

Pertanggungjawaban Pidana Korporasi dalam Kasus Kebocoran Data (Studi Kasus: Tokopedia 2020)

Madeline Agnes Bawedo

Fakultas Hukum Universitas Kristen Satya Wacana, E-mail: madelinebawedo1@gmail.com

Info Artikel

Masuk :
Diterima :
Terbit :

Keywords :

Corporate Criminal Liability,
Data Breach

Kata kunci:

Pertanggungjawaban Pidana
Korporasi, Kebocoran Data

Corresponding Author:

Madeline Agnes Bawedo,
E-mail:
madelinebawedo1@gmail.com

DOI :

Xxxxxxx

Abstract

The 2020 Tokopedia data breach of 91 million users set a significant precedent, highlighting the cyber vulnerability of corporations in Indonesia and its cybereconomic implications. This study aims to analyze the potential and forms of criminal liability for Tokopedia corporations under the Indonesian legal framework, specifically the Electronic Information and Transactions Law (UU ITE). The method used is a juridical-normative case study approach. The analysis shows that although direct criminal prosecution of corporations in data breach cases is rare, the Indonesian legal framework is strengthened by the principle of vicarious liability and management system regulations that fail to allow corporations to be subject to criminal law. Corporations, as Electronic System Operators (ESOs), are obliged to guarantee the reliability and security of their systems and are responsible for their operations. Gross negligence in these obligations can be the basis for criminal prosecution, highlighting the urgency of strict cyber law enforcement to protect personal data and the stability of the national digital economy.

Abstrak

Kasus kebocoran 91 juta data pengguna Tokopedia pada tahun 2020 menjadi preseden penting yang menyoroti kerentanan siber korporasi di Indonesia dan implikasi ekonomi-siber. Penelitian ini bertujuan menganalisis potensi dan bentuk pertanggungjawaban pidana korporasi Tokopedia di bawah kerangka hukum Indonesia, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Metode yang digunakan adalah yuridis-normatif dengan pendekatan studi kasus. Hasil analisis menunjukkan bahwa meskipun penuntutan pidana langsung terhadap korporasi dalam kasus kebocoran data jarang terjadi, kerangka hukum Indonesia diperkuat oleh prinsip vicarious liability dan regulasi sistem manajemen yang gagal memungkinkan korporasi menjadi subjek hukum pidana. Korporasi sebagai Penyelenggara Sistem Elektronik (PSE) wajib menjamin keandalan dan keamanan sistem serta bertanggung jawab terhadap operasionalnya. Kelalaian berat dalam kewajiban ini dapat menjadi dasar tuntutan pidana, menyoroti urgensi penegakan hukum siber yang tegas untuk melindungi data pribadi dan stabilitas ekonomi digital nasional.

I. Pendahuluan

Perekonomian digital Indonesia berkembang pesat, ditandai dengan menjamurnya platform digital dan e-commerce. Tokopedia, sebagai salah satu raksasa e-commerce, merupakan Penyelenggara Sistem Elektronik (PSE) yang mengelola data sensitif milik jutaan pengguna. Insiden kebocoran data pada tahun 2020, di mana 91 juta data pribadi, termasuk hash kata sandi, dicuri dan diperdagangkan di dark web, mengguncang kepercayaan publik dan menunjukkan kerentanan sistem keamanan siber korporasi¹. Kasus ini bukan sekadar masalah privasi, tetapi juga isu ekonomi siber yang mengancam keamanan finansial dan berpotensi memicu tindak kejahatan lanjutan seperti penipuan dan peretasan.

Implikasi ini membawa isu mengenai sejauh mana korporasi dapat dimintai pertanggungjawaban hukum, khususnya dalam aspek pidana, atas kelalaiannya dalam mengamankan sistem. Kerangka hukum siber nasional (terutama UU ITE dan peraturan turunannya) mewajibkan PSE untuk menyelenggarakan sistem yang andal dan aman. Oleh karena itu, kegagalan dalam menjaga keamanan data menimbulkan pertanyaan hukum mengenai *mens rea* (niat jahat) dan *actus reus* (perbuatan) dari korporasi sebagai entitas hukum.

2. Metode Penelitian

Artikel yang bersumber dari hasil penelitian hukum normatif yang berfokus pada analisis terhadap norma-norma hukum positif, asas-asas hukum, dan doktrin-doktrin hukum yang berlaku. Pendekatan penelitian yang digunakan adalah Pendekatan Perundang-undangan (*Statute Approach*), menganalisis secara komprehensif Undang-Undang Nomor 11 Tahun 2008 tentang ITE (dan perubahannya), Peraturan Mahkamah Agung (PERMA) Nomor 13 Tahun 2016 tentang Pertanggungjawaban Korporasi, serta peraturan pelaksana terkait Penyelenggara Sistem Elektronik (PSE). Pendekatan Konseptual (*Conceptual Approach*), menganalisis doktrin-doktrin hukum seperti *vicarious liability* (pertanggungjawaban pengganti) dan teori identifikasi (kegagalan sistem manajemen) yang relevan dalam konteks pertanggungjawaban pidana korporasi. Pendekatan Kasus (*Case Approach*), Menggunakan Kasus Kebocoran Data Tokopedia 2020 sebagai studi kasus untuk melihat relevansi dan potensi penerapan norma-norma hukum yang dianalisis.

Tujuan Penelitian menganalisis Apa saja bentuk dan dasar hukum potensial untuk menerapkan pertanggungjawaban pidana korporasi terhadap Tokopedia atas dugaan kelalaian dalam menjaga keamanan sistem elektronik?

3. Hasil Dan Pembahasan

Peristiwa kebocoran data Tokopedia melibatkan pencurian data pengguna, yang mencakup nama lengkap, email, jenis kelamin, dan hash kata sandi, yang kemudian dijual secara publik. Data yang dicuri tidak hanya mengandung informasi demografis, tetapi juga elemen krusial yang, jika dikombinasikan dengan teknik phishing atau peretasan lanjutan, dapat mengarah pada kejahatan

¹ Ari Santoso, 'Implikasi Ekonomi-Siber Pasca Kebocoran Data 91 Juta Pengguna Tokopedia' (2020) Media Siber Nasional, 16.

finansial atau peretasan akun di platform lain (*credential stuffing*)². Tanggapan dari Pihak Berwenang (Polri dan BSSN) fokus pada penyelidikan teknis dan aspek kelalaian korporasi, sebagaimana diamanatkan oleh peraturan perlindungan data dan keamanan siber. Secara ekonomi-siber, kebocoran data memiliki implikasi serius. Kerugian tersebut meliputi kerugian finansial langsung pada pengguna, biaya pemulihan korporasi (audit keamanan dan litigasi), dan penurunan kepercayaan konsumen. Penurunan kepercayaan ini secara langsung mempengaruhi nilai ekonomi perusahaan dan stabilitas ekosistem digital nasional.

Kewajiban utama korporasi sebagai PSE diatur dalam Pasal 15 Undang-Undang Nomor 11 Tahun 2008 tentang ITE yang menyatakan: "Penyelenggara Sistem Elektronik bertanggung jawab terhadap dioperasikannya Sistem Elektronik termasuk pengamanan Sistem Elektronik."³ Berikut pada Pasal 32 ayat (2) dan (3) UU ITE yang melarang akses ilegal (*unauthorized access*) dan memerintahkan tindakan preventif, serta Pasal 48 ayat (2) dan (3) yang mengatur sanksi pidana terhadap pelanggaran tersebut. Kelalaian dalam memenuhi standar keamanan siber yang memadai, sehingga menyebabkan kebocoran data, dapat diinterpretasikan sebagai pemenuhan unsur pidana dalam UU ITE jika ditemukan unsur kesengajaan atau kelalaian berat yang mengakibatkan kerugian signifikan, meskipun sanksi utamanya biasanya menasar pelaku langsung⁴.

1. Doktrin Vicarious Liability (Pertanggungjawaban Pengganti)

Doktrin ini menyatakan bahwa korporasi dapat bertanggung jawab atas tindakan pidana yang dilakukan oleh karyawan atau agennya dalam lingkup pekerjaan, asalkan tindakan tersebut dilakukan untuk dan atas nama korporasi. Dalam konteks data breach, jika kelalaian operasional oleh karyawan (misalnya, patching sistem yang gagal) menyebabkan kebocoran, korporasi dapat dikenakan pertanggungjawaban pengganti.

2. Kegagalan Sistem Manajemen (Teori Identifikasi)

Pertanggungjawaban dapat timbul dari kegagalan sistem manajemen korporasi dalam menerapkan langkah-langkah keamanan siber yang memadai, sebagaimana diwajibkan oleh Pasal 15 UU ITE. Kelalaian ini mencerminkan kesalahan pada level tertinggi (manajemen) yang gagal membangun dan mengawasi sistem keamanan yang andal. Kegagalan sistemik seperti ini dapat diidentifikasi sebagai kesalahan korporasi itu sendiri, yang berujung pada sanksi berupa denda atau tindakan administratif lainnya sesuai PERMA 13/2016.

² *Op Cit* Ari Santoso, 19.

³ Undang-Undang Informasi dan Transformasi Elektronik pada Pasal 15.

⁴ Undang-Undang Informasi dan Transformasi Elektronik pada Pasal 48 ayat (2) dan (3).

4. Kesimpulan

Berdasarkan pembahasan diatas, maka dapat disimpulkan bahwa Kasus kebocoran data Tokopedia 2020 merupakan contoh nyata di mana kerentanan siber korporasi memiliki implikasi ekonomi-siber yang luas. Berdasarkan kerangka hukum Indonesia, terutama UU ITE dan PERMA 13/2016, Tokopedia berpotensi dimintai pertanggungjawaban pidana sebagai korporasi. Dasar pertanggungjawabannya terletak pada kewajiban PSE untuk menjamin keamanan dan keandalan sistemnya (Pasal 15 UU ITE). Jika terbukti ada unsur kesengajaan atau kelalaian berat dari pihak internal yang menyebabkan kerugian, doktrin vicarious liability atau kegagalan sistem manajemen dapat diterapkan. Kasus ini menegaskan bahwa mekanisme hukum untuk menghukum korporasi telah tersedia, menuntut penegakan yang lebih tegas untuk memaksa korporasi meningkatkan keamanan siber dan melindungi hak-hak pengguna.

Daftar Pustaka / Daftar Referensi

Jurnal

Handoko, Budi. (2021). "Analisis Penerapan Doktrin Pertanggungjawaban Pidana Korporasi Dalam Kasus Kebocoran Data di Indonesia." *Jurnal Hukum Pidana*. Vol. X, No. 2.

Santoso, Ari. (2020). "Implikasi Ekonomi-Siber Pasca Kebocoran Data 91 Juta Pengguna Tokopedia." *Media Siber Nasional*. [Diakses pada 28 November 2025].

Simanjuntak, Dewi. (2018). *Hukum Pidana Korporasi: Doktrin Vicarious Liability dan Teori Identifikasi*. Jakarta: Penerbit Yudisial.

Peraturan Perundang-Undangan

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, diubah dengan Undang-Undang Nomor 19 Tahun 2016. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251.

Peraturan Mahkamah Agung Nomor 13 Tahun 2016 tentang Tata Cara Penanganan Tindak Pidana oleh Korporasi.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.