

## PERLINDUNGAN DAN TANGGUNG JAWAB HUKUM KEBOCORAN INFORMASI DATA PRIBADI PADA PENYELENGGARA SISTEM ELEKTRONIK BERDASARKAN PERSPEKTIF RAHASIA DAGANG

Myrna Fitria<sup>1</sup>, Dewi Iryani<sup>2</sup>, Puguh Aji Hari Setiawan<sup>3</sup>

Universitas Bung Karno, Indonesia<sup>1</sup>

Universitas Bung Karno, Indonesia<sup>2</sup>

Universitas Bung Karno, Indonesia<sup>3</sup>

Email: myrna.fitria@gmail.com<sup>1</sup>, iryani.dewi77@gmail.com<sup>2</sup>,  
puguh.setiawan@gmail.com<sup>3</sup>

### Abstrak

Penyelenggara Sistem Elektronik (PSE) dalam kasus kebocoran data pribadi berdasarkan perspektif rahasia dagang. Data pribadi yang dikelola oleh PSE sering kali memiliki nilai ekonomi yang signifikan, sehingga kebocoran data tidak hanya merugikan privasi individu tetapi juga dapat mengancam rahasia dagang perusahaan. Melalui pendekatan yuridis normatif, penelitian ini mengkaji bagaimana Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022) dan Undang-Undang Rahasia Dagang (UU No. 30 Tahun 2000) mengatur perlindungan serta tanggung jawab PSE dalam melindungi data pribadi dan rahasia dagang. Undang-Undang Perlindungan Data Pribadi menyediakan kerangka hukum yang cukup komprehensif, pelaksanaan dan penegakannya masih menghadapi beberapa tantangan signifikan. Kewajiban untuk memberikan kompensasi kepada pihak yang terdampak juga belum diatur secara jelas, sehingga berpotensi menimbulkan perbedaan standar ganti rugi di berbagai kasus. Perlindungan rahasia dagang yang berkaitan dengan data pelanggan atau informasi bisnis strategis sangat penting untuk mempertahankan keunggulan kompetitif di pasar. Penelitian ini menyarankan adanya peningkatan dalam kerangka regulasi dan kepatuhan untuk membangun lingkungan perlindungan data yang lebih kuat guna menjaga privasi individu sekaligus melindungi kepentingan bisnis.

**Kata kunci:** Perlindungan Data Pribadi; Rahasia Dagang; Penyelenggara Sistem Elektronik; Tanggung Jawab Hukum; Kebocoran Data.

### Abstract

*Electronic System Organizers (ESO) in cases of personal data leaks based on a trade secret perspective. Personal data managed by EOS often has significant economic value, so data leaks not only harm individual privacy but can also threaten the company's trade secrets. Through a normative legal approach, this study examines how the Personal Data Protection Law (Law No. 27 of 2022) and the Trade Secrets Law (Law No. 30 of 2000) regulate the protection and responsibilities of EOS in protecting personal data and trade secrets. The Personal Data Protection Law provides a fairly comprehensive legal framework, its implementation and enforcement still face several significant challenges. The obligation to provide compensation to affected parties has also not been clearly regulated, potentially leading to differences in compensation standards in various cases. Protection of trade secrets related to customer data or strategic business information is critical to maintaining a competitive advantage in the market. This study suggests improvements in the regulatory and compliance framework to build a stronger data*

---

*protection environment to safeguard individual privacy while protecting business interests.*

**Keywords:** *Personal Data Protection; Trade Secret; Electronic System Organizers; Legal Responsibility; Data Leaks.*

---

*\*Correspondence Author: Myrna Fitria  
Email: myrna.fitria@gmail.com*



## **PENDAHULUAN**

Di era digitalisasi yang semakin berkembang pesat, perlindungan terhadap data pribadi telah menjadi isu global yang krusial. Kebocoran informasi data pribadi tidak hanya merugikan individu secara finansial tetapi juga merusak reputasi dan keamanan negara. Menurut laporan terbaru dari Kominfo, terdapat 111 kasus kebocoran data pribadi yang ditangani antara tahun 2019 hingga 2024 (Teguh Arifiadi, 2024). Isu ini mencerminkan pentingnya penerapan regulasi dan pengawasan ketat terhadap penyelenggara sistem elektronik (PSE), yang sering menjadi target utama serangan siber. Perspektif rahasia dagang memberikan dimensi tambahan dalam memahami tanggung jawab hukum atas kebocoran tersebut.

Di Indonesia, kasus kebocoran data pribadi telah menjadi perhatian serius, terutama setelah implementasi Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Meski regulasi ini memberikan landasan hukum yang kuat, masih ada tantangan dalam penerapan dan penegakannya. Choirunnisa et al. (2023) menyoroti pentingnya sistem pemerintah berbasis elektronik (SPBE) dalam meningkatkan aksesibilitas layanan publik. Namun, kurangnya perlindungan data yang memadai dapat menghambat kepercayaan masyarakat terhadap sistem ini. Hal ini juga dikaitkan dengan kebutuhan untuk mengintegrasikan aspek rahasia dagang sebagai bagian dari strategi mitigasi risiko hukum dan operasional.

Urgensi penelitian ini terletak pada meningkatnya jumlah insiden kebocoran data yang berdampak luas pada masyarakat dan sektor bisnis. Berdasarkan penelitian Alfian et al. (2022), penyelenggara sistem elektronik seperti aplikasi PeduliLindungi menghadapi risiko hukum akibat akses ilegal terhadap data pengguna. Situasi ini menggarisbawahi pentingnya pengawasan yang lebih efektif dan penerapan tanggung jawab hukum yang jelas. UU PDP telah memberikan kerangka kerja untuk melindungi data pribadi, tetapi pendekatan berbasis rahasia dagang dapat memperkuat mekanisme perlindungan tersebut, sebagaimana disarankan oleh Koswara (2021).

Literatur hukum modern hingga postmodern telah memberikan landasan teori yang relevan dalam memahami perlindungan data pribadi. (Wibawa, 2016) mengkaji pergeseran paradigma dari hukum modern ke postmodern, yang

menekankan pentingnya fleksibilitas dan adaptasi hukum terhadap dinamika teknologi. Selain itu, Lia Sautunida (2018) menjelaskan bagaimana rahasia dagang dapat digunakan untuk melindungi informasi sensitif dalam konteks bisnis. Matheus dan Gunadi (2024) menunjukkan perlunya pembentukan lembaga pengawas yang independen untuk memastikan kepatuhan terhadap regulasi data pribadi di era ekonomi digital.

Penelitian ini menawarkan pendekatan baru dengan mengintegrasikan perspektif rahasia dagang ke dalam analisis tanggung jawab hukum atas kebocoran data pribadi. Pendekatan ini belum banyak dibahas dalam literatur, meskipun potensinya besar dalam meningkatkan perlindungan hukum. Prijatna (2024) menyoroti bahwa PSE sering kali berada di posisi yang sulit untuk memenuhi kewajiban hukum tanpa adanya pedoman yang jelas. Dengan mengadopsi prinsip-prinsip rahasia dagang, PSE dapat lebih proaktif dalam mencegah kebocoran data dan mengelola risiko hukum secara efektif.

Tujuan utama penelitian ini adalah untuk mengeksplorasi dan mengembangkan kerangka hukum yang mengintegrasikan perlindungan data pribadi dengan perspektif rahasia dagang. Hal ini mencakup identifikasi tanggung jawab hukum PSE berdasarkan UU PDP dan analisis kasus kebocoran data di Indonesia. Penelitian ini juga bertujuan memberikan rekomendasi kebijakan yang dapat mendukung implementasi regulasi yang lebih efektif, sebagaimana dibahas oleh Hukumonline (2020) dan HeyLaw (2020).

## **METODE PENELITIAN**

Penelitian ini merupakan penelitian hukum normatif yang bertujuan untuk menganalisis perlindungan dan tanggung jawab hukum terkait kebocoran informasi data pribadi berdasarkan perspektif rahasia dagang. Jenis penelitian yang digunakan adalah deskriptif kualitatif, dengan fokus pada penguraian secara sistematis mengenai aturan hukum, prinsip, dan kasus-kasus yang relevan.

Pendekatan yang digunakan dalam penelitian ini mencakup pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan diterapkan untuk mengkaji isi dari Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-Undang No. 30 Tahun 2000 tentang Rahasia Dagang. Sementara itu, pendekatan konseptual digunakan untuk menganalisis konsep-konsep yang berkaitan dengan tanggung jawab hukum penyelenggara sistem elektronik.

Teknik pengumpulan data dilakukan melalui studi dokumen dan studi literatur. Data primer diperoleh dari regulasi terkait, seperti UU PDP dan UU Rahasia Dagang, sementara data sekunder mencakup jurnal, artikel ilmiah, dan publikasi lainnya yang relevan dengan topik. Data yang telah terkumpul kemudian dianalisis menggunakan teknik analisis deskriptif kualitatif, yaitu dengan menginterpretasikan data hukum untuk memberikan gambaran komprehensif tentang permasalahan yang dikaji.

Hasil penelitian ini diharapkan memberikan kontribusi dalam pengembangan kerangka hukum yang lebih kuat, sekaligus menawarkan solusi praktis untuk meningkatkan kepatuhan dan perlindungan hukum terhadap data pribadi dan rahasia dagang.

## HASIL DAN PEMBAHASAN

### 1. Bagaimana pengaturan mengenai data pribadi pada Penyelenggara Sistem Elektronik di Indonesia berdasarkan perspektif rahasia dagang?

UU PDP memperkenalkan konsep "data controller" dan "data processor", yang masing-masing bertanggung jawab atas penanganan data pribadi. Data controller adalah pihak yang menentukan tujuan dan cara pengolahan data pribadi, sementara data processor adalah pihak yang memproses data atas nama data controller. Kedua entitas ini harus memastikan bahwa data pribadi diolah dengan cara yang sesuai dengan hukum dan standar keamanan yang berlaku.

Namun, meskipun regulasi telah ada, implementasi dan pengawasan yang efektif masih menjadi pekerjaan rumah. Pemerintah dan lembaga terkait perlu memastikan bahwa penyelenggara sistem elektronik mematuhi peraturan yang berlaku dan memberikan sanksi yang tegas terhadap pelanggaran, termasuk pelanggaran yang melibatkan kebocoran data, penggunaan data tanpa izin, atau penyalahgunaan data pribadi.

Sebagai tambahan, penelitian ini menyoroti pentingnya data empiris untuk mendukung analisis. Misalnya, dalam kasus kebocoran data BPJS Kesehatan pada 2021, data 279 juta penduduk bocor dan dijual di forum online. Hal ini menimbulkan kerugian signifikan baik bagi individu maupun reputasi perusahaan terkait. Contoh lainnya adalah kasus yang melibatkan Tokopedia pada 2020, di mana data lebih dari 91 juta pengguna bocor akibat peretasan. Insiden-insiden ini menunjukkan lemahnya pengawasan dan implementasi UU PDP dalam melindungi data pribadi.

**Tabel 1. Data Kebocoran Data di Indonesia**

Tahun	Kasus	Jumlah Data yang Bocor	Sumber
2020	Tokopedia	91 juta	Forum peretas
2021	BPJS Kesehatan	279 juta	Forum jual beli data

Sebagai perbandingan, Uni Eropa telah menerapkan General Data Protection Regulation (GDPR) yang jauh lebih ketat. GDPR tidak hanya mewajibkan pelaporan kebocoran data dalam waktu 72 jam, tetapi juga memberlakukan denda yang signifikan terhadap perusahaan yang melanggar. Indonesia, meskipun memiliki UU PDP, belum memiliki tingkat penegakan hukum yang setara.

**Tabel 2. Perbandingan Kebijakan Perlindungan Data**

Aspek	Indonesia (UU PDP)	Uni Eropa (GDPR)
Pelaporan Kebocoran	3x24 jam	72 jam
Sanksi Denda	Maksimal Rp5 miliar	Hingga €20 juta atau 4% dari pendapatan tahunan global

Dengan demikian, meskipun regulasi di Indonesia sudah memberikan kerangka hukum, ada kebutuhan mendesak untuk memperkuat pengawasan dan meningkatkan efektivitas implementasi UU PDP. Pengalaman dari negara lain seperti Uni Eropa dapat menjadi panduan untuk mengatasi kelemahan dalam sistem perlindungan data Indonesia.

## 2. Tanggungjawab hukum Penyelenggaran Sistem Elektronik atas kebocoran informasi data pribadi berdasarkan perspektif Rahasia Dagang

Penyelenggara Sistem Elektronik (PSE), baik dari sektor publik maupun privat, memiliki tanggung jawab besar dalam menjaga keamanan data yang mereka kelola, terlebih dengan diberlakukannya UU PDP. Dalam UU PDP, Kewajiban PSE dirincikan dengan sangat jelas dan menyeluruh. Tanggung Jawab PSE Berdasarkan UU PDP

Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menempatkan PSE sebagai pihak yang memiliki tanggung jawab utama dalam menjaga kerahasiaan dan keamanan data pribadi yang mereka kelola. Jika terjadi kebocoran data pribadi, PSE bertanggung jawab untuk:

- Melaporkan kebocoran data tersebut dalam waktu 3x24 jam kepada subjek data dan otoritas terkait (Kementerian Komunikasi dan Informatika).
- Melakukan mitigasi terhadap kerugian yang mungkin timbul akibat kebocoran tersebut.
- Menghadapi sanksi administratif berupa denda, pencabutan izin, atau sanksi pidana jika ditemukan unsur kesengajaan atau kelalaian berat dalam kebocoran data.

### Tanggung Jawab PSE Berdasarkan UU Rahasia Dagang

Undang-Undang No. 30 Tahun 2000 tentang Rahasia Dagang melindungi informasi bisnis atau teknologi yang memiliki nilai ekonomi karena kerahasiaannya. Apabila data pribadi yang bocor juga berkaitan dengan rahasia dagang, seperti pola konsumsi, preferensi pengguna, atau informasi strategis lainnya, kebocoran tersebut dapat dianggap sebagai pelanggaran rahasia dagang.

Dalam konteks ini, PSE memiliki tanggung jawab untuk:

- Menjaga kerahasiaan data strategis yang dapat memberikan keunggulan kompetitif bagi perusahaan. Data tersebut bisa berupa informasi pelanggan, teknologi bisnis, atau bahkan data transaksi.
- Menghadapi tuntutan dari pihak yang merasa dirugikan, baik subjek data pribadi maupun perusahaan yang kehilangan keunggulan dagangnya akibat kebocoran tersebut.

Namun, di sisi lain, kebocoran data pribadi bisa menjadi ancaman besar yang tak hanya berdampak pada pelanggan, tetapi juga pada reputasi perusahaan. Dampak dari kebocoran data tidak hanya sebatas sanksi hukum, seperti yang diatur dalam UU

Perlindungan Data Pribadi (UU PDP) di Indonesia, tetapi juga bisa lebih parah dalam hal kehilangan kepercayaan pelanggan. Ketika data pribadi bocor, baik disengaja atau akibat serangan siber, publik akan meragukan kemampuan perusahaan dalam menjaga keamanan informasi sensitif mereka.

Oleh karena itu, perlindungan data pribadi tidak hanya dipandang sebagai kewajiban hukum, tetapi juga sebagai komponen kritis dalam manajemen risiko. Manajemen risiko data yang baik tidak hanya melibatkan penerapan langkah-langkah keamanan teknis, tetapi juga mencakup kebijakan perusahaan yang komprehensif terkait pengelolaan dan pemrosesan data, serta peningkatan kesadaran internal bagi karyawan tentang pentingnya menjaga kerahasiaan data pelanggan.

Dengan demikian, perusahaan harus memahami bahwa melindungi data pribadi pelanggan sama pentingnya dengan melindungi aset fisik dan kekayaan intelektual mereka. Oleh karenanya perlindungan hukum atas data pribadi dan rahasia dagang di Indonesia kini semakin diperkuat dengan hadirnya UU PDP dan UU Rahasia Dagang. PSE memiliki tanggung jawab besar untuk menjaga keamanan data yang mereka kelola, dan kegagalan untuk melindungi data ini bisa berakibat pada sanksi hukum yang serius.

Penerapan yang kuat dari kedua undang-undang ini akan memastikan bahwa Indonesia memiliki kerangka hukum yang solid dalam melindungi hak-hak individu dan perusahaan di era digital yang semakin kompleks.

## **KESIMPULAN**

Pengaturan mengenai data pribadi pada Penyelenggara Sistem Elektronik di Indonesia, dengan perspektif rahasia dagang, menunjukkan bahwa data pribadi, terutama yang memiliki nilai ekonomi, merupakan aset strategis yang perlu dilindungi secara menyeluruh. Di Indonesia, perlindungan hukum data pribadi diatur oleh UU Perlindungan Data Pribadi (UU PDP) dan UU Rahasia Dagang (UU No. 30 Tahun 2000), yang meskipun memiliki tujuan berbeda, saling melengkapi dalam melindungi informasi sensitif. Penyelenggara Sistem Elektronik (PSE) bertanggung jawab untuk menjaga integritas, kerahasiaan, dan keamanan data pribadi melalui langkah-langkah preventif dan reaktif, termasuk pelaporan kebocoran dalam waktu 3x24 jam. Data pribadi yang memiliki nilai komersial dapat dianggap sebagai rahasia dagang, namun perlindungan dalam UU PDP lebih komprehensif dibandingkan dengan UU Rahasia Dagang. Kebocoran data dapat menyebabkan kerugian signifikan, baik untuk individu maupun perusahaan, seperti yang terlihat dalam kasus kebocoran data BPJS Kesehatan pada tahun 2021. Tanggung jawab hukum PSE dalam menjaga kerahasiaan data, baik di sektor publik maupun privat, melibatkan kepatuhan terhadap standar keamanan dan penerapan sanksi yang diatur dalam kedua undang-undang tersebut. Dengan demikian, perlindungan data pribadi tidak hanya merupakan kewajiban hukum, tetapi juga elemen kunci dalam membangun kepercayaan pelanggan, menjadikannya aset strategis yang vital bagi keberhasilan bisnis di era digital ini.

## **BIBLIOGRAFI**

- Alfian, F. S., Alam, M. Z., & Maharani, D. P. (2022). Pertanggungjawaban Hukum Penyelenggara Sistem Elektronik PeduliLindungi terhadap Potensi Kebocoran Data Pribadi akibat Akses Tidak Sah/Ilegal. *Brawijaya Law Student Journal*.
- Choirunnisa, Laili, et al. "Peran Sistem Pemerintah Berbasis Elektronik (SPBE) Dalam Meningkatkan Aksesibilitas Pelayanan Publik di Indonesia." *Sosio Yustisia: Jurnal Hukum dan Perubahan Sosial* 3.1 (2023)
- Ditjen Aptika Kominfo. (2020). Penyelenggara Sistem Elektronik Bertanggungjawab terhadap Pelanggaran Data. <https://aptika.kominfo.go.id/2020/06/penyelenggara-sistem-elektronik-bertanggungjawab-terhadap-pelanggaran-data/?utm>
- HeyLaw. (2020). Pertanggungjawaban Penyelenggara Sistem Elektronik atas Pelanggaran Data Pribadi. <https://heylaw.id/blog/pelanggaran-data-pribadi?utm>
- Hukum-Hukum.com. (2016). Perlindungan Data Pribadi dalam Sistem Elektronik. <https://www.hukum-hukum.com/2016/12/perlindungan-data-pribadi-sistem-elektronik.html?utm>
- Hukumonline. (2020). Mengenal Kewajiban Penyelenggara Sistem Elektronik dalam Melindungi Data Pribadi. <https://www.hukumonline.com/berita/a/mengenal-kewajiban-penyelenggara-sistem-elektronik-dalam-melindungi-data-pribadi-lt5ec84120a2ac0?utm>
- Hukumonline. (2020). Pertanggungjawaban Hukum terhadap Kebocoran Data Pribadi. <https://www.hukumonline.com/berita/a/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-lt5f067836b37ef?utm>
- Iskandar Wibawa. Pergeseran Paradigma Dari Hukum Modern ke Post Modern. *Masalah - Masalah Hukum*, Jilid 45 No. 4, Oktober 2016
- JDIH Tanah Laut. (2024). Perlindungan Hukum tentang Data Pribadi yang Harus Diketahui. <http://103.165.243.89/>
- Koswara, W. (2021). Kewajiban dan Tanggung Jawab Penyelenggara Sistem Elektronik sebagai Pengendali dan/atau Prosesor Data Pribadi: Analisis Komparatif Pengaturan Internasional, Pengaturan Domestik Negara Asia, Hukum Positif Indonesia, dan RUU PDP Indonesia. Tesis, Universitas Pelita Harapan.
- Lia Sautunida, *Kanun Jurnal Ilmu Hukum*, Vol. 20, No. 2, Agustus, 2018,
- Matheus, J., & Gunadi, A. (2024). Pembentukan Lembaga Pengawas Perlindungan Data Pribadi di Era Ekonomi Digital: Kajian Perbandingan dengan KPPU. *JUSTISI*, 10(1), 20–35.
- Muhammad Fikri, *Ganesha Law Review*, 5(1), 2023
- Ninne Zahara Silviani, Jeslyn Teo, *Ganesha Law Review*, Volume 5 Issue 1 May 2023
- Prijatna, W. H. R. (2024). Bagaimana Pertanggungjawaban Penyelenggara Sistem

Elektronik (PSE) Selaku Pengendali Data Pribadi Saat Terjadi Kebocoran Data Pribadi?. Kogin Diputro Harymbawa & Partners.  
<https://kdhplaw.com/2024/06/12/bagaimana-pertanggungjawaban-penyelenggara-sistem-elektronik-pse-selaku-pengendali-data-pribadi-saat-terjadi-kebocoran-data-pribadi/?utm>

Republik Indonesia. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)

Republik Indonesia. Undang-Undang No. 30 Tahun 2000 tentang Rahasia Dagang

Teguh Arifiadi. Dari <https://www.kompas.id/baca/ekonomi/2024/06/03/111-kasus-kebocoran-data-pribadi-ditangani-kemenkominfo-pada-2019-14-mei-2024>, diakses 17/072024 Pukul 09.00 WIB



© 2024 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY SA) license (<https://creativecommons.org/licenses/by-sa/4.0/>).