

URGENSI PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI DARI PENYALAHGUNAAN ORANG LAIN DENGAN PENDEKATAN SOSIOLOGI HUKUM

¹ Nurus Zuadi, ²Mahsun Ismail, ³Gatot Subroto, ⁴Mohammad,

¹⁾ Mahasiswa Fakultas Hukum Universitas Madura

^{2,3,4)} Dosen Fakultas Hukum Universitas Madura

Email: nuruszuadi007@gmail.com

Abstrack

The development of information technology and the internet has changed the way humans communicate, one of which is the development of social networks, social networks have become a part of life for receiving, sharing and disseminating information. The aim of this research is to find out and determine the form of legal protection and legal remedies that can be taken by parties who experience losses due to misuse of personal data. The legal sociology approach method is based on Law Number 27 of 2022 concerning the protection of personal data. The research results from this thesis obtained answers, namely, first, that the forms of legal protection are preventive legal protection from the government in order to prevent violations from occurring as well as repressive legal protection. This form of repressive protection is in the form of fines, sanctions and imprisonment according to articles 67 to 68 of Law Number 27 of 2022 concerning personal data protection. Second, legal action that can be taken by victims of the crime of personal data theft can be done through the penalty route of making a report to the authorities supported by concrete evidence relevant to the crime. Apart from that, the victim has compensation and restitution as regulated by Perma Number 1 of 2022 in conjunction with Government Regulation Number 35 of 2020 concerning amendments to Government Regulation number 7 of 2018 concerning the provision of compensation, restitution and assistance to witnesses and victims. Non-penal legal remedies with out-of-judicial resolution as regulated by Minister of Communication and Information Regulation number 20 of 2016 concerning protection of personal data in electronic system.

Keyword : Personal Data, Electronic Information, Crime, Legal Remedies.

Abstrak

Perkembangan teknologi informasi dan internet telah mengubah cara manusia berkomunikasi salah satunya perkembangan jejaring sosial, jejaring sosial telah menjadi bagian dari kehidupan untuk menerima, berbagi dan menyebarkan informasi. Adapun tujuan dari penelitian ini adalah mengetahui dan menentukan bentuk perlindungan hukum serta upaya hukum yang dapat dilakukan oleh pihak yang mengalami kerugian atas penyalahgunaan data pribadi. Metode pendekatan sosiologi hukum yaitu dengan berdasarkan Undang-Undang-Nomor 27 tahun 2022 tentang perlindungan data pribadi. Hasil penelitian dari skripsi ini memperoleh jawaban yaitu, pertama, bahwa bentuk-bentuk perlindungan hukum adalah perlindungan hukum preventif dari pemerintah dalam rangka pencegahan terjadinya suatu pelanggaran serta perlindungan hukum represif. Bentuk perlindungan represif ini adalah berupa denda, sanksi, dan penjara menurut pasal 67 sampai 68 Undang-Undang Nomor 27 tahun 2022 tentang perlindungan data pribadi. Kedua, upaya hukum yang dapat dilakukan oleh korban kejahatan pencurian data pribadi bisa dilakukan dengan jalur penal membuat laporan kepada pihak berwajib dengan didukung bukti yang kongkrit yang relevan dengan kejahatan tersebut selain itu korban mempunyai kompensasi dan restitusi sebagaimana diatur Perma Nomor 1 tahun 2022 jo

Peraturan Pemerintah Nomor 35 tahun 2020 tentang perubahan atas Peraturan Pemerintah nomor 7 tahun 2018 tentang pemberian kompensasi, restitusi, dan bantuan kepada saksi dan korban. Upaya hukum non penal dengan penyelesaian diluar peradilan sebagaimana diatur dengan Peraturan Menteri Komunikasi dan Informasi nomor 20 tahun 2016 tentang perlindungan data pribadi dalam sistem elektronik.

Kata Kunci : Data Pribadi, Informasi Elektronik, Tindak Pidana, Upaya Hukum.

PENDAHULUAN

Perkembangan teknologi informasi dan internet telah mengubah cara manusia berkomunikasi salah satunya perkembangan jejaring sosial, jejaring sosial telah menjadi bagian dari kehidupan untuk menerima, berbagi dan menyebarkan informasi sehingga media online merupakan salah satu media yang paling populer saat ini karena menawarkan kemudahan dan kecepatan yang memungkinkan seseorang untuk berkreasi dan menyebarkan informasi oleh karena itu era teknologi informasi saat ini tidak hanya menjawab pesan, bertukar informasi tetapi juga membuat segalanya menjadi mudah dan banyak manfaat yang didapat dari kemajuan teknologi informasi (Alvian Dwiangga Wijaya, 2022). Cara manusia berkomunikasi dari masa ke masa mengalami perubahan dan perkembangan. Apabila pada zaman dahulu, manusia menggunakan tanda untuk berkomunikasi, mengirimkan pesan bahkan menggunakan burung merpati sebagai penyampai pesan dan berkembang menggunakan telegraf kemudian telepon kabel serta akhirnya berkembang menjadi smartphone, dan didukung dengan media internet.

Adanya perkembangan teknologi informasi dan internet seluruh kehidupan manusia menjadi mudah dan bergantung kepada teknologi. Melakukan kegiatan ekonomi tidak hanya dilakukan dengan cara-cara konvensional namun dapat dilakukan melalui teknologi informasi, misalnya menjual barang dapat dilakukan secara online, memesan tiket kereta dan pesawat secara online bahkan pemerintahan juga menerapkan pelayanan dengan teknologi internet misalnya berbagai informasi sensitif seperti Kartu Tanda Penduduk (KTP), Surat Izin Mengemudi (SIM), Paspor, Kartu Keluarga (KK), Nomor Pokok Wajib Pajak (NPWP), Nomor Rekening, sidik jari, ciri khas individu, dan lain-lain telah diunggah ke internet sebagai kemudahan dalam melakukan berbagai hal.

Penggunaan teknologi internet membuat segala sesuatu menjadi lebih cepat dan efisien namun masih rentan terjadi peretasan sehingga data-data pribadi dapat disalahgunakan oleh orang yang tidak bertanggung jawab oleh karena itu Pemerintah bertanggung jawab dalam melindungi dan mengawasi penggunaan teknologi informasi dan internet.

Dalam siaran pers no.138/MH/KOMINFO/07/2023 menyatakan bahwa terdapat dugaan kebocoran data paspor 34,9 juta warga Indonesia. Selain itu Lebih dari 337 juta data yang diduga berasal dari server Ditjen Dukcapil Kemendagri dijual di forum peretas breachforums pada 14 Juli 2023. Hal tersebut menandakan bahwa perlindungan data pribadi masih kurang di Indonesia. Dalam rangka perlindungan data pribadi pada tanggal 17 Oktober 2022 pemerintah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Basyari, 2023). Undang-Undang ini disahkan bertujuan untuk menjamin hak warga negara atas perlindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya perlindungan data pribadi. Hukum Pelindungan Data Pribadi memerlukan dasar teoretis untuk memastikan dicapainya stabilitas (*stability*), dapat memprediksi (*predicta bility*), dan keadilan (*fairness*) dalam suatu keseluruhan sistem hukum ekonomi, dan teknologi terhadap peradaban manusia sehingga adaptasi kebiasaan Baru hukum Pelindungan Data Pribadi.

Hasil data pribadi Pemerintah berencana mengubah E-KTP menjadi Identitas Kependudukan Digital agar mempermudah masyarakat ketika melakukan transaksi pada pelayanan publik, karena dokumen kependudukan telah ada di dalam telepon genggam sehingga pemberlakuan Identitas Kependudukan Digital (IKD) di masa depan akan menekan anggaran untuk pengadaan blangko Kartu Tanda Penduduk (KTP) elektronik dan tinta yang dilakukan oleh pusat serta penghematan anggaran tersebut dapat digunakan untuk biaya pengembangan layanan adminduk.

Selain mempermudah resiko kebocoran data pribadi masih menjadi permasalahan utama dengan banyaknya kasus kebocoran data pribadi masyarakat

menjadi mempertanyakan kebijakan pemerintah tersebut sehingga kebocoran data pribadi di Internet dapat menyebabkan kerugian terhadap masyarakat ditambah lagi dengan diterapkannya Identitas Kependudukan Digital (IKD).

METODE PENELITIAN

Penelitian ini menggunakan metode empiris melalui pendekatan sosiologi hukum. Hal ini dilakukan untuk menganalisis permasalahan mengenai penyalahgunaan data pribadi yang dilakukan orang lain sehingga perlu mendapatkan solusi terhadap masyarakat yang mengalami kasus tersebut.

Peneliti menggunakan teori etis dengan perlindungan data pribadi hukum semata-mata hanya bertujuan untuk mewujudkan keadilan agar semua orang dalam situasi yang sama diperlakukan sama. semua berhak atas perlindungan hukum dan tidak ada yang kebal terhadap hukum sehingga masyarakat merasa aman dengan Teori Ethis untuk melindungi data pribadi dari penyalahgunaan orang lain

HASIL DAN PEMBAHASAN

1. Bentuk Perlindungan Hukum Terhadap Data Pribadi Dari Penyalahgunaan Orang Lain

Perlindungan hukum adalah suatu upaya proteksi atau benteng dalam mempertahankan suatu hak yang telah dimiliki setiap orang yang mana hal itu sudah dijamin oleh hukum, agar setiap orang dapat menikmati haknya. Dalam arti singkat Perlindungan ini adalah upaya tindakan yang harus dilakukan dalam hal ini aparat penegak hukum dalam rangkalah menciptakan rasa aman dan nyaman dan terbebas dari semua gangguan-gangguan yang ada (Pramono, 2020). Penyalahgunaan data pribadi tanpa disadari dapat terjadi karena merupakan kelalaian dari calon korban (masyarakat) itu sendiri dalam melaksanakan aktivitasnya sehari-hari.

Misalnya Big data yang dianggap sebagai suatu solusi yang menjanjikan dalam mengolah data karena mampu mengolah data yang besar dan bervariasi serta dapat membuat lampiran yang akurat, sehingga membuat big data tidak saja hanya digunakan oleh pihak pemerintah namun digunakan juga oleh pihak swasta. Akan tetapi di sisi lain penyalahgunaan big data tidak dapat dipungkiri

dapat juga mengancam privasi seseorang. Misalnya saja gejala yang muncul ketika harus melakukan registrasi data pribadi seperti kartu tanda penduduk (KTP) serta kartu keluarga (KK), contoh lain misalnya *history* pada aplikasi ojek online, dimana hal tersebut terdapat peluang terjadinya penyalahgunaan data yang menimbulkan kerugian (Diah Puspitasari, 2023).

Indonesia dalam hal ini untuk mewujudkan perlindungan hukum melalui di bentuknya lembaga-lembaga Negara dalam penegakan hukum seperti Pengadilan, Kejaksaan, dan Kepolisian. Lembaga-Lembaga ini adalah wujud konsistensi bahwa Negara Indonesia adalah Negara Hukum, Yang mana semua aspek dalam berkehidupan dan berbangsa diatur dan berpedoman kepada peraturan perundang undangan yang berlaku, sehingga hukum hadir di dalam sendi-sendi kehidupan di negeri ini. Untuk itu dengan adanya Perlindungan Hukum diharapkan dapat mencapai tujuan untuk memberikan keadilan, khususnya keadilan terkait dengan data pribadi. Dalam perlindungan hukum itu sendiri di bedakan menjadi 2 jenis, antara lain (Firdaus, 2022):

- a. Perlindungan hukum preventif Perlindungan ini adalah suatu upaya dari pemerintah dalam rangkah pencegahan terjadinya suatu pelanggaran, Perlindungan ini biasanya dapat dijumpai dalam suatu bentuk peraturan perundang-undangan, selain perlindungan berupa hak terdapat juga pedoman untuk melakukan suatu kewajiban dalam bentuk Batasan-batasan.
- b. Perlindungan hukum represif Bentuk perlindungan represif ini adalah berupa denda, sanksi, dan penjara, Hal ini merupakan suatu wujud nyata dari adanya suatu aturan dan perundang-undangan, siapa pun yang telah melanggar akan mendapatkan ganjaran atas perbuatannya.

Hak Hak Yang Harus Diperoleh Korban Kejahatan Penyalahgunaan Data Pribadi, meliputi (Rizky P.P. Karo Karo, 2020):

- a. Hak Korban
 - 1) Menerima ganti rugi penderitaan yang dialami, disesuaikan peran korban pada kejahatan yang terjadi

- 2) Menolak kompensasi bila korban tidak memerlukan diberikan kompensasi
 - 3) Menerima ganti rugi untuk ahli warisnya jika korban meninggal dunia
 - 4) Menerima rehabilitasi dan pembinaan
 - 5) Menerima kembali hak miliknya
 - 6) Menolak menjadi saksi apabila hal itu akan memberi bahaya untuk korban
 - 7) Dilindungi dari ancaman pihak korban jika menjadi saksi atau melapor
 - 8) Mendapat layanan penasehat hukum
 - 9) Menggunakan upaya hukum(rechtmiddelen)
- b. Kewajiban Korban
- 1) Korban yang melakukan pembalasan dendam, orang lain (hakim sendiri)
 - 2) Mencegah bertambahnya korban dengan bergabung di masyarakat
 - 3) Mencegah korban dihancurkan oleh dirinya sendiri atau orang lain.
 - 4) Berpartisipasi dalam pembinaan pembuat korban.
 - 5) Mempersiapkan diri menjadi mandiri / dituntun agar tidak menjadi sasaran.
 - 6) Restitusi yang tidak sesuai dengan kesanggupan pembuat korban tidak dituntut oleh korban atau menjadi korban kejahatan
 - 7) Pembuat korban membayarkan restitusi korban diberikan kesempatan mencicil bertahap atau imbalan jasa atau sesuai dengan kemampuannya.

Mendapat jaminan dan tidak membahayakan diri sendiri apabila menjadi saksi. Dalam hal ini peran korban perlu dipertanyakan agar aspek pengukuran kesalahan pelaku benar- benar sesuai dengan tingkat kesalahan yang dilakukannya. Hal ini untuk memastikan bahwa pelaku dan korban secara adil bertanggung jawab terhadap terjadinya suatu perbuatan pidana.

Upaya Hukum Yang Dapat Dilakukan Oleh Pihak Yang Mengalami Kerugian Atas Penyalahgunaan Data Pribadi adalah sebagai berikut (Munawaroh, 2022);

1. Melaporkan kepada pihak yang berwajib, Pasal 24 KUHAP menyebutkan laporan adalah pemberitahuan yang disampaikan oleh seseorang karena hak atau kewajiban berdasarkan Undang-Undang kepada pejabat yang berwenang tentang telah atau sedang atau diduga akan terjadinya peristiwa pidana. Dari pengertian tersebut, peristiwa yang dilaporkan belum tentu perbuatan pidana, sehingga perlu dilakukan penyelidikan oleh pejabat yang berwenang terlebih dahulu untuk menentukan perbuatan itu merupakan tindak pidana atau bukan. Kita sebagai orang yang melihat suatu tindak kejahatan memiliki kewajiban untuk melaporkan perbuatan tersebut.
2. Mengumpulkan bukti yang kongkrit sehingga dapat membantu mempermudah proses penyidikan aparat penegak hukum, Bukti Elektronik ialah Informasi Elektronik dan/atau Dokumen Elektronik yang memenuhi persyaratan formil dan persyaratan materil yang diatur dalam Undang-Undang Informasi dan Telekomunikasi Elektronik. Hal mana dapat dijumpai dalam Pasal 5 ayat (1) Undang-Undang Informasi dan Telekomunikasi Elektronik (ITE) mengatur bahwa Informasi Elektronik dan/atau Dokumen Elektronik dan/ atau hasil cetaknya merupakan alat bukti hukum yang sah. Dengan demikian jelas bahwa macam- macam alat bukti yang diatur di dalam lapangan hukum acara pidana mengalami penambahan atau perluasan yang semula dokumen elektronik merupakan “barang bukti” jika ditemukan di tempat kejadian perkara, maka mengalami *up grading* menjadi alat bukti yang sebelumnya tidak diatur di dalam Pasal 184 KUHAP.
3. Mengajukan kompensasi dan restitusi jika perlu, Proses penegakan hukum melalui peradilan pidana tidak hanya terfokus dalam pemberian sanksi pidana terhadap pelaku. Selain pemberian sanksi pidana pelaku, peradilan pidana juga mengakomodasi kepentingan dan hak korban,

melalui pemberian ganti rugi korban. Dalam hukum acara pidana, ganti kerugian terhadap korban terbagi menjadi 2 (dua) jenis, yakni restitusi dan kompensasi.

4. Meningkatkan keamanan(*security*) dalam alat alat elektronik dan yang berhubungan dengan data pribadi.

Prinsip hak privasi terhadap data pribadi merupakan aspek kritis dalam era digital yang semakin maju ini. Setiap harinya, kita berinteraksi dengan teknologi dan memberikan data pribadi secara online. Data pribadi merujuk pada informasi apa pun yang dapat mengidentifikasi secara langsung atau tidak langsung seseorang. Ini termasuk, namun tidak terbatas pada, nama, alamat, nomor telepon, alamat email, tanggal lahir, nomor identifikasi, data keuangan, dan informasi medis. Namun, dengan memberikan informasi ini, kita juga membuka peluang bagi potensi penyalahgunaan data dan pelanggaran privasi. Hak privasi terhadap data pribadi mencakup hak setiap individu untuk mengetahui apa yang terjadi dengan data pribadi mereka, siapa yang mengaksesnya, untuk tujuan apa data tersebut digunakan, dan bagaimana data tersebut diolah dan disimpan

2. Faktor Faktor Yang Menyebabkan Terjadinya Kejahatan Penyalah Gunaaan Data Pribadi

Tindakan yang melanggar hukum dan norma sosial serta perilaku memalukan adalah perbuatan yang tidak dapat diterima oleh masyarakat. Kejahatan seringkali dipicu oleh berbagai faktor, seperti faktor ekonomi (pengangguran), faktor psikis atau fisik, faktor pribadi, sosial, dan faktor lainnya yang beragam. Kejahatan dan perilaku yang tidak pantas melanggar hukum dan norma sosial. Tindak pidana dan kejahatan dapat memakan korban jiwa warga negara Indonesia yang sangat besar dan menimbulkan ketakutan, teror, terror dan kepanikan di kalangan warga negara Indonesia. Kenaikan kejahatan dan perubahan global, terutama kenaikan kejahatan online, sangat memprihatinkan. Penegakan hukum menjadi kunci dalam melawan kejahatan online, sehingga badan penegak hukum harus bekerja dengan keras. Lima faktor yang harus diperhatikan adalah aspek hukum, budaya, kelembagaan, perilaku

manusia dan pemikiran hukum. Informasi pribadi dan data tidak berwujud sering diabaikan, terutama dalam kehidupan sosial. Individu-individu rentan karena mereka tak harus berbagi di dunia maya untuk menjaga kerahasiaan data pribadi mereka serta mencegah orang lain mengganggunya.

Langkah Mengamanan Meningkatkan Keamanan Data Pribadi

Teknologi Big Data bukanlah pengganti teknologi saat ini; mereka adalah pelengkap. Big Data harus diintegrasikan dengan infrastruktur perusahaan lainnya. Selain solusi terkini untuk analisis big data, ada beberapa tantangan baru, misalnya kebutuhan akan metode statistik yang kuat dan pengelolaan data yang hilang (Dimas Prayoga, 2022). *Cloud computing* memberikan kemampuan baru untuk melakukan analisis di semua data dalam suatu organisasi. Ini menggunakan pendekatan teknis baru untuk menyimpan, mencari, menambang, dan mendistribusikan data dalam jumlah besar. Masalah seperti pemrosesan gambar skala besar, korelasi data sensor, analisis jaringan sosial, *enkripsi/dekripsi*, penambangan data, simulasi, dan pengenalan pola dapat diselesaikan di *domain cloud computing*.

Untuk perkembangan konvergensi jaringan dan internet plus, informatisasi sosial telah merambah ke segala bidang dan masalah keamanan informasi lebih menonjol dari sebelumnya. Menghadapi ancaman dan tantangan keamanan informasi di era big data, pemerintah dan perusahaan harus berbuat lebih banyak dan solusi termasuk membangun platform manajemen keamanan big data, mempercepat pembentukan sistem keamanan informasi dan meningkatkan kesadaran masyarakat. Kerahasiaan, integritas, dan ketersediaan dalam urutan itu sebagai masalah keamanan terpenting yang dihadapi penyedia *cloud*.

Kerahasiaan dalam skenario ini berarti perlindungan data terhadap gangguan atau penggunaan yang tidak sah. Integritas akan menjadi pencegahan modifikasi data yang tidak sah dan tidak tepat. Ketersediaan akan mirip dengan pemulihan data dari kesalahan perangkat keras, perangkat lunak dan sistem, dan juga dari penolakan akses data. Namun, kerahasiaan adalah aspek terpenting dalam perlindungan big data. Beberapa Teknik kerahasiaan data ada dengan yang paling menonjol adalah kontrol akses dan *enkripsi*. *Enkripsi* dan *access control* serupa

dalam arti keduanya identik dengan privasi dan pencegahan. Namun perbedaan penting adalah bahwa, *enkripsi* biasanya berkaitan dengan kerahasiaan data. Data dapat tersedia untuk entitas terpercaya atau tidak terpercaya.

Enkripsi memastikan bahwa hanya entitas terpercaya yang berwenang yang dapat melihat data. Namun *access control* mencoba membatasi akses ke data. Keterbatasan data biasanya terjadi pada pihak-pihak yang terpercaya. Untuk alasan ini, teknik enkripsi harus lebih kuat daripada teknik *access control*. *Enkripsi* memberlakukan batasan yang sangat kuat atas kerahasiaan data. Big data memiliki kompleksitas yang sebagian besar orang dan perusahaan tidak siap. Kompleksitas ini mencakup keamanan dan tata kelola data secara umum.

Tata kelola informasi adalah menciptakan sumber informasi yang dapat dipercaya oleh karyawan, mitra, dan pelanggan, serta organisasi pemerintah. Selain enkripsi, beberapa teknik pengamanan data yang disarankan adalah:

- 1) *Data Anonymization* proses menghapus semua data pada seorang individu,
- 2) *Tokenization* melindungi data sensitif dengan mengganti token/ nilai yang tidak berarti bagi orang yang tidak berwenang.
- 3) *Cloud Database Controls* yaitu menyiapkan kontrol akses ke yang lebih besar, dan metodologi harus diubah. Masalah keamanan big data diperbesar dengan kecepatan, volume, dan variasi big data. Pemrosesan big data membutuhkan waktu respons yang sangat cepat untuk komputasi, dan menambahkan beberapa fitur kerangka menambah implikasi keamanan. Namun, masalah keamanan ini dapat ditangani dengan mengambil langkah-langkah memadai yang tepat. Lima rekomendasi terbaik untuk keamanan big data telah dibahas dibawah ini:
 - a. Melakukan Pengamanan Kode Komputasi Untuk mencegah data berbahaya memasuki solusi big data, maka dapat diterapkan kontrol akses, penandatanganan kode, dan analisis dinamis kode komputasi. Strategi yang tepat perlu dibuat dengan kemampuan mengendalikan dampak kode yang tidak dipercaya pada data, setelah dapat masuk ke solusi bigdata.

- b. Menerapkan Validasi Penyaringan Input Menyeluruh. Untuk pemrosesan dan keamanan lebih baik, penerapan validasi dan penyaringan input yang komprehensif di hampir semua sumber internal dan eksternal adalah wajib.
- c. Menerapkan *Access Control Granular*. Meninjau matriks peran dan hak istimewa dari berbagai jenis pengguna data besar yang dapat berupa admin, pekerja pengetahuan, pengguna akhir, pengembang, dan lain-lain adalah bagian inti untuk penerapan kontrol akses *granular*.
- d. Mengamankan Penyimpanan, Perhitungan data Melindungi penyimpanan data dan bagian komputasi dari analitik data besar menjadi area utama untuk difokuskan pada banyak bagian dari bagian kebocoran data sensitif yang ditemui dalam fase ini. Untuk ini, data sensitif harus dipisahkan.
- e. Meninjau dan Menerapkan Privasi, Pemeliharaan Data *Mining* dan Analisis. Untuk pelestarian informasi sensitif yang tepat, verifikasi algoritma analitik yang dirancang untuk penambangan data, klasifikasi pola, dan pengenalan diperlukan.

KESIMPULAN

Bentuk perlindungan hukum terhadap data pribadi dari penyalahgunaan orang lain adalah Perlindungan hukum preventif Perlindungan ini adalah suatu upaya dari pemerintah dalam rangka pencegahan terjadinya suatu pelanggaran, Perlindungan ini biasanya dapat dijumpai dalam suatu bentuk peraturan perundang-undangan, selain perlindungan berupa hak terdapat juga pedoman untuk melakukan suatu kewajiban dalam bentuk Batasan-batasan. Perlindungan hukum represif Bentuk perlindungan represif ini adalah berupa denda, sanksi, dan penjara, Hal ini merupakan suatu wujud nyata dari adanya suatu aturan dan perundangundangan, siapa pun yang telah melanggar akan mendapatkan ganjaran atas perbuatannya. Upaya hukum yang dapat dilakukan oleh pihak yang mengalami kerugian atas penyalahgunaan data pribadi adalah Melaporkan kepada pihak yang berwajib Pasal 24 KUHAP menyebutkan laporan adalah pemberitahuan yang disampaikan oleh seseorang karena hak atau kewajiban berdasarkan Undang-Undang kepada pejabat yang berwenang tentang telah atau sedang atau diduga akan terjadinya peristiwa pidana. Kedua mengumpulkan bukti bukti yang kongkrit

sehingga dapat membantu mempermudah proses penyidikan aparat penegak hukum Bukti Elektronik ialah Informasi Elektronik dan/atau Dokumen Elektronik yang memenuhi persyaratan formil dan persyaratan materil yang diatur dalam Undang-Undang Informasi dan Telekomunikasi Elektronik.

DAFTAR PUSTAKA

- Alvian Dwiangga Wijaya, T. P. (2022). Perlindungan Hukum Terhadap Data Pribadi Dalam Penggunaan Aplikasi di Smartpone. *Jurnal Inicio Legis Universitas Trunojoyo Madura* , 63-72.
- Basyari, I. (2023, juli). Diambil kembali dari kompas: <https://www.kompas.id/baca/polhuk/2023/07/17/337-juta-data-dukcapil-diduga-bocor>
- Diah Puspitasari, I. K. (2023). Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Mengatasi Masalah Keamanan Data Penduduk. *Journal of Administrative and Sosial Science (JASS)*, 195-205 .
- Dimas Prayoga. (2022). Risiko Keamanan Data Pribadi Pelanggan Dalam Penggunaan Big Data. *Jurnal Nasional Komputasi dan Teknologi Informasi*, 459-463.
- Firdaus, I. (2022). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan . *Jurnal Rechten*, 23-31.
- Munawaroh, N. (2022, 12). Diambil kembali dari Hukum Online: <https://www.hukumonline.com/klinik/a/mau-melaporkan-tindak-pidana-ke-polisi-begini-prosedurnya-lt504d52481c208/>
- Pramono, B. (2020). *Sosiologi Hukum*. Surabaya: Scopindo Media.
- Rizky P.P. Karo Karo, T. P. (2020). *Pengaturan Perlindungan Data Pribadi Di Indonesia Perspektif Teori KEadilan Bermartabat*. Bandung: Nusa Media.