

Perlindungan Hukum Terhadap Korban *Cyber Crime* di Indonesia dalam Aliran Hukum Pada Kasus Pencurian Data Pribadi

Alfi Salsabilah Idriansyah¹, Nur Afifah²

¹²Hukum Pidana Islam, Universitas Islam Negeri Sunan Ampel Surabaya, Jl. Ahmad Yani No. 117, Indonesia
Email: alfisalsabilah552@gmail.com

Abstract

With the rapid development of information and communication technology, various types of cybercrime, especially personal data theft, are becoming more possible. In today's digital era, legal protection for victims of personal data theft is an important issue. This article examines the legal protection provided to victims of personal data theft on the internet from the perspective of Indonesian law. This study uses qualitative methodology and literature study. The study shows that Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and Regulation of the Minister of Communication and Informatics Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems are the main laws in Indonesia that regulate personal data protection. Victims have rights protected by this legal protection, such as the right to be notified in the event of a data leak, the right to compensation, and other rights. However, these regulations still need to be improved to accommodate rapid technological developments and provide legal certainty for all parties.

Abstract

Dengan berkembangnya teknologi informasi dan komunikasi yang cepat, berbagai jenis kejahatan siber, terutama pencurian data pribadi, menjadi lebih mungkin. Di era digital saat ini, perlindungan hukum terhadap korban pencurian data pribadi adalah masalah penting. Artikel ini mengkaji perlindungan hukum yang diberikan kepada korban pencurian data pribadi di internet dari sudut pandang hukum Indonesia. Studi ini menggunakan metodologi kualitatif dan studi literatur. Penelitian menunjukkan bahwa Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik adalah undang-undang utama di Indonesia yang mengatur perlindungan data pribadi. Korban memiliki hak-hak yang dilindungi oleh perlindungan hukum ini, seperti hak untuk diberitahu jika terjadi kebocoran data, hak untuk mendapatkan kompensasi, dan hak lainnya.

Article History

Received Okt 27, 2024
Revised Okt 29, 2024
Accepted 09 Nov 2024
Available online 21 Nov. 2024

Keywords :

cyber crime, theft of personal data, legal protection

Keywords :

cyber crime, pencurian data pribadi, perlindungan hukum.



<https://doi.org/10.5281/zenodo.14210930>

This is an open-access article under the **CC-BY-SA License**.



PENDAHULUAN

Penumbuhan yang semakin pesat dalam teknologi informasi dan komunikasi telah membawa banyak manfaat bagi masyarakat, tetapi juga telah membuka jalan bagi berbagai jenis kejahatan baru. Kejahatan siber atau *cyber crime*, khususnya yang berkaitan dengan pencurian data pribadi, mencakup berbagai tindakan ilegal seperti *hacking*, *phishing*, dan malware yang bertujuan untuk mencuri, mengakses, atau menyalahgunakan data pribadi seseorang tanpa izin.¹ Pencurian data pribadi dapat menyebabkan kerugian finansial dan emosional yang signifikan bagi korban.

Perlindungan hukum mencakup peraturan yang menentukan siapa yang bertanggung jawab atas pengelolaan data pribadi. Pihak-pihak seperti perusahaan teknologi, penyedia layanan internet, dan lembaga keuangan yang mengumpulkan dan mengelola informasi pribadi harus memastikan bahwa sistem keamanan yang memadai digunakan untuk melindungi data tersebut. Jika data bocor, mereka

¹ “Fadli, M., Widijowati, D., & Andayani, D. (2024). Pencurian Data Pribadi di Dunia Maya (*Phising Cybercrime*) yang ditinjau dalam Perspektif Kriminologi. Co-Value Jurnal Ekonomi Koperasi dan kewirausahaan, Vol. 14, No. 12”.

bertanggung jawab dan membayar korban.² Dalam hal ini, undang-undang yang mengatur perlindungan data pribadi harus dapat mengakomodasi perkembangan teknologi yang cepat sehingga semua pihak yang terlibat memiliki kepastian hukum. Dalam hal ini, undang-undang yang mengatur perlindungan data pribadi harus dapat mengakomodasi perkembangan teknologi yang cepat sehingga semua pihak yang terlibat memiliki kepastian hukum.

Di era komputer dan internet saat ini, perlindungan hukum terhadap korban pencurian data pribadi adalah masalah yang sangat penting. Langkah-langkah pencegahan dan represif serta tanggung jawab pihak-pihak yang mengelola data pribadi harus menjadi bagian dari perlindungan tersebut. Selain itu, kerja sama internasional sangat penting untuk memerangi kejahatan siber. Dengan perlindungan hukum yang luas, korban pencurian data pribadi siber diharapkan mendapatkan keadilan dan pemulihan yang layak.

METODE PENELITIAN

Metode yuridis normatif digunakan, seperti yang ditunjukkan dalam Undang-Undang Nomor 11 Tahun 2008, pasal 30-35, dan pasal 28. Ini juga termasuk peraturan perbandingan perlindungan hukum terhadap beberapa negara mengenai perlindungan hukum terhadap data pribadi dengan menggunakan data sekunder yang dikumpulkan dari artikel, buku, catatan ilmiah, dan sumber lainnya.³

Penelitian ini dilakukan secara deksriptif kualitatif dan dilakukan secara terus menerus. Penelitian ini memperjelas tujuan utama penelitian dengan meninjau artikel dan jurnal tentang perlindungan hukum terhadap korban *cyber crime*.

HASIL DAN PEMBAHASAN

Perlindungan Hukum Bagi Korban Cyber Crime Terhadap Kebocoran Data Pribadi

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah beberapa kali diubah, mengatur berbagai aspek informasi elektronik, termasuk perlindungan data pribadi. Pasal 26 UU ITE menetapkan bahwa penggunaan informasi melalui media elektronik yang berkaitan dengan data pribadi seseorang memerlukan persetujuan orang tersebut. Selain itu, Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik mewajibkan penyelenggara sistem elektronik untuk melindungi data pribadi pengguna dan memastikan bahwa data tidak disalahgunakan.⁴

Korban kebocoran data pribadi memiliki beberapa hak yang dilindungi oleh perlindungan hukum ini. Pertama, mereka memiliki hak untuk diberitahu jika terjadi kebocoran data yang melibatkan informasi pribadi. Kewajiban ini membantu penyelenggara sistem elektronik menjadi lebih transparan dan bertanggung jawab. Kedua, korban berhak untuk mendapatkan kompensasi atas kerugian yang disebabkan oleh penyebaran data. Korban biasanya dapat menuntut ganti rugi melalui proses hukum yang memadai, di mana mereka dapat menuntut pihak yang bertanggung jawab atas kelalaian dalam melindungi data pribadi.⁵

Selain itu, hak untuk mengajukan keluhan dan mendapatkan perlindungan dari otoritas yang berwenang merupakan bagian dari perlindungan hukum bagi korban. Di Indonesia, Kementerian Komunikasi dan Informatika (Kemenkominfo) bertanggung jawab untuk menerima dan menangani keluhan tentang pelanggaran data pribadi. Kemenkominfo juga memiliki wewenang untuk melakukan

² “Yudha, M. A. (2023). Tanggung Jawab Penyedia Atas Keamanan Data Penggunaan Layanan Dalam Transaksi Online Melalui Tokopedia. *Jurnal Notarius*, Vol. 2, No. 1.,” t.t.

³ “Soejono Soekantor dan Sri Mamudji, *Penelitian Yuridis Normatif*, PT Raja Grafindo, Jakarta, 2014, hal. 251-252,”.

⁴ “Sonjaya, A., & Setiawan, D. A. (2022, January). Perlindungan Hukum bagi Korban Kebocoran Data Pribadi Pengguna Aplikasi Tokopedia berdasarkan UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi. In *Bandung Conference Series: Law Studies* (Vol. 2, No. 1, pp. 420-427)”.

⁵ “Disemadi, H. S., Sudirman, L., Girsang, J., & Aninda, A. M. (2023). *Loc.cit.*,”.

investigasi dan mengambil tindakan yang diperlukan terhadap pelanggaran tersebut. Korban akan merasa lebih aman dan memiliki cara untuk mencari keadilan jika ada mekanisme ini.

Berbagai pihak, seperti penegak hukum, penyedia layanan internet, dan perusahaan teknologi, harus bekerja sama dengan baik untuk penegakan hukum yang efektif. Untuk memastikan bahwa pelanggaran dapat segera diidentifikasi dan ditindaklanjuti, koordinasi yang baik antara instansi ini sangat penting. Keterlibatan internasional sangat penting dalam menangani kasus kebocoran data pribadi karena cybercrime biasanya bersifat internasional. Negara-negara dapat bekerja sama untuk menangkap dan menghukum pelaku kejahatan siber yang seringkali beroperasi dari luar negeri melalui perjanjian bantuan hukum timbal balik dan pertukaran informasi.⁶

Regulasi seperti Peraturan Perlindungan Data Umum (GDPR) Uni Eropa menetapkan standar global untuk perlindungan data pribadi. GDPR menekankan perusahaan untuk lebih serius dalam menjaga keamanan data pengguna dan menerapkan langkah-langkah perlindungan yang memadai, karena GDPR memberikan hak-hak yang luas kepada orang-orang terkait data pribadi, termasuk hak untuk mengakses, mengoreksi, dan menghapus data.⁷

Peraturan global seperti GDPR dapat diterapkan di Indonesia untuk meningkatkan perlindungan hukum terhadap data pribadi. Salah satu langkah penting dalam upaya ini adalah pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP). RUU PDP dimaksudkan untuk membuat kerangka hukum yang lebih jelas dan tegas mengenai hak dan kewajiban yang terkait dengan data pribadi serta sanksi yang lebih berat bagi pelanggar. Dengan undang-undang yang lebih kuat, penegakan hukum terhadap kebocoran data akan lebih efisien dan masyarakat akan lebih aman.

Penggunaan teknologi enkripsi, sistem otentikasi multi-faktor, dan pemantauan keamanan real-time adalah beberapa contoh tindakan teknis yang dapat diambil untuk meningkatkan keamanan data pribadi. Teknologi juga berperan penting dalam perlindungan data pribadi. Organisasi dan perusahaan yang menangani data pribadi harus memastikan bahwa mereka mengikuti praktik keamanan siber terbaik dan menggunakan teknologi terbaru. Penilaian risiko dan audit berkala juga penting untuk menemukan dan memperbaiki masalah keamanan.⁸

Upaya pemulihan bagi korban kebocoran data juga merupakan bagian dari perlindungan hukum terhadap korban kebocoran data. Setelah kebocoran data terjadi, prosedur pemulihan harus dilakukan untuk membantu korban mendapatkan kembali identitas mereka dan mencegah kerugian yang lebih besar. Ini dapat mencakup layanan pemantauan kredit, bantuan dalam mengajukan pengaduan, dan dukungan psikologis bagi mereka yang mengalami dampak emosional dari kebocoran data. Selain itu, penyelenggara sistem elektronik yang bertanggung jawab atas kebocoran data harus memberikan kompensasi yang wajar kepada korban.

Perbandingan Hukum Di Indonesia Dan Luar Negeri Mengenai Cyber Crime

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah beberapa kali diubah untuk mengikuti kemajuan teknologi, adalah undang-undang utama di Indonesia yang mengatur kejahatan cyber. Berbagai aspek kejahatan siber diatur oleh UU ITE, seperti hacking, pencurian data, dan penipuan online. Selain itu, Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik membuat penyelenggara sistem elektronik bertanggung jawab untuk menjaga data pribadi pengguna.⁹

⁶ "Wulandari, I. W., & Hwihanus, H. (2023). Peran Sistem Informasi Akuntansi Dalam Pengaplikasian Enkripsi Terhadap Peningkatan Keamanan Perusahaan. *Jurnal Kajian dan Penalaran Ilmu Manajemen*, Vol.1, No. 1, hlm. 11-25".

⁷ "Yudha, M. A. (2023). Tanggung Jawab Penyedia Atas Keamanan Data Penggunaan Layanan Dalam Transaksi Online Melalui Tokopedia. *Jurnal Notarius*, Vol. 2, No. 1."

⁸ "Suharto, M. A., & Apriyani, M. N. (2021). Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional. *Risalah Hukum*, hlm. 98-107."

⁹ "Supiyati, S. (2020). Penerapan Pasal 27 Ayat 3 Undang-undang No 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik Terhadap Tindak Pidana Pencemaran NAMA Baik Melalui Internet Sebagai Cybercrime Di Hubungkan Dengan Kebebasan Berekspreasi. *Pamulang Law Review*, Vol. 2, No. 1, hlm. 23-36".

Karena UU ITE dan peraturan terkait memberikan dasar hukum yang penting, pelaksanaan dan penegakannya seringkali sulit. Banyak kasus kebocoran data pribadi tidak segera ditangani atau diinvestigasi. Hal ini sebagian disebabkan oleh sumber daya yang terbatas dan kurangnya kerja sama antar lembaga penegak hukum. Selain itu, masyarakat kurang menyadari pentingnya melindungi data pribadi.

Sebagai perbandingan, Peraturan Perlindungan Data Umum (GDPR), yang ditetapkan oleh Uni Eropa pada tahun 2018, merupakan peraturan perlindungan data pribadi yang paling ketat dan menyeluruh di dunia. Peraturan ini memberikan hak-hak yang luas kepada orang-orang yang terkait dengan data pribadi, termasuk hak untuk mengakses, mengoreksi, dan menghapus data. GDPR juga menetapkan bahwa setiap kebocoran data harus dilaporkan kepada otoritas perlindungan data dalam waktu 72 jam, dan perusahaan.¹⁰

GDPR mengatur perusahaan di Uni Eropa dan perusahaan di seluruh dunia yang memproses data pribadi warga UE. Ini menunjukkan komitmen Uni Eropa untuk melindungi data pribadi warganya, tidak peduli di mana mereka diproses. Meningkatnya kesadaran akan pentingnya perlindungan data pribadi di seluruh dunia disebabkan oleh GDPR, yang juga mendorong banyak negara untuk membuat peraturan yang lebih kuat di bidang ini.¹¹

Mengingat bahwa ada banyak undang-undang federal dan negara bagian di Amerika Serikat yang mengatur berbagai aspek data pribadi, metode yang digunakan untuk melindungi data pribadi menjadi lebih kompleks. Salah satu undang-undang negara bagian yang memberikan hak-hak penting kepada konsumen terkait data pribadi adalah Undang-Undang Privasi Konsumen California (CCPA), yang berlaku mulai tahun 2020. CCPA memberikan konsumen hak untuk mengetahui informasi yang dikumpulkan dan untuk memilih untuk tidak menjual data pribadi.¹²

Amerika Serikat memiliki Gramm-Leach-Bliley Act (GLBA) dan Health Insurance Portability and Accountability Act (HIPAA) di tingkat federal yang mengatur perlindungan data keuangan. Meskipun tidak ada undang-undang federal satu-satunya yang menyeluruh seperti GDPR, kerangka kerja perlindungan data yang kuat dibangun di berbagai bidang.

Beberapa negara di Asia juga telah mengambil langkah-langkah besar untuk melindungi data pribadi mereka. Misalnya, Singapura memiliki Personal Data Protection Act (PDPA) yang berlaku pada tahun 2012. PDPA menetapkan organisasi untuk melindungi data pribadi dari akses, pengumpulan, penggunaan, dan pengungkapan yang tidak sah, serta memberikan hak kepada individu yang terkait dengan data tersebut. Jika seseorang melanggar PDPA, mereka dapat dikenakan denda hingga satu juta dolar Singapura.¹³

Melalui Act on the Protection of Personal Information (APPI), Jepang juga memperkuat perlindungan data pribadi. APPI terbaru mulai tahun 2020 mengharuskan perusahaan untuk meminta persetujuan orang sebelum mengumpulkan dan menggunakan data pribadi, dan memberi orang hak untuk mengakses dan mengoreksi data.¹⁴

Perbandingan antara Indonesia dan negara lain menunjukkan bahwa meskipun ada upaya untuk meningkatkan perlindungan data pribadi, penegakan undang-undang seperti GDPR di Uni Eropa dan PDPA di Singapura dapat diterapkan dengan efektif dan menyeluruh, memberikan hak-hak yang jelas kepada orang-orang dan menetapkan sanksi yang keras untuk pelanggaran.

Untuk memperkuat perlindungan data pribadi di Indonesia, langkah-langkah sedang diambil, seperti pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP). RUU PDP

¹⁰ "Farhan, F., Hamdani, F., et.al. (2022). Reformasi hukum perlindungan data pribadi korban pinjaman online (perbandingan Uni Eropa dan Malaysia). *Indonesia Berdaya*, Vol. 3, No. 3, hlm. 567-576".

¹¹ "ibid," t.t.

¹² "Satria, M. K., & Yusuf, H. (2024). Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Jurnal Intelek Dan Cendekiawan Nusantara*, Vol. 1, No. 2, hlm. 2442-2456".

¹³ "Heriyanto, H. (2023). Analisis perbandingan regulasi dan perlindungan hukum atas privasi data pasien di tiga Negara Asia Tenggara (Indonesia, Singapura, dan Laos). *Jurnal Ners*, Vol. 7, No. 2, hlm. 1247-1259.

¹⁴ "Sugeng, (2024). *Hukum Telematika Indonesia: Edisi Revisi*. Prenada Media."

dimaksudkan untuk membuat kerangka hukum yang lebih jelas dan tegas mengenai hak dan kewajiban yang terkait dengan data pribadi serta menetapkan sanksi yang lebih berat bagi mereka yang melanggarnya. Pengesahan RUU PDP akan menjadi langkah penting dalam memperkuat perlindungan hukum terhadap korban pelanggaran data pribadi.

Untuk meningkatkan perlindungan data pribadi di Indonesia, tindakan sedang diambil, seperti pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP). RUU PDP dimaksudkan untuk membuat kerangka hukum yang lebih jelas dan tegas mengenai hak dan kewajiban yang terkait dengan data pribadi serta menetapkan sanksi yang lebih berat bagi mereka yang melanggarnya. Pengesahan RUU PDP akan menjadi langkah penting dalam memperkuat perlindungan hukum terhadap korporasi yang melindungi data pribadi.

Ketentuan Pidana berdasarkan Undang-Undang Nomor 19 tahun 2016 Tentang Informasi dan Transaksi Elektronik

Tujuan dari UU ITE adalah untuk menindak berbagai jenis kejahatan siber. Jika seseorang dengan sengaja mengakses komputer atau sistem elektronik milik orang lain dengan cara apapun, tanpa hak atau melawan hukum, mereka akan dikenakan hukuman pidana menurut Pasal 30 UU ITE. Hukuman yang dapat diberikan untuk pelanggaran ini berbeda-beda tergantung pada seberapa buruk dan kuat akses ilegal tersebut. Misalnya, jika akses tersebut mengakibatkan kerugian bagi pemilik sistem elektronik, pelaku dapat dikenakan pidana penjara hingga enam tahun dan/atau denda hingga Rp 600 juta.¹⁵

Pasal 31 UU ITE mengatur penyadapan ilegal. Kejahatan siber yang diatur dalam UU ITE juga mencakup penyadapan atau pengintersepsian transmisi data pribadi secara tidak sah. Penyadapan atau pengintersepsian informasi elektronik atau dokumen elektronik tertentu yang tidak dimiliki seseorang dengan sengaja dapat dikenakan pidana penjara hingga sepuluh tahun dan/atau denda hingga Rp 800 juta. Ketentuan ini sangat penting untuk melindungi data pribadi karena pelaku kejahatan siber sering menggunakan penyadapan ilegal untuk mencuri data pribadi.¹⁶

Pasal 32 UU ITE menekankan bahwa orang yang dengan sengaja mengubah, menambah, mengurangi, menghapus, menghilangkan, atau memindahkan informasi elektronik atau dokumen elektronik orang lain akan dikenakan hukuman. Pelanggaran ini dapat mengakibatkan hukuman delapan tahun penjara dan/atau denda hingga Rp 2 miliar. Artikel ini sangat penting karena membahas jenis manipulasi data yang dapat mengancam keamanan data elektronik yang dimiliki oleh individu atau organisasi.¹⁷

Tindak lanjut yang mengarah pada kebocoran data pribadi juga diperhatikan dalam UU ITE. Pemalsuan informasi atau dokumen elektronik diatur dalam Pasal 35 UU ITE. Jika seseorang dengan sengaja, tanpa hak, atau melakukan pelanggaran hukum, mengubah, menciptakan, mengubah, atau menghilangkan informasi elektronik atau dokumen elektronik dengan tujuan agar informasi tersebut dianggap sebagai data asli, mereka dapat dikenakan pidana 12 tahun penjara dan/atau denda hingga 12 miliar rupiah. Untuk melindungi integritas data dan mencegah upaya pemalsuan yang dapat merugikan pemilik data asli, ketentuan ini dibuat.¹⁸

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, yang merupakan turunan dari UU ITE, menetapkan standar keamanan yang harus dipenuhi oleh penyelenggara sistem elektronik untuk melindungi data pribadi pengguna. Meskipun ketentuan pidana UU ITE cukup luas, ada banyak masalah untuk menerapkannya.

¹⁵ "Luthiya, A. N., Irawan, B., & Yulia, R. (2021). Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi. Jurnal Hukum Pidana dan Kriminologi, Vol. 2, No. 2, hlm. 14-29".

¹⁶ "Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. LN.2016/NO.251, TLN NO.5952, LL Setneg : 13 hlm".

¹⁷ "ibid."

¹⁸ "ibid."

Keterbatasan sumber daya dan kemampuan penegak hukum untuk menangani kasus kejahatan siber yang kompleks merupakan masalah utama.¹⁹

Akibatnya, beberapa langkah strategis perlu diambil untuk meningkatkan efektivitas penegakan UU ITE. Pertama-tama, peningkatan kemampuan dan keterampilan penegak hukum dalam bidang TI dan komunikasi sangat penting. Penegak hukum harus dididik untuk memahami dan menangani teknik kejahatan siber yang semakin kompleks. Kedua, pemerintah harus meningkatkan kerjasama internasional dalam memerangi kejahatan siber, termasuk perjanjian ekstradisi dan bantuan hukum timbal balik dengan negara lain. Ketiga, masyarakat harus lebih dididik tentang pentingnya melindungi data pribadi dan bagaimana melindungi diri dari kejahatan siber. Ini termasuk kampanye publik untuk meningkatkan kesadaran tentang risiko yang ada dan tindakan pencegahan.²⁰

SIMPULAN

Perlindungan hukum terhadap korban *cyber crime*, terutama terkait kebocoran data pribadi merupakan isu yang sangat penting di era digital ini. Di Indonesia, perlindungan tersebut diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) dan beberapa peraturan turunannya. UU ITE memberikan dasar hukum untuk menangani berbagai bentuk kejahatan siber, termasuk akses ilegal, penyadapan, manipulasi data, dan kebocoran data pribadi.

Perbandingan dengan regulasi di negara lain, seperti GDPR di Uni Eropa dan PDPA di Singapura, menunjukkan bahwa perlindungan data pribadi dapat diimplementasikan dengan cara yang lebih komprehensif dan efektif, memberikan hak-hak yang jelas kepada individu dan menetapkan sanksi yang berat bagi pelanggaran. Di Indonesia, langkah-langkah untuk memperkuat perlindungan data pribadi sedang berlangsung, termasuk melalui pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) yang diharapkan dapat memberikan kerangka hukum yang lebih jelas dan tegas serta sanksi yang lebih berat bagi pelanggar.

SARAN

Saran untuk meningkatkan perlindungan hukum terhadap korban *cyber crime* dan kebocoran data pribadi, beberapa langkah strategis perlu diambil. Pertama, peningkatan kapasitas dan keterampilan penegak hukum dalam bidang teknologi informasi dan komunikasi sangat penting. Penegak hukum perlu dilatih untuk memahami dan mengatasi teknik-teknik kejahatan siber yang semakin kompleks. Kedua, pemerintah perlu memperkuat kerjasama internasional dalam menangani kejahatan siber, termasuk melalui perjanjian ekstradisi dan bantuan hukum timbal balik dengan negara-negara lain. Ketiga, sosialisasi dan edukasi masyarakat tentang pentingnya perlindungan data pribadi dan cara-cara melindungi diri dari kejahatan siber harus ditingkatkan.

REFERENSI

- Bahtiar, N. (2024). Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah. *Development Policy and Management Review (DPMR)*, hlm. 85-100.
- Disemadi, H. S., Sudirman, L., Girsang, J., & Aninda, A. M. (2023). *Loc.cit.*
- Fadli, M., Widijowati, D., & Andayani, D. (2024). Pencurian Data Pribadi di Dunia Maya (Phising Cybercrime) yang ditinjau dalam Perspektif Kriminologi. *Co-Value Jurnal Ekonomi Koperasi dan kewirausahaan*, Vol. 14, No. 12.
- Farhan, F., Hamdani, F., et.al. (2022). Reformasi hukum perlindungan data pribadi korban pinjaman online (perbandingan Uni Eropa dan Malaysia). *Indonesia Berdaya*, Vol. 3, No. 3, hlm. 567-576.

¹⁹ "Bahtiar, N. (2024). Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah. *Development Policy and Management Review (DPMR)*, hlm. 85-100".

²⁰ "Sugeng. (2020). *Hukum Telematika Indonesia*. Prenada Media".

- Heriyanto, H. (2023). Analisis perbandingan regulasi dan perlindungan hukum atas privasi data pasien di tiga Negara Asia Tenggara (Indonesia, Singapura, dan Laos). *Jurnal Ners*, Vol. 7, No. 2, hlm. 1247-1259.
- Luthiya, A. N., Irawan, B., & Yulia, R. (2021). Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi. *Jurnal Hukum Pidana dan Kriminologi*, Vol. 2, No. 2, hlm. 14-29.
- Satria, M. K., & Yusuf, H. (2024). Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Jurnal Intelek Dan Cendekiawan Nusantara*, Vol. 1, No. 2, hlm. 2442-2456.
- Soejono Soekantor dan Sri Mamudji, *Penelitian Hukum Normatif*, PT Raja Grafindo, Jakarta, 2014, hal. 251-252.
- Sonjaya, A., & Setiawan, D. A. (2022, January). Perlindungan Hukum bagi Korban Kebocoran Data Pribadi Pengguna Aplikasi Tokopedia berdasarkan UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi. In *Bandung Conference Series: Law Studies* (Vol. 2, No. 1, pp. 420-427).
- Sugeng, (2024). *Hukum Telematika Indonesia: Edisi Revisi*. Prenada Media.
- Suharto, M. A., & Apriyani, M. N. (2021). Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional. *Risalah Hukum*, hlm. 98-107.
- Supiyati, S. (2020). Penerapan Pasal 27 Ayat 3 Undang-undang No 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik Terhadap Tindak Pidana Pencemaran NAMA Baik Melalui Internet Sebagai Cybercrime Di Hubungkan Dengan Kebebasan Berekspresi. *Pamulang Law Review*, Vol. 2, No. 1, hlm. 23-36.
- Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. LN.2016/NO.251, TLN NO.5952, LL Setneg : 13 hlm.
- Wulandari, I. W., & Hwihanus, H. (2023). Peran Sistem Informasi Akuntansi Dalam Pengaplikasian Enkripsi Terhadap Peningkatan Keamanan Perusahaan. *Jurnal Kajian dan Penalaran Ilmu Manajemen*, Vol.1, No. 1, hlm. 11-25.
- Yudha, M. A. (2023). Tanggung Jawab Penyedia Atas Keamanan Data Penggunaan Layanan Dalam Transaksi Online Melalui Tokopedia. *Jurnal Notarius*, Vol. 2, No. 1.