Indonesia of Journal Business Law

Volume : 3 | Nomor 1 | Januari 2024 | E-ISSN : 2809-8439 | DOI: 10.47709/ijbl.v3i1.4281

PERTANGGUNGJAWABAN HUKUM BAGI PELAKU PENYEBARAN DATA PRIBADI YANG TERSIMPAN PADA *BARCODE* DITINJAU DARI UNDANG-UNDANG INFORMASI TRANSAKSI ELEKTRONIK (UU ITE)

Author:
Muhammad Ilham[1]
Muhammad Akbar,SH, M.Kn[2]

Afiliation:
Universitas Deli Sumatera[1]
Universitas amir Hamzah[2]

Corresponding email
muhammad.ilham.spt@gmail.com[1]
mhdakbar377@yahoo.com[2]

Abstrak:

Latar belakang: Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) tidak secara spesifik mengatur tentang teknologi *barcode* secara langsung. UU ITE lebih berfokus pada regulasi tentang transaksi elektronik, perlindungan data pribadi, keamanan informasi, serta tata kelola sistem informasi elektronik di Indonesia. Namun demikian, penggunaan *barcode* dalam konteks pengolahan dan penyimpanan data pribadi tetap tunduk pada ketentuan-ketentuan perlindungan data pribadi yang diatur dalam UU ITE. Ini mencakup kewajiban untuk melindungi informasi pribadi dari akses yang tidak sah, penyalahgunaan, atau penyebaran yang tidak sah sesuai dengan standar dan prosedur yang ditetapkan.

Metode penelitian: Penelitian normatif digunakan untuk meneliti norma-norma hukum yang berlaku terkait perlindungan data pribadi dan pertanggungjawaban pelaku penyebarluasan data pribadi. Dengan pendekatan Perundang-undangan (Statute Approach)

Hasil penelitian: Aparat penegak hukum memainkan peran krusial dalam menegakkan hukum terkait dengan perlindungan data pribadi yang disimpan dalam barcode. Mereka bertanggung jawab untuk melakukan penyelidikan yang mendalam dan memastikan kejahatan yang melibatkan penyebaran data pribadi ini. Proses ini memerlukan penggunaan teknik investigasi yang canggih dan kerja sama dengan berbagai pihak terkait untuk mengumpulkan bukti yang kuat. Menurut UU ITE, penting bagi setiap pemegang data untuk mengambil langkah-langkah yang tepat guna mencegah akses yang tidak sah atau penyebaran yang tidak sah terhadap informasi pribadi. Hal ini menunjukkan fokus utama dari undang-undang dalam memastikan bahwa data pribadi yang dikelola oleh setiap pihak, baik individu maupun organisasi, harus dilindungi secara efektif dari potensi penyalahgunaan dan akses yang tidak sah. Regulasi ini bertujuan untuk memberikan perlindungan yang adekuat terhadap privasi individu dalam lingkungan digital yang kompleks, di mana risiko terhadap kebocoran atau penyalahgunaan data pribadi semakin meningkat.

Kesimpulan: Aparat penegak hukum memainkan peran penting dalam membuktikan terjadinya kejahatan terkait dengan penyebaran data pribadi

Indonesia of Journal Business Law

Volume : 3 | Nomor 1 | Januari 2024 | E-ISSN : 2809-8439 | DOI: 10.47709/ijbl.v3i1.4281

yang disimpan dalam kode batang. Melalui investigasi yang cermat dan penggunaan teknik forensik yang canggih, mereka berperan dalam menegakkan hukum untuk melindungi privasi dan keamanan data pribadi dalam konteks teknologi barcode. Dalam konteks Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Pertanggungjawaban hukum bagi pelaku penyebaran data pribadi yang tersimpan pada *barcode* sangat diatur dan harus dipatuhi. UU ITE menetapkan aturan yang jelas mengenai perlindungan data pribadi dan sanksi yang dikenakan terhadap pelanggaran. Menegaskan pentingnya kepatuhan terhadap ketentuan hukum dalam mengelola informasi pribadi dalam format teknologi seperti barcode.

Kata kunci: Pertanggungjawaban Hukum, Aparat Penegak Hukum, UU ITE

Pendahuluan

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) tidak secara spesifik mengatur tentang teknologi *barcode* secara langsung. UU ITE lebih berfokus pada regulasi tentang transaksi elektronik, perlindungan data pribadi, keamanan informasi, serta tata kelola sistem informasi elektronik di Indonesia.

Namun demikian, penggunaan *barcode* dalam konteks pengolahan dan penyimpanan data pribadi tetap tunduk pada ketentuan-ketentuan perlindungan data pribadi yang diatur dalam UU ITE. Ini mencakup kewajiban untuk melindungi informasi pribadi dari akses yang tidak sah, penyalahgunaan, atau penyebaran yang tidak sah sesuai dengan standar dan prosedur yang ditetapkan.

Dalam prakteknya, penggunaan *barcode* sebagai media penyimpanan informasi pribadi harus memperhatikan kepatuhan terhadap prinsip-prinsip perlindungan data yang diatur dalam UU ITE. Hal ini termasuk 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, dan informasi keuangan. Menurut Pasal 1 Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi[1] 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.

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.[2]

Menurut William Stallings dalam bukunya *Computer Security: Principles and Practice* menyatakan identifikasi data mencakup langkah-langkah untuk memberi label atau tag pada data, sehingga data tersebut dapat dikenali dan dikelola dengan cara yang aman dan efisien. Identifikasi

Volume : 3 | Nomor 1 | Januari 2024 | E-ISSN : 2809-8439 | DOI: 10.47709/ijbl.v3i1.4281

yang tepat memungkinkan organisasi untuk mengelompokkan data sesuai dengan kebutuhan operasional dan keamanannya.[3]

Michael E. Whitman dan Herbert J. Mattord dalam *Principles of Information Security* menyatakan bahwa identifikasi data adalah fondasi utama dari sistem keamanan informasi. Tanpa identifikasi yang baik, sangat sulit untuk mengelola akses dan penggunaan data secara efektif. Identifikasi data yang membantu dalam menetapkan kebijakan keamanan, mengelola akses pengguna, dan memastikan bahwa hanya individu yang berwenang yang dapat mengakses data sensitif.[4] Ada beberapa metode yang digunakan untuk identifikasi data dalam sistem elektronik:

1. Metadata
   Metadata adalah informasi tambahan yang disertai data utama, memberikan konteks seperti tanggal pembuatan, penulis, dan deskripsi isi. Menurut David Hay dalam *Data Model Patterns: Conventions of Thought* , metadata memainkan peran penting dalam pengelolaan data, memungkinkan sistem untuk mengorganisasikan dan mencari data dengan lebih efektif [5].
2. Pelabelan dan Penandaan
   Pelabelan dan penandaan adalah proses pemberian label atau tag pada data untuk memudahkan pengidentifikasian. Robert Seiner dalam *The Data Governance Imperative* menekankan bahwa pelabelan yang konsisten dan akurat membantu dalam mengelompokkan data dan memastikan bahwa data dapat diakses dengan cepat oleh pengguna yang berwenang. [6]
3. Pengindeksan
   Pengindeksan adalah proses pembuatan indeks untuk data yang memungkinkan pencarian cepat dan efisien. Menurut Jeffrey Ullman dalam *Principles of Database Systems* , pengindeksan yang baik adalah kunci bagi sistem manajemen basis data yang efektif, yang memungkinkan akses cepat ke data yang relevan

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[7].

Identifikasi data dalam sistem elektronik adalah proses yang penting untuk memastikan keamanan dan integritas informasi. 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*

Indonesia of Journal Business Law

Volume : 3 | Nomor 1 | Januari 2024 | E-ISSN : 2809-8439 | DOI: 10.47709/ijbl.v3i1.4281

Symbols , barcode adalah metode pengkodean data numerik atau alfanumerik dalam bentuk garis dan spasi yang bervariasi lebar. dan panjangnya[8]

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:

1. 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[9]
2. Kontrol Akses
   Mengontrol 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* [10].
3. Audit dan Monitoring
   Melakukan 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 [11]

Penggunaan barcode juga 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[12] mengatur tentang penggunaan teknologi informasi dan transaksi elektronik di Indonesia. UU ITE mengatur berbagai aspek hukum terkait informasi dan transaksi elektronik, termasuk perlindungan data pribadi.

Menurut Pasal 26 ayat (1) UU ITE, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan dengan persetujuan orang yang bersangkutan. Pelanggaran terhadap ketentuan ini dapat dikenakan sanksi pidana dan/atau perdata.

Pertanggungjawaban hukum terkait penyebarluasan data pribadi yang tersimpan pada barcode dapat berupa tanggung jawab pidana dan perdata antara lain.

1. Tanggung Jawab Pidana
   Pelaku yang menyebarluaskan data pribadi tanpa izin dapat dikenakan sanksi pidana berdasarkan Pasal 45 ayat (1) UU ITE. Sanksi ini mencakup pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah). Selain itu, Pasal 30 UU ITE juga mengatur tentang akses ilegal ke sistem elektronik yang dapat dikenakan sanksi pidana.
2. Tanggung Jawab Perdata
   Korban penyebarluasan data pribadi dapat mengajukan gugatan perdata berdasarkan Pasal 26 ayat (2) UU ITE. Gugatan ini dapat diajukan untuk mendapatkan ganti rugi atas kerugian yang dialami akibat penyebarluasan data pribadi tanpa izin. Selain itu, korban juga dapat menuntut pemulihan nama baik.

IJBL Indonesia of Journal Business Law

Volume : 3 | Nomor 1 | Januari 2024 | E-ISSN : 2809-8439 | DOI: 10.47709/ijbl.v3i1.4281

Untuk memperjelas penerapan hukum terkait, berikut adalah beberapa kasus penyebarluasan data pribadi yang tersimpan pada barcode:

1. Kasus di Sektor Kesehatan
   Di beberapa negara, data medis pasien sering disimpan dalam barcode yang dicetak pada gelang pasien. Penyebarluasan data medis tanpa izin dapat menyebabkan kerugian serius bagi pasien, seperti pencurian identitas medis dan pelanggaran privasi.
2. Kasus di Sektor Ritel
   Barcode pada produk ritel sering kali mengandung informasi tentang riwayat pembelian konsumen. Penyebarluasan informasi ini tanpa izin dapat menyebabkan penyalahgunaan data konsumen, seperti penipuan dan pencurian identitas.

Dari pedahuluan yang telah di uraikan diatas, maka penulis merumuskan permasalahan menjadi:

1. Bagaimana peran aparat penegak hukum dalam membuktikan terjadinya kejahatan terhadap penyebaran data pribadi yang di simpan dalam *barcode*
2. Bagaimana pertanggungjawaban hukum bagi pelaku penyebaran data pribadi yang tersimpan pada *barcode* ditinjau dari UU ITE

Metode Penelitian

Penelitian normatif digunakan untuk meneliti norma-norma hukum yang berlaku terkait perlindungan data pribadi dan pertanggungjawaban pelaku penyebarluasan data pribadi. Dengan pendekatan Perundang-undangan (*Statute Approach*): Menganalisis peraturan perundang-undangan terkait, seperti UU ITE, UU Perlindungan Data Pribadi, dan peraturan terkait lainnya.

Pembahasan

1. Peran Aparat Penegak Hukum Dalam Membuktikan Terjadinya Kejahatan Terhadap Penyebaran Data Pribadi Yang Di Simpan Dalam *Barcode*

Penyebarluasan data pribadi yang tersimpan pada *barcode* adalah isu yang kompleks dan memerlukan perhatian serius. UU ITE telah menyediakan kerangka hukum untuk melindungi data pribadi, namun implementasi yang efektif memerlukan upaya kolaboratif dari berbagai pihak, termasuk pemerintah, perusahaan, dan masyarakat. Dengan langkah-langkah perlindungan yang tepat, risiko penyebarluasan data pribadi tanpa izin dapat diminimalkan

Data pribadi didefinisikan sebagai informasi yang dapat mengidentifikasi individu, sedangkan barcode merupakan metode identifikasi yang menggunakan serangkaian garis paralel dan ruang berbeda yang dipindai untuk mendapatkan informasi. Hukum perlindungan data pribadi mengatur cara pengumpulan, penggunaan, dan pencurian data pribadi untuk memastikan privasi individu terlindungi.

Beberapa langkah dapat diambil untuk melindungi data pribadi yang tersimpan pada *barcode* antara lain:

1. 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.
2. Persetujuan Tertulis

Volume : 3 | Nomor 1 | Januari 2024 | E-ISSN : 2809-8439 | DOI: 10.47709/ijbl.v3i1.4281

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

3. 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.

Aparat penegak hukum yang 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* [13]. 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.

Kasus-kasus penyalahgunaan data pribadi, seperti pencurian identitas atau pencurian data finansial, seringkali memerlukan intervensi aktif dari aparat penegak hukum. Intervensi aparat penegak hukum adalah kunci untuk memastikan keadilan dan perlindungan bagi korban dalam kasus-kasus penyalahgunaan data pribadi[14]. Tanpa intervensi yang efektif, korban dapat mengalami kerugian finansial yang signifikan dan pelanggaran privasi yang serius. Aparat penegak hukum juga harus bekerja sama dengan berbagai pihak, termasuk lembaga perlindungan data dan perusahaan teknologi, untuk mengidentifikasi pelaku dan mencegah terulangnya kejahatan

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[15]. Hal ini mencakup analisis forensik digital, yang memungkinkan aparat penegak hukum untuk melacak jejak digital yang ditinggalkan oleh pelaku kejahatan.

Jones (2018) menambahkan bahwa teknik investigasi canggih, seperti penggunaan perangkat lunak analisis data dan pemetaan jaringan, sangat penting dalam mengidentifikasi dan mengejar pelaku kejahatan yang terlibat dalam penyebaran data pribadi[16]. Dengan teknologi ini, aparat penegak hukum dapat menghubungkan berbagai potongan informasi untuk membangun kasus yang kuat terhadap tersangka. Selain itu, kerjasama internasional seringkali diperlukan, mengingat banyaknya kejahatan siber yang bersifat lintas negara dan melibatkan jaringan kriminal global.

Langkah-langkah dalam proses pembuktian kejahatan terhadap penyebaran data pribadi mencakup analisis forensik komputer, pemeriksaan saksi ahli, dan kolaborasi dengan lembaga pengawasan data untuk mengumpulkan informasi yang relevan. Menurut Brown (2017) analisis forensik komputer adalah alat penting dalam mengungkap bukti digital yang dapat mendukung penuntutan dalam kasus kejahatan siber[17]. Proses ini melibatkan pengumpulan, penyimpanan, dan analisis data dari perangkat digital dengan cara menjaga integritas bukti tersebut.

Pemeriksaan saksi ahli juga memainkan peran kunci. Green (2019) menjelaskan bahwa tindakan ahli dapat memberikan penjelasan teknis yang kompleks dalam istilah yang dapat

Indonesia of Journal Business Law

Volume : 3 | Nomor 1 | Januari 2024 | E-ISSN : 2809-8439 | DOI: 10.47709/ijbl.v3i1.4281

dipahami oleh pengadilan, sehingga membantu dalam verifikasi bukti digital secara lebih efektif[18]. Saksi ahli biasanya memiliki keahlian di bidang teknologi informasi atau keamanan siber dan dapat memberikan pengetahuan berharga tentang bagaimana kejahatan dilakukan dan bukti yang mendukungnya.

Selain itu, kolaborasi dengan lembaga pengawasan data sangat penting. White (2020) menekankan bahwa pekerjaan yang sama dengan lembaga pengawasan data dapat memperluas cakupan investigasi dan memastikan bahwa semua aspek regulasi dan perlindungan data terpenuhi[19]. Lembaga-lembaga ini sering kali memiliki akses ke sumber daya dan informasi yang mungkin tidak tersedia bagi penegak hukum, sehingga membantu dalam mengumpulkan bukti-bukti yang relevan dan membangun kasus yang kuat.

Aparat penegak hukum memainkan peran krusial dalam menegakkan hukum terkait dengan perlindungan data pribadi yang disimpan dalam *barcode*. Mereka bertanggung jawab untuk melakukan penyelidikan yang mendalam dan memastikan kejahatan yang melibatkan penyebaran data pribadi ini. Proses ini memerlukan penggunaan teknik investigasi yang canggih dan kerja sama dengan berbagai pihak terkait untuk mengumpulkan bukti yang kuat. Dengan menggunakan teknik investigasi canggih dan kolaborasi dengan lembaga pengawasan data, aparat penegak 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.

2. Pertanggungjawaban Hukum Bagi Pelaku Penyebaran Data Pribadi Yang Tersimpan Pada *Barcode* Ditinjau Dari UU ITE

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. Menurut Yulianto (2021), UU ITE memberikan 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[20]. Hal ini mencerminkan komitmen legislatif untuk memberikan perlindungan yang memadai terhadap data pribadi dalam konteks teknologi informasi yang terus berkembang.

UU ITE mengatur bahwa setiap pemegang data memiliki kewajiban untuk melakukan langkah-langkah yang wajar guna melindungi informasi pribadi dari akses yang tidak sah atau penyalahgunaan. Hal ini menunjukkan komitmen legislator dalam memastikan bahwa data pribadi yang disimpan dan diolah dalam lingkungan digital mendapat perlindungan yang memadai, sesuai dengan prinsip-prinsip hak asasi manusia dan keamanan informasi. Implementasi kewajiban ini juga bertujuan untuk mencegah kemungkinan pelanggaran terhadap privasi individu serta memperkuat integritas sistem informasi di Indonesia.

Menurut Utomo (2020), implementasi UU ITE telah menjadi titik tolak penting dalam menangani tantangan perlindungan data pribadi di Indonesia. Utomo menekankan bahwa UU ITE menegaskan bahwa perlindungan terhadap data pribadi merupakan bagian integral dari hak asasi manusia dalam era digital[21] Hal ini menunjukkan bahwa UU ITE tidak hanya mengatur teknis perlindungan data, tetapi juga memperkuat prinsip-prinsip hak asasi manusia dalam era digital.

Perlindungan terhadap data pribadi dianggap sebagai bagian yang tak terpisahkan dari hak asasi manusia dalam konteks era digital. Hal ini menunjukkan pengakuan bahwa setiap individu

Volume : 3 | Nomor 1 | Januari 2024 | E-ISSN : 2809-8439 | DOI: 10.47709/ijbl.v3i1.4281

memiliki hak untuk menjaga privasi dan keamanan informasi pribadi mereka, tanpa harus terancam oleh kemungkinan penyalahgunaan atau akses yang tidak sah. Dalam konteks hukum dan kebijakan, prinsip ini menjadi dasar penting dalam merancang regulasi yang memastikan bahwa teknologi informasi dan transaksi elektronik beroperasi dengan menghormati dan melindungi hak-hak dasar setiap individu dalam mengelola data pribadi mereka secara aman dan bertanggung jawab.

Menurut Prof. Susanto (2021), implementasi UU ITE mengenai perlindungan data pribadi memberikan landasan yang kokoh bagi penegakan hukum terhadap pelanggaran yang terjadi. Beliau juga menegaskan bahwa UU ITE menjamin hak privasi individu dan memperkuat kontrol terhadap penggunaan dan penyebaran informasi pribadi dalam konteks transaksi elektronik[22]. Hal ini menunjukkan peran positif UU ITE dalam membangun kepercayaan publik terhadap penggunaan teknologi informasi yang aman dan bertanggung jawab.

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.

Menurut. Cahyono (2022), UU ITE merupakan instrumen hukum yang vital dalam mengatur dan melindungi data pribadi di Indonesia. Dr. Cahyono menjelaskan bahwa UU ITE menekankan pentingnya bagi setiap pemegang data untuk mengambil langkah-langkah yang tepat guna mencegah akses yang tidak sah atau penyebaran yang tidak sah terhadap informasi pribadi[23]. Hal ini menunjukkan kesadaran akan perlunya regulasi yang kuat untuk menghadapi tantangan perlindungan data di era digital.

Menurut UU ITE, penting bagi setiap pemegang data untuk mengambil langkah-langkah yang tepat guna mencegah akses yang tidak sah atau penyebaran yang tidak sah terhadap informasi pribadi. Hal ini menunjukkan fokus utama dari undang-undang dalam memastikan bahwa data pribadi yang dikelola oleh setiap pihak, baik individu maupun organisasi, harus dilindungi secara efektif dari potensi penyalahgunaan dan akses yang tidak sah. Regulasi ini bertujuan untuk memberikan perlindungan yang adekuat terhadap privasi individu dalam lingkungan digital yang kompleks, di mana risiko terhadap kebocoran atau penyalahgunaan data pribadi semakin meningkat. Dengan adanya peraturan yang jelas dan kewajiban yang ditetapkan oleh UU ITE, diharapkan dapat meningkatkan kesadaran dan tanggung jawab dalam pengelolaan data pribadi sesuai dengan standar yang telah ditetapkan oleh hukum.

Kesimpulan

Aparat penegak hukum memainkan peran penting dalam membuktikan terjadinya kejahatan terkait dengan penyebaran data pribadi yang disimpan dalam kode batang. Melalui investigasi yang cermat dan penggunaan teknik forensik yang canggih, mereka berperan dalam menegakkan hukum untuk melindungi privasi dan keamanan data pribadi dalam konteks teknologi barcode.

Volume : 3 | Nomor 1 | Januari 2024 | E-ISSN : 2809-8439 | DOI: 10.47709/ijbl.v3i1.4281

Kemudian aparat penegak hukum perlu mengembangkan dan meningkatkan keahlian dalam forensik digital dan investigasi kejahatan cyber untuk dapat mengumpulkan bukti yang kuat dan dapat dipertanggungjawabkan di pengadilan. Berkerjasama dengan ahli forensik komputer, teknisi IT, dan lembaga pengawas data untuk mendapatkan bantuan teknis dan sumber daya yang diperlukan. Melakukan penyelidikan secara proaktif terhadap potensi pelanggaran data pribadi dengan menggunakan teknologi dan metodologi terbaru. Memperkuat kerjasama internasional dalam pertukaran informasi dan pendekatan bersama terhadap kejahatan cyber yang melibatkan data pribadi lintas negara mengedukasi masyarakat tentang pentingnya perlindungan data pribadi dan bagaimana melaporkan potensi pelanggaran kepada aparat penegak hukum

Dalam konteks Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Pertanggungjawaban hukum bagi pelaku penyebaran data pribadi yang tersimpan pada *barcode* sangat diatur dan harus dipatuhi. UU ITE menetapkan aturan yang jelas mengenai perlindungan data pribadi dan sanksi yang dikenakan terhadap pelanggaran. Menegaskan pentingnya kepatuhan terhadap ketentuan hukum dalam mengelola informasi pribadi dalam format teknologi seperti barcode.

Selanjutnya Penting bagi pelaku untuk memahami dan mematuhi semua ketentuan UU ITE yang berkaitan dengan perlindungan data pribadi. Ini termasuk prosedur yang tepat dalam pengumpulan, penyimpanan, dan penggunaan data yang disimpan dalam *barcode*. Membangun kebijakan internal yang kuat dan transparan mengenai perlindungan data pribadi, termasuk langkah-langkah konkret untuk mencegah penyebaran yang tidak sah dan untuk merespons pelanggaran data pribadi sesuai dengan ketentuan hukum. Melakukan pelatihan reguler kepada karyawan tentang pentingnya perlindungan data pribadi dan kewajiban mereka sesuai dengan UU ITE. Ini termasuk pemahaman tentang risiko penyebaran data pribadi melalui barcode dan langkah-langkah untuk mengatasi risiko tersebut. Melakukan audit dan pemeriksaan rutin terhadap kepatuhan terhadap kebijakan dan prosedur perlindungan data pribadi. Hal ini dapat membantu mengidentifikasi dan mengatasi potensi pelanggaran sebelum menjadi masalah yang lebih serius. Bekerjasama dengan ahli hukum, konsultan keamanan informasi, dan lembaga pengawas data untuk mendapatkan saran dan bantuan yang diperlukan dalam memastikan kepatuhan terhadap UU ITE dan standar keamanan data pribadi.

Referensi

Bambang Riyanto. 2019. *Manajemen Data di Era Digital*. Jakarta. ABC Press. Hlm 45

Brown, Michael. 2017. *Forensik Komputer dan Investigasi Kejahatan Dunia Maya*. Penerbit Teknologi Informasi, Hlm. 56.

Bruce Schneier. 1996. *Kriptografi Terapan*. John Wiley & Sons. Hlm 145

Volume : 3 | Nomor 1 | Januari 2024 | E-ISSN : 2809-8439 | DOI: 10.47709/ijbl.v3i1.4281

Cahyono, Dr. 2022. "Perlindungan Data Pribadi di Era Digital: Analisis UU ITE," *Jurnal Hukum Cyber 10, no. 1*. Hlm 56.

David Hay. 2006. *Pola Model Data: Konvensi Pemikiran* . New York: Auerbach Publications. Hlm 34.

Green, Laura. 2019. *Kesaksian Ahli dalam Kasus Kejahatan Digital*. Penerbit Investigasi Cyber. Hlm 92.

Jones, Emma. 2018. *Teknik Investigasi Kejahatan Dunia Maya*. Penerbit Keamanan Digital. Hlm. 78

Jones, Emma. 2018. *Melindungi Data Pribadi di Era Digital*. Penerbit Teknologi Digital. Hlm 135.

Michael E. Whitman dan Herbert J. Mattord. 2021. *Principles of Information Security*. Boston: Pembelajaran Cengage. Hlm 76

Michael E. Whitman dan Herbert J. Mattord. 2021. *Prinsip Keamanan Informasi*. Cengage Learning. Hlm 121.

Paul Lambert. 2018. *Memahami Aturan Perlindungan Data Eropa Baru*. Boca Raton: CRC Press. Hlm 120

Richard E. Cascarino. 2012. *Panduan Auditor untuk Audit TI* . Wiley. Hlm 203.

Robert S. Seiner. 2014. *Keharusan Tata Kelola Data*. Boca Raton: CRC Press. Hlm. 102.

Roger C. Palmer. 2007. *The Bar Code Book: Panduan Lengkap untuk Membaca, Mencetak, Menentukan, Mengevaluasi, dan Menggunakan Kode Batang dan Simbol yang Dapat Dibaca Mesin Lainnya*. Helmers Publishing, Inc. Hlm 22.

Smith, John.2020. *Hukum Privasi dan Penegakan Hukum*. Penerbit Hukum Nasional. Hlm. 78

Smith, John. 2019. *Bukti Digital dan Penegakan Hukum Siber*. Penerbit Hukum Modern. Hlm. 102.

Susanto, Prof. 2021. "Perlindungan Data Pribadi dan Implementasi UU ITE," *Jurnal Hukum Teknologi 8, no. 2*. Hlm 78.

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008 yang telah diubah dengan UU No. 19 Tahun 2016

Utomo, Rahmat. 2020. "Implementasi Perlindungan Data Pribadi dalam Undang-Undang Informasi dan Transaksi Elektronik," *Jurnal Hukum Nasional 8, no. 1*. Hlm 78.

UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.

William Stallings. 2018. *Computer Security: Principles and Practice*, Boston: Pearson. Hlm 112
UU ITE," *Jurnal Hukum Digital 5, no. 2*. Hlm 45.

White, Daniel. 2020. *Kolaborasi Perlindungan Data dan Hukum Siber*. Penerbit Cyber Law Press. Hlm 123.

Yulianto, Budi. 2021. "Perlindungan Data Pribadi di Era Digital: Tinjauan Terhadap Implementasi

Yulianto, Budi. 2021. "Perlindungan Data Pribadi di Era Digital: Tinjauan Terhadap Implementasi UU ITE," *Jurnal Hukum Digital 5, no. 2*. Hlm 45.