



Perlindungan Data Pribadi dalam Era *Internet of Things* (Studi Kasus Kebocoran Data Lion Air)

Josephine Yenni Sijabat

Fakultas Hukum dan Ilmu Sosial, Jurusan Hukum dan Kewarganegaraan,

Universitas Pendidikan Ganesha, Indonesia

Korespondensi penulis: yenisijabat447@gmail.com

Abstract : *The rapid development of the Internet of Things (IoT) in Indonesia brings new challenges in personal data protection. This study aims to analyze the suitability of the legal framework in Indonesia in protecting personal data collected by IoT devices. This study identifies data collection and use practices, as well as uncovers existing legal loopholes. This study intends to conduct an in-depth analysis of the level of compliance with personal data protection laws in the context of IoT solutions. The normative legal research method with the library search technique is to search for journal or article materials related to the title and theme that the author is studying. Therefore, this study has a strategic goal to investigate the extent to which applicable regulations can be effectively implemented in the IoT ecosystem, with a special focus on security and privacy aspects that are the main pillars of personal data protection regulations. Based on these findings, this study provides policy recommendations to improve personal data protection in the IoT era, such as the need for a revision of the ITE Law, strengthening supervision by related institutions, or increasing public awareness.*

Keywords: *Development, IoT, Personal Data.*

Abstrak : Perkembangan pesat Internet of Things (IoT) di Indonesia membawa tantangan baru dalam perlindungan data pribadi. artikel ini bertujuan untuk menganalisis kesesuaian kerangka hukum di Indonesia dalam melindungi data pribadi yang dikumpulkan oleh perangkat IoT. artikel ini mengidentifikasi praktik pengumpulan dan penggunaan data, serta mengungkap celah-celah hukum yang ada. artikel ini bermaksud mengadakan analisis mendalam terhadap tingkat kepatuhan hukum perlindungan data pribadi dalam konteks solusi IoT. Metode penelitian hukum normatif dengan teknik library search yang dimana adalah mencari bahan-bahan jurnal ataupun artikel yang berkaitan dengan judul serta tema yang penulis kaji. Oleh karena itu, penelitian ini memiliki tujuan strategis untuk menyelidiki sejauh mana regulasi-regulasi yang berlaku dapat diimplementasikan dengan efektif dalam ekosistem IoT, dengan fokus khusus pada aspek keamanan dan privasi yang menjadi pilar utama dalam regulasi perlindungan data pribadi. Berdasarkan temuan tersebut, artikel ini memberikan rekomendasi kebijakan untuk meningkatkan perlindungan data pribadi dalam era IoT, seperti perlu adanya revisi UU ITE, penguatan pengawasan oleh lembaga terkait, atau peningkatan kesadaran masyarakat.

Kata Kunci: Perkembangan, Data Pribadi, IoT.

1. PENDAHULUAN

“Pasal 1 ayat (3) Undang-Undang Dasar Negara Kesatuan Republik Indonesia 1945 yang menyebutkan bahwa: “Negara Indonesia adalah negara hukum”. Dalam kaitannya di era masa lalu maupun sekarang era digital, hukum sangat dipandang menjadi tolak ukur perlindungan dari masa ke masa. Dalam era transformasi digital yang menggebu, Internet of Things (IoT) telah menjadi pilar utama revolusi teknologi dengan menawarkan konektivitas yang tak tertandingi antara perangkat. Mendefinisikan IoT adalah tantangan karena kompleksitas teknis dan tantangan konsepnya, pada dasarnya IoT merupakan fenomena yang ditemukan dalam jaringan objek, yang menghubungkan ke hari atau microchip dan mengirim data ke sistem penerima. IoT mencakup koneksi antar objek.

Oleh karena itu, IoT memiliki sistem komunikasi. Internet of Things (IoT) adalah sebuah konsep yang menggunakan internet sebagai jaringan infrastruktur utama yang mengkoneksikan objek- objek tertentu (Miorandi, 2012). Namun, seiring dengan kemajuan ini, muncul pula kekhawatiran serius terkait keamanan dan privasi data pribadi yang terkandung dalam interaksi IoT. Di era digital saat ini, Internet of Things (IoT) telah menjadi bagian integral dari kehidupan sehari- hari. Berbagai perangkat, mulai dari rumah pintar, wearable technology, hingga alat kesehatan terhubung, semakin umum digunakan. IoT adalah konsep yang memperluas manfaat dari koneksi berkelanjutan dari koneksi internet. Mengenai keterampilan seperti berbagi data termasuk objek dunia nyata remote control dan banyak lagi (ariyanti, 2016).

Meskipun menawarkan banyak manfaat, seperti efisiensi dan kenyamanan, penggunaan IoT juga memunculkan tantangan serius dalam perlindungan data pribadi. Data yang dikumpulkan oleh perangkat IoT dapat mencakup informasi sensitif yang jika tidak dilindungi dengan baik, dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. Keberhasilan implementasi IoT tidak hanya bergantung pada efisiensi dan keterhubungan perangkat, tetapi juga pada upaya untuk memitigasi risiko terkait pengelolaan dan perlindungan data individu dan peran hukum guna melindungi data pribadi. Berdasarkan survei, tingkat kejahatan siber seperti pencurian data pribadi meningkat dari 7,96% menjadi 20,97% selama tahun 2023.

Kesimpulannya, kasus pencurian data pribadi di Indonesia menunjukkan peningkatan yang cukup besar, menggarisbawahi perlunya peningkatan keamanan dan kesadaran digital di kalangan masyarakat. Dari penjelasan data diatas maka dapat kita lihat pentingnya kesadaran diri untuk sadar dan patuh regulasi serta perlu untuk eksplorasi tingkat kepatuhan, penelitian ini juga akan melibatkan perspektif etika dalam memahami dampak sosial dan individu dari implementasi solusi IoT. Kajian ini akan memberikan ruang bagi refleksi lebih lanjut tentang bagaimana perkembangan teknologi harus sejalan dengan nilai-nilai moral dan prinsip-prinsip keadilan, terutama dalam konteks sensitif seperti perlindungan data pribadi. Internet of Things (IoT) telah mengubah cara kita berinteraksi dengan dunia sekitar. Perangkat-perangkat yang terhubung. Mulai dari rumah pintar hingga kendaraan otonom, mengumpulkan data dalam jumlah besar setiap saat. Data ini dapat mencakup berbagai informasi pribadi, mulai dari lokasi hingga kebiasaan sehari-hari. Berdasarkan latar belakang diatas, terdapat dua permasalahan yaitu Bagaimana risiko yang dihadapi pengguna terkait data pribadi di era IoT? dan Apa saja praktik terbaik untuk perlindungan data pribadi?

2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif dengan teknik library search yang dimana adalah mencari bahan-bahan jurnal ataupun artikel yang berkaitan dengan judul serta tema yang penulis kaji untuk dijadikan sebagai referensi dalam pembuatan artikel ini. Penelitian yang digunakan dalam penulisan penelitian ini adalah tipe penelitian yuridis normatif yang dilakukan dengan cara mengkaji berbagai macam aturan hukum yang bersifat formal seperti undang-undang, literatur-literatur yang berisi konsep teoritis yang kemudian dihubungkan dengan permasalahan yang menjadi pokok pembahasan dalam penelitian.

3. HASIL DAN PEMBAHASAN

Risiko yang dihadapi pengguna terkait data pribadi di era IoT

a. Pengumpulan Data Berlebihan

Perangkat IoT sering kali mengumpulkan lebih banyak data daripada yang sebenarnya diperlukan untuk fungsinya. Data ini dapat mencakup lokasi, kebiasaan sehari-hari, dan informasi kesehatan yang sangat sensitif. Ketika data ini dikumpulkan dan disimpan tanpa perlindungan yang memadai, risiko penyalahgunaan semakin meningkat.

b. Kerentanan Keamanan

Banyak perangkat IoT yang tidak dilengkapi dengan protokol keamanan yang kuat. Misalnya, perangkat yang menggunakan password default atau yang tidak mendukung enkripsi data dapat dengan mudah diretas. Serangan siber dapat menyebabkan pencurian data pribadi, yang dapat berdampak serius pada individu.

c. Kurangnya Transparansi

Banyak perusahaan yang tidak menjelaskan dengan jelas bagaimana data pengguna dikumpulkan dan digunakan. Pengguna sering kali tidak menyadari bahwa data mereka dijual kepada pihak ketiga untuk tujuan iklan atau analisis perilaku. Hal ini mengurangi kontrol individu terhadap informasi pribadi mereka.

d. Contoh Kasus

Sebagai contoh, pada tahun 2019, laporan menyebutkan bahwa data dari jutaan perangkat IoT terancam bocor akibat kerentanan dalam sistem keamanan yang lemah. Data yang bocor mencakup informasi pengguna yang sangat sensitif. Pada tahun 2019, kebocoran data menjadi isu serius, terutama terkait dengan perangkat Internet of Things (IoT). Laporan menunjukkan bahwa lebih dari 105 juta serangan siber terdeteksi pada perangkat IoT di paruh pertama tahun tersebut, meningkat sembilan kali lipat

dibandingkan tahun sebelumnya. Serangan ini memanfaatkan kerentanan dalam sistem keamanan yang lemah, yang mengakibatkan data sensitif pengguna berisiko bocor. Salah satu contoh konkret adalah kebocoran data yang melibatkan 21 juta data penumpang dari anak perusahaan Lion Air, Malindo Air dan Thai Lion Air. Data ini diunggah ke forum daring, menyoroti betapa rentannya sistem keamanan di sektor penerbangan. Kasus ini menggarisbawahi kebutuhan mendesak untuk perlindungan data yang lebih baik, terutama mengingat bahwa banyak organisasi belum memiliki kebijakan keamanan yang memadai. Kebocoran data juga terjadi di berbagai sektor lainnya. Di Indonesia, misalnya, terdapat laporan mengenai kebocoran data dari 29 lembaga sejak 2019, termasuk Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan. Menteri Komunikasi dan Informatika menyatakan bahwa banyak dari kebocoran ini disebabkan oleh kelemahan teknologi keamanan dan kolaborasi dengan pelaku kejahatan siber.

Secara global, insiden kebocoran data tidak hanya terbatas pada perangkat IoT. Kasus besar seperti kebocoran data 540 juta pengguna Facebook pada tahun yang sama menunjukkan tantangan besar dalam melindungi informasi pribadi di era digital. Hal ini menegaskan pentingnya meningkatkan kesadaran akan keamanan siber dan menerapkan langkah-langkah perlindungan yang lebih ketat terhadap data pribadi.

Regulasi dan Kebijakan Perlindungan Data

a) RUU Perlindungan Data Pribadi di Indonesia

Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) di Indonesia bertujuan untuk memberikan perlindungan hukum yang lebih baik terhadap data pribadi. RUU ini menetapkan hak-hak individu, termasuk:

- Hak untuk mengakses
Pengguna memiliki hak untuk mengetahui data pribadi apa yang dikumpulkan.
- Hak untuk memperbaiki
Pengguna dapat meminta perbaikan atas data yang tidak akurat.
- Hak untuk menghapus
Pengguna berhak untuk meminta penghapusan data pribadi mereka.

Praktik Terbaik untuk Perlindungan Data Pribadi

Pendidikan masyarakat tentang perlindungan data pribadi sangat penting. Pengguna perlu dilengkapi dengan pengetahuan tentang risiko dan cara melindungi informasi mereka. Program edukasi dapat dilakukan melalui seminar, workshop, dan

kampanye informasi. Sebelum membeli perangkat IoT, penting untuk melakukan riset tentang tingkat keamanan perangkat. Memilih perangkat dari produsen yang memiliki reputasi baik dan menyediakan pembaruan keamanan secara teratur dapat mengurangi risiko. Perangkat IoT harus diperbarui secara berkala untuk melindungi dari kerentanan keamanan. Pembaruan firmware dan software dapat membantu menjaga perangkat tetap aman dari serangan siber. Pengguna sebaiknya membatasi jumlah data yang dibagikan dengan perangkat IoT. Selalu periksa pengaturan privasi dan hanya berikan izin yang benar-benar diperlukan untuk fungsi perangkat. Menggunakan jaringan Wi-Fi yang aman sangat penting untuk melindungi perangkat IoT. Hindari menggunakan perangkat di jaringan publik yang tidak terjamin keamanannya, karena dapat meningkatkan risiko peretasan. Perusahaan yang mengembangkan perangkat IoT harus mengimplementasikan protokol keamanan yang ketat. Ini termasuk enkripsi data, otentikasi yang kuat, dan audit keamanan secara berkala.

4. KESIMPULAN

Perlindungan data pribadi di era Internet of Things merupakan tantangan yang kompleks dan memerlukan perhatian dari semua pihak. Dengan memahami risiko yang ada, menerapkan praktik terbaik, dan mematuhi regulasi yang berlaku, kita dapat memanfaatkan teknologi IoT secara aman tanpa mengorbankan privasi. Kesadaran akan perlindungan data pribadi merupakan langkah awal menuju penggunaan teknologi yang lebih bertanggung jawab dan aman. Artikel ini memberikan wawasan yang mendalam tentang perlindungan data pribadi dalam solusi IoT.

Daftar Referensi

- Ariyanti, S., et al. (2016). *Implementasi Internet of Things untuk sektor kesehatan*. Badan Penelitian dan Pengembangan Sumber Daya Manusia Kementerian Komunikasi dan Informatika Republik Indonesia.
- California Consumer Privacy Act (CCPA). (2018).
- Choi, J. (2020). The impact of IoT on personal data protection. *Journal of Information Security*.
- European Commission. (2016). *General Data Protection Regulation*.
- Fabiano, N. (2017). Internet of Things and the legal issues related to the data protection law according to the new European General Data Protection Regulation. *Athens Journal of Law*, 3(3).

- Irfan, M., Elvia, M., & Dania, S. (2023). Ancaman cybercrime dan peran cybersecurity pada e-commerce: Systematic literature review. *JURSIMA*, 11(1).
- Kementerian Komunikasi dan Informatika Republik Indonesia. *Rancangan Undang-Undang Perlindungan Data Pribadi*.
- Kusnadi, S. A., & Wijaya, A. U. (2021). Perlindungan hukum data pribadi sebagai hak privasi. *JA: Jurnal Al-Wasath*, 2(1).
- Miorandi, D., et al. (2012). Internet of Things: Vision, applications, and research challenges. *Elsevier Journal*, 10(7).
- Setiawan, M. N. (2021). Mengkritisi Undang-Undang ITE Pasal 27 Ayat (3) dilihat dari sosio-politik hukum pidana Indonesia. *Datin Law Jurnal*, 2(1), 14–16.
- Siahaan, A. L. S. (2022). Urgensi perlindungan data pribadi di platform marketplace terhadap kemajuan teknologi. *Majalah Hukum Nasional*, 52(2).
- Symantec. (2018). Internet of Things: Security challenges and recommendations.
- Tan, D. (2021). Metode penelitian hukum: Mengupas dan mengulas metodologi dalam menyelenggarakan penelitian hukum. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, 8(8), 2463-2478.
- Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review*.
- Zwick, A. (2019). The Internet of Things: Privacy and security concerns. *Journal of Cyber Policy*.