

Penegakan Hukum terhadap Pelaku Penyalahgunaan Penyebaran Data Pribadi Melalui *Barcode* Ditinjau dari UU ITE dan UU Nomor 27 Tahun 2022 Tentang (UU PDP)

Kadek Reza Ayuning Pranindya

Universitas Pendidikan Ganesha Singaraja, Indonesia

Jl. Udayana No. 11, Banjar Tegal, Singaraja, Kabupaten Buleleng, Bali 81116

Email : reza.ayuning@student.undiksha.ac.id

Abstract. *Personal data dissemination is a new type of crime that has emerged in the digital world. The rapid development of technology has led to various innovations in data storage, one of which is through barcode technology. Although it provides convenience, this technology also opens up new gaps in cybercrime, especially the misuse and dissemination of personal data stored in barcodes. The impacts of the spread of personal data include damage to personal reputation due to the widespread dissemination of personal data on the internet, the emergence of cyber bullying and sexual harassment, personal data that has the potential to be sold, and the distress and psychological trauma experienced by victims of personal data dissemination. The purpose of this study is to analyze how law enforcement against perpetrators of abuse of the spread of personal data stored in barcodes is reviewed from the ITE Law and the PDP Law, and identify preventive efforts that can be made to prevent these crimes. This research uses a normative juridical approach method used to examine applicable legal norms related to personal data protection. With a statute approach, books, scientific journals, and the internet. The results showed that, although the ITE Law does not specifically regulate barcode technology, the protection of personal data stored in barcodes is still subject to the provisions of the ITE Law and Law Number 27 of 2022 concerning Personal Data Protection.*

Keywords: *Law Enforcement, Dissemination of Personal data, Barcode, ITE Law, PDP Law*

Abstrak. Penyebaran data pribadi adalah jenis kejahatan baru yang muncul di dunia digital. Perkembangan teknologi yang pesat telah memunculkan berbagai inovasi dalam penyimpanan data, salah satunya melalui teknologi *barcode*. Meskipun memberikan kemudahan, teknologi ini juga membuka celah baru dalam kejahatan siber, khususnya penyalahgunaan dan penyebaran data pribadi yang tersimpan dalam *barcode*. Dampak dari penyebaran data pribadi ini antara lain: rusaknya reputasi pribadi karena penyebaran data pribadi yang meluas di internet, munculnya perundungan siber dan pelecehan seksual, data pribadi yang berpotensi dijual, dan tertekannya serta trauma psikologis yang dialami oleh korban penyebaran data pribadi. Tujuan dari penelitian ini untuk menganalisis bagaimana penegakan hukum terhadap pelaku penyalahgunaan penyebaran data pribadi yang tersimpan dalam *barcode* ditinjau dari UU ITE dan UU PDP, serta mengidentifikasi upaya preventif yang dapat dilakukan untuk mencegah kejahatan tersebut. Penelitian ini menggunakan metode pendekatan yuridis normatif digunakan untuk meneliti norma-norma hukum yang berlaku terkait perlindungan data pribadi. Dengan pendekatan Perundang-undangan (Statute Approach), buku-buku, jurnal karya ilmiah, dan internet. Hasil penelitian menunjukkan bahwa, Meskipun UU ITE tidak secara spesifik mengatur tentang teknologi *barcode*, perlindungan data pribadi yang tersimpan dalam *barcode* tetap tunduk pada ketentuan UU ITE dan UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Kata kunci: Penegakan Hukum, Penyebaran data Pribadi, *Barcode*, UU ITE, UU PDP

1. LATAR BELAKANG

Saat ini teknologi dan sistem informasi mengalami perkembangan yang sangat pesat. Dengan adanya kemajuan seperti ini tentu akan memberikan sebuah perubahan yang merubah berbagai tananan masyarakat dalam menjalani aktivitas yang terdiri dari beberapa kebutuhan dimana dalam hal ini kebutuhan informasi yang sangat dibutuhkan oleh masyarakat dengan perkmbangan zaman yang ada, apalagi informasi yang

dihasilkan mengandung nilai yang berguna, benar, akurat, cepat dan tepat, sehingga siapapun yang menggunakan informasi tersebut dapat menangani berbagai masalah yang terjadi. Seperti halnya *barcode* yang sudah beredar di kemasan pembelian, barang, ataupun data-data informasi pribadi yang diinputkan di dalam *barcode*. Dengan menggunakan *barcode* dapat membantu untuk menyimpan informasi pribadi atau *Id card* yang digunakan oleh anggota organisasi maupun karyawan di sebuah instansi (Saepulloh & Adeyadi, 2019). Namun seiring dengan perkembangan teknologi dan sistem informasi yang semakin canggih, hal ini juga menyebabkan semakin mudahnya seseorang didalam melakukan suatu perbuatan kejahatan yang ada di dalam pikirannya tanpa harus memikirkan adanya suatu dampak dan konsekuensi yang akan di dapatkan. Sehingga tidak menutup kemungkinan mengakibatkan terjadinya perbuatan-perbuatan yang melanggar hukum (Dade, Waha, & Nachrawy, 2024).

Di era digital yang terus berkembang dengan pesat, data pribadi telah menjadi aset yang sangat berharga. Informasi pribadi seperti nama, alamat, nomor telepon, dan preferensi pribadi kita kini dikumpulkan, dimanfaatkan, disalahgunakan, dan diperdagangkan oleh berbagai entitas, mulai dari perusahaan teknologi besar, lembaga keuangan hingga aplikasi yang ada di ponsel (Gunadi, Subrian, Lee, Gunawan, & Baretta, 2023). Setiap proses pelayanan publik, masyarakat juga diwajibkan untuk mengisi data pribadi di formulir pendaftaran, baik pendaftaran secara manual maupun online, serta menggunakan *barcode*. Pelayanan secara online maupun menggunakan *barcode* memberikan adanya suatu manfaat yang besar karena mempercepat dalam suatu proses dalam setiap kegiatan yang ingin dilakukan dimanapun. Namun disisi lain, memberikan data pribadi melalui jaringan online maupun scan *barcode* sangat rawan terhadap keamanan data pribadi. Dengan memberikan data pribadi tersebut sangat mungkin terjadi penyalahgunaan data pribadi oleh pihak-pihak yang tidak bertanggung jawab sehingga merugikan bagi pemilik data pribadi tersebut (Permadi & Rokhman, 2023). Data pribadi, menurut Undang-Undang Nomor 24 Tahun 2013 tentang perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, selanjutnya disingkat UU Adminduk, adalah data diri seseorang yang harus disimpan, dirawat, dan dijaga kebenarannya serta dilindungi kerahasiaan identifikasi yang nyata dan dapat diidentifikasi secara langsung maupun tidak langsung sesuai dengan peraturan perundang-undangan.

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) tidak secara khusus mengatur tentang teknologi *barcode* secara langsung. UU ITE lebih fokus pada pengaturan transaksi elektronik, perlindungan data pribadi, keamanan informasi, dan tata

kelola sistem informasi elektronik di Indonesia. Namun, jika data pribadi diproses dan disimpan menggunakan kode batang (*barcode*), peraturan mengenai perlindungan data pribadi dari akses yang tidak sah, penyalahgunaan, atau penyebaran yang tidak sah sesuai dengan standar dan prosedur yang ditetapkan maka dalam konteks pengolahan dan penyimpanan data pribadi tetap tunduk pada ketentuan-ketentuan perlindungan data pribadi. Dalam hal prakteknya, penggunaan *barcode* sebagai media penyimpanan informasi pribadi harus memperhatikan kepatuhan terhadap prinsip-prinsip perlindungan data yang diatur dalam UU ITE. Hal ini termasuk ke dalam langkah-langkah untuk memastikan keamanan data, pengelolaan akses yang tepat, dan respons yang tepat dalam menghadapi pelanggaran data pribadi yang melibatkan teknologi *barcode*. Data pribadi adalah informasi yang dapat mengidentifikasi seseorang, seperti nama, alamat, nomor telepon, informasi keuangan, dan lain sebagainya. Menurut Pasal 1 Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi “data pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non-elektronik (Ilham & Akbar, 2024).

Identifikasi data dalam sistem elektronik mengacu pada proses pengenalan dan pengklasifikasian data yang disimpan dan diproses dalam sistem elektronik. Menurut Bambang Riyanto, Identifikasi data adalah langkah awal yang penting dalam manajemen data, karena menentukan bagaimana data tersebut akan diproses, disimpan, dan dilindungi. Proses ini mencakup pengumpulan metadata, pemberian label, dan pengkategorian data berdasarkan karakter. Identifikasi data juga harus mempertimbangkan aspek perlindungan data pribadi. Menurut GDPR (Peraturan Perlindungan Data Umum), setiap proses pengumpulan dan pengelolaan data harus memastikan bahwa data pribadi dilindungi dari akses yang tidak sah. Menurut Paul Lambert dalam *Understanding the New European Data Protection Rules*, identifikasi data harus disertai dengan langkah-langkah perlindungan yang ketat untuk mematuhi peraturan internasional mengenai privasi data. Identifikasi data dalam sistem elektronik adalah proses yang penting untuk memastikan keamanan dan integritas informasi (Lambert, 2017). Pendapat para ahli menunjukkan bahwa metode seperti metadata, pelabelan, dan pengindeksan adalah penting untuk pengelolaan data yang efektif. Namun, tantangan seperti volume data yang besar dan perlindungan data pribadi harus diatasi dengan pendekatan yang tepat. Dengan identifikasi data yang baik, organisasi dapat mengelola data mereka dengan lebih efisien dan aman.

Kode Batang (*Barcode*) adalah representasi data yang dapat dibaca oleh mesin, yang berfungsi untuk menyimpan informasi dalam bentuk visual yang dapat di-scan. *Barcode* telah menjadi komponen integral dalam berbagai industri, termasuk ritel, kesehatan, dan logistik. *Barcode* adalah pola garis dan ruang yang menyimpan data yang dapat dibaca oleh perangkat optik. Menurut Roger C. Palmer dalam bukunya *The Bar Code Book: A Comprehensive Guide to Reading, Printing, Specifying, Evaluating and Using Bar Code and Other Machine-Readable Symbols*, barcode adalah metode pengkodean data numerik atau alfanumerik dalam bentuk garis dan spasi yang bervariasi lebar dan panjangnya. Keamanan data yang disimpan dalam *barcode* adalah aspek penting yang sering diabaikan (Palmer, 2007). Para ahli menekankan perlunya langkah-langkah keamanan untuk melindungi informasi yang tersimpan dalam *barcode* antara lain: Keamanan data yang disimpan dalam *barcode* adalah aspek penting yang sering diabaikan. Para ahli menekankan perlunya langkah-langkah keamanan untuk melindungi informasi yang tersimpan dalam *barcode* antara lain:

Pertama, Enkripsi Data, salah satu cara untuk melindungi data dalam barcode adalah dengan enkripsi. Menurut Bruce Schneier dalam *Applied Cryptography*, enkripsi dapat memastikan bahwa data dalam barcode hanya dapat dibaca oleh perangkat yang berwenang. Kedua, Kontrol Akses, dengan mengontrol bisa mengetahui siapa yang dapat mengakses data dalam barcode juga penting. Michael E. Whitman dan Herbert J. Mattord dalam *Principles of Information Security* menyarankan penerapan kebijakan akses yang ketat untuk memastikan bahwa hanya pengguna berwenang yang dapat memindai dan memproses data dalam *barcode*. Ketiga, Audit dan Monitoring, menerapkan sistem audit dan monitoring secara berkala dapat membantu mendeteksi dan mencegah penyalahgunaan data. Menurut Richard E. Cascarino dalam *Auditor's Guide to IT Auditing*, “audit berkala memungkinkan organisasi untuk memverifikasi integritas dan keamanan data yang disimpan dalam barcode”.

Dalam Penggunaan *barcode* juga kita dapat menghadapi beberapa tantangan. Salah satunya adalah kerusakan fisik pada barcode yang dapat menyebabkan kesulitan dalam pemindaian. Selain itu, ada risiko bahwa data dalam *barcode* dapat diakses oleh pihak yang tidak berwenang jika langkah-langkah keamanan tidak diterapkan dengan benar. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008 yang telah diubah dengan UU No. 19 Tahun 2016 mengatur tentang penggunaan teknologi informasi dan transaksi elektronik di Indonesia. Dan Undang-Undang ITE terbaru adalah UU No. 1 Tahun 2024 tentang Perubahan Kedua Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. UU ITE mengatur berbagai aspek

hukum terkait informasi dan transaksi elektronik, termasuk perlindungan data pribadi. Dan Undang-Undang No. 27 tentang Perlindungan Data Pribadi yang memang sudah disahkan pada tahun 2022 lalu.

Perumusan Masalah

Dari pendahuluan yang telah diuraikan diatas, maka penulis merumuskan beberapa permasalahan sebagai berikut:

- Bagaimana peran aparat hukum saat ini dalam mengatur perlindungan data pribadi yang di simpan dalam *barcode*?
- Bagaimana pertanggungjawaban hukum bagi pelaku penyebaran data pribadi yang tersimpan pada *barcode* ditinjau dari UU ITE dan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi?

2. METODE PENELITIAN

Penelitian ini menggunakan metode pendekatan yuridis normatif digunakan untuk meneliti norma-norma hukum yang berlaku terkait perlindungan data pribadi dan pertanggungjawaban pelaku penyebarluasan data pribadi (Sahir, 2021). Dengan pendekatan Perundang-undangan (Statute Approach), buku-buku, jurnal karya ilmiah, dan internet. Cara mengumpulkan data dengan menggunakan metode studi pustaka (*library research*) (Diantha, 2016). Sumber data yang digunakan di dalam penelitian menggunakan data sekunder yang berasal dari menganalisis undang-undang terkait, seperti UU ITE, Undang-Undang No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi, dan peraturan terkait lainnya.

3. HASIL DAN PEMBAHASAN

Peran Aparat Hukum dalam Mengatur Perlindungan Data Pribadi Yang di Simpan Dalam *Barcode*

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi menjelaskan pengertian Perlindungan Data Pribadi adalah keseluruhan upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak konstitusional subjek data pribadi (Rosadi, 2023). Menurut Pasal 4, terdapat 2 jenis Data Pribadi yang terdiri atas, Pertama Data Pribadi yang bersifat spesifik, seperti data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi, dan data lainnya sesuai dengan ketentuan peraturan perundang-undangan. Lalu, yang Kedua yaitu Data Pribadi yang bersifat umum

seperti, nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang.

Data pribadi dapat didefinisikan sebagai informasi yang dapat mengidentifikasi individu, sedangkan *barcode* merupakan metode identifikasi yang menggunakan serangkaian garis paralel dan ruang yang berbeda dipindai untuk mendapatkan informasi. Hukum perlindungan data pribadi mengatur cara pengumpulan, penggunaan, dan pencurian data pribadi untuk memastikan privasi individu terlindungi. Dalam Undang-Undang Perlindungan Data Pribadi (UU PDP), disebutkan bahwa adanya suatu larangan dalam penggunaan Data Pribadi milik orang lain yang di jelaskan dalam Pasal 65 dan Pasal 67 ayat 1, 2, dan 3 bahwa:

- Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).
- Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).
- Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

Beberapa solusi diberikan pada UU PDP seperti pada pasal 16, dengan adanya pemrosesan Data Pribadi maka akan melindungi keamanan Data Pribadi dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, pengubahan yang tidak sah, kerusakan, dan penghilangan Data Pribadi. Pemrosesan Data Pribadi juga dilakukan dengan memberitahukan tujuan dan aktivitas pemrosesan, serta kegagalan perlindungan Data Pribadi. UU ini juga menyebutkan bahwa pemerintah berperan dalam penyelenggaraan perlindungan Data Pribadi sesuai dengan pasal 58 ayat (1). Negara juga harus membuat suatu lembaga seperti yang disebutkan juga pada pasal 58 ayat (2), yaitu “Penyelenggaraan Perlindungan Data Pribadi sebagaimana dimaksud pada ayat (1) dilaksanakan oleh lembaga”. Dengan begitu perlindungan Data pribadi dilaksanakan dengan teratur. Lembaga juga mengatur jika terjadi adanya pelaporan perlindungan Data

Pribadi sesuai pasal 60, lembaga bisa melakukan pengaduan, laporan, dan hasil pengawasan terhadap dugaan terjadinya pelanggaran perlindungan Data Pribadi.

Adapun beberapa langkah-langkah yang dapat diambil untuk melindungi data pribadi yang tersimpan pada *barcode* antara lain:

- Enkripsi Data

Data yang tersimpan dalam *barcode* harus dienkripsi untuk mencegah akses tidak sah. Enkripsi memastikan bahwa data hanya dapat dibaca oleh pihak yang berwenang.

- Persetujuan Tertulis

Sebelum menyimpan data pribadi dalam *barcode*, persetujuan tertulis dari pemilik data harus diperoleh. Persetujuan ini harus mencakup penjelasan tentang tujuan penyimpanan dan penggunaan data.

- Audit Keamanan Berkala

Perusahaan yang menggunakan *barcode* untuk menyimpan data pribadi harus melakukan audit keamanan secara berkala. Audit ini memastikan bahwa sistem keamanan selalu diperbarui dan dapat mengatasi ancaman baru.

Disini peran aparat penegak hukum sangat diperlukan, karena aparat penegak hukum memegang peranan penting dalam penegakan hukum terkait dengan perlindungan data pribadi. Mereka bertanggung jawab untuk menyelidiki dan menindak kejahatan terkait dengan penyebaran data pribadi yang disimpan dalam *barcode*. Aparat penegak hukum harus memiliki pemahaman mendalam tentang teknologi dan metode yang digunakan untuk menyimpan dan mengakses data pribadi dalam *barcode*, serta cara-cara kejahatan dapat terjadi dalam konteks ini. Hal ini mencakup kemampuan untuk melakukan analisis forensik dan mengumpulkan bukti yang kuat untuk mendukung prosa. Proses hukum untuk membuktikan kejahatan terhadap penyebaran data pribadi dalam *barcode* melibatkan pengumpulan bukti yang kuat dan penggunaan teknik investigasi yang canggih. Pakar hukum digital, *Smith*, menjelaskan bahwa pengumpulan bukti dalam kasus kejahatan siber memerlukan pendekatan yang sangat cermat dan terstruktur untuk memastikan validitas dan integritas bukti tersebut. Hal ini mencakup analisis forensik digital, yang memungkinkan aparat penegak hukum untuk melacak jejak digital yang ditinggalkan oleh pelaku kejahatan. Dengan menggunakan adanya teknik investigasi canggih dan kolaborasi dengan lembaga pengawasan data, aparat hukum dapat menangkap pelaku kejahatan yang mencoba memanfaatkan teknologi untuk keuntungan pribadi. Perlindungan data pribadi tidak hanya menjadi tanggung jawab hukum, tetapi juga penting untuk melindungi hak privasi individu dan memastikan bahwa keadilan ditegakkan dalam kasus-kasus penyalahgunaan data.

Pertanggungjawaban Hukum bagi Pelaku Penyebaran Data Pribadi yang Tersimpan Pada Barcode ditinjau Dari UU ITE dan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi

Kasus atau Tindakan Penyebaran data pribadi yang tersimpan pada *barcode* merupakan bentuk Kejahatan dan bentuk pelanggaran serius terhadap hak privasi individu yang dilindungi oleh hukum di Indonesia. UU ITE dan UU No. 27 Tahun 2022 memberikan suatu landasan hukum yang jelas, tidak hanya dalam pengaturan perlindungan data pribadi tetapi juga dalam memberikan sanksi kepada pelaku yang melanggar hukum. UU ITE, meskipun tidak secara spesifik mengatur mengenai penyimpanan data dalam *barcode*, tetapi UU ini memberikan perlindungan terhadap data pribadi yang terekam atau tersimpan secara elektronik. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) merupakan payung hukum utama yang mengatur perlindungan data pribadi di Indonesia. UU ini mengatur kewajiban bagi pemegang data untuk melindungi informasi pribadi dari pihak ketiga. Disini menurut Yulianto UU ITE memberikan adanya suatu landasan yang kuat dalam menjaga privasi data pribadi di Indonesia. Yulianto menjelaskan bahwa UU ITE mengharuskan setiap pemegang data untuk mengambil langkah-langkah yang wajar untuk melindungi informasi pribadi dari akses yang tidak sah atau penyalahgunaan (Yuliyanto, 2021). Hal ini mencerminkan komitmen legislatif untuk memberikan perlindungan yang memadai terhadap data pribadi dalam konteks teknologi informasi yang terus berkembang.

Menurut UU ITE, hak privasi individu dijamin dengan memperkuat kontrol terhadap penggunaan dan penyebaran informasi pribadi dalam konteks transaksi elektronik. Hal ini menunjukkan komitmen undang-undang dalam melindungi kepentingan privasi individu dalam era digital yang terus berkembang. Regulasi ini tidak hanya mengatur teknisitas perlindungan data, tetapi juga memberikan landasan hukum yang kuat bagi penegakan hak-hak individu terhadap data pribadi mereka, dengan mengatur batasan-batasan yang jelas terhadap cara informasi pribadi dapat diakses, digunakan, dan disebarluaskan. Dengan demikian, UU ITE berperan penting dalam membangun kepercayaan masyarakat terhadap penggunaan teknologi informasi yang aman dan bertanggung jawab.

Dalam UU ITE, penyebaran data pribadi yang dilakukan tanpa adanya persetujuan dari pemiliknya merupakan pelanggaran yang serius sebagaimana di atur dalam Pasal 26 ayat (1) yang menyatakan bahwa “ Penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan”. Ketentuan ini memberikan perlindungan hukum kepada pemilik data agar

data pribadi mereka tidak dapat digunakan atau disebarluaskan tanpa izin. Apabila data pribadi yang tersimpan dalam *barcode* diakses tanpa otoritas, pelaku dapat dikenakan sanksi sesuai dengan pasal 30 ayat (1) UU ITE, yang melarang akses ilegal terhadap sistem elektronik milik pihak lain. Dalam konteks penyebaran data pribadi, jika perbuatan tersebut dilakukan dengan sengaja dan melanggar hukum, pelaku dapat dijerat dengan Pasal 36 yang mengatur tentang perbuatan melawan hukum yang menyebabkan kerugian. Pelaku yang terbukti bersalah dapat dikenakan sanksi pidana sebagaimana tercantum dalam Pasal 48 menyatakan bahwa:

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).
- (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).
- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

Sementara itu, UU Perlindungan Data Pribadi (UU PDP) memberikan landasan hukum yang lebih rinci dan spesifik terkait dengan pelanggaran terhadap data pribadi termasuk data yang tersimpan pada *barcode*. Konsep perlindungan data pada dasarnya merupakan bagian dari perlindungan privasi sehingga entitas yang dilindungi dalam mekanisme perlindungan data privasi adalah “orang perseorangan” yang pada dirinya melakat data pribadi (Rosadi, 2022). Secara eksplisit, bentuk perlindungan dan pertanggungjawaban data pribadi yang tersimpan pada *barcode* dalam UU PDP adalah pengakuan terhadap hak-hak yang dimiliki oleh subjek dan data pribadi yaitu untuk:

- Mendapatkan kejelasan informasi tentang siapa, mengapa dan bagaimana data pribadi tersebut akan digunakan, meliputi kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan data pribadi, serta akuntabilitas pihak yang meminta;
- Melengkapi data pribadi termasuk memperbarui dan memperbaiki kesalahan atau ketidakakuratan data pribadi;
- Mengakses dan memperoleh salinan data pribadi;
- Mengakhiri pemrosesan, menghapus, dan memusnahkan data pribadi miliknya;
- Menarik kembali persetujuan pemrosesan;

- Mengajukan keberatan atas tindakan profiling yang menjadi dasar pengambilan keputusan yang berdampak hukum;
- Menunda atau membatasi pemrosesan;
- Menuntut dan menerima ganti rugi atas pelanggaran; serta
- Mendapatkan, menggunakan, dan mengirimkan data pribadi dalam bentuk yang dapat dibaca oleh sistem elektronik.

Dalam Undang-Undang Perlindungan Data Pribadi (UU PDP), telah disebutkan bahwa adanya suatu larangan dalam penggunaan Data Pribadi milik orang lain yang di jelaskan dalam Pasal 65 bahwa:

- Setiap Orang dilarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi.
- Setiap Orang dilarang secara melawan hukum mengungkapkan Data Pribadi yang bukan miliknya.
- Setiap Orang dilarang secara melawan hukum menggunakan Data Pribadi yang bukan miliknya.

Selain itu, UU PDP juga memberikan perhatian besar terhadap perlindungan dan pengelolaan data pribadi. Pasal 16 mengatur bahwa setiap pengolahan data pribadi harus dilakukan dengan langkah-langkah yang memastikan keamanan data dari akses tidak sah, pengubahan tanpa izin, pengungkapan, atau kerusakan data yang melanggar hukum. Pelaku yang tidak mematuhi prinsip ini, termasuk dalam konteks penyebaran data pribadi melalui *barcode*, dapat dianggap melanggar kewajiban pengelolaan data pribadi yang aman. UU PDP juga memberikan kewenangan kepada pemerintah untuk mengambil langkah pengawasan dan penegakan hukum melalui lembaga yang diamanatkan oleh Pasal 58 dan Pasal 60, yang bertugas menerima laporan, melakukan pengawasan, serta menindak pelanggaran perlindungan data pribadi.

Dalam hal pelaku menyebarkan data pribadi yang tersimpan dalam barcode, tanggung jawab hukum yang dihadapi tidak hanya berupa sanksi pidana dan denda sebagaimana diatur dalam UU ITE dan UU PDP, tetapi juga tanggung jawab moral dan sosial untuk memulihkan hak-hak subjek data. Penyebaran data pribadi ini dapat menyebabkan berbagai kerugian, seperti pencemaran nama baik, penipuan identitas, hingga trauma psikologis bagi korban. Oleh karena itu, kedua undang-undang tersebut dirancang untuk memberikan perlindungan maksimal terhadap data pribadi serta memberikan efek jera kepada pelaku kejahatan.

4. KESIMPULAN

Jadi dapat disimpulkan bahwa, penyebaran data pribadi yang tersimpan dalam *barcode* menjadi ancaman serius di era digital karena perkembangan teknologi informasi yang pesat, di mana *barcode* yang awalnya dimanfaatkan untuk mempermudah penyimpanan data kini rentan terhadap penyalahgunaan oleh pihak tidak bertanggung jawab, sehingga dapat merugikan individu baik secara moral, material, maupun psikologis. Berdasarkan pembahasan, perlindungan data pribadi ini diatur oleh UU ITE dan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang memberikan landasan hukum terhadap penanganan pelanggaran termasuk ancaman pidana bagi pelaku penyebaran data tanpa izin, dengan upaya preventif berupa enkripsi data, kontrol akses, audit keamanan berkala, dan peran aparat penegak hukum yang memiliki kemampuan analisis forensik untuk memastikan keamanan data pribadi serta mencegah potensi kerugian yang lebih besar bagi masyarakat.

5. REKOMENDASI

Adapun saran yang dapat diberikan sebagai rekomendasi yaitu, diperlukan peningkatan kesadaran masyarakat mengenai pentingnya menjaga kerahasiaan data pribadi, terutama yang disimpan dalam teknologi *barcode*, melalui edukasi publik yang berkesinambungan tentang risiko penyalahgunaan data pribadi dan cara melindunginya. Pemerintah juga perlu memperkuat implementasi UU ITE dan UU PDP dengan pengawasan yang ketat serta penegakan hukum yang tegas terhadap pelanggaran, termasuk membentuk lembaga pengawas yang khusus menangani keamanan data pribadi. Selain itu, pihak pengelola data seperti perusahaan atau institusi harus memastikan penerapan langkah-langkah keamanan yang memadai, seperti enkripsi data, pembatasan akses, serta audit keamanan berkala, untuk mencegah akses tidak sah. Terakhir, kolaborasi antara Aparat Penegak Hukum, Pemerintah, Institusi, dan masyarakat diperlukan untuk menciptakan ekosistem digital yang lebih aman dan terpercaya. Apalagi pada kemajuan teknologi ini apapun dapat terjadi walaupun kita sudah berusaha untuk menjaga keamanan dan kerahasiaan dimana hal perlunya peran kita sebagai masyarakat untuk cermat dan berpendidikan Teknologi yang baik guna memahami berbagai situasi dan kondisi janggal dalam penggunaan Teknologi di bidang apapun.

DAFTAR REFERENSI

- Dade, L. L., Waha, C. J., & Nachrawy, N. (2024). Kajian yuridis tentang tindak pidana penyebaran data pribadi melalui internet (doxing) di Indonesia. *Jurnal Fakultas Hukum Universitas Sam Ratulangi*, 13(3), 1–12.
- Diantha, I. M. (2016). *Metodologi penelitian hukum normatif dalam justifikasi teori hukum*. Prenada Media Group.
- Gunadi, C. G., Subrian, D., Lee, E. P., Gunawan, L. A., & Baretta, N. (2023). Perlindungan hukum atas kebocoran data pribadi. *Prosiding Conference on Law and Social Studies*, 1–13.
- Ilham, M., & Akbar, M. (2024). Pertanggungjawaban hukum bagi pelaku penyebaran data pribadi yang tersimpan pada barcode ditinjau dari Undang-Undang Informasi Transaksi Elektronik (UU ITE). *Indonesia of Journal Business Law*, 3(1), 43–52.
- Lambert, P. (2017). *Understanding the new European data protection rules*. Auerbach Publications.
- Lustarini, M. (2024). Kepastian hukum perlindungan data pribadi pasca pengesahan UU Nomor 27 Tahun 2022. *Kementerian Komunikasi dan Informatika*, 1–15.
- Palmer, R. C. (2007). *The bar code book: A comprehensive guide to reading, printing, specifying, evaluating and using bar code and other machine-readable symbols*. Trafford Publishing.
- Permadi, I. B., & Rokhman, A. (2023). Implementasi identitas kependudukan digital dalam upaya pengamanan data pribadi. *Journal of Public Policy and Administration*, 4(2), 80–88.
- Putri, W. A., & Sarjana, I. M. (2023). Perlindungan hukum terhadap konsumen korban kebocoran dan penyalahgunaan data pribadi pada perdagangan elektronik. *Jurnal Kertha Negara*, 11(4), 412–422.
- Rosadi, S. D. (2022). *Cyber law: Aspek data privasi menurut hukum internasional, regional dan nasional*. Refika Aditama.
- Rosadi, S. D. (2023). *Pembahasan UU Perlindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Sinar Grafika.
- Saepulloh, A., & Adeyadi, M. (2019). Aplikasi scanner berbasis Android untuk menampilkan data ID card menggunakan barcode. *Jurnal Manajemen dan Teknik Informasi (JUMANTAKA)*, 3(1), 250–255.
- Sahir, S. H. (2021). *Metodologi penelitian*. KBM Indonesia.
- Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016.
- Undang-Undang Republik Indonesia Nomor 23 Tahun 2006 tentang Administrasi Kependudukan sebagaimana telah diubah dengan Undang-Undang Nomor 24 Tahun 2013.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Utomo, R. (2020). Implementasi perlindungan data pribadi dalam Undang-Undang Informasi dan Transaksi Elektronik. *Jurnal Hukum Nasional*, 8(1), 78–93.
Yuliyanto, B. (2021). Perlindungan data pribadi di era digital: Tinjauan terhadap implementasi UU ITE. *Jurnal Hukum Digital*, 5(2), 45–55.