan peraturan, merupakan masalah yang mendesak. Fintech yang bergerak cepat menciptakan tantangan bagi regulator, sehingga memerlukan kerangka kerja yang tangkas dan adaptif untuk melawan potensi risiko keamanan (Fascual dan Natalucci, 2023).

Tantangan ketiga yang menjadi pertimbangan pemerintah negara ketiga adalah tantangan utama dalam industri Fintech yakni kurangnya kejelasan peraturan. Perusahaan Fintech sering kali beroperasi di wilayah abu-abu sehingga membuat mereka rentan terhadap potensi kerentanan keamanan. Mengatasi kesenjangan ini memerlukan kerangka peraturan yang jelas dan adaptif (Ruof, 2023).

ANALISIS MASALAH

Kemajuan teknologi dan pertumbuhan internet tidak diragukan lagi merupakan kontributor yang sangat signifikan terhadap pengaruhnya. Namun tidak semua hal mempunyai dampak yang baik, dan pasti ada dampak negatifnya jika ada dampak positifnya. Ada kalanya kita membiarkan diri kita terlalu terpikat dengan kecanggihan internet, yang justru membuat segalanya lebih mudah bagi kita. Namun, kami lupa bahwa potensi konsekuensi dari memposting informasi pribadi di internet sangatlah berbahaya. Hal lain yang menjadi isu dalam keamanan data adalah ketika kita terlibat dalam perjanjian elektronik dimana setiap kali terjadi proses jual beli atau ketika terjadi peralihan kepemilikan dari pelaku usaha kepada pemilik konsumen. Perjanjian elektronik dalam e-commerce seringkali tidak melibatkan interaksi tatap muka. Dalam kebanyakan kasus, setelah kami menyelesaikan proses pengisian informasi pribadi kami di aplikasi e-commerce, aplikasi tersebut pada halaman web akan menentukan perjanjian yang ada antara pengguna aplikasi dan konsumen. Dalam perjanjian ini pihak ecommerce sendiri sudah menjelaskannya, dan hanya kami sebagai pengguna yang diberikan penjelasan tersebut. Terdapat kolom yang bisa kita centang sebagai persetujuan, terlepas dari setuju atau tidaknya kita dengan kesepakatan yang telah diberikan. Kesimpulannya adalah kami, sebagai pengguna, tidak mempunyai peran apa pun dalam proses pembuatan perjanjian. Oleh karena itu, dapat dikatakan bahwa mendaftarkan diri di internet berisiko. Bisa jadi perjanjian tersebut akan menjadi bumerang bagi kita jika tidak membacanya secara menyeluruh (Putri dan Fahrozi, 2021). Dalam konteks Indonesia, maraknya kasus kebocoran data antara lain disebabkan oleh lemahya kekuatan hukum terkait perlindungan data pribadi. Regulasi terkait perlindungan data pribadi hanya ada di tataran Peraturan Menteri Komunikasi dan Informasi No.20 Tahun 2016 tentang Perlindungan Data pribadi yang merupakan turunan dari Peraturan Pemerintah No.82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Jadi secara regulasi, perlindungan Data Pribadi belum mempunyai regulasi setingkat Undang-Undang sehingga kekuatan hukumnya masih belum baik. Saat ini, ia masih berupa Rancangan Undang-Undang dan masih dalam pembahasan di Dewan Perwakilan Rakyat (DPR). Undang-Undang ITE yang saat ini juga berlaku, belum mampu memberikan perlindungan yang optimal bagi perlindungan data pribadi masyarakat. Saat ini, kasus kebocoran data seringkali menggunakan UU ITE sebagai landasan hukum yang mengatur terkait perlindungan data pribadi, namun regulasi ini tentunya belum mengatur secara khusus terkait perlindungan data pribadi yang tentunya tidak hanya berfokus pada tindakan pasca kasus terjadi, namun juga dibutuhkan regulasi sebagai yang mengatur baagaimana melindungi data sebagai langkah preventif untuk mencegah kejadian berulang terkait kebocoran data pribadi masyarakat.

Sering kali juga terdapat kurangnya pemahaman dan komitmen dari berbagai pihak, termasuk pemerintah dan sektor swasta, terhadap pentingnya perlindungan data pribadi. Oleh sebab itu, perlu penguatan kapasitas institusi, peningkatan kerjasama antarlembaga, dan penerapan sanksi yang efektif untuk memastikan bahwa regulasi perlindungan data pribadi diimplementasikan dengan baik. Perlindungan data pribadi tidak hanya tentang regulasi, tetapi juga tentang implementasi efektif dan pembangunan budaya kesadaran privasi di seluruh masyarakat.

AGENDA KEBIJAKAN

Digitalisasi data yang kemudian disimpan sebagai bank data oleh instansi untuk berbagai keperluan dan tingginya angka penggunaan internet saat ini, dapat menjadi momentum yang dimanfaatkan oleh berbagai orang atau kelompok untuk menyalahgunakan data tersebut atau bahkan melakukan kejahatan siber.

Untuk mencegah dan menanggulangi kebocoran data pribadi, kami mengusulkan dua rekomendasi kebijakan sebagai berikut:

Pertama, RUU Perlindungan Data Pribadi (RUU PDP) Harus segera disahkan. Regulasi yang ada saat ini mulai dari UU ITE, PP No.82 Tahun 2016, hingga Permen Kominfo No.20 Tahun 2016 belum mengatur secara kompherensif dan khusus terkait Perlindungan Data Pribadi. Untuk itu, RUU PDP harus segera di sahkan dimana ia dapat menjadi payung hukum yang memberikan perlindungan optimal terhadap data pribadi masyarakat. RUU PDP juga dapat menjadi regulasi yang mengatur terkait hak masyarakat dalam memberikan informasi pribadinya, sanksi kepada instansi yang mengalami kebocoran data, dan standar sistem keamanan data yang harus dimiliki oleh instansi yang memiliki Bank Data masyarakat. Pembahasan RUU ini sudah berlarut dari tahun 2012, namun hingga kini belum di sahkan padahal kebutuhan akan regulasi ini mendesak mengingat banyaknya kasus kebocoran data di Indonesia, sehingga kebutuhan akan adanya UU Perlindungan Data Pribadi juga semakin meningkat.

Meningkatnya jumlah pengguna internet tidak menutup kemungkinan juga akan menyebabkan peningkatan kejahatan dunia maya. Terdapat 71 kasus manipulasi data, 39 kasus pencurian data, dan 18 kasus peretasan sistem elektronik yang tercatat dalam Laporan Kasus Kejahatan Siber Indonesia (Putri dan Fahrozi, 2021). Oleh karena itu, RUU Perlindungan Data Pribadi perlu disahkan secepatnya. Peningkatan jumlah masyarakat yang melakukan aktivitas di dunia digital kemungkinan besar akan dibarengi dengan peningkatan jumlah kejahatan siber.

Ada sejumlah elemen yang menimbulkan aktivitas kriminal online. Pertama, Curtis et al. (2022) menekankan fakta bahwa tidak adanya pencegahan yang memadai, serta adanya insentif yang memotivasi, merupakan kontributor besar terhadap kejahatan dunia maya. Ada kemungkinan bahwa individu akan merasa berani untuk terlibat dalam tindakan ilegal secara online jika tidak ada tindakan hukuman yang tegas. Tata kelola dalam skala global dan supremasi hukum adalah faktor kedua. Penelitian yang dilakukan oleh Chen et al. (2023) menyoroti fakta bahwa korupsi politik, tata kelola yang tidak efisien, kelemahan kelembagaan, dan kurangnya supremasi hukum sering disebut-sebut sebagai penyebab kejahatan dunia maya. Temuan ini konsisten dengan temuan mereka. Perbedaan yang ada dalam fitur-fitur tata kelola yang mutlak diperlukan ini berdampak pada geografi kejahatan dunia maya di seluruh dunia. Faktor yang berdampak pada perkembangan kebijakan keamanan siber merupakan faktor ketiga. Hal ini didukung oleh penelitian yang dilakukan oleh Mishra et al. (2022) yang menyoroti berbagai faktor yang mempengaruhi perumusan kebijakan keamanan siber. Ada sejumlah variabel yang berkontribusi terhadap kompleksitas pemberantasan kejahatan dunia maya. Beberapa kekhawatiran tersebut mencakup perolehan informasi sensitif, kerugian terhadap kedaulatan suatu negara, dan landasan ideologis.

Kedua, peningkatan literasi digital. Berdasarkan survei yang dilakukan oleh kementerian informasi dan komunikasi pada 2020 di 34 provinsi, secara nasional indeks literasi digital berada pada kategori sedang, dimana subindeks dari informasi dan literasi data memiliki skor yang paling rendah. Hal tersebut mengindikasikan, perlunya peningkatan literasi data dan informasi yang lebih baik kepada masyarakat secara umum dengan fokus pada urgensi keamanan data pribadi mengingat jumlah pengguna internet di Indonesia kian meningkat. Literasi digital memainkan peran penting dalam memperkuat keamanan data bagi pengguna internet. Dengan memberdayakan individu dengan pengetahuan dan keterampilan yang diperlukan untuk menavigasi lanskap digital dengan aman, risiko pelanggaran data dan ancaman dunia maya dapat dikurangi secara signifikan. Literasi digital memainkan peran penting dalam memperkuat keamanan data bagi pengguna internet. Dengan memberdayakan individu dengan pengetahuan dan keterampilan yang diperlukan untuk menavigasi lanskap digital dengan aman, risiko pelanggaran data dan ancaman dunia maya dapat dikurangi secara signifikan.

Literasi digital, jika dilihat dari sudut pandang komunikatif, melibatkan penerapan langkah-langkah keamanan mendasar untuk melindungi data pribadi (Karanfiloğlu, 2022). Hal ini mencakup

kemampuan untuk mengadopsi langkah-langkah keamanan dasar, memastikan privasi dan perlindungan informasi sensitif. Selain itu, beberapa penelitian berpendapat bahwa keamanan diidentifikasi sebagai dimensi baru dalam literasi digital. Pengakuan ini menekankan sifat ancaman digital yang terus berkembang dan perlunya individu untuk tetap mendapat informasi tentang praktik keamanan yang terkonsolidasi dan yang sedang berkembang (Estrada et al., 2022).

Untuk itu, merekomendasi direktorat jenderal pendidikan tinggi dan dinas pendidikan provinsi dan kab/kota, kalangan pelajar, serta dinas komunikasi dan informasi provinsi dan kab/kota bagi kalangan masyarakat umum untuk mendorong peningkatan literasi digital sehingga kasus serupa dapat diminimalisir.

REFERENSI

Akbari, A., Zaman, A., Anwar, J., & Fadlian, A. (2021). Pertanggungjawaban Pidana Kebocoran Data BPJS dalam Perspektif UU ITE. Universitas Singaperbangsa Karawang.

Aswandi, Ririn, Putri Muchsin, Muhammad Sultan. (2020). Perlindungan Data dan Informasi Pribadi Melalui Indonesia Data Protection System (IDPS). Lembaga Penalaran dan Penulisan Karya Ilmiah Fakultas Hukum Universitas Hasanuddin 3(2) 170-180.

Borgesius, F. Z., Gray, J., & van Eechoud, M. (2015). Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework. Berkeley Technology Law Journal, 30(3), 2073–2131. https://www.jstor.org/stable/26377585

Chen S, Hao M, Ding F, Jiang D, Dong J, Zhang S, Guo Q, Gao C. (2023) Exploring the global geography of cybercrime and its driving forces. Humanity Social Science Community. 10(1):71. doi: 10.1057/s41599-023-01560-x.

Curtis, J., & Oxburgh, G. (2023). Understanding Cybercrime in 'Real World' Policing and Law Enforcement. The Police Journal, 96(4), 573 592. https://doi.org/10.1177/0032258X221107584

Dhirani LL, Mukhtiar N, Chowdhry BS, Newe T. (2023) Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. Sensors (Basel). 23(3):1151. doi: 10.3390/s23031151

Djafar, W. (2019). Hukum perlindungan data pribadi di indonesia: lanskap, urgensi dan kebutuhan pembaruan. In Seminar Hukum dalam Era Analisis Big Data, Program Pasca Sarjana Fakultas Hukum UGM (Vol. 26).

Estrada, Francisco Javier Rocha, Carlos Enrique George-Reyes, dan Leonardo David Glasserman-Morales (2022) Security as an Emerging Dimension of Digital Literacy for education: a Systematic Literature Review , Journal of eLearning and Knowledge Society, , 22-33

FISIP UI (2021). Cyber Crime Meningkat Tajam di Masa Pandemi. https://fisip.ui.ac.id/bhakti-cybercrime-menjadi-jenis-kejahatan-yangmengalami-peningkatan-cukup-tinggi/

Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang Perlindungan Data Pribadi. Jurnal Hukum UNISSULA, 37(2).

Jafri, Johan Ariff , Syajarul Imna Mohd Amin, Aisyah Abdul Rahman, Shifa Mohd Nor, (2024)A Systematic Literature Review of The Role of Trust And Security On Fintech Adoption In Banking, Heliyon, 10(1). Https://Doi.Org/10.1016/J.Heliyon.2023.E22980

Kaewkungwal J, Adams P, Sattabongkot J, Lie RK, Wendler D. (2020) Issues and Challenges Associated with Data-Sharing in LMICs: Perspectives of Researchers in Thailand. American Journal of Tropical Medicine Hygiene. 103(1):528-536. doi: 10.4269/ajtmh.19-0651

Karale, Ashwin (2021) The Challenges of IOT Addressing Security, Ethics, Privacy, And Laws, Internet of Things, 15: https://doi.org/10.1016/j.iot.2021.100420

Kompas (2021). Orang Indonesia Hanya Bisa Pasrah Kalau Ada Kebocoran Data. https://tekno.kompas.com/read/2021/09/02/13020027/orang-indonesiahanya-bisa-pasrah-kalau-ada-kebocoran-data?page=all

Kompas (2021). Sistem Keamanan Siber Indonesia Lemah , Perlu Ada Aturan untuk Perlindungan Data https://www.kompas.tv/article/211282/sistem-keamanansiber-indonesia-lemah-perlu-ada-aturan-untuk-perlindungan-data.

Karanfiloğlu, Mehmet (2022) Digital Literacy In Increasing Data Security:An Evaluation From The Communicator's Perspective, In Muzaffer Yilmaz Ismail Çalişkan (Eds.) Privacy in The Digital Age Digital Communication and Personal Data. Istanbul: Republic of Turkey Ministry of Culture and Tourism

Lee, Wanbil W., Zankl, Wolfgang dan Chang, Henry (2016) An Ethical Approach to Data Privacy Protection, ISACA Journal, 6,1-9

Lane, Julia and Schur, Claudia (2010) Balancing Access to Health Data and Privacy: A Review of The Issues and Approaches for The Future, Health Service Research. 45(5), 1456–1467.

Marqués, José Manuel, Fernando Ávila, Anahí Rodríguez-Martínez, Raúl MoralesReséndiz, Antonio Marcos, Tamara Godoy, Pablo Villalobos, Andrea Ocontrillo, Valerie Ann Lankester, Clemente Blanco, Karla Reyes, Silvia Irina Lopez, Ana Fernández, Román Santos, Luis Ángel Maza, Manuel Sánchez, Carlos Domínguez, Natalie Haynes, Novelette Panton, Mario Griffiths, Kurt Murray, Michelle DoyleLowe, Leslie Ann Des Vignes, Michelle Francis-Pantor, (2021) Policy Report On Fintech Data Gaps, Latin American Journal Of Central Banking,2(3), Https://Doi.Org/10.1016/J.Latcb.2021.100037

Media Indonesia (2021). Kejahatan Siber di RI Terus Meningkat, Capai 448 Juta Kasus. https://mediaindonesia.com/politik-dan-hukum/414225/serangan-siber-di-riterus-meningkat- capai-448-juta-kasus

Mishra, Alok Yehia Ibrahim Alzoubi, Memoona Javeria Anwar, Asif Qumer Gill, (2022) Attributes Impacting Cybersecurity Policy Development: An Evidence From Seven Nations,Computers & Security, 120. https://doi.org/10.1016/j.cose.2022.102820.

Mutiara, U., & Maulana, R. (2020). Perlindungan Data Pribadi sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi. Indonesian Journal of Law and Policy Studies, 1(1).

Niffari, H. (2020). Perlindungan Data Pribadi sebagai Bagian dari Hak Asasi Manusia atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif dengan Peraturan Perundang-undangan di Negara Lain). Jurnal Yuridis, 7(1), 105-119.

Nurhidayati, Sugiyah, & Yuliantari, K. (2021). Pengaturan Perlindungan Data Pribadi dalam Penggunaan Aplikasi PeduliLindungi. Widya Cipta: Jurnal Sekretari dan Manajemen, 5(1).

Pascual, Antonio dan Natalucci, Fabio (2022) Fast-Moving Fintech Poses Challenge For Regulators . https://www.imf.org/en/blogs/articles/2022/04/13/blog041322- sm2022-gfsr-ch3

Putri, Deanne Destriani Firmansyah dan Fahrozi, Muhammad Helmi (2021) Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com). Borneo Law Review, 5(1), 46-68

Ruof, C. (2023). Conceptualizing A Regulatory Response to Fintech. In: Regulating Financial Innovation . Ebi Studies in Banking And Capital Markets Law. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-32971-5_8

Tovi, Muli David dan Muthama, Mutua Nicholas (2013) Addressing The Challenges Of Data Protection In Developing Countries, European Journal of Computer Science and Information Technology.1(1),1- 9

Tempo (2021). Darurat Regulasi Perlindungan Data Pribadi. https://koran.tempo.co/read/info-tempo/467843/darurat-regulasipelindungan-data-pribadi

Universitas Gajah Mada (2021). Pentingnya Ratifikasi RUU Perlindungan Data Pribadi. https://www.ugm.ac.id/id/berita/21171-pentingnya-ratifikasi-ruuperlindungan-data-pribadi

Walters, Robert (2022) Cross-Border Data Flows: An Evolving Multi-Layered Regulatory Approach Required. Global Privacy Law Review, 3(1), 29 – 45

Yuniarti, S. (2019). Perlindungan Hukum Data Pribadi di Indonesia. Jurnal BECOSS (Business Economic Communication and Social Sciences), 1(1), 147-154.