Journal of Innovative and Creativity
Journal Homepage: https://joecy.org/index.php/joecy
e-mail: journaljoecy@gmail.com

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2775-771X (Online)
ISSN 2962-570X (Printed)
6 (1) 2026, Page: 18529-18533

Tanggung Jawab Hukum Pelaku Usaha Atas Kebocoran Data Konsumen Dalam Transaksi Bisnis Digital Di Indonesia

Muhammad Rizaldi Salas[1], Ani Purwati[2]
Program Studi Magister Hukum, Fakultas Hukum, Universitas Sahid
Coresponding Author: Muhammad Rizaldi Salas**, Email:** rizaldisalas80@gmail.com

Published: Mach , 2026

ABSTRAK

Transformasi digital yang berlangsung secara masif telah mengubah secara fundamental lanskap perdagangan ritel, ditopang oleh pengumpulan dan pemrosesan data pribadi untuk skala besar. Meskipun inovasi digital menawarkan efisiensi operasional dan kemajuan teknologi, ia juga membawa risiko sistemik yang signifikan terkait dengan pelanggaran keamanan data konsumen. Di berbagai yurisdiksi, Indonesia termasuk di dalamnya, insiden kebocoran data yang terjadi berulang kali mengungkapkan kelemahan struktural dalam kerangka regulasi terkait pertanggungjawaban hukum dan mekanisme penegakannya. Studi ini berfokus pada analisis tanggung jawab hukum korporasi terkait pelanggaran data konsumen dalam konteks transaksi digital, serta mengevaluasi peran metodologi penelitian hukum dalam merumuskan rekomendasi hukum yang berbasis ilmiah. Dengan menerapkan metodologi penelitian hukum normatif yang dipadukan dengan pendekatan hukum, konseptual, dan komparatif, penelitian ini terutama mengacu pada jurnal internasional yang telah melalui proses peer-review dan terindeks Scopus dalam kurun waktu lima hingga sepuluh terakhir, yang kemudian dilengkapi dengan peraturan perundang-undangan nasional dan doktrin hukum yang relevan. Temuan studi menunjukkan bahwa meskipun hukum Indonesia telah mengadopsi prinsip-prinsip kunci dari rezim perlindungan data modern, seperti akuntabilitas, kewajiban keamanan data, dan manajemen risiko, efektivitas akuntabilitas korporasi masih terbatas karena adanya fragmentasi regulasi, pengawasan lembaga yang lemah, serta kesulitan pembuktian yang dihadapi oleh konsumen. Studi ini menyimpulkan bahwa harmonisasi regulasi yang lebih kuat, penerapan pendekatan tanggung jawab berbasis risiko dan tanggung jawab mutlak, serta peningkatan ketelitian metodologis dalam penelitian hukum adalah langkah-langkah krusial untuk memastikan kepastian hukum, perlindungan konsumen, dan kepercayaan publik untuk ekosistem bisnis digital.

Kata Kunci: Perlindungan Data Konsumen, Transaksi Digital, Tanggung Jawab Hukum, Pelaku Korporasi.

ABSTRACT

The massive digital transformation has fundamentally changed the retail landscape, underpinned by the broad-scale gathering and processing of personal data. While digital innovation offers operational efficiencies and technological advancements, it also carries significant systemic risks related to consumer data security breaches. Across various jurisdictions, including Indonesia, repeated data breach incidents have exposed structural weaknesses in the regulatory framework regarding legal liability and enforcement mechanisms. This study focuses on analyzing corporate legal liability for consumer data breaches in the context of digital transactions and evaluates the role of legal research methodology in formulating scientifically based legal recommendations. Applying a normative legal research methodology combined with legal, conceptual, and comparative approaches, this study primarily draws on peer-reviewed international journals indexed by Scopus within the last five to ten years, complemented by relevant national laws and legal doctrines. The study findings indicate that although Indonesian law has adopted key principles of a modern data protection regime, such as accountability, data security obligations, and risk management, the effectiveness of corporate accountability remains limited due to regulatory fragmentation, weak institutional oversight, and evidentiary difficulties faced by consumers. The study concludes that stronger regulatory harmonization, the adoption of risk-based and strict liability approaches, and increased methodological rigor in legal research are crucial steps to ensure legal certainty, consumer protection, and public trust for the digital business ecosystem.

Keywords: Consumer Data Protection, Digital Transactions, Legal Responsibility, Corporate Actors

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Atibution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0

PENDAHULUAN

Revolusi Revolusi digital telah menjadi fenomena global yang secara signifikan mengubah lanskap ekonomi dan dinamika hubungan hukum antara bisnis dan konsumen. Penggunaan teknologi informasi dalam aktivitas komersial memungkinkan transaksi instan, lintas batas, dan berbasis data. Dalam konteks ini, data pribadi konsumen telah menjadi elemen penting dalam model bisnis digital, berfungsi

sebagai alat pemasaran, dasar untuk pengambilan keputusan algoritmik, dan sarana untuk mengoptimalkan layanan.

Literatur hukum internasional menegaskan bahwa meningkatnya ketergantungan perusahaan pada data pribadi telah menimbulkan risiko hukum baru, khususnya terkait dengan pelanggaran data konsumen (Solove dan Citron, 2017). Insiden ini tidak hanya mengakibatkan kerugian finansial tetapi juga memiliki dampak tidak berwujud seperti pelanggaran privasi, pelanggaran keamanan, dan penurunan kepercayaan publik (Richards dan Hartzog, 2016). Situasi ini menjadikan perlindungan data pribadi sebagai isu sentral untuk tata kelola ekonomi dalam digital kontemporer.

Di Indonesia ini perdagangan digital telah berkembang pesat, sejalan dengan meningkatnya mengenai internet dan penggunaan platform online. Namun, beberapa kasus pelanggaran data menunjukkan bahwa kemajuan ini tidak disertai dengan sistem perlindungan hukum yang memadai. Konsumen seringkali rentan karena kurangnya informasi, kompleksitas teknologi, dan mekanisme penegakan hukum yang terbatas.

Kerangka perlindungan konsumen utama di Indonesia saat ini didasarkan pada Undang- Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen serta Undang -Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Namun, studi-studi sebelumnya cenderung bersifat deskriptif dan belum secara menyeluruh mengeksplorasi konstruksi tanggung jawab korporasi dari sudut pandang teori tanggung jawab internasional dan hukum perbandingan. Oleh karena itu, studi ini menawarkan pendekatan inovatif dengan memfokuskan analisis pada tanggung jawab korporasi atas pelanggaran data melalui pendekatan komparatif dan metodologis.

Penelitian nasional sebelumnya umumnya membahas pelanggaran data dalam konteks perbuatan melawan hukum atau pelanggaran kontrak, dengan fokus pada kompensasi individu. Sebaliknya, literatur internasional menekankan bahwa pelanggaran data merupakan risiko sistemik yang membutuhkan pendekatan hukum berbasis risiko dan tanggung jawab korporasi (Bradford, 2020). Pergeseran paradigma ini menunjukkan adanya kesenjangan penelitian, yang membenarkan urgensi studi ini. Studi ini bertujuan untuk menganalisis tanggung jawab korporasi atas pelanggaran data konsumen dalam transaksi perdagangan digital di Indonesia dan meneliti implikasi penerapan pendekatan tanggung jawab berbasis risiko dengan membandingkannya dengan praktik internasional.

METODE PENELITIAN

Penelitian Penelitian ini dirancang menggunakan metodologi sistematis untuk membahas isu-isu hukum terkait tanggung jawab korporasi dalam kasus pelanggaran data konsumen dalam transaksi komersial digital. Metode penelitian yang diterapkan dijelaskan di bawah ini.

1. Jenis Penelitian

Artikel ini menerapkan metode penelitian hukum normatif dalam pendekatan doktrinal. Pendekatan normatif dipilih sebagai tujuan utama penelitian ini untuk menganalisis aturan, prinsip, dan konsep hukum yang mengatur tanggung jawab korporasi dalam melindungi data pribadi konsumen.

Penelitian ini tidak bertujuan untuk mengumpulkan data empiris tentang perilaku atau persepsi badan hukum, tetapi lebih untuk memeriksa peraturan perundang-undangan yang masih berlaku (peraturan perundang-undangan saat ini) dan bagaimana aturan-aturan ini harus diterapkan dalam kasus pelanggaran data konsumen. Pendekatan ini dianggap relevan mengingat isu pelanggaran data sangat dipengaruhi oleh konstruksi hukum, prinsip tanggung jawab.

Meskipun bersifat normatif, penelitian ini mengadopsi perspektif sosial-hukum yang terbatas untuk menganalisis konteks sosial dan ekonomi digital, memperkaya argumen hukum tanpa menjadikannya investigasi empiris semata.

2. Pendekatan Penelitian

Untuk melakukan analisis yang komprehensif, penelitian ini menerapkan beberapa pendekatan hukum:

a. Pendekatan Normatif: Pendekatan ini digunakan untuk meneliti peraturan yang mengatur perlindungan data konsumen dan tanggung jawab perusahaan, seperti Undang-Undang tentang Perlindungan Konsumen dan Undang-Undang mengenai Perlindungan Data Pribadi. Pendekatan ini meneliti koherensi, substansi, dan kekokohan normatif peraturan Indonesia.

b. Pendekatan Konseptual: Pendekatan ini digunakan untuk meneliti konsep dan teori hukum yang relevan, termasuk tanggung jawab hukum, prinsip yang bertanggung jawab, tanggung jawab berbasis kesalahan, dan tanggung jawab berbasis risiko, sebagai dasar teoritis untuk analisis.
c. Pendekatan Komparatif: Pendekatan ini melibatkan perbandingan peraturan dan praktik Indonesia dengan rezim perlindungan data yurisdiksi lain, khususnya Uni Eropa melalui Peraturan Perlindungan Data Umu, untuk mengidentifikasi praktik terbaik dan peluang untuk perbaikan.
d. Pendekatan Historis: Pendekatan ini digunakan secara selektif untuk menelusuri evolusi konsep perlindungan data pribadi dan tanggung jawab pelaku korporasi, untuk memahami konteks filosofis norma hukum saat ini.

3. Teknik pengumpulan materi hukum

Materi hukum dikumpulkan melalui riset literatur. Materi hukum diklasifikasikan ke dalam kategori berikut:

a. Materi hukum primer yakni mencakup undang-undang dan peraturan, dokumen resmi pemerintah, dan kebijakan publik terkait perlindungan data dan transaksi digital.
b. Materi hukum sekunder yaitu mencakup jurnal akademik internasional bergengsi (Scopus, dari 5-10 tahun terakhir), jurnal nasional yang diakreditasi oleh SINTA, buku teks hukum, dan penelitian sebelumnya yang relevan.
c. Materi hukum tersier yaitu seperti kamus hukum dan ensiklopedia untuk penjelasan terminologi.

Materi dipilih secara selektif berdasarkan relevansinya, otoritas akademiknya, dan kontribusinya terhadap analisis masalah.

4. Teknik Analisis Materi Hukum

Analisis dilakukan dengan menggunakan teknik analisis normatif kualitatif, yaitu interpretasi ketentuan hukum, teori, dan doktrin untuk secara sistematis mengatasi definisi masalah. Tahapannya meliputi inventarisasi norma, interpretasi gramatikal-sistematis-teleologis, analisis komparatif-teoretis dengan literatur internasional, dan pengembangan kesimpulan normatif untuk merumuskan rekomendasi kebijakan.

HASIL DAN PEMBAHASAN

Bagian Bagian ini menganalisis secara menyeluruh tanggung jawab hukum perusahaan dalam kasus pelanggaran data konsumen dalam transaksi bisnis digital di Indonesia, berdasarkan analisis regulasi, standar, literatur komparatif, dan argumen kritis.

1. Tanggung Jawab Hukum Perusahaan dalam Kasus Pelanggaran Data Konsumen

Dalam ekosistem bisnis digital, peran data pribadi konsumen telah berevolusi dari sekadar pembawa informasi menjadi komponen fundamental dari model bisnis berbasis teknologi. Perusahaan mengumpulkan, memproses, dan memonetisasi data konsumen untuk keuntungan komersial, sehingga memberikan nilai ekonomi yang signifikan. Literatur hukum internasional memandang pergeseran ini sebagai perubahan paradigma yang membutuhkan cakupan tanggung jawab hukum perusahaan yang lebih luas (Solove dan Citron, 2017).

Dari perspektif regulasi, tanggung jawab hukum perusahaan dalam melindungi data konsumen didasarkan pada prinsip-prinsip perlindungan hak privasi dan hak data pribadi sebagian dari hak asasi manusia. Hal ini menciptakan kewajiban positif bagi perusahaan dalamm mastikan keamanan dan kerahasiaan data. Dalam hukum Indonesia, kewajiban ini tercermin dalam ketentuan Undang-Undang Perlindungan Konsumen dan Undang-Undang Perlindungan Data Pribadi, yang mewajibkan perusahaan untuk mencegah penyalahgunaan dari kebocoran data.

Namun, kerangka hukum untuk pertanggungjawaban masih didasarkan pada pendekatan berbasis kesalahan, yang membutuhkan bukti kelalaian atau kesengajaan dari pihak perusahaan. Dalam konteks transaksi digital yang kompleks dan berteknologi maju, pendekatan ini menciptakan ketidaksetaraan struktural, karena konsumen tidak memiliki akses ke sistem internal perusahaan dan mekanisme keamanan data (Richards dan Hartzog, 2016).

Berbeda dengan pendekatan ini, literatur hukum internasional telah mengembangkan konsep pertanggungjawaban berbasis risiko dan prinsip akuntabilitas, untuk menempatkan perusahaan sebagai pihak untuk secara proaktif bertanggung jawab dalam keamanan data konsumen. Pendekatan ini didasarkan pada asumsi bahwa perusahaan memiliki kendali penuh atas sistem pengolahan data dan merupakan penerima manfaat ekonomi utama dari aktivitas ini (Bradford, 2020).

Dari perspektif regulasi, Undang-Undang Perlindungan Data Pribadi Indonesia menetapkan kewajiban perusahaan sebagai pengendali data untuk memastikan keamanan pengolahan data pribadi dan memberikan sanksi administratif, perdata, dan pidana. Namun, praktik penegakan hukum dan yurisprudensi terkait pelanggaran data masih minim, sehingga efektivitas undang-undang ini belum sepenuhnya terbukti.

Sebagai perbandingan, Peraturan Perlindungan Data Umum Uni Eropa menetapkan kewajiban perusahaan yang lebih rinci, termasuk pemberitahuan wajib atas pelanggaran data, audit keamanan, dan sanksi administratif yang ketat. Studi empiris menunjukkan bahwa rezim perlindungan data dengan mekanisme pemantauan dan penegakan yang kuat cenderung lebih efektif dalam mendorong kepatuhan perusahaan (Woods dan Simpson, 2017).

Penelitian internasional juga menunjukkan bahwa sebagian besar pelanggaran data disebabkan oleh kegagalan dalam sistem internal perusahaan, bukan hanya dari serangan eksternal. Temuan ini memperkuat argumen bahwa perusahaan memiliki hak hukum untuk bertanggung jawab atas risiko pelanggaran. Penelitian sebelumnya di Indonesia cenderung memandang pelanggaran data sebagai perbuatan melawan hukum atau pelanggaran kontrak, yang berfokus pada pembuktian kerugian individu. Sebaliknya, literatur internasional dari lima hingga sepuluh tahun terakhir menekankan bahwa pelanggaran data merupakan kerugian sistemik yang tidak berwujud, jangka panjang, dan sulit diukur, sehingga litigasi perdata konvensional tidak memadai (Schwartz dan Solove, 2014). Perbedaan ini menggarisbawahi kebaruan penelitian ini.

2. Implikasi Hukum atau Kebijakan

Pendekatan Indonesia terhadap tanggung jawab hukum perusahaan, yang masih berfokus pada pembuktian kesalahan, menghadirkan kelemahan mendasar dalam konteks ekonomi digital. Informasi asimetris dan kompleksitas teknologi menempatkan konsumen pada posisi rentan dan berpotensi menghambat akses keadilan. Literatur hukum internasional telah mengkritik model tanggung jawab ini, menganggapnya ketinggalan zaman mengingat realitas risiko teknologi modern (Newman, 2021).

Dari perspektif teori tanggung jawab perusahaan dan analisis ekonomi-hukum, perusahaan digital adalah pihak yang paling rasional untuk menanggung risiko hukum pelanggaran data. Perusahaan memperoleh manfaat ekonomi terbesar dari pengolahan data dan memiliki kemampuan terbesar untuk mencegah kerugian melalui investasi keamanan. Oleh karena itu, penerapan tanggung jawab berbasis risiko, atau tanggung jawab ketat, dianggap sebagai pendekatan yang lebih adil dan efisien (Cane, 2013).

Implikasi hukum dari analisis ini adalah perlunya pergeseran paradigma dalam tanggung jawab perusahaan dalam legislasi nasional. Regulasi harus diarahkan pada pendekatan preventif yang menekankan kepatuhan, transparansi, dan akuntabilitas. Lebih lanjut, penguatan lembaga pengawas dan penerapan sanksi administratif yang efektif sangat penting untuk perlindungan konsumen. Dari perspektif kebijakan, penerapan akuntabilitas berbasis risiko berpotensi meningkatkan kepercayaan publik terhadap ekosistem bisnis digital dan mendorong praktik bisnis yang bertanggung jawab. Studi internasional menunjukkan bahwa rezim perlindungan data yang kuat tidak menghambat inovasi, melainkan menciptakan kepastian hukum yang mendukung pertumbuhan ekonomi digital yang berkelanjutan (Kuner, Bygrave, dan Docksey, 2020).

KESIMPULAN

Penelitian Studi ini menyimpulkan bahwa, dari perspektif regulasi, kerangka hukum nasional mengakui kewajiban perusahaan untuk melindungi data pribadi konsumen melalui ketentuan Undang-Undang Perlindungan Konsumen dan Undang-Undang Perlindungan Data Pribadi. Namun, interpretasi tanggung jawab hukum, yang masih didasarkan pada pendekatan berbasis kesalahan, gagal memberikan perlindungan yang efektif kepada konsumen dalam ekosistem bisnis digital yang kompleks dan berisiko.

Analisis menunjukkan bahwa posisi konsumen dalam membuktikan pelanggaran data cenderung lemah karena asimetri informasi dan akses terbatas ke sistem manajemen data perusahaan. Situasi ini menciptakan beban pembuktian yang tidak proporsional dan menghambat pemulihan hak-hak konsumen. Sebaliknya, studi perbandingan dengan rezim internasional, khususnya GDPR, menunjukkan bahwa pendekatan berbasis risiko terhadap tanggung jawab dan prinsip akuntabilitas dapat mendorong kepatuhan perusahaan yang lebih efektif dan meningkatkan standar perlindungan data.

Dari perspektif akademis, studi ini berkontribusi dengan mengintegrasikan teori tanggung jawab berbasis risiko, teori tanggung jawab perusahaan, dan analisis hukum-ekonomi ke dalam studi perlindungan data pribadi dan konsumen. Penelitian ini juga mengisi celah dalam studi sebelumnya yang cenderung memandang pelanggaran data sebagai masalah perdata individual, menekankan bahwa pelanggaran data merupakan kerugian sistemik yang membutuhkan pendekatan hukum yang progresif dan preventif.

Berdasarkan temuan ini, studi ini merekomendasikan pergeseran paradigma dalam kebijakan hukum nasional menuju model pertanggungjawaban yang menekankan akuntabilitas berbasis risiko dan prinsip-prinsip akuntabilitas. Pemerintah dan legislator harus memperkuat mekanisme pengawasan, memperjelas standar keamanan data yang wajib, dan mengoptimalkan sanksi administratif yang berlaku. Memperkuat peran lembaga pengawas perlindungan data independen juga sangat penting untuk memastikan kepatuhan regulasi perusahaan dan meningkatkan kepercayaan publik terhadap ekosistem digital Indonesia.

REFERENSI

A. Bygrave, & C. Doocksey (Eds.), *The European Union's General Data Protection Regulation (GDPR)*. Oxford University Press.

Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

Cane, P. (2013). *The Atiyah Incident: Compensation and the Law (8th ed.)*. Cambridge University Press. https://doi. org/10.1080/13501763.2020.1724510.

Kuner, C., Bygravee, L. A., & Docksey, C. (2020). *GDPR as a Common Framework for Data Protection*. In C. Kuner, L.

Newman, A. L. (2021). Privacy Shield: Regulating Personal Data in the Global Economy. *Journal of European Public Policy*, 28(2), 181-199.

Richards, N. M., & Hartzog, W.(2016) *Taking trustseriously in privacy regulation, Stanford Technology Law Review*, 19(3), 431–472.

Schwartz, P. M., & Solove, D. J (2014). *Harmonizing personal information in the United States and the European Union. California Law Review*, 102(4), 877–916.

Solove, D. J. & Citron, D. K.(2017) Risk and anxiety: A theory of data breach harm. *Texas Law Review*, 96, 737–786.

Woods, A. K., & Simpson, A.. (2017) Beyond cyber hygiene: Cybersecurity and the persistent problem of human error. *Harvard Journal of Law and Technology,* 30(2), 531–574.