Aladalah: Jurnal Politik, Sosial, Hukum dan Humaniora
Vol. 2, No. 4 Oktober 2024
e-ISSN : 2962-8903, p-ISSN : 2962-889X, Hal 176-181
DOI: https://doi.org/10.59246/aladalah.v2i4.968
Available Online at : https://ejurnalqarnain.stisnq.ac.id/index.php/ALADALAH

Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektlf Hukum Siber

Fara Anindita Salsabila[1], Andi Aina IImih[2]
[1,2]Universitas Islam Sultan Agung, Indonesia
Korespondensi penulis: aninditafr28@gmail.com

Abstract*. The misuse of personal data has become a highly relevant issue in the digital age, where cases of privacy violations are increasing sharply. Personal data such as contact information, transaction history, and online activities have become prime targets for cybercriminals to use for fraud, identity theft, and even political manipulation. These crimes often occur in various locations around the world, taking advantage of regulatory breaks and jurisdictional differences, making law enforcement difficult. To address this problem, a multi-dimensional approach is required. Stricter regulations, such as the General Data Protection Regulation (GDPR) in the European Union, are needed to protect personal data with strict sanctions for violations. In addition, international collaboration is essential as cybercrime often crosses national borders, requiring close cooperation between countries to track and apprehend perpetrators. Public awareness and education are also key components in reducing the risk of cybercrime. People should be encouraged to take proactive measures such as the use of strong passwords and two-step verification. Companies and service providers also need to take responsibility for customer data security by implementing strong protection measures and transparency in data management. In conclusion, the use of personal data as a form of perfect crime is a complex issue, requiring strict regulation, international collaboration, and awareness raising to create a safer digital environment.*

Keywords*: Cybercrime, Personal Data Misuse, Privacy Breach*

Abstrak. Penyalahgunaan data pribadi telah menjadi isu yang sangat relevan dalam era digital, dimana kasus pelanggaran privasi meningkat tajam. Data pribadi seperti informasi kontak, riwayat transaksi, dan aktivitas online menjadi target utama bagi pelaku kejahatan siber untuk digunakan daiam penipuan, pencurian identitas, dan bahkan manipulasi politik. Kejahatan ini seringkali terjadi di berbagai iokasi di seiuruh dunia, memanfaatkan celah daiam peraturan dan perbedaan yurisdiksi, sehingga menyulitkan penegakan hukum. Untuk mengatasi masalah ini, diperlukan pendekatan multi-dimensi. Regulasi yang lebih ketat, seperti General Data Protection Regulation (GDPR) di Uni Eropa, diperlukan untuk melindungi data pribadi dengan sanksi yang tegas bagi pelanggaran. Selain itu, kolaborasi internasional sangat penting karena kejahatan siber sering kali melintasi batas negara, memerlukan kerjasama erat antara negara- negara untuk melacak dan menangkap pelaku. Kesadaran dan pendidikan masyarakat juga menjadi komponen kunci dalam mengurangi risiko kejahatan siber. Masyarakat harus didorong untuk mengambil tindakan proaktif seperti penggunaan kata sandi yang kuat dan verifikasi dua langkah. Perusahaan dan penyedia layanan juga perlu bertanggung jawab atas keamanan data pelanggan dengan menerapkan langkah-langkah perlindungan yang kuat dan transparansi dalam pengelolaan data. Kesimpulannya, penggunaan data pribadi sebagi bentuk kejahatan sempurna adalah masalah yang kompleks, memerlukan regulasi yang ketat, kolaborasi internasional, dan peningkatan kesadaran untuk menciptakan lingkungan digital yang lebih aman.

Kata kunci: Kejahatan Siber, Penyalahgunaan Data Pribadi, Pelanggaran Pivasi

1. LATAR BELAKANG

Penggunaan data pribadi sebagai bentuk kejahatan sempurna daiam perspektif hukum siber telah menjadi isu yang sangat relevan dan kompleks dalam era digital saat ini. Dalam beberapa tahun terakhlr, kasus-kasus pelanggaran privasi telah meningkat drastis, sehingga perlu adanya perhatian yang lebih serius terhadap perlindungan data pribadi. Data pribadi yang terkait dengan individu, seperti informasi kontak, riwayat transaksi, dan riwayat online, telah menjadi sumber daya yang sangat berharga bagi pihak-pihak yang ingin mengumpulkan dan

Received: Mei 22, 2024; Revised: Juni 28, 2024; Accepted: Juli 20, 2024; Online Available: Juli 23, 2024
*Fara Anindita Salsabila, aninditafr28@gmail.com

memanfaatkan data tersebut untuk tujuan yang tidak sah. Dalam beberapa kasus, data pribadi tersebut telah digunakan untuk tujuan yang sangat berbahaya, seperti penipuan, pencurian identitas, dan penggunaan data untuk tujuan politik. Oleh karena itu, perlu adanya perhatian yang lebih serius terhadap perlindungan data pribadi dan adanya hukum yang lebih ketat untuk menghambat kejahatan data prlbadl.

Dalam artikel ini, kita akan membahas lebih lanjut tentang penggunaan data pribadi sebagai bentuk kejahatan sempurna dalam perspektif hukum siber dan bagaimana hukum dapat digunakan untuk menghambat kejahatan tersebut. Dengan adanya teknologi yang semakin maju dan konektivitas Internet yang semakin luas, data prlbadl menjadi komoditas yang dapat dieksploitasi dengan mudah oleh pelaku kejahatan siber. Kasus- kasus seperti pelanggaran data oleh perusahaan besar, kebocoran informasi sensitif, dan akses legal ke data pengguna telah menimbulkan kekhawatiran serius bagi masyarakat dan regulator. Ketika data pribadi jatuh ke tangan yang salah, dampaknya bisa sangat merusak. Pelaku kejahatan dapat menggunakan data ini untuk melakukan tindakan kriminal sepertl pencurian identitas, penipuan fnansial, dan bahkan manipulasi opini publik.

Selain itu, penlngkatan kesadaran dan pendidikan masyarakat tentang pentingnya perlindungan data pribadi juga merupakan langkah kunci dalam mengurangi risiko kejahatan siber. Masyarakat harus didorong untuk mengambil langkah- langkah proaktif dalam melindungi informasi pribadi mereka, seperti penggunaan kata sandi yang kuat, verifikasi dua langkah, dan kehati- hatian dalam berbagi informasi oniine. Perusahaan dan penyedia layanan juga harus bertanggung jawab atas perlindungan data pelanggan mereka, menerapkan langkah-langkah keamanan yang kuat, dan transparansi dalam pengelolaan data.

Kesimpulannya, penggunaan data pribadi sebagai bentuk kejahatan sempurna daiam perspektif hukum siber adalah masaiah yang kompieks dan memerlukan perhatian serius dari berbagai pihak. Dengan regulasi yang lebih ketat, kolaborasi internasional, peningkatan kesadaran masyarakat, dan tanggung jawab perusahaan, kita dapat mengurangi risiko kejahatan data pribadi dan menclptakan lingkungan digital yang lebih aman.

2. LANDASAN TEORI

2.1 Data Pribadi

Data diri (juga dikenal sebagal data pribadi) merujuk pada konsep dan kerangka kerja yang mendasari pemahaman tentang apa yang termasuk dalam kategori data pribadi dan mengapa perlindungannya sangat penting dalam era digital saat ini. Data diri mengacu pada lnformasl yang berkaitan dengan individu yang dapat digunakan untuk mengidentifikasi mereka, baik secara langsung maupun tidak langsung. Informasi ini mencakup, tetapi tidak

terbatas pada, nama, alamat, nomor telepon, alamat email, nomor identifikasi, informasi keuangan, riwayat medis, dan data biometrlk.

Menurut General Data Protection Regulation (GDPR) Uni Eropa, data pribadi mencakup "setiap informasi yang terkait dengan orang alami yang teridentifikasi atau dapat diidentifikasi." Seseorang dianggap dapat diidentifikasi jlka dapat dikenal, secara langsung atau tidak langsung, melalui pengenal seperti nama, nomor identifikasi, data lokasi, atau melalui atribut fisik, fisiologis, genetik, mental, ekonomi, budaya, atau sosial (European Commision, 2016). Hal ini menunjukkan bahwa data pribadi mencakup berbagal jenis informasi yang bisa digunakan untuk mengindentifikasi individu.

Landasan teori ini juga menekankan pentingnya perlindungan data pribadi dalam konteks keamanan dan privasi. Menurut laporan World Economic Forum (WEF), data pribadi telah menjadi salah satu aset paling berharga di era digital, dan pelanggaran data dapat mengakibatkan konsekuensi serius, termasuk pencurian identitas, penipuan, dan kerusakan reputasi (WEF, 2020). Oleh karena itu, perlindungan data pribadi menjadi prioritas utama dalam kebijakan keamanan siber dan hukum siber.

2.2 Tindak Pidana

Hukum pidana dalam konteks penyalahgunaan data pribadi mengacu pada kerangka hukum yang dirancang untuk menangani dan menghukum tindakan ilegal yang berkaitan dengan pencurian, penyalahgunaan, atau eksploitasi data pribadi. Seiring dengan pesatnya perkembangan teknologi dan peningkatan kejahatan siber, kebutuhan akan hukum pidana yang efektif untuk melindungi data pribadi telah menjadi semakin mendesak.

Konsep dasar hukum pidana adalah untuk memberikan konsekuensi yang jelas bagi tindakan yang melanggar hukum dan untuk melindungi hak dan kepentingan individu serta masyarakat luas. Dalam kasus penyalahgunaan data pribadi, tindakan kriminal dapat mencakup berbagal bentuk pelanggaran, seperti akses tanpa izin ke data pribadi, penggunaan data pribadi untuk tujuan iilegal, dan distribusi informasi pribadi tanpa persetujuan. Menurut undang-undang perlindungan data di banyak negara, tindakan ini dapat dikenal sanksi pidana, termasuk denda dan hukuman penjara.

2.3 Hak Asasi Manusia

Hak asasi manusia dalam konteks penyalahgunaan data pribadi berfokus pada prinsip-prinsip fundamental yang mengatur perlindungan hak individu atas prlbadl dan keamanan informasi pribadi mereka. Hak atas privasi diakui sebagal bagian dari hak asasi manusia yang dilindungi oleh berbagal instrumen internasional dan nasional. Penyalahgunaan data pribadi

dapat secara langsung melanggar hak ini dan mengakibatkan dampak yang signifikan terhadap kehidupan individu.

Menurut Deklarasi Universal Hak Asasl Manusia (Universal Declaration of Human Rights, UDHR), yang diadopsi oleh Perserikatan Bangsa-Bangsa pada tahun 1948, Pasal 12 menyatakan bahwa "tidak seorang pun boleh dikenakan campur tangan sewenang- wenang terhadap privasinya, keluarganya, rumahnya, atau korespondensinya, atau terhadap serangan terhadap kehormatan dan reputasinya." Deklarasi ini menegaskan bahwa privasi adalah hak asasi manusia yang harus dihormati dan dilindungi (United Nations, 1948).

2.4 Kejahatan Lintas Negara

Kejahatan lintas negara dalam konteks penyalahgunaan data pribadi mengkaji aspek-aspek yang menjadikan kejahatan siber, terutama yang berkaitan dengan data pribadi, sebagal fenomena yang mellntasl batas yuridiksi dan memerlukan kerjasama internasional untuk mengataslnya. Kejahatan lintas negara terjadi ketika pelaku melakukan tindakan kriminal di berbagai negara atau dari loaksi yang berbeda dengan korban atau dampak kejahatannya, seringkali menggunakan teknologi digital sebagal sarana utama.

3. METODE PENELITIAN

Metode penulisan mengenai Tindak Kejahatan Perdagangan Manusia di Dunia sebagai Bentuk Pelanggaran Hak Asasi Manusia dl Era Globalisasi dilaksanakan menggunakan metode studi literatur. Metode studi literatur adalah metode yang dilakukan dengan cara meneliti dan memahami jurnal, buku-buku, dokumen, atau dari sumber tertulis lainnya yang bersifat relevan dan mendukung laporan penelitian ini. Informasi yang diperoleh dikompulasi, dianalisis, dan disimpulkan sehingga mendapatkan kesimpulan mengenal studi literatur. Informasi studi literatur disajikan dengan menggunakan metode deskriptif yaitu dengan mengumpulkan data sebanyak- banyaknya yang berkaitan dengan faktor-faktor yang mendukung laporan atau artikel.

4. HASIL DAN PEMBAHASAN

Penyalahgunaan data pribadi telah menjadi salah satu bentuk kejahatan yang paling mengkhawatirkan dalam era digital, seringkali disebut sebagai kejahatan sempurna dalam perspektif hukum siber. Dengan kemajuan teknologi dan penyebaran Internet yang luas, data pribadi menjadi komoditas berharga yang dapat dengan mudah diakses, dicuri, dan disalahgunakan oleh pelaku kejahatan. Kejahatan siber seperti pencurian identitas, penipuan, dan akses ilegal ke sistem komputer seringkali bergantung pada pengumpulan data pribadi, yang kemudian digunakan untuk tujuan kriminal.

Menurut laporan darl Identlty Theft Resource Center (LTRC), kasus pencurian data pribadi meningkat secara signifikan dalam beberapa tahun terakhir, dengan jutaan orang menjadi korban setiap tahun. Laporan tersebut menunjukkan bahwa informasi yang serlng menjadi target pencurian termasuk nomor jaminan Sosial, nomor kartu kredit, dan informasi kesehatan pribadi (LTRC, 2022). Data ini dapat digunakan untuk berbagal kejahatan, seperti penipuan kartu kredit, pencurian identitas, dan bahkan pembobolan akun bank.

Solusi untuk mengatasi penyalahgunaan data pribadi memerlukan pendekatan multi-dimensi. Di satu sisi, diperlukan regulasi yang lebih ketat dan kerjasama internasional untuk menghadapi kejahatan siber lintas negara. Di sisi lain, individu dan perusahaan harus lebih waspada dan proaktif dalam melindungi data pribadi mereka. Edukasl tentang pentingnya perlindungan data, penggunaan kata sandi yang kuat, dan implementasi langkah-langkah keamanan seperti verifikasl dua langkah dapat membantu mengurangi risiko penyalahgunaan data pribadi.

Dengan demikian, penyalahgunaan data pribadi sebagai bentuk kejahatan sempurna dalam perspektif hukum siber adalah tantangan besar yang memerlukan kolaborasi global dan upaya terpadu dari berbagal pihak, termasuk pemerintah, perusahaan, dan masyarakat luas.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Penyalahgunaan data pribadi telah menjadi bentuk kejahatan sempurna dalam perspektif hukum siber, dengan berbagal dampak negatif yang mempengaruhi individu dan organisasi. Peningkatan kejahatan siber seperti pencurian identitas, penipuan, dan akses ilegal ke sistem komputer menggarisbawahi betapa pentingnya perlindungan data pribadi di era digital. Kemampuan pelaku kejahatan untuk beroperasi secara anonim dan lintas negara membuat penegakan hukum menjadi tantangan besar. Meski regulasli seperti General Data Protectoon Regulation (GDPR) dan upaya kerjasama internasional melalui Konvensi Budapest telah memperkuat perlindungan data pribadi, masih banyak pekerjaan yang harus dilakukan untuk mengatasi kejahatan siber ini secara efektif.

Pendekatan multi-dimensi diperlukan untuk melawan penyalahgunaan data pribadi. Selain peraturan yang ketat dan kerjasama internasional yang kuat, edukasi dan kesadaran publik tentang pentingnya menjaga privasi juga sangat penting

5.2 Saran

Untuk mengatasi penyalahgunaan data pribadi, pemerintah dan lembaga penegak hukum harus memperkuat regulasi dan penegakan hukum terkait kejahatan siber, dengan memastlkan bahwa pelaku pelanggaran mendapatkan sanksi yang setimpal. Kerjasama internasional perlu ditingkatkan untuk menangani kejahatan siber lintas negara, dengan memanfaatkan perjanjian seperti Konvensi Budapest dan lembaga seperti Interpol untuk mengkoordinasikan upaya global. Di tingkat lokal.

DAFTAR REFERENSI

Aina, A. (2011). Legal Protection of Personal Data Based on Electronic Transactions in the Era of the Digital Economy. Faculty of Law, Sultan Agung Islamic University.

Asyfei, I. (2018). Legal Construction and Development in Comparative Study (The Role of Indigenous and Global Community in Constructing National Law). Faculty of Law, Sultan Agung Islamic University.

Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). Retrieved from https://www.coe.int/en/

European Commission. (2016). General Data Protection Regulation (GDPR). Retrieved from https://eur-lex.europa.eu/

Europol. (2020). Cybercrime: The Dark Web and Cryptocurrency. Retrieved from https://www.europol.europa.eu/

U.S. Department of Justice. (2020). Computer Fraud and Abuse Act (CFAA). Retrieved from https://www.justice.gov/

United Nations. (1948). Universal Declaration of Human Rights (UDHR). Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights

United Nations. (1966). International Covenant on Civil and Political Rights (ICCPR). Retrieved from https://www.ohchr.org/

Zulkarnain, A. (2019). Ideal Electronic Contract Model as a Form of E-commerce Disputes Settlement. Jurnal Pembaharuan Hukum, 77(6).