Jurnal Dialogica

Volume 1 Issue 2 Tahun 2026

Penegakan Hukum Tindak Pidana Pencurian Data Pribadi Oleh Kepolisian Studi Kasus Polrestabes Makassar

Nurul Hikmah B[1], Nasrullah Arsyad[2], Farah Syah Rezah[3]

Fakultas Hukum, Universitas Muslim Indonesia, Indonesia

Email Koresponden: nurulhikmahb040@gmail.com

Abstract

This study aims to determine and analyze the law enforcement of personal data theft crimes by the Makassar City Police Department, as well as to determine the police's role in minimizing personal data theft cases within the Makassar City Police Department. This research is an empirical legal research conducted through data collection based on interviews, supported by legal materials, and using qualitative data analysis techniques. The results indicate that law enforcement against personal data theft crimes has been carried out in accordance with the police's duties and functions as law enforcement agencies that provide protection, care, and service to the public. In practice, the case handling process is carried out through stages of inquiry and investigation, adhering to applicable legal procedures and involving collaboration with relevant parties in handling digital evidence. Preventive efforts are also carried out through outreach and education to the public to be more careful in protecting personal data to minimize losses due to cybercrime.

Keywords: *Crime, Personal Data Theft, Police.*

Abstrak

Penelitian ini bertujuan untuk mengetahui dan menganalisis penegakan hukum tindak pidana pencurian data pribadi oleh kepolisian di Polrestabes Makassar, serta mengetahui aparat kepolisian dalam meminimalisir kasus pencurian data pribadi di Polrestabes Makassar. Penelitian ini merupakan jenis penelitian hukum empiris yang dilaksanakan melalui pengumpulan data berdasarkan hasil wawancara, diperkuat dengan bahan-bahan hukum, serta menerapkan teknik analisis data kualitatif. Hasil penelitian menunjukkan bahwa penegakan hukum terhadap tindak pidana pencurian data pribadi telah dilaksanakan sesuai dengan tugas dan fungsi kepolisian sebagai aparat penegak hukum yang memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat. Dalam praktiknya, proses penanganan perkara dilakukan melalui tahapan penyelidikan dan penyidikan dengan memperhatikan prosedur hukum yang berlaku, serta melibatkan kerja sama dengan pihak terkait dalam penanganan bukti digital. Upaya pencegahan juga dilakukan melalui sosialisasi dan edukasi kepada masyarakat agar lebih berhati-hati dalam menjaga data pribadi guna meminimalisir kerugian akibat kejahatan siber.

Kata Kunci: *Tindak Pidana, Pencurian Data Pribadi, Kepolisian*

A. PENDAHULUAN

Kesadaran akan pentingnya regulasi yang mengatur perlindungan data pribadi secara bertahap mulai diperhatikan oleh pemerintah, yang tercermin dalam upaya mereka untuk menyusun dan mengesahkan Undang-Undang Nomor 27 tahun 2022. Kesulitan dalam menangani tindak kejahatan cyber dengan mengandalkan hukum positif konvensional sangatlah besar. Ini disebabkan karena kejahatan tersebut melibatkan lima faktor yang saling terkait, yaitu pelaku kejahatan, korban kejahatan, reaksi sosial terhadap kejahatan, dan hukum. Meskipun hukum memiliki peran penting dalam mencegah dan mengatasi kejahatan, menciptakan peraturan hukum yang sesuai dengan perkembangan teknologi informasi yang cepat bukanlah hal yang mudah.

Oleh karena itu, Aturan mengenai sanksi denda dan pidana atas pencurian atau penyalahgunaan data pribadi di Indonesia yang diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi ('UU PDP'):

1) Pasal 67 Ayat 1: setiap orang yang dengan sengaja melawan hukum memperoleh atau mengumpulkan data pribadi bukan miliknya untuk menguntungkan diri sendiri atau orang lain yang dapat merugikan subjek data, diancam pidana penjara paling lama 5 tahun dan/atau denda paling banyak Rp5 miliar.
2) Pasal 68 mengatur pembuatan atau pemalsuan data pribadi dengan ancaman pidana paling lama 6 tahun dan/atau denda paling banyak Rp6 miliar.
3) Sanksi administratif juga terdapat, misalnya Pasal 57 menyebut denda administratif paling tinggi 2% dari pendapatan tahunan bagi penyelenggara sistem elektronik yang melanggar.

Di Indonesia, perkembangan kejahatan di dunia maya telah mencapai tingkat yang mengkhawatirkan, sehingga negara ini sering disebut sebagai negara dengan tingkat kejahatan internet yang tinggi. Pada tahun 2022, Kepolisian Indonesia berhasil mengungkap 109 kasus tindak pidana Teknologi Informasi (TI), yang melibatkan 124 tersangka yang merupakan warga negara Indonesia dan melakukan aksi mereka di berbagai kota di Indonesia. Secara umum,

kejahatan terkait dengan teknologi informasi dapat diklasifikasikan ke dalam dua kategori. Pertama, kejahatan yang bertujuan merusak atau menyerang sistem atau jaringan komputer. Kedua, kejahatan yang menggunakan komputer atau internet sebagai alat untuk melakukan tindakan kejahatan. Ada banyak literatur dan situs yang membahas berbagai jenis kejahatan siber yang terjadi.

Dasar hukum yang jelas yaitu Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) Peraturan ini menjadi landasan utama yang mengatur berbagai aspek perlindungan data pribadi. Di dalamnya, dijelaskan dengan rinci mengenai larangan dan sanksi bagi setiap individu yang secara sengaja dan melawan hukum mengungkapkan, mengumpulkan, atau menggunakan data pribadi yang bukan miliknya.Ancaman pidana Undang-Undang Perlindungan Data Pribadi menetapkan ancaman pidana penjara maksimal 5 tahun dan/atau denda maksimal Rp5 miliar bagi pelaku pencurian data pribadi (disebut juga *identity theft*).

Kepolisian sebagai garda terdepan dalam sistem peradilan pidana memiliki peran strategis dalam memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat, termasuk dalam penanganan kejahatan siber. Proses penegakan hukum tidak hanya mencakup aspek represif melalui penindakan terhadap pelaku, tetapi juga aspek preventif melalui edukasi dan sosialisasi kepada masyarakat agar lebih waspada dalam menjaga data pribadinya. Efektivitas penegakan hukum sangat bergantung pada profesionalitas penyidik, dukungan sarana dan prasarana teknologi, serta koordinasi antar lembaga terkait. Namun sayangnya, masyarakat Indonesia dengan penduduk mayoritas pemeluk ajaran Islam, disebut minim literasi digital tentang pentingnya perlindungan data pribadi. Padahal syariat Islam mempunyai landasan etik berdasarkan nash-nash agama yang sangat memandang penting perlindungan data pribadi seseorang. Dalam surat An-Nur ayat 27 Allah SWT berfirman yang Artinya : “Wahai orang-orang yang beriman, janganlah memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Demikian itu lebih baik bagimu agar kamu mengambil pelajaran”.

Rendahnya tingkat pemahaman masyarakat menyebabkan banyak korban tidak menyadari bahwa pencurian data pribadi merupakan tindak pidana yang dapat dilaporkan kepada pihak kepolisian. Sebagian korban bahkan tidak mengetahui bahwa data pribadinya telah diambil atau disalahgunakan oleh pihak yang tidak bertanggung jawab. Kondisi ini berdampak pada minimnya pelaporan dan lambatnya penanganan perkara

Selain itu, keterbatasan sumber daya manusia dan teknologi juga menjadi kendala. Tidak seluruh satuan kepolisian, khususnya di daerah, memiliki personel dengan kompetensi khusus di bidang kejahatan siber dan forensik digital. Keterbatasan tersebut dapat menghambat proses identifikasi pelaku, pelacakan jejak digital, hingga penyelesaian perkara. Dalam kasus pencurian data pribadi, alat bukti yang digunakan umumnya berupa bukti digital yang rentan hilang, rusak, atau dimanipulasi. Oleh karena itu, diperlukan keahlian khusus dalam proses pengumpulan, pengamanan, dan analisis bukti agar sah dan dapat dipertanggungjawabkan di persidangan. Di samping itu, luasnya yurisdiksi juga menjadi tantangan tersendiri, karena pelaku kejahatan siber kerap beroperasi dari luar wilayah hukum Indonesia. Hal ini membuat proses penegakan hukum menjadi lebih kompleks dan memerlukan kerja sama lintas negara.

B. METODE

Penelitian ini menggunakan metode hukum empiris dengan pendekatan kualitatif untuk mengatahui penegakan hukum tindak pidana pencurian data pribadi oleh kepolisian. Lokasi penelitian berada di wilayah hukum Polrestabes Makassar karena tingginya angka kasus penipuan online di daerah tersebut. Data primer diperoleh melalui wawancara mendalam dengan informan yang dipilih secara purposive, terdiri atas dua anggota kepolisian. Teknik wawancara dilakukan secara tatap muka dengan panduan semi-terstruktur untuk menggali informasi faktual dan kontekstual. Data sekunder diperoleh melalui studi kepustakaan dari dokumen hukum, literatur akademik, serta peraturan perundang-undangan yang relevan. Seluruh data dianalisis secara deskriptif-kualitatif melalui proses reduksi data,

kategorisasi, hingga penarikan kesimpulan yang mencerminkan realitas hukum di lapangan dan solusi terhadap maraknya pencurian data.

C. PEMBAHASAN

1. Penegakan Hukum Tindak Pidana Pencurian Data Pribadi Oleh Kepolisian di Polrestabes Makassar

Penegakan hukum terhadap tindak pidana pencurian data pribadi oleh kepolisian merupakan bagian dari upaya negara dalam memberikan perlindungan hukum kepada masyarakat di era digital. Secara normatif, dasar hukum penanganan perkara ini merujuk pada Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya. Dalam praktiknya, kepolisian menjalankan tahapan penegakan hukum melalui penerimaan laporan masyarakat, penyelidikan, penyidikan, pengumpulan dan analisis alat bukti digital, hingga pelimpahan berkas perkara kepada penuntut umum. Proses ini menuntut kemampuan teknis di bidang forensik digital karena karakteristik kejahatan yang dilakukan melalui sistem elektronik dan sering kali melibatkan jaringan lintas wilayah bahkan lintas negara.

Dalam konteks implementasi di daerah, seperti pada Polrestabes Makassar, penegakan hukum tidak hanya bersifat represif tetapi juga didukung langkah preventif melalui edukasi dan sosialisasi kepada masyarakat. Tantangan utama yang dihadapi meliputi keterbatasan sumber daya manusia yang memiliki kompetensi khusus di bidang siber, kompleksitas pembuktian digital yang mudah dihapus atau dimanipulasi, serta modus operandi pelaku yang semakin terorganisir. Oleh karena itu, efektivitas penegakan hukum sangat bergantung pada peningkatan kapasitas aparat, koordinasi antar lembaga, serta partisipasi aktif masyarakat dalam melaporkan setiap dugaan penyalahgunaan data pribadi.

Berdasarkan data yang diperoleh hasil penyelidikan mengenai Kasus Pencurian Data Pribadi di Wilayah Hukum Kepolisian di Kota Makassar tahun 2023 s.d. 2025 oleh Satreskrim pada tabel berikut:

Tabel 1,Jumlah Kasus Pencurian Data Pribadi di Kota Makassar Tahun 2023-2025

Tahun	Kasus Pencurian Data Pribadi
2023	7 Kasus
2024	11 Kasus
2025	2 Kasus
Jumlah Total	**20 Kasus**

Sumber : Satreskrim Polretabes Makassar Tahun 2023 s.d. 2025

Berdasarkan tabel jumlah kasus, penyidikan tindak pidana cybercrime oleh satuan kerja Satreskrim Polrestabes Makassar pada tahun 2023 tercatat sebanyak 7 kasus. Jumlah tersebut meningkat pada tahun 2024 menjadi 11 kasus, yang disebabkan semakin maraknya penyalahgunaan data pribadi, dalam bentuk penyebaran maupun penjualan data, serta meningkatnya pelaporan dari masyarakat. Pada tahun 2025 jumlah kasus mengalami penurunan menjadi 2 kasus, dengan peretasan dan penipuan online sebagai kategori utama. Penurunan ini dipengaruhi oleh upaya pencegahan dan penegakan hukum yang lebih intensif, serta adanya perubahan klasifikasi penanganan perkara dan sejumlah kasus yang masih dalam tahap penyelidikan sehingga belum tercatat dalam data penyidikan.

Berikut penegakan hukum tindak pidana dalam kasus pencurian data pribadi di Polrestabes Makassar, yaitu:

a. **Laporan Kejadian**

Upaya awal dalam penanganan tindak pidana pencurian data pribadi dilakukan melalui penerimaan laporan masyarakat. Korban yang merasa dirugikan dapat melapor ke SPKT (Sentra Pelayanan Kepolisian Terpadu). Di tahap ini dilakukan pengkajian awal untuk menilai kelayakan laporan. Jika dinyatakan memenuhi unsur, laporan dibuatkan tanda terima dan laporan polisi, kemudian dilimpahkan ke unit Reserse Kriminal Khusus untuk ditindaklanjuti. Namun, tidak semua korban memahami bahwa

pencurian data pribadi merupakan tindak pidana yang dapat dilaporkan, sehingga masih banyak kasus yang tidak terungkap.

b. **Penyelidikan Awal**

Pada tahap penyelidikan, tim penyidik terlebih dahulu mengklasifikasikan permasalahan guna menentukan metode dan teknik investigasi yang tepat. Penentuan penyidik dilakukan berdasarkan kompetensi, khususnya dalam bidang kejahatan siber dan forensik digital, mengingat karakteristik perkara yang berbasis sistem elektronik.

c. **Pengumpulan Bukti dan Pemeriksaan Saksi**

Proses pengumpulan alat bukti dan pemeriksaan saksi sering menghadapi hambatan. Kejahatan siber umumnya tidak disaksikan secara langsung sehingga sulit menemukan saksi fakta. Jika barang bukti berupa perangkat elektronik bukan milik pelaku, maka pemegang perangkat diperiksa terlebih dahulu sebagai saksi. Selain itu, bukti digital seperti website atau tautan bersifat dinamis, mudah dihapus, dan tidak selalu dapat disita secara fisik, sehingga memerlukan teknik khusus untuk mengamankan dan menganalisisnya agar sah di persidangan.

d. **Penanganan Kasus dan Penerapan Sanksi**

Salah satu contoh kasus yang ditangani adalah penguasaan akun media sosial Instagram pasca berakhirnya kerja sama usaha. Awalnya, akun tersebut dikelola bersama oleh pemilik usaha dan mitra, termasuk berbagi kredensial akses. Setelah terjadi konflik dan kerja sama berakhir, mitra diduga mengganti kata sandi dan nomor telepon tanpa persetujuan, sehingga pemilik usaha kehilangan akses. Akun tersebut kemudian digunakan untuk kepentingan pribadi yang merugikan reputasi usaha.

Perbuatan tersebut dapat dikualifikasikan sebagai akses ilegal terhadap sistem elektronik sebagaimana diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah, khususnya Pasal 30 ayat (1) juncto Pasal 46, dengan ancaman pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp600.000.000,00.

Contoh lain terjadi pada 5 Agustus 2025, di mana pelaku menggunakan modus pesan teks, telepon acak, dan aplikasi tertentu untuk memperoleh nomor telepon korban sehingga data pribadi korban muncul dan disalahgunakan. Dalam penanganannya, polisi menyita komputer, CPU, serta ribuan kartu SIM yang telah diregistrasi. Pelaku kemudian dijerat dengan ketentuan dalam Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Secara umum, proses penanganan perkara pencurian data pribadi memerlukan ketelitian, keahlian teknis, serta penerapan ketentuan hukum yang tepat sesuai karakteristik tindak pidana berbasis elektronik.

2. Srtaregi Aparat Kepolisian dalam Meminimalisir Kasus Pencurian Data Pribadi di Polrestabes Makassar

Pihak kepolisian bekerja sama dengan stakeholder yang ada yaitu bagaimana menangkap pelaku yang tertangkap tangan melakukan kejahatan ataupun melalui laporan masyarakat kemudian mendatangi tempat kejadian perkara (TKP) guna melakukan penangkapan dan penahanan terhadap tersangka kasus Tindak Pidana Siber, setelah dilakukan penangkapan kemudian diproses dikepolisian dan sebelum dilimpahkan berkas perkaranya ke kejaksaan.

Dalam upaya meminimalisir tindak pidana pencurian data pribadi, aparat kepolisian di Polrestabes Makassar menerapkan strategi preventif dan represif secara terpadu. Pendekatan preventif dilakukan melalui edukasi dan sosialisasi kepada masyarakat mengenai pentingnya perlindungan data pribadi serta risiko penyalahgunaan data di ruang digital. Kegiatan ini dilaksanakan melalui penyuluhan hukum, kampanye media sosial, serta kerja sama dengan instansi pemerintah, pelaku usaha, dan lembaga pendidikan agar masyarakat lebih waspada terhadap modus kejahatan siber. Selain itu, penguatan kapasitas sumber daya manusia di bidang siber serta pemanfaatan perangkat teknologi pendukung menjadi langkah penting dalam mendeteksi dan mencegah potensi serangan sejak dini. Upaya ini sejalan dengan implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang menekankan kewajiban perlindungan dan pengamanan data pribadi.

Di sisi represif, kepolisian bertindak tegas melalui proses penyelidikan dan penyidikan apabila telah terjadi tindak pidana. Penanganan perkara dilakukan berdasarkan prosedur sistem peradilan pidana, mulai dari penerimaan laporan, pengumpulan alat bukti digital, hingga pelimpahan berkas perkara kepada penuntut umum. Dalam praktiknya, seperti yang dilakukan oleh Polrestabes Makassar, strategi ini juga didukung dengan koordinasi antar lembaga serta evaluasi berkala terhadap kasus yang ditangani guna meningkatkan efektivitas penegakan hukum. Dengan kombinasi langkah preventif dan represif tersebut, diharapkan angka pencurian data pribadi dapat ditekan serta tercipta keamanan dan kepercayaan masyarakat dalam penggunaan teknologi digital. Berdasarkan hasil wawancara dengan Bapak Rizko Tri Revo selaku perwakilan personel Gakkum Satuan Reserse Kriminal Khusus Polrestabes Makassar, strategi yang diterapkan dalam meminimalisir kasus pencurian data pribadi dibagi ke dalam pendekatan preventif (pencegahan) dan represif (penegakan hukum).

a. Upaya Preventif

Upaya preventif dilakukan melalui langkah preemtif dan pencegahan langsung di tengah masyarakat. Tindakan preemtif dilaksanakan dengan menanamkan nilai dan norma hukum kepada masyarakat agar terbentuk kesadaran hukum sejak dini. Hal ini bertujuan mencegah timbulnya niat maupun kesempatan melakukan kejahatan. Selanjutnya, tindakan preventif diwujudkan melalui edukasi dan penyuluhan hukum. Polrestabes Makassar secara aktif melaksanakan sosialisasi di sekolah dan kampus di Kota Makassar. Materi yang diberikan meliputi pentingnya perlindungan data pribadi, risiko kebocoran data, serta modus-modus kejahatan siber yang terus berkembang. Langkah ini menjadi penting karena meningkatnya penggunaan media sosial dan aplikasi digital sejak masa pandemi, yang turut membuka peluang terjadinya penyalahgunaan data.

Dari sisi internal, penguatan pencegahan juga dilakukan dengan peningkatan kapasitas sumber daya manusia Polri di bidang siber. Personel diberikan pelatihan, pendidikan khusus, serta dikirim

mengikuti kursus terkait cybercrime guna meningkatkan kemampuan penyidikan dan analisis forensik digital. Selain itu, Polri dilengkapi dengan alat khusus (alsus) berbasis teknologi untuk mendukung tugas pemeliharaan keamanan dan ketertiban masyarakat (Harkamtibmas). Penguatan sistem dan perangkat ini merupakan bagian dari transformasi digital Polri dalam menghadapi ancaman kejahatan siber yang semakin kompleks dan terorganisir. Koordinasi antar lembaga juga menjadi strategi preventif yang penting. Polrestabes Makassar menjalin kerja sama dengan berbagai instansi terkait, seperti Kementerian Komunikasi dan Informatika Republik Indonesia, Kementerian Dalam Negeri Republik Indonesia, Pusat Data Nasional, serta Lembaga Pelindungan Data Pribadi. Sinergi ini bertujuan memperkuat sistem pengawasan, pengamanan data, dan pertukaran informasi dalam penanganan kejahatan siber. Dalam membangun kepercayaan publik, kepolisian juga mengimbau masyarakat agar lebih berhati-hati dalam melakukan registrasi atau pengisian data pada aplikasi yang belum terverifikasi. Mengingat kejahatan pencurian data pribadi kini banyak dilakukan secara terorganisir, kewaspadaan masyarakat menjadi faktor penting dalam pencegahan.

b. Upaya Represif

Upaya represif dilakukan apabila telah terjadi tindak pidana. Tindakan ini merupakan bagian dari sistem peradilan pidana yang dilaksanakan sesuai prosedur hukum yang berlaku. Penegakan hukum dilakukan melalui proses penyelidikan, penyidikan, penuntutan, hingga pelaksanaan putusan pengadilan oleh aparat yang berwenang, yaitu kepolisian, kejaksaan, pengadilan, dan lembaga pemasyarakatan. Dalam konteks pencurian data pribadi, penerapan sanksi pidana mengacu pada ketentuan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta peraturan perundang-undangan lain yang relevan. Penegakan hukum ini bertujuan memberikan efek jera kepada pelaku sekaligus menciptakan kepastian dan perlindungan hukum bagi korban.

Pihak kepolisian memiliki peran penting dalam upaya penanggulangan cyber, dimana kemampuan pihak kepolisian sangat dibutuhkan untuk mengungkap kasus-kasus cyber. Adanya unit cybercrime di lingkungan kepolisian membuktikan bahwa dibutuhkannya penyidik khusus yang memiliki kemampuan di bidang informasi dan transaksi elektronik guna menangani kejahatan-kejahatan di dunia maya. Oleh karena itu dibutuhkannya pendidikan khusus untuk memberikan pengetahuan terkait cyber kepada para penegak hukum yang khusus menangani masalah cybercrime.

D. KESIMPULAN

Penegakan hukum dalam kasus pencurian data pribadi meliputi tahapan laporan kejadian, penyelidikan awal, pengumpulan bukti dan pemeriksaan saksi, hingga penanganan perkara dan penerapan sanksi pidana. Salah satu tantangan terbesar yang dihadapi penyidik adalah serangan siber, seperti malware, phishing, dan hacking, yang dilakukan oleh pelaku dengan kemampuan teknologi tinggi. Untuk itu, pihak kepolisian secara berkala melakukan evaluasi terhadap kasus yang ditangani guna meningkatkan efektivitas penanganan di tahun berikutnya. Adapun strategi aparat kepolisian dalam meminimalisir kasus pencurian data pribadi dilakukan melalui langkah preventif dan represif, yakni upaya pencegahan, edukasi dan penyuluhan hukum, penguatan perangkat serta pengamanan sistem, koordinasi antar lembaga, dan pembangunan kepercayaan masyarakat. Sosialisasi terus dilakukan agar masyarakat lebih berhati-hati dalam melakukan registrasi dan penginputan data pada aplikasi yang belum terverifikasi, sekaligus untuk mencegah serangan siber dan memantau aktivitas digital yang mencurigakan. Kepada pihak kepolisian diharapkan meningkatkan kualitas pelayanan sebagai pelindung, pengayom, dan pelayan masyarakat, khususnya dalam penanganan kasus pencurian data pribadi. Pelayanan presisi perlu dioptimalkan melalui kemudahan akses pelaporan, integrasi layanan yang telah ada, serta standarisasi penanganan perkara secara menyeluruh dari awal hingga selesai. Aparat kepolisian juga

diharapkan mengoptimalkan sarana dan prasarana, baik dari segi jumlah maupun pemanfaatannya, guna meningkatkan efektivitas penanganan kejahatan siber dan memulihkan kepercayaan masyarakat. Di sisi lain, masyarakat perlu meningkatkan keamanan sistem elektronik yang digunakan serta aktif melaporkan setiap dugaan atau kejadian kejahatan siber kepada pihak kepolisian.

REFERENSI

[1] Amelia, R. (2023). Perlindungan hukum terhadap korban kebocoran data pribadi dalam sistem elektronik. *Jurnal Arena Hukum, 16*(2), 233–248.

[2] Amelia, R. (2023). Perlindungan hukum terhadap korban kebocoran data pribadi dalam sistem elektronik. *Jurnal Arena Hukum, 16*(2), 233–248.

[3] 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*, *14*(12).

[4] Fikri, M., & Alhakim, A. (2022). Urgensi Pengaturan Hukum Terhadap Pelaku Tindak Pidana Pencurian Data Pribadi di Indonesia. *YUSTISI Учредители: LPPM Universitas Ibn Khaldun* Bogor, *9*(1).

[5] Hidayat, T., & Kurniawan, B. (2021). Hambatan penyidikan tindak pidana cybercrime di Indonesia. *Jurnal Legislasi Indonesia, 18*(4), 489–502.

[6] Latif, H. (2023). Integrasi metode normatif dan sosiologis dalam penelitian hukum pidana. *Jurnal Al-Daulah: Jurnal Hukum dan Perundangan Islam, 12*(1), 33–47. Fakultas Hukum Universitas Muslim Indonesia.

[7] Lestari, F. A. (2023). Pertanggungjawaban pidana pelaku pencurian data pribadi dalam perspektif hukum pidana Indonesia. *Jurnal Ilmiah Kebijakan Hukum, 17*(1), 14.

[8] 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*, *2*(2), 14-29.

[9]. Pratama, R., & Wibowo, A. (2022). Peran kepolisian dalam penanganan kejahatan siber terkait penyalahgunaan data pribadi. *Jurnal Hukum Ius Quia Iustum, 29*(3), 517–534.

[10] Ramadhan, M., & Putri, N. A. (2024). Implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam penegakan hukum oleh aparat kepolisian. *Jurnal Penelitian Hukum De Jure, 24*(1), 55–70.

[11] Saleh, A. R. (2021). Perlindungan Data Pribadi Dalam Perspektif Kebijakan Hukum Pidana. *HUKMY: Jurnal Hukum*, *1*(1), 91-108.

[12] Sari, D. P., & Nugroho, A. (2023). Penegakan hukum terhadap tindak pidana pencurian data pribadi berdasarkan Undang-Undang Perlindungan Data Pribadi. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 12*(2), 145–160.

[13] Rafasya, R., Citra, H., & Fauzi, E. (2023). Perlindungan hukum terhadap konsumen atas pencurian data pribadi dalam transaksi elektronik. *Jurnal Ilmu Sosial, Humaniora Dan Seni*, *2*(1), 29-33.

[14]. Triadi, M. (2023). Perlindungan Terhadap Korban Pencurian Data Pribadi Melalui Media Digital. *REUSAM: Jurnal Ilmu Hukum*, *11*(1), 45-64.

[15] Saly, J. N., Artamevia, H., Kheista, K., Gulo, B. J. S., Rhemrev, E. A., & Christie, M. (2023). Analisis perlindungan data pribadi terkait uu no. 27 tahun 2022. *Jurnal Serina Sosial Humaniora*, *1*(3), 145-153.