DOI: https://doi.org/10.62017/syariah

"DINAMIKA HUKUM TELEMATIKAN DALAM ERA DIGITAL: PERLINDUNGAN PRIVASI DAN KEAMANAN DATA DI INDONESIA"

Rifla Mufarihana Zahira *[1]
Rayhan Muktafin Zharfan [2]
Dewi Asri Puannandini [3]

[1,2,3] Universitas Islam Nusantara
*e-mail: riflamufarihana@gmail.com [1], mzrayhan1@gmail.com [2]

Abstrak

Dinamika hukum telematika dalam era digital menunjukkan pentingnya perlindungan privasi dan keamanan data di Indonesia. Berbagai temuan mengindikasikan bahwa masih terdapat celah dalam regulasi dan penegakan hukum, yang diperburuk oleh rendahnya kesadaran masyarakat terhadap risiko keamanan digital. Kebocoran data pribadi telah memberikan dampak nyata, baik dalam bentuk kerugian finansial maupun ancaman terhadap privasi individu, sehingga mendorong perlunya tindakan segera dari semua pemangku kepentingan. Metode penelitian yang digunakan adalah metode yuridis normatif, yang bertumpu pada analisis terhadap peraturan perundang-undangan, doktrin hukum, serta berbagai literatur yang relevan. Penelitian ini memanfaatkan data sekunder sebagai sumber utama, termasuk undang-undang dan dokumen hukum lainnya. Implikasi hukum dari dinamika ini mencakup perlunya implementasi tegas terhadap peraturan yang ada, khususnya Undang-Undang Perlindungan Data Pribadi, serta penguatan kapasitas kelembagaan untuk menangani pelanggaran yang semakin kompleks.

***Kata kunci**: Hukum Telematika, Privasi, Keamanan Data*

Abstract

The dynamics of telematics law in the digital era highlight the importance of protecting privacy and data security in Indonesia. Various findings indicate that regulatory and enforcement gaps persist, exacerbated by the public's low awareness of digital security risks. Personal data breaches have had tangible impacts, ranging from financial losses to threats to individual privacy, emphasizing the urgent need for action from all stakeholders. The research methodology employed is normative juridical, focusing on the analysis of legislation, legal doctrines, and relevant literature. This study utilizes secondary data as its primary source, including laws and other legal documents. The legal implications of these dynamics include the necessity for strict implementation of existing regulations, particularly the Personal Data Protection Act, and strengthening institutional capacity to address increasingly complex violations.

***Keywords**: Telematics Law, Privacy, Data Security*

PENDAHULUAN

Perkembangan teknologi telematika telah membawa perubahan signifikan dalam berbagai aspek kehidupan manusia. Sebagai integrasi antara teknologi telekomunikasi, informatika, dan multimedia, telematika memungkinkan pengumpulan, pengolahan, dan distribusi data secara cepat dan efisien. Dengan hadirnya teknologi seperti Internet of Things (IoT), big data, kecerdasan buatan (AI), dan jaringan 5G, aktivitas digital semakin mempermudah kehidupan masyarakat, termasuk dalam bidang ekonomi, pendidikan, kesehatan, dan pemerintahan. Di Indonesia, transformasi digital ini terlihat dari tingginya penetrasi internet, yang menurut laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mencapai 77% pada tahun 2023, dengan mayoritas aktivitas digital melibatkan interaksi berbasis data.

Namun, di balik kemajuan tersebut, perlindungan privasi dan keamanan data menjadi isu yang semakin mendesak. Data pribadi kini menjadi salah satu aset paling berharga dalam era digital, baik untuk keperluan bisnis maupun kebijakan publik. Sayangnya, data pribadi juga rentan terhadap penyalahgunaan, baik oleh pihak swasta maupun aktor jahat, seperti peretasan, pencurian identitas, dan penyalahgunaan data untuk tujuan yang melanggar hukum. Di Indonesia, berbagai kasus kebocoran data telah mencuat dalam beberapa tahun terakhir, seperti kebocoran data pelanggan pada platform e-commerce besar dan instansi pemerintah, yang mengakibatkan

DOI: https://doi.org/10.62017/syariah

kerugian bagi jutaan pengguna serta menurunkan tingkat kepercayaan masyarakat terhadap pengelolaan data digital.

Dalam konteks hukum, Indonesia telah mengambil langkah-langkah untuk mengatur perlindungan privasi dan keamanan data melalui berbagai regulasi. Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menjadi salah satu kerangka awal yang mengatur aktivitas digital, termasuk perlindungan data. Namun, kebutuhan akan regulasi yang lebih spesifik dan komprehensif mendorong lahirnya Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang sering dibandingkan dengan General Data Protection Regulation (GDPR) di Uni Eropa. UU PDP memberikan landasan hukum bagi pengelolaan data pribadi, termasuk hak-hak individu atas data mereka dan kewajiban pengelola data untuk memastikan keamanan serta transparansi.

Meskipun regulasi telah ada, tantangan dalam implementasi tetap signifikan. Keterbatasan infrastruktur hukum, kurangnya kesadaran masyarakat akan hak privasi, serta lemahnya penegakan hukum menjadi hambatan utama dalam menciptakan ekosistem digital yang aman dan terpercaya. Oleh karena itu, dinamika hukum telematika di Indonesia perlu dikaji lebih dalam untuk memahami bagaimana regulasi dapat mengikuti perkembangan teknologi dan menjawab kebutuhan perlindungan privasi serta keamanan data di era digital. Penelitian ini bertujuan untuk menganalisis perkembangan hukum telematika di Indonesia, menyoroti tantangan dalam perlindungan data pribadi, serta menawarkan solusi yang relevan dalam konteks transformasi digital yang terus berlangsung.

METODOLOGI PENELITIAN

Metode penelitian yang digunakan dalam kajian mengenai *Dinamika Hukum Telematika dalam Era Digital: Perlindungan Privasi dan Keamanan Data di Indonesia* adalah metode yuridis normatif, yang bertumpu pada analisis terhadap peraturan perundang-undangan, doktrin hukum, serta berbagai literatur yang relevan. Penelitian ini memanfaatkan data sekunder sebagai sumber utama, termasuk undang-undang, peraturan pemerintah, perjanjian internasional, artikel ilmiah, dan dokumen hukum lainnya.

Pendekatan yang digunakan adalah pendekatan konseptual dan perundang-undangan. Pendekatan konseptual berfokus pada pemahaman mendalam mengenai konsep hukum telematika, privasi, dan keamanan data, serta kaitannya dengan hak-hak asasi manusia dalam kerangka hukum nasional dan internasional. Pendekatan perundang-undangan bertujuan untuk menganalisis sejauh mana regulasi di Indonesia mampu memberikan perlindungan hukum terhadap privasi dan keamanan data, dengan membandingkan kebijakan domestik dan praktik global yang relevan.

Analisis dilakukan secara kualitatif, yang melibatkan interpretasi mendalam terhadap teks hukum dan data sekunder untuk mengidentifikasi kekuatan, kelemahan, dan peluang pengembangan kerangka hukum telematika di Indonesia. Penelitian ini juga mempertimbangkan perkembangan teknologi informasi dan komunikasi serta dampaknya terhadap perlindungan privasi dan keamanan data. Hasil analisis ini diharapkan mampu memberikan gambaran komprehensif mengenai dinamika hukum telematika di era digital serta rekomendasi untuk penguatan regulasi di Indonesia.

HASIL DAN PEMBAHASAN

Konsep Telematika

Telematika merupakan bidang yang menggabungkan teknologi telekomunikasi, informatika, dan multimedia untuk mendukung pengelolaan, pengolahan, dan pengiriman informasi secara efisien. Istilah telematika berasal dari gabungan kata "telekomunikasi" dan "informatika," yang mencerminkan sinergi antara jaringan komunikasi dan teknologi informasi. Hukum telematika, atau yang sering disebut sebagai cyber law, merupakan kumpulan asas, norma, kaidah, lembaga, institusi, dan proses yang berfungsi untuk mengatur aktivitas di dunia maya yang dilakukan melalui penggunaan teknologi informasi dan komunikasi (TIK) (Ramli, 2016). Dalam praktiknya,

DOI: https://doi.org/10.62017/syariah

telematika mencakup berbagai aplikasi, seperti sistem navigasi, layanan berbasis internet, Internet of Things (IoT), dan infrastruktur digital lainnya.
Ruang lingkup telematika mencakup berbagai aspek yang berkaitan dengan penerapan teknologi informasi dan komunikasi di berbagai sektor. Hal ini meliputi penyediaan layanan digital, pengembangan aplikasi berbasis data, pengelolaan jaringan telekomunikasi, serta sistem keamanan informasi. Selain itu, telematika juga mencakup pengaturan mengenai penggunaan teknologi dalam layanan publik, seperti e-government, transportasi pintar, dan layanan kesehatan digital.

Di Indonesia, perkembangan telematika ditopang oleh pesatnya adopsi teknologi digital dan akses internet, yang memungkinkan berbagai inovasi dalam sektor ekonomi, pendidikan, dan pemerintahan. Namun, implementasi telematika juga memunculkan tantangan, seperti kebutuhan akan regulasi yang memadai, perlindungan data pribadi, serta penguatan infrastruktur digital untuk menjamin akses yang merata bagi seluruh masyarakat.
Telematika memainkan peran penting dalam kehidupan sehari-hari dengan mendukung berbagai aktivitas yang mengandalkan teknologi informasi dan komunikasi. Dalam era digital saat ini, telematika tidak hanya menjadi pelengkap, tetapi juga menjadi bagian integral dari cara manusia berinteraksi, bekerja, dan memenuhi kebutuhan.
Dalam bidang komunikasi, telematika memfasilitasi konektivitas global melalui layanan internet, telepon seluler, dan aplikasi pesan instan. Hal ini memungkinkan komunikasi yang lebih cepat dan efisien, baik dalam konteks pribadi maupun profesional. Kehadiran platform media sosial, konferensi video, dan layanan berbasis cloud juga memperkuat hubungan sosial dan mendukung kerja jarak jauh.
Di sektor transportasi, telematika digunakan untuk mengembangkan sistem navigasi, seperti GPS, yang membantu pengguna menemukan rute tercepat dan menghindari kemacetan. Selain itu, teknologi telematika mendukung pengembangan kendaraan otonom dan manajemen lalu lintas pintar, yang bertujuan meningkatkan efisiensi dan keselamatan dalam berkendara.
Dalam bidang ekonomi, telematika menjadi tulang punggung perdagangan elektronik (e-commerce) yang memungkinkan masyarakat melakukan transaksi kapan saja dan di mana saja. Platform pembayaran digital dan pengelolaan inventaris berbasis telematika juga membantu pelaku usaha meningkatkan produktivitas dan efisiensi.
Di sektor pendidikan, telematika mendukung pembelajaran jarak jauh melalui platform e-learning yang memungkinkan siswa dan guru berinteraksi secara virtual. Teknologi ini mempermudah akses ke sumber belajar digital, sehingga meningkatkan inklusivitas pendidikan.
Selain itu, telematika juga berperan dalam layanan kesehatan melalui telemedicine, yang memungkinkan pasien berkonsultasi dengan dokter tanpa perlu datang langsung ke fasilitas medis. Teknologi ini sangat membantu terutama dalam situasi darurat atau di daerah terpencil dengan akses terbatas ke layanan kesehatan.
Secara keseluruhan, telematika telah menjadi pilar utama dalam kehidupan modern, menciptakan efisiensi, kenyamanan, dan inovasi dalam berbagai aspek kehidupan sehari-hari. Namun, seiring dengan manfaatnya, penggunaan telematika juga memerlukan pengelolaan yang bijak untuk mengatasi tantangan, seperti perlindungan data pribadi dan keamanan informasi.

Privasi dan Keamanan Data
Privasi Data
Privasi data adalah hak individu untuk mengontrol informasi pribadi mereka, termasuk pengumpulan, penyimpanan, penggunaan, dan distribusinya. Privasi data memastikan bahwa data pribadi seseorang, seperti nama, alamat, nomor identitas, riwayat kesehatan, atau data keuangan, hanya digunakan untuk tujuan yang telah disetujui oleh pemilik data. Dalam konteks hukum dan etika, privasi data bertujuan untuk melindungi individu dari penyalahgunaan data yang dapat merugikan, seperti pencurian identitas, pelacakan tanpa izin, atau penyebaran informasi tanpa persetujuan.

DOI: https://doi.org/10.62017/syariah

Keamanan data adalah serangkaian tindakan, kebijakan, dan teknologi yang dirancang untuk melindungi data dari ancaman seperti akses tidak sah, pencurian, perusakan, atau modifikasi. Keamanan data melibatkan langkah-langkah teknis, seperti enkripsi, pengelolaan kata sandi, firewall, dan pengendalian akses, serta prosedur operasional, seperti audit keamanan dan pelatihan pengguna. Tujuan utama dari keamanan data adalah memastikan bahwa data tetap rahasia (confidentiality), utuh (integrity), dan dapat diakses sesuai kebutuhan (availability).
Privasi dan keamanan data saling berkaitan tetapi memiliki fokus yang berbeda. Privasi data berfokus pada pengelolaan hak individu atas data pribadinya, sementara keamanan data berfokus pada perlindungan teknis dan operasional untuk menjaga data dari ancaman atau pelanggaran. Untuk menjamin privasi, keamanan data yang kuat harus diterapkan. Sebaliknya, tanpa kebijakan privasi yang jelas, keamanan data tidak dapat memastikan bahwa hak individu atas data pribadinya terlindungi. Privasi data berkaitan dengan pengelolaan akses terhadap informasi pribadi seseorang, memastikan hanya pihak yang berwenang yang dapat mengaksesnya. Sementara itu, keamanan data berfokus pada perlindungan integritas dan kerahasiaan informasi agar terhindar dari akses tidak sah atau potensi kerusakan (Ramli, 2016).

Kerangka Hukum Telematika di Indonesia

Kerangka hukum telematika mencakup empat elemen utama yang saling terkait:

1. **Isi (Content):** Merupakan substansi dari data atau informasi yang menjadi masukan dan keluaran dari pengoperasian sistem informasi yang tersedia untuk publik. Elemen ini mencakup berbagai jenis data atau informasi, baik yang tersimpan dalam format cetak maupun digital, serta yang dikelola dalam basis data (database) atau disampaikan melalui pesan data (data messages).
2. **Komputasi (Computing):** Berkaitan dengan sistem pengolahan informasi yang berbasis komputer (Computer-Based Information System). Sistem ini adalah jaringan informasi organisasi yang dirancang untuk beroperasi secara efisien, efektif, dan sesuai hukum. Dalam hal ini, sistem informasi mencerminkan penerapan teknologi informasi dalam struktur organisasi atau perusahaan (bisnis).
3. **Komunikasi (Communication):** Menunjukkan sistem komunikasi yang mencakup keterhubungan (interconnection) dan interoperabilitas global antara jaringan komputer atau sistem informasi. Elemen ini juga mencakup penyelenggaraan layanan dan jaringan telekomunikasi yang mendukung proses komunikasi.
4. **Komunitas (Community):** Mengacu pada keberadaan masyarakat dan sistem sosial yang berperan sebagai pelaku intelektual (brainware) dalam kerangka telematika. Peran masyarakat mencakup pelaku usaha, profesional pendukung, serta pengguna yang terlibat dalam sistem tersebut. Tingkat efektivitas hukum sebagai aturan (rule of law) bergantung pada pemahaman dan kesadaran hukum masyarakat terhadap peraturan yang berlaku.

Kerangka hukum telematika ini menunjukkan hubungan erat antara teknologi, informasi, komunikasi, dan masyarakat dalam pengaturan aktivitas digital dan penggunaan teknologi informasi. Sumber hukum telematika dapat dikategorikan ke dalam sumber hukum yang bersifat internasional, yang meliputi (Safiranita et al., n.d.):

1. Konvensi internasional di ranah publik maupun perdata.
2. Praktik atau kebiasaan yang telah diterima secara internasional.
3. Kebijakan internasional di bidang hukum siber, seperti Uniform Domain Name Resolution Dispute Policy (UDRP).

Dinamika Hukum Telematika di Indonesia

Hukum telematika di Indonesia terus berkembang seiring dengan pesatnya transformasi digital dan meningkatnya kebutuhan akan regulasi yang mampu mengakomodasi perubahan teknologi. Dinamika hukum telematika mencerminkan upaya pemerintah untuk menyeimbangkan antara kemajuan teknologi informasi dan komunikasi (TIK), perlindungan hak-hak masyarakat, serta kebutuhan akan keamanan siber.

DOI: https://doi.org/10.62017/syariah

Salah satu tonggak utama adalah pengesahan **Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Nomor 11 Tahun 2008**, yang menjadi dasar hukum untuk mengatur aktivitas digital, termasuk transaksi elektronik, penyebaran informasi, dan perlindungan data elektronik. Perubahan pada UU ITE melalui **Undang-Undang Nomor 19 Tahun 2016** menunjukkan respons pemerintah terhadap tantangan yang muncul, seperti penyalahgunaan media sosial, pencemaran nama baik, dan penyebaran hoaks.

Selain itu, Indonesia juga telah memiliki **Undang-Undang Pelindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022**, yang memberikan kerangka kerja untuk melindungi data pribadi masyarakat di era digital. UU ini menjadi langkah penting dalam menjawab kebutuhan akan regulasi yang melindungi privasi individu sekaligus meningkatkan kepercayaan masyarakat terhadap layanan digital.

Dalam konteks keamanan siber, peran **Badan Siber dan Sandi Negara (BSSN)**, yang dibentuk berdasarkan **Peraturan Presiden Nomor 53 Tahun 2017**, sangat vital. BSSN bertugas melindungi infrastruktur informasi kritis nasional dan menangani ancaman siber yang semakin kompleks.

Namun, dinamika hukum telematika di Indonesia juga menghadapi berbagai tantangan, termasuk:

1. **Tantangan Literasi Digital:** Rendahnya tingkat literasi digital masyarakat sering kali menyebabkan penyalahgunaan teknologi dan pelanggaran hukum, seperti penyebaran konten negatif dan penipuan daring.
2. **Penegakan Hukum:** Masih terdapat kesenjangan dalam penegakan hukum terkait kejahatan siber, perlindungan data pribadi, dan pelanggaran lainnya di ruang digital.
3. **Kesenjangan Infrastruktur Digital:** Akses teknologi yang belum merata di seluruh wilayah Indonesia menjadi hambatan dalam penerapan hukum telematika secara menyeluruh.

Meski begitu, pemerintah terus berupaya menyempurnakan kerangka hukum telematika untuk mendukung inovasi teknologi, perlindungan konsumen, dan keamanan nasional. Ke depan, penguatan kolaborasi antara pemerintah, sektor swasta, dan masyarakat sangat diperlukan untuk menciptakan ekosistem digital yang aman, adil, dan berkelanjutan di Indonesia.

Pengaruh Globalisasi terhadap Hukum Telematika

Globalisasi telah membawa dampak yang signifikan terhadap perkembangan hukum telematika di seluruh dunia, termasuk di Indonesia. Dengan meningkatnya konektivitas global dan pertukaran informasi lintas negara, hukum telematika mengalami berbagai dinamika yang dipengaruhi oleh aspek teknologi, ekonomi, dan sosial yang semakin terintegrasi. Berikut adalah beberapa pengaruh utama globalisasi terhadap hukum telematika:

1. Peningkatan Kompleksitas Regulasi

Globalisasi telah menyebabkan meningkatnya transaksi lintas batas dan penggunaan teknologi informasi secara global. Hal ini menimbulkan kebutuhan akan regulasi yang mampu mengatasi isu-isu hukum yang bersifat transnasional, seperti perlindungan data pribadi, keamanan siber, dan sengketa domain. Sebagai contoh, Indonesia harus menyesuaikan regulasi lokal dengan standar internasional, seperti General Data Protection Regulation (GDPR) di Uni Eropa, untuk menjaga daya saing dan perlindungan data dalam transaksi lintas negara.

2. Harmonisasi Hukum Internasional

Globalisasi mendorong upaya harmonisasi hukum telematika antarnegara. Misalnya, berbagai konvensi internasional, seperti **Budapest Convention on Cybercrime**, menjadi acuan bagi banyak negara dalam mengembangkan kerangka hukum siber. Indonesia, meskipun belum menjadi pihak dalam konvensi tersebut, perlu menyelaraskan regulasi telematika domestik dengan prinsip-prinsip hukum internasional untuk memperkuat posisi dalam kerja sama global.

3. Meningkatnya Ancaman Siber Lintas Negara

Globalisasi memungkinkan ancaman siber, seperti serangan malware, pencurian data, dan peretasan, terjadi secara lintas negara. Hal ini menuntut hukum telematika untuk beradaptasi dengan cepat dalam menghadapi tantangan global, seperti kejahatan siber yang terorganisir dan sulit dilacak. Kerja sama internasional melalui mekanisme ekstradisi, mutual legal assistance, dan koordinasi penegakan hukum menjadi semakin penting.

DOI: https://doi.org/10.62017/syariah

4. Pengaruh Kebijakan Ekonomi Digital Global
Ekonomi digital yang berkembang pesat sebagai dampak globalisasi memengaruhi hukum telematika, khususnya dalam regulasi terkait e-commerce, fintech, dan platform digital. Indonesia harus mengatur aktivitas ekonomi digital ini agar sesuai dengan hukum domestik sekaligus mendukung keterlibatan dalam pasar global. Peraturan seperti **UU Nomor 11 Tahun 2020 tentang Cipta Kerja** dan aturan turunannya mencerminkan respons terhadap dinamika ekonomi global yang berbasis teknologi.

5. Percepatan Inovasi Teknologi
Globalisasi mendorong adopsi teknologi baru secara cepat, seperti kecerdasan buatan (AI), blockchain, dan Internet of Things (IoT). Hukum telematika harus mampu mengikuti perkembangan teknologi ini dengan mengatur penggunaannya, seperti aspek keamanan, privasi, dan etika teknologi, agar tidak tertinggal dari negara-negara lain.
6. Tantangan Budaya dan Etika
Globalisasi juga membawa pengaruh budaya, yang dapat menciptakan konflik nilai antara norma hukum lokal dengan praktik global. Misalnya, perlindungan privasi data di beberapa negara mungkin berbeda standar dengan di Indonesia, sehingga memerlukan adaptasi hukum yang tetap menghormati nilai-nilai lokal.

Globalisasi telah mempercepat perkembangan hukum telematika dengan membuka peluang baru sekaligus menghadirkan tantangan yang kompleks. Untuk menghadapi pengaruh globalisasi, Indonesia perlu terus memperbarui kerangka hukum telematika dengan mengacu pada standar internasional, meningkatkan literasi digital masyarakat, serta memperkuat kerja sama global di bidang telematika. Hal ini penting untuk menciptakan ekosistem digital yang aman, adil, dan sesuai dengan kebutuhan zaman.

A. Perlindungan Privasi dan Keamanan Data di Era Digital
A. Mekanisme Perlindungan Data Pribadi
Keamanan data pribadi merupakan hak asasi manusia yang harus dijamin dan dihormati. Indonesia, sebagai negara berkembang dengan adopsi teknologi yang pesat, memiliki tanggung jawab untuk melindungi data pribadi sebagai hak privasi (Anggen Suari & Sarjana, 2023). Setiap individu dapat memilih untuk melakukan privacy terhadap data yang dimiliki atau membagikannya, kebebasan tersebut di dilindungi oleh undangundang yang berlaku di Indonesia (Erna, 2019). Berdasarkan dasar hukum yang berlaku, masyarakat Indonesia memiliki hak konstitusional untuk melindungi privasi mereka, termasuk privasi terkait informasi pribadi. Negara memiliki kewajiban, berdasarkan ketentuan konstitusional, untuk menyediakan perlindungan hukum dalam berbagai aspek kehidupan warga negaranya. Perlindungan hukum ini bertujuan untuk memastikan adanya manfaat hukum, keadilan, serta kejelasan dalam pelaksanaannya.
Terkait perlindungan data pribadi, Pemerintah Indonesia telah mengambil sejumlah langkah dan inisiatif, antara lain:

- **Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)**

UU ITE, meskipun berfokus pada transaksi elektronik dan keamanan informasi, juga mencakup ketentuan perlindungan data pribadi dalam sistem elektronik. Pengelola data diwajibkan melindungi data pribadi dan dikenakan sanksi atas pelanggaran yang melanggar hak privasi individu.

- **Penyusunan Undang-Undang Perlindungan Data Pribadi**

Pemerintah telah menginisiasi rancangan undang-undang (RUU) yang secara spesifik mengatur perlindungan data pribadi. Langkah ini menunjukkan komitmen untuk memberikan perlindungan data yang lebih terarah, meskipun pada saat penyusunan, RUU ini belum disahkan menjadi undang-undang.

DOI: https://doi.org/10.62017/syariah

- **Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016**
Peraturan ini mengatur tata kelola data pribadi dalam sistem elektronik, memberikan pedoman terkait pengelolaan data yang benar, serta menjamin praktik perlindungan yang sesuai dengan standar hukum.
- **Regulasi Perlindungan Data Pribadi di Sektor-Sektor Tertentu**
Sektor-sektor seperti perbankan, kesehatan, dan telekomunikasi memiliki aturan khusus terkait perlindungan data pribadi. Contohnya, Bank Indonesia telah mengeluarkan regulasi yang mengatur perlindungan data nasabah.
- **Pengawasan dan Penegakan Hukum**
Pemerintah melakukan pengawasan terhadap pihak-pihak yang mengelola data pribadi. Pelanggaran terhadap ketentuan perlindungan data dapat dikenakan sanksi untuk memastikan kepatuhan.
- **Kampanye Kesadaran Publik**
Kampanye publik dilakukan untuk meningkatkan kesadaran masyarakat mengenai pentingnya melindungi data pribadi serta memberikan edukasi tentang praktik berbagi informasi yang aman.
- **Pengembangan Kerangka Kerja Keamanan Data**
Pemerintah juga merancang kerangka kerja keamanan data untuk membantu organisasi dan perusahaan melindungi data pribadi yang mereka kelola dari ancaman atau penyalahgunaan.
- **Kerja Sama Internasional**
Indonesia terlibat dalam kerja sama global terkait perlindungan data pribadi dengan mengacu pada standar internasional. Ini menunjukkan upaya untuk menyesuaikan regulasi nasional dengan praktik terbaik yang diakui secara global.

Pemerintah Indonesia memiliki tanggung jawab untuk merumuskan dan mengimplementasikan regulasi yang efektif terkait perlindungan data pribadi. Pemerintah perlu berperan aktif dalam menetapkan aturan yang relevan, memberikan edukasi serta meningkatkan kesadaran masyarakat tentang hak privasi, dan memastikan pengawasan serta penegakan hukum terhadap pelanggaran privasi data. Saat ini, meskipun Indonesia telah menyusun rancangan undang-undang terkait perlindungan data pribadi, belum ada regulasi khusus yang secara eksplisit mengatur hal ini. Namun demikian, terdapat beberapa undang-undang yang mengatur perlindungan data pribadi secara tidak langsung, di antaranya:

1. **Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan**
Dalam undang-undang ini, istilah "rahasia bank" merujuk pada semua informasi yang berkaitan dengan nasabah dan simpanannya, sebagaimana diatur dalam Pasal 1 Ayat (28). Pasal 40 Ayat (1) menyatakan bahwa bank wajib menjaga kerahasiaan informasi nasabah, kecuali dalam kondisi tertentu sebagaimana dijelaskan dalam Pasal 41, 41A, 42, 44, dan 44A. Hal ini menegaskan kewajiban bank untuk melindungi data pribadi nasabah dari akses yang tidak sah.
2. **Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi**
Meskipun tidak secara khusus mengatur perlindungan data pribadi, UU Telekomunikasi mencakup kewajiban penyelenggara jasa telekomunikasi untuk menjaga kerahasiaan informasi yang dikirimkan atau diterima oleh pelanggan, sebagaimana tercantum dalam Pasal 42 Ayat (1). Penyelenggara jasa telekomunikasi diwajibkan untuk menjamin keamanan data yang dikirim atau diterima melalui jaringan telekomunikasi.

Selain itu, Pasal 42 Ayat (2) memberikan izin kepada penyelenggara jasa telekomunikasi untuk merekam dan memberikan informasi yang diperlukan dalam proses peradilan pidana, dengan syarat adanya permintaan tertulis dari Kejaksaan Agung atau Kepala Kepolisian Negara Republik Indonesia. Pelanggaran terhadap Pasal 42 Ayat (1) dapat dikenakan sanksi berupa pidana penjara hingga dua tahun atau denda maksimal Rp200.000.000, sebagaimana diatur dalam Pasal 57.

Undang-Undang Telekomunikasi juga mencakup ketentuan sanksi terhadap pelanggaran yang berkaitan dengan keamanan informasi dan kerahasiaan data. Hal ini menunjukkan upaya untuk menjamin perlindungan privasi dan keamanan informasi, meskipun pengaturannya masih bersifat sektoral.

DOI: https://doi.org/10.62017/syariah

3. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (UU HAM)
Hukum yang mengatur hak asasi manusia memberikan landasan hukum bagi perlindungan hak individu. Berdasarkan Pasal 14 Ayat (1) UU HAM, setiap orang memiliki hak untuk berkomunikasi dan memperoleh informasi yang diperlukan guna mengembangkan kepribadian serta lingkungan sosialnya. Ketentuan ini menegaskan bahwa hak individu untuk mendapatkan informasi yang relevan sangat penting dalam mendukung perkembangan pribadi dan kualitas lingkungan tempat mereka tinggal.
Selain itu, Pasal 29 Ayat (1) menyatakan bahwa setiap orang berhak melindungi diri sendiri, keluarganya, kehormatan, martabat, serta hak miliknya. Hak ini juga dijamin dalam Pasal 28G Ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUDNRI 1945). Dalam Pasal 32 UU HAM, dijelaskan bahwa kebebasan dan kerahasiaan dalam komunikasi, termasuk melalui sarana elektronik, tidak boleh diganggu kecuali berdasarkan perintah hakim atau pejabat berwenang sesuai dengan undang-undang. Ketentuan ini menunjukkan bahwa hak atas perlindungan data pribadi dan privasi dalam komunikasi telah menjadi bagian penting dari kerangka hukum hak asasi manusia.
4. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)
Pasal 26 Ayat (1) UU ITE menjadi salah satu ketentuan yang secara eksplisit menjamin perlindungan data pribadi, khususnya setelah data tersebut diproses. Meski demikian, UU ITE secara keseluruhan lebih banyak mengatur aktivitas ilegal terkait informasi elektronik, seperti yang dijabarkan dalam Pasal 27 hingga Pasal 37. Ketentuan-ketentuan ini secara umum melarang tindakan yang melanggar hak atau menyalahgunakan informasi elektronik secara sengaja yang dapat merugikan pihak lain, termasuk pemilik data. Dengan demikian, meskipun perlindungan data pribadi belum menjadi fokus utama UU ITE, aturan-aturan ini tetap memberikan dasar hukum untuk melindungi hak-hak pemilik informasi dari penyalahgunaan.
Menyusul beberapa kasus peretasan, Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) yang diharapkan DPR RI dapat disahkan menjadi undang-undang tampaknya menjadi angin segar bagi warga Indonesia. Penyadaran sektor komersial, organisasi pemerintah, dan masyarakat merupakan masalah terbesar pemerintah dalam mewujudkan UU PDP (Anggen Suari & Sarjana, 2023).

B. Tantangan dalam Implementasi Perlindungan Data

Kesadaran masyarakat tentang privasi semakin penting seiring dengan berkembangnya teknologi digital. Banyak orang kini lebih menyadari bahwa data pribadi mereka, seperti informasi identitas, lokasi, dan kebiasaan online, bisa dengan mudah diakses dan disalahgunakan oleh pihak ketiga. Teknologi seperti media sosial, aplikasi, dan platform digital lainnya sering kali mengumpulkan data pengguna tanpa mereka sadari atau dengan izin yang tidak sepenuhnya jelas. Oleh karena itu, penting bagi masyarakat untuk memahami cara melindungi privasi mereka, seperti mengelola pengaturan privasi di aplikasi, menggunakan kata sandi yang kuat, dan lebih berhati-hati dalam membagikan informasi pribadi secara online.
Banyak tantangan yang akan dihadapi dalam pelaksanaan UU PDP ini. Meminimalkan risiko adalah tanggung jawab bersama, tetapi beban di pundak pemerintah jauh lebih berat. Data personal penduduk banyak dikelola pemerintah untuk kebutuhan pelayanan public (Miftahul, 2022). Data pribadi warga banyak dikelola oleh pemerintah untuk mendukung pelayanan publik. Sebagian data diberikan atas dasar kewajiban, seperti nomor induk kependudukan (NIK) dan nomor kartu keluarga (KK). Namun, ada juga yang diserahkan secara sukarela, misalnya saat melamar sebagai aparatur sipil negara (ASN). Dalam konteks ini, terdapat dua poin utama yang perlu diperhatikan: bagaimana menjaga keamanan data dan memastikan pemanfaatannya tetap sesuai tujuan. Data pribadi tidak boleh berubah menjadi komoditas ekonomi yang diperjualbelikan.
Tantangan berikutnya adalah soal kelembagaan. Undang-Undang menyebutkan bahwa perlindungan data pribadi akan diatur oleh lembaga khusus yang ditetapkan dan bertanggung jawab kepada presiden. Namun, hingga kini, belum ada kejelasan terkait kedudukan, struktur, maupun kewenangan lembaga tersebut.

DOI: https://doi.org/10.62017/syariah

Pemilu 2024 menjadi tantangan lain yang perlu diantisipasi. Dalam persaingan politik untuk kursi presiden, kepala daerah, hingga anggota dewan, banyak pihak berupaya mengungkap latar belakang para kandidat. Informasi ini sering digunakan masyarakat untuk menentukan pilihan, tetapi risiko penyalahgunaan data pribadi juga meningkat. Para pengendali dan pemroses data pribadi harus ekstra hati-hati, karena pelanggaran dapat dikenai hukuman pidana hingga 6 tahun penjara dan/atau denda hingga Rp 6 miliar. Data pribadi yang bocor bisa saja diperdagangkan atau digunakan untuk kepentingan yang tidak semestinya.

Selain itu, perilaku masyarakat yang cenderung mudah berbagi data pribadi menjadi perhatian serius. Literasi digital perlu ditingkatkan secara masif agar masyarakat lebih memahami pentingnya melindungi data pribadi. Untuk mempercepat tercapainya tujuan perlindungan data, tata kelola kolaboratif (collaborative governance) juga harus didorong.

Berdasarkan survei "Persepsi Publik atas Perlindungan Data Pribadi 2021" yang dilakukan Kominfo (dikutip dari Databoks), dari lebih dari 11.000 responden, sebanyak 28,7% mengaku pernah mengalami kebocoran data. Dampaknya, 44,1% responden melaporkan kehilangan uang dari rekening bank, sementara 32,2% mengalami pengurangan saldo pada e-wallet. Produk seperti e-wallet dan rekening bank dianggap masyarakat sebagai yang paling rentan terhadap kebocoran data. Survei tersebut juga mengungkapkan bahwa mayoritas masyarakat menolak praktik berbagi atau menjual data pribadi antar lembaga.

Untuk mengantisipasi kebocoran data pribadi, diperlukan langkah-langkah strategis yang melibatkan semua pihak, baik pemerintah, lembaga, maupun masyarakat. Pemerintah harus memperkuat regulasi perlindungan data dan memastikan penegakannya dilakukan secara tegas, termasuk memberi sanksi berat bagi pelanggaran. Selain itu, lembaga keuangan dan platform digital perlu meningkatkan keamanan sistem mereka dengan teknologi terkini, seperti enkripsi data dan autentikasi ganda, untuk meminimalkan risiko akses tidak sah.

Masyarakat juga perlu lebih berhati-hati dalam menjaga data pribadinya. Hal ini mencakup tidak sembarangan membagikan informasi sensitif, seperti nomor kartu identitas atau data finansial, terutama di platform yang tidak terpercaya. Menggunakan kata sandi yang kuat dan berbeda untuk setiap akun, serta rutin menggantinya, juga menjadi langkah penting. Selain itu, literasi digital perlu ditingkatkan melalui kampanye edukasi yang masif agar masyarakat lebih paham tentang risiko dan cara melindungi data pribadi mereka.

Kolaborasi antara sektor publik dan swasta juga sangat diperlukan untuk menciptakan ekosistem digital yang aman. Dengan kerja sama ini, standar keamanan dapat disepakati dan diterapkan secara luas, sekaligus memberikan edukasi yang berkesinambungan kepada pengguna tentang pentingnya menjaga privasi di era digital.

I. Rekomendasi dan Solusi

Rekomendasi dan Solusi terkait Dinamika Hukum Telematika dalam Era Digital: Perlindungan Privasi dan Keamanan Data di Indonesia

1. Penegakan Hukum yang Lebih Ketat

Penegakan hukum perlu ditingkatkan untuk memastikan bahwa pelanggaran terhadap perlindungan data pribadi mendapatkan sanksi yang setimpal. Pemerintah harus memastikan implementasi Undang-Undang Perlindungan Data Pribadi (UU PDP) berjalan efektif, termasuk dengan membentuk lembaga khusus yang memiliki otoritas jelas untuk menangani perlindungan data. Selain itu, pengadilan harus memiliki panduan khusus untuk menangani kasus pelanggaran privasi secara adil dan cepat. Kolaborasi dengan penegak hukum internasional juga penting untuk mengatasi pelanggaran lintas negara.

2. Program Pendidikan tentang Privasi

Pendidikan mengenai pentingnya privasi dan keamanan data harus menjadi bagian dari kurikulum di tingkat sekolah hingga perguruan tinggi. Program ini dapat mencakup pengajaran tentang cara melindungi informasi pribadi, mengidentifikasi ancaman digital, dan memahami hak-hak individu dalam perlindungan data. Di luar pendidikan formal, pelatihan bagi tenaga kerja dan komunitas juga perlu dilakukan untuk memastikan pemahaman yang lebih luas di masyarakat.

3. **Kampanye Kesadaran tentang Keamanan Data**
Pemerintah, organisasi non-pemerintah, dan perusahaan teknologi harus bekerja sama untuk mengadakan kampanye nasional yang menyadarkan masyarakat tentang risiko kebocoran data. Kampanye ini bisa dilakukan melalui media massa, media sosial, dan kegiatan komunitas, dengan fokus pada langkah-langkah praktis seperti mengenali phishing, pentingnya menggunakan autentikasi ganda, dan manfaat dari pembaruan perangkat lunak secara berkala.
4. **Inovasi dalam Teknologi Keamanan**
Perusahaan teknologi perlu terus mengembangkan inovasi untuk meningkatkan keamanan data, seperti penggunaan teknologi blockchain untuk transaksi yang lebih aman, pengembangan sistem enkripsi yang lebih kuat, dan implementasi kecerdasan buatan untuk mendeteksi ancaman siber secara dini. Pemerintah juga dapat memberikan insentif bagi perusahaan yang berinvestasi dalam pengembangan teknologi keamanan atau menerapkan standar tinggi dalam melindungi data pengguna.
Dengan langkah-langkah ini, Indonesia dapat mengatasi dinamika hukum telematika dan menciptakan ekosistem digital yang aman serta memberikan perlindungan optimal terhadap privasi dan data pribadi masyarakat.

KESIMPULAN

Dinamika hukum telematika dalam era digital menunjukkan pentingnya perlindungan privasi dan keamanan data di Indonesia. Berbagai temuan mengindikasikan bahwa masih terdapat celah dalam regulasi dan penegakan hukum, yang diperburuk oleh rendahnya kesadaran masyarakat terhadap risiko keamanan digital. Kebocoran data pribadi telah memberikan dampak nyata, baik dalam bentuk kerugian finansial maupun ancaman terhadap privasi individu, sehingga mendorong perlunya tindakan segera dari semua pemangku kepentingan.
Implikasi hukum dari dinamika ini mencakup perlunya implementasi tegas terhadap peraturan yang ada, khususnya Undang-Undang Perlindungan Data Pribadi, serta penguatan kapasitas kelembagaan untuk menangani pelanggaran yang semakin kompleks. Secara sosial, rendahnya literasi digital di masyarakat menuntut upaya edukasi yang lebih intensif agar pengguna teknologi memiliki pemahaman yang baik tentang hak dan kewajiban mereka dalam dunia digital.
Ke depan, diharapkan hukum telematika di Indonesia dapat berkembang menjadi kerangka yang tidak hanya melindungi hak-hak individu, tetapi juga mendorong inovasi yang aman dan bertanggung jawab. Kolaborasi antara pemerintah, sektor swasta, dan masyarakat harus diperkuat untuk menciptakan ekosistem digital yang tangguh. Dengan langkah-langkah yang terintegrasi, hukum telematika dapat menjadi landasan yang kokoh bagi perkembangan teknologi di Indonesia, sekaligus memastikan privasi dan keamanan data tetap terjaga dalam setiap inovasi yang dilakukan.

DAFTAR PUSTAKA

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

Erna, P. (2019). Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online (The Urgency of Personal Protection in Peer to Peer Lending). *Majalah Hukum Nasional*, No.2 Hal1-27.

Miftahul, L. (2022). UU Perlindungan Data Ptibadi dan Tantangan Implementasinya. *Fakultas Ilmu Administrasi Universitas Indonesia*. https://fia.ui.ac.id/Id/uu-perlindungan-data-pribadi-dan-tantangan-implementasinya/

Ramli, A. M. (2016). Hukum Telematika. *Pengertian Dan Ruang Lingkup Telematika*, *2*(membahas pengertian dan ruang lingkup), 1–2.

Safiranita, T., Wahyuningsih, T., & Mutiara, D. (n.d.). ASPEK HUKUM ATAS KONTEN HAK CIPTA DIKAITKAN DENGAN UNDANG UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK NO 19 TAHUN 2016. *Jurnal Legislasi Indonesia*. https://e-jurnal.peraturan.go.id/index.php/jli/article/downloadSuppFile/589/80