



Perbandingan Penyelesaian Hukum Perkara Penyebaran Data Pribadi di Media Massa Antar Indonesia dan Singapura

INFO PENULIS

Heilynn
Universitas Esa Unggul, Jakarta
joana.aloysia@student.esaunggul.ac.id

Markoni
Universitas Esa Unggul, Jakarta
markoni@esaunggul.ac.id

I Made Kantikha
Universitas Esa Unggul, Jakarta
Kanthika@esaunggul.ac.id

Dyah Permata Budi Asri
Universitas Esa Unggul, Jakarta
dyah.permata@esaunggul.ac.id

INFO ARTIKEL

ISSN: 3046-8507
Vol. 2, No. 3, November 2025
<http://almufi.com/index.php/ASH>

© 2025 Almufi All rights reserved

Saran Penulisan Referensi:

Heilynn., Markoni., Kantikha, I. M., & Asri, D. P. B. (2025). Perbandingan Penyelesaian Hukum Perkara Penyebaran Data Pribadi di Media Massa Antar Indonesia dan Singapura. *Almufi Jurnal Sosial dan Humaniora*, 2 (3), 491-500.

Abstrak

Dalam era digital, data pribadi menjadi objek hukum yang sangat penting karena berkaitan erat dengan perlindungan hak privasi sebagai bagian dari hak asasi manusia. Indonesia mengatur perlindungan data pribadi melalui dua rezim hukum, yaitu rezim kejahatan siber dalam Undang- Undang Informasi dan Transaksi Elektronik (UU ITE) serta rezim administrasi dan perdata dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Sementara itu, Singapura menerapkan sistem perlindungan data yang terintegrasi melalui Personal Data Protection Act (PDPA) Tahun 2012 yang didukung oleh lembaga pengawas independen, yaitu Personal Data Protection Commission (PDPC). Artikel ini mengkaji pengaturan hukum mengenai penyebaran dan perlindungan data pribadi di Indonesia dan Singapura melalui pendekatan hukum komparatif. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan perbandingan hukum. Hasil penelitian menunjukkan bahwa meskipun lahirnya UU PDP merupakan kemajuan signifikan dalam rezim perlindungan data pribadi di Indonesia, implementasinya masih menghadapi berbagai tantangan struktural dan kelembagaan, termasuk belum beroperasinya otoritas pengawas independen serta tumpang tindih norma hukum. Sebaliknya, sistem perlindungan data di Singapura menunjukkan tingkat kepastian hukum dan efektivitas penegakan yang lebih tinggi dengan pendekatan regulasi yang bersifat preventif. Oleh karena itu, Indonesia perlu memperkuat kelembagaan, melakukan harmonisasi regulasi, serta meningkatkan literasi digital masyarakat guna menjamin perlindungan data pribadi yang efektif dan sesuai dengan standar internasional.

Kata kunci: perlindungan data pribadi, hak privasi, UU PDP, PDPA, hukum perbandingan.

Abstract

In the digital era, personal data has become a crucial legal object closely related to the protection of privacy as a fundamental human right. Indonesia regulates personal data protection through a dual legal regime, namely the cybercrime regime under the Electronic Information and Transactions Law (ITE Law) and the administrative–civil regime under Law Number 27 of 2022 on Personal Data Protection (PDP Law). Meanwhile, Singapore adopts an integrated regulatory framework through the Personal Data Protection Act (PDPA) of 2012, which is supported by an independent supervisory authority, the Personal Data Protection Commission (PDPC). This article examines the legal framework governing the dissemination and protection of personal data in Indonesia and Singapore through a comparative legal approach. This research employs normative legal research methods with statutory, conceptual, and comparative approaches. The findings indicate that although the enactment of the PDP Law represents significant progress in Indonesia’s personal data protection regime, its implementation still faces structural and institutional challenges, including the absence of an operational independent supervisory authority and overlapping regulatory norms. In contrast, Singapore’s integrated regulatory system demonstrates higher legal certainty, effective enforcement mechanisms, and a strong preventive regulatory framework. This thesis concludes that Indonesia needs to strengthen institutional arrangements, harmonize related regulations, and enhance digital literacy to ensure effective personal data protection in accordance with international standards and the needs of a modern digital society.

Keywords: personal data protection, privacy rights, PDP Law, PDPA, comparative law.

A. Pendahuluan

Media sosial dan platform daring memungkinkan masyarakat berkomunikasi secara instan dan luas, menciptakan jaringan informasi global. Perubahan ini berdampak positif terhadap kemudahan akses informasi serta efisiensi komunikasi lintas wilayah. Namun, kemajuan tersebut juga melahirkan tantangan baru, terutama terkait dengan keamanan data pribadi pengguna. Banyak individu tidak menyadari bahwa aktivitas daring mereka menghasilkan jejak digital yang dapat disalahgunakan. Dengan demikian, transformasi teknologi tidak hanya membawa manfaat, tetapi juga tanggung jawab besar bagi individu dan institusi untuk menjaga privasi di dunia maya. Dengan demikian, perubahan teknologi membuat arus informasi semakin cepat, namun bukan berarti selalu lebih akurat atau lebih terkontrol. Namun, kemajuan ini tidak datang tanpa risiko, khususnya terkait penyebaran data pribadi pengguna teknologi dan media. Terlebih lagi, ketika batas antara pribadi dan publik makin kabur dalam ruang siber. Maka dari itu, pemahaman mengenai hak atas data pribadi serta kontrol atas informasi diri sendiri menjadi semakin penting.

Indonesia telah merespons tantangan tersebut melalui pembentukan Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan pada tahun 2022 (Jimly, 2018). Undang-undang ini memberikan payung hukum terhadap setiap bentuk pengumpulan, pemrosesan, dan penyebaran data pribadi. Meski demikian, pelaksanaannya di lapangan masih menghadapi berbagai kendala, terutama dalam aspek penegakan hukum. Banyak lembaga dan perusahaan belum sepenuhnya menerapkan prinsip perlindungan data secara konsisten (Budhijanto, 2010). Oleh karena itu, diperlukan kolaborasi antara pemerintah dan masyarakat untuk memastikan efektivitas regulasi tersebut. Selain itu, media massa juga harus menyesuaikan standar etika pemberitaan agar tidak melanggar hak privasi.

Di Indonesia, banyak ditemukan berbagai kasus penyalahgunaan dan penyebaran data pribadi yang terjadi. Misalnya pada kasus kebocoran data pelanggan PLN yang mencapai sekitar 17 juta data, peretasan data oleh sosok yang dikenal dengan nama “Bjorka” yang mengklaim memiliki data registrasi 1,3 miliar kartu SIM, hingga dugaan kebocoran data paspor dan data kependudukan yang dijual secara ilegal di forum daring, hal ini menunjukkan betapa rentannya data pribadi masing-masing orang dan dibutuhkan adanya perlindungan data pribadi tersebut.

Indonesia sebenarnya telah memiliki perangkat hukum berupa Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 (Marzuki, 2008). Pasal 26 UU ITE secara jelas mengatur bahwa penggunaan informasi elektronik yang berkaitan dengan data pribadi harus memperoleh persetujuan dari pemilik data. Selain itu, dengan adanya Undang-Undang Nomor 27 Tahun 2022

tentang Perlindungan Data Pribadi (UU PDP) menjadi tonggak baru dalam sistem hukum nasional yang secara khusus mengatur aspek perlindungan data pribadi, termasuk ancaman pidana terhadap pengungkapan data secara melawan hukum (Nonet, 1978). Namun demikian, implementasi UU PDP masih relatif baru sehingga efektivitasnya dalam menyelesaikan perkara penyebaran data pribadi belum maksimal. Meskipun UU ITE sudah mengandung norma perlindungan data pribadi, banyak ahli menilai bahwa cakupannya masih bersifat parsial dan belum komprehensif.

Pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) secara eksplisit mengatur pengumpulan, pemrosesan, penyimpanan, dan penghapusan data pribadi, serta kewajiban bagi pengendali data untuk menjaga keamanan data yang mereka kelola. Selain itu, undang-undang ini memperkenalkan ancaman pidana dan sanksi administratif bagi pihak-pihak yang dengan sengaja atau lalai mengungkapkan data pribadi secara melawan hukum (Gustryan, 2025). Dengan demikian, UU PDP hadir untuk menutup celah hukum yang belum diatur secara rinci dalam UU ITE, serta memberikan kepastian hukum bagi masyarakat di era digital.

Dari aspek aturan hukum, Indonesia mengatur perlindungan data pribadi melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 26 UU ITE menegaskan bahwa penggunaan data pribadi dalam media elektronik harus memperoleh persetujuan pemilik data. Namun, ketentuan ini masih bersifat parsial karena hanya menyentuh aspek persetujuan tanpa mengatur secara rinci hak subjek data dan kewajiban pengendali data. Sebaliknya, UU PDP hadir sebagai regulasi komprehensif yang mengatur seluruh siklus pengelolaan data pribadi, termasuk sanksi pidana dan administratif. Meskipun demikian, karena masih relatif baru, efektivitas UU PDP dalam menyelesaikan perkara penyebaran data pribadi belum sepenuhnya teruji dalam praktik peradilan (Gustryan, 2025).

Berbeda dengan Indonesia, Singapura telah lebih dahulu memiliki kerangka hukum perlindungan data melalui Personal Data Protection Act (PDPA) 2012 yang telah diamandemen pada tahun 2020. PDPA mengatur secara rinci prinsip-prinsip dasar seperti consent, purpose limitation, dan accountability dalam pengelolaan data pribadi. Regulasi ini menempatkan perlindungan data sebagai kewajiban hukum yang mengikat bagi seluruh organisasi, baik sektor publik maupun swasta. Dalam konteks penyelesaian perkara, PDPA memberikan kejelasan norma serta mekanisme sanksi yang tegas terhadap pelanggaran data pribadi (Latumahina, 2014). Hal ini terlihat dari berbagai putusan dan sanksi administratif yang dijatuhkan oleh otoritas pengawas terhadap organisasi yang lalai menjaga keamanan data. Dengan demikian, dari sisi aturan hukum, Singapura menunjukkan tingkat kematangan regulasi yang lebih tinggi dibandingkan Indonesia.

Kasus kebocoran data SingHealth tahun 2018 menjadi contoh konkret efektivitas kelembagaan PDPC dalam menangani pelanggaran data pribadi di Singapura. Kebocoran data yang melibatkan sekitar 1,5 juta pasien tersebut ditindaklanjuti melalui investigasi mendalam oleh PDPC dan pembentukan Committee of Inquiry. Hasil investigasi mengungkap adanya kelalaian organisasi dan kelemahan sistem keamanan, yang kemudian berujung pada sanksi administratif dan perbaikan sistem keamanan nasional. Pendekatan ini menunjukkan bahwa penyelesaian perkara di Singapura tidak hanya berorientasi pada penghukuman, tetapi juga pada perbaikan sistemik dan pencegahan di masa depan. Sebaliknya, kasus-kasus kebocoran data besar di Indonesia, seperti kebocoran data PLN dan Kominfo, sering kali belum diikuti dengan penyelesaian hukum yang transparan dan tuntas (Sutanto, 2020).

Berdasarkan perbandingan aspek aturan, kelembagaan, dan kultur hukum, dapat disimpulkan bahwa Singapura memiliki sistem penyelesaian perkara penyebaran data pribadi yang lebih efektif dibandingkan Indonesia. Keberhasilan tersebut didukung oleh regulasi yang matang, lembaga pengawas yang kuat, serta budaya hukum yang mendukung kepatuhan. Sementara itu, Indonesia masih berada pada tahap awal penguatan sistem perlindungan data pribadi, meskipun telah memiliki UU PDP sebagai landasan hukum yang komprehensif. Oleh karena itu, Indonesia dapat mengambil pelajaran dari praktik Singapura, terutama dalam memperkuat kelembagaan pengawas, meningkatkan literasi digital masyarakat, serta memastikan penegakan hukum yang konsisten. Dengan langkah tersebut, diharapkan penyelesaian perkara penyebaran data pribadi di Indonesia dapat berjalan lebih efektif dan memberikan perlindungan nyata bagi hak privasi masyarakat.

B. Metodologi

Metode penelitian ini bersifat yuridis-normatif, menekankan pada analisis peraturan perundang-undangan, putusan pengadilan, dan literatur hukum, sehingga setiap kesimpulan yang dihasilkan dapat dipertanggungjawabkan secara yuridis dan sesuai dengan praktik hukum yang berlaku.

a. Jenis Penelitian

Penelitian ini menggunakan jenis penelitian deskriptif dengan pendekatan yuridis normatif. Penelitian deskriptif dipilih untuk memberikan gambaran yang sistematis, faktual, dan akurat mengenai Penyelesaian Hukum Perkara Penyebaran Data Pribadi Di Media Massa. Melalui pendekatan ini, penelitian tidak hanya memaparkan norma hukum yang berlaku, tetapi juga menganalisis bagaimana Penyelesaian Hukum Perkara Penyebaran Data Pribadi Di Media Massa diselesaikan.

b. Sumber Bahan Hukum

Penelitian ini menggunakan data sekunder yang bersumber dari bahan kepustakaan hukum. Bahan hukum tersebut terdiri atas bahan hukum primer dan bahan hukum sekunder. Bahan hukum meliputi peraturan perundang-undangan dan putusan pengadilan yang relevan, antara lain Undang-Undang nomor 19 Tahun 2016 tentang adanya Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi Republik Indonesia. Dan Undang-Undang Nomor 27 Tahun 202202 tentang Perlindungan Data Pribadi (UU PDP).

c. Analisis Bahan Hukum

Analisis bahan hukum dilakukan secara kualitatif dengan metode yuridis normatif. Bahan hukum primer dan sekunder dianalisis secara kritis untuk menilai konsistensi, relevansi, dan kesesuaiannya dengan prinsip Perlindungan Data Pribadi dalam kerangka perkembangan politik hukum pidana di Indonesia. Analisis ini tidak hanya bertujuan untuk memahami norma hukum yang berlaku, tetapi juga untuk mengevaluasi apakah pengaturan dan Penyelesaian Hukum Perkara Penyebaran Data Pribadi Di Media Massa telah mencerminkan kepastian hukum, perlindungan Hak Asasi Manusia (HAM), dan tujuan pembaruan hukum pidana. Hasil analisis kemudian disintesis untuk merumuskan kesimpulan yang bersifat normatif dan analitis.

C. Hasil dan Pembahasan

Tinjauan Fakta Dan Norma Melalui Undang-Undang Dalam Memberikan Perlindungan Terhadap Penyebaran Data Pribadi Dan Penggunaan Teknologi Informasi

1. Landasan Hukum Di Indonesia

Perkembangan teknologi informasi saat ini telah membawa perubahan yang sangat mendasar terhadap cara manusia berinteraksi, berkomunikasi, dan melakukan aktivitas ekonomi di ruang digital. Internet telah berevolusi dari sekadar media penyampaian informasi menjadi infrastruktur utama kehidupan sosial modern. Dunia maya kini menjadi ruang interaksi yang sangat penting yang dapat menembus batas geografis dan waktu, sehingga memungkinkan terjadinya komunikasi dan transaksi lintas negara secara instan. Transformasi digital ini pun telah mengubah paradigma masyarakat dari aktivitas fisik menjadi aktivitas berbasis data dan jaringan. Hampir setiap tindakan manusia meninggalkan jejak digital yang dapat dianalisis dan dimanfaatkan untuk berbagai kepentingan. Oleh sebab itu, data pribadi menjadi sumber daya baru yang memiliki nilai ekonomi dan strategis yang sangat tinggi.

Selain teori perlindungan hukum, prinsip hukum privasi juga menjadi dasar filosofis penting dalam membentuk kebijakan terkait data pribadi. Konsep privasi sebagai hak fundamental telah diakui dalam berbagai instrumen hukum internasional, seperti Universal Declaration of Human Rights Pasal 12 dan International Covenant on Civil and Political Rights Pasal 17. Privasi diartikan sebagai hak seseorang untuk menentukan sejauh mana informasi pribadinya dapat diketahui atau digunakan oleh pihak lain. Dalam konteks ini, hukum privasi berperan untuk menjaga keseimbangan antara keterbukaan informasi dan perlindungan individu. Oleh karena itu, perlindungan data pribadi merupakan perwujudan konkret dari hak privasi dalam dunia digital.

Penelitian ini menggunakan pendekatan hukum normatif dengan menelaah norma-norma yang berlaku, menganalisis teori hukum yang relevan, serta membandingkan penerapannya secara empiris terbatas. Dengan pendekatan ini, diharapkan diperoleh gambaran objektif mengenai efektivitas pengaturan hukum di kedua negara. Landasan hukum yang menjadi pijakan utama adalah UUD 1945, UU No. 11 Tahun 2008 tentang ITE beserta perubahannya, UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP), serta PDPA 2012 di Singapura.

Dalam konteks hukum, data pribadi berkaitan erat dengan hak privasi yang merupakan hak asasi manusia. Hak ini diakui secara universal, termasuk dalam konstitusi Indonesia dan sistem hukum Singapura melalui berbagai instrument internasional seperti Universal Declaration of Human Rights (UDHR) Pasal 12 dan International Covenant on Civil and Political Rights (ICCPR) Pasal 17, yang menegaskan larangan intervensi sewenang-wenang terhadap kehidupan pribadi seseorang. Dalam konteks nasional, UUD 1945 melalui Pasal 28G ayat (1) menegaskan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya. Dengan demikian, pengaturan terhadap data pribadi bukan hanya kebutuhan administratif, melainkan kewajiban negara untuk menjamin hak konstitusional warga. Namun, penyebaran data pribadi tanpa persetujuan pemiliknya kerap terjadi, baik melalui media sosial, platform e-commerce, maupun lembaga publik. Di Indonesia, berbagai kasus kebocoran data memperlihatkan lemahnya pengawasan terhadap penyelenggara sistem elektronik.

Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan regulasi pertama yang mengatur aktivitas digital, termasuk pengelolaan informasi elektronik. Pasal 26 UU ITE memberikan perlindungan terhadap data pribadi dengan mengatur bahwa penggunaan data pribadi seseorang melalui media elektronik harus dilakukan atas persetujuan yang bersangkutan. Namun, norma tersebut bersifat umum dan belum mengatur detail tentang pengumpulan, penyimpanan, serta penghapusan data pribadi. Oleh karena itu, UU ITE kemudian dilengkapi dengan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang menjadi regulasi khusus (*lex specialis*) di bidang ini.

2. Landasan Hukum di Singapura

Singapura merupakan negara pertama di kawasan Asia Tenggara dan menjadi pelopor yang berhasil menerapkan kerangka hukum komprehensif dalam bidang perlindungan data pribadi melalui Personal Data Protection Act (PDPA) yang disahkan pada tahun 2012. Undang-undang ini mulai diimplementasikan secara penuh pada tahun 2014 dan diamandemen secara signifikan pada tahun 2020 untuk menyesuaikan diri dengan perkembangan teknologi digital, ekonomi berbasis data, serta meningkatnya ancaman terhadap keamanan siber. Langkah Singapura ini menandai komitmen serius negara tersebut dalam menyeimbangkan antara kebutuhan inovasi ekonomi digital dengan perlindungan hak privasi warga negaranya.

PDPA mulai diimplementasikan secara penuh pada tahun 2014 setelah melalui masa transisi yang memungkinkan pelaku usaha dan lembaga publik menyesuaikan kebijakan internalnya. Pemerintah Singapura, melalui Personal Data Protection Commission (PDPC), memainkan peran sentral dalam pengawasan pelaksanaan undang-undang ini. PDPC diberi kewenangan untuk mengeluarkan pedoman teknis, melakukan penyelidikan, serta menjatuhkan sanksi administratif terhadap pelanggaran. Langkah ini menunjukkan pendekatan *compliance-based enforcement*, di mana pengawasan lebih menekankan kepatuhan dan edukasi daripada sekadar pemberian hukuman.

Salah satu keunggulan PDPA terletak pada kejelasan prinsip dasar perlindungan data yang mencakup sepuluh pilar utama, di antaranya *consent*, *purpose limitation*, *access and correction*, dan *protection obligation*. Prinsip *consent* mewajibkan organisasi memperoleh persetujuan individu sebelum mengumpulkan atau memproses data pribadinya (Gustryan & Hoesein, 2025). Sementara *protection obligation* mengharuskan organisasi menerapkan langkah keamanan yang wajar untuk mencegah akses tidak sah atau kebocoran data. Melalui prinsip-prinsip ini,

PDPA tidak hanya berfungsi sebagai instrumen hukum, tetapi juga panduan etis bagi pengelolaan data secara bertanggung jawab.

Pendekatan integratif antara PDPA dan CMCA memungkinkan Singapura menjalankan mekanisme *ex ante* compliance dan *ex post* enforcement secara seimbang. Melalui mekanisme *ex ante*, organisasi dituntut membangun tata kelola data yang baik sebelum insiden terjadi. Sebaliknya, *ex post* enforcement memastikan bahwa ketika pelanggaran tetap terjadi, negara memiliki perangkat hukum untuk menindak semua pihak, baik pelaku kriminal maupun organisasi yang lalai. Pola ini menciptakan sistem hukum yang menysar seluruh rantai risiko digital. Dengan adanya pencegahan sebelum kejadian dan penindakan setelahnya, Singapura mampu menutup ruang bagi potensi kebocoran data dari kedua sisi. Pendekatan dualistik ini juga menegaskan bahwa perlindungan data bukan hanya kewajiban organisasi tetapi juga tanggung jawab negara. Sinergi ini menjadikan penegakan hukum lebih efektif. Struktur semacam ini jarang ditemukan pada yurisdiksi lain di Asia Tenggara.

Pendekatan yang menekankan kepatuhan korporasi sekaligus penghormatan terhadap hak-hak media menjadikan PDPA sebagai model regulasi yang stabil dan adaptif. Negara tidak hanya menuntut tanggung jawab dari pelaku usaha, tetapi juga menyediakan ruang kebebasan yang terkontrol bagi media untuk menjalankan fungsi sosialnya. Dengan demikian, hukum berperan sebagai mediator antara berbagai kepentingan yang saling beririsan.

Dengan mempertahankan keseimbangan antara perlindungan privasi individu dan kebutuhan keterbukaan informasi publik, Singapura menunjukkan bahwa regulasi perlindungan data dapat berjalan seiring dengan prinsip transparansi dan kebebasan berekspresi. Model ini menegaskan bahwa tata kelola data pribadi yang efektif harus berakar pada nilai hukum, institusi yang kuat, dan kepekaan terhadap dinamika sosial yang terus berkembang.

Perbandingan Penyelesaian Perkara Dan Sistem Pembuktian Perkara Terkait Dengan Undang-Undang Ite Dan Perlindungan Data Pribadi Di Indonesia Dan Singapura

Perbandingan Pengaturan dan Penyelesaian Perkara Penyebaran Data Pribadi di Indonesia

Perbandingan antara Indonesia dan Singapura dalam hal penyelesaian perkara penyebaran data pribadi sangat penting untuk melihat sejauh mana kedua negara mampu memberikan perlindungan hukum yang efektif bagi korban. Indonesia mengandalkan kombinasi dua instrumen hukum—UU ITE dan UU PDP—yang masing-masing memiliki ruang lingkup berbeda namun saling melengkapi (Ramli, 2021). UU ITE fokus pada larangan tindakan penyebaran informasi secara melawan hukum, termasuk data pribadi, sedangkan UU PDP mengatur secara komprehensif tata kelola data oleh pengendali dan prosesor data. Di sisi lain, Singapura menggunakan PDPA sebagai regulasi utama yang telah lama berlaku dan lebih matang, disertai dukungan Computer Misuse and Cybersecurity Act (CMCA) sebagai basis penegakan pidana. Perbedaan historis dan struktur kelembagaan ini membuat Singapura dianggap lebih siap dalam menangani pelanggaran data pribadi dibanding Indonesia. Namun, perkembangan regulasi ini baru dimulai dalam beberapa tahun terakhir. Sebaliknya, Singapura telah mengembangkan kerangka hukum perlindungan data sejak 2012 melalui PDPA.

Perbedaan lainnya terlihat pada lembaga pengawas yang menangani perlindungan data pribadi. Indonesia baru membentuk struktur kelembagaan di bawah Kementerian Komunikasi dan Informatika serta mempersiapkan badan pengawas PDP yang masih dalam tahap pembentukan. Kekosongan kelembagaan ini sering menyebabkan ketidakseragaman dalam penyelesaian sengketa. Sebaliknya, Singapura telah memiliki Personal Data Protection Commission (PDPC) sejak 2013 sebagai regulator yang independen. PDPC memiliki kewenangan investigatif, edukatif, dan adjudikatif yang jelas. Keberadaan lembaga ini mempercepat proses penyelesaian perkara. Struktur kelembagaan tersebut menambah keunggulan Singapura dalam governance data pribadi.

Dari segi efektivitas, Singapura juga unggul dalam hal konsistensi penegakan hukum. PDPC secara rutin menerbitkan laporan investigasi, pedoman teknis, dan putusan yang dapat diakses publik, sehingga menciptakan transparansi dan predictability dalam proses hukum. Sementara itu, Indonesia masih menghadapi tantangan dalam konsistensi penegakan karena infrastruktur hukum digital belum sepenuhnya mapan. Selain itu, koordinasi antarinstansi sering menjadi kendala dalam penanganan kasus penyebaran data pribadi. Kurangnya preseden hukum juga membuat banyak kasus sulit ditangani secara cepat. Kekuatan regulasi Singapura muncul dari pengalaman panjang dan sistem yang sudah teruji.

Perbandingan Pengaturan dan Penyelesaian Perkara Penyebaran Data Pribadi P di Indonesia

Prinsip accountability merupakan pilar lain yang menjadi ciri khas PDPA dan membedakannya dari banyak model perlindungan data di kawasan Asia Tenggara. Di bawah prinsip ini, organisasi tidak hanya diwajibkan memenuhi ketentuan PDPA, tetapi juga harus dapat membuktikan bahwa kepatuhan tersebut dilaksanakan secara nyata (Nonet, Philippe, and Philip Selznick, 1978). Artinya, dokumentasi internal harus menunjukkan bahwa kebijakan dan prosedur sebenarnya diterapkan dalam operasional sehari-hari. Pendekatan ini menciptakan standar tata kelola data yang tinggi dan mendorong organisasi menerapkan budaya perlindungan data. Dengan adanya kewajiban akuntabilitas, proses audit PDPC dapat berjalan lebih efektif. Selain itu, organisasi dituntut untuk membangun mekanisme mitigasi risiko yang berkelanjutan. Prinsip ini pada akhirnya memperkuat posisi PDPA sebagai instrumen regulasi modern.

Keterbatasan inilah yang mendorong lahirnya UU PDP pada tahun 2022 sebagai upaya memperbaiki fragmentasi regulasi yang sebelumnya ada. UU PDP memperkenalkan kerangka perlindungan data pribadi yang lebih komprehensif sekaligus menyediakan mekanisme administratif yang memungkinkan penegakan hukum lebih cepat dan terarah. Dalam rezim baru ini, pengendali data dapat dikenai sanksi administratif tanpa perlu melalui proses pengadilan. Meskipun demikian, implementasi penuh UU PDP masih menunggu pembentukan otoritas pengawas yang memiliki kewenangan operasional. Artinya, selama masa transisi, korban tetap menghadapi tantangan struktural dalam mencari pemulihan.

Di Indonesia, perlindungan data pribadi awalnya tersebar dalam berbagai peraturan sektoral, terutama melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). UU ITE memberikan dasar hukum terhadap penyalahgunaan data dalam sistem elektronik, meskipun belum mengatur secara rinci hak subjek data. Kebutuhan akan regulasi yang lebih komprehensif mendorong lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Kehadiran UU PDP menandai perubahan signifikan dalam sistem hukum Indonesia. Regulasi ini menyatukan prinsip, hak, kewajiban, serta sanksi dalam satu instrumen hukum. Dengan demikian, Indonesia mulai membangun rezim perlindungan data yang lebih terstruktur.

Keunggulan utama sistem Singapura terletak pada keberadaan Personal Data Protection Commission (PDPC) sebagai lembaga pengawas independen. PDPC memiliki kewenangan luas dalam pengawasan, investigasi, dan penjatuhan sanksi terhadap pelanggaran PDPA. Lembaga ini juga aktif mengeluarkan pedoman teknis untuk membantu organisasi memahami kewajiban hukumnya. Kejelasan peran dan kewenangan PDPC memperkuat efektivitas penegakan hukum data pribadi. Hal ini menciptakan kepastian hukum bagi pelaku usaha dan perlindungan nyata bagi masyarakat. Struktur kelembagaan yang kuat menjadi faktor kunci keberhasilan sistem Singapura.

Kesulitan identifikasi pelaku menjadi tantangan lain yang cukup signifikan, terutama ketika tindakan dilakukan oleh pihak luar negeri. Banyak serangan atau kebocoran data berasal dari jaringan yang menggunakan server anonim atau berlokasi di yurisdiksi asing. Hal ini menyebabkan proses tracing membutuhkan kerja sama lintas negara yang tidak selalu mudah dijalankan. Mekanisme mutual legal assistance membutuhkan waktu dan persyaratan administratif yang panjang. Di sisi lain, pelaku kejahatan siber biasanya bergerak cepat dan

adaptif. Kompleksitas teknis dan hukum ini menyebabkan banyak kasus akhirnya tidak terselesaikan (Budhijanto,2010). Banyak kasus besar di Indonesia seperti kebocoran data KPU (Komisi Pemilihan Umum), Tokopedia dan Bukalapak tidak berujung pada pemidanaan yang jelas. Meskipun kasus tersebut telah menarik perhatian masyarakat luas, proses penanganannya sering kali berhenti pada tahap investigasi awal. Minimnya pembaruan informasi dari pihak pemerintah menyebabkan publik tidak mengetahui perkembangan selanjutnya. Kondisi ini menunjukkan adanya kesenjangan antara ekspektasi publik dan kapasitas lembaga penegak hukum. Ketiadaan penyelesaian yang tegas memperkuat persepsi bahwa kejahatan siber tidak dipandang sebagai ancaman serius. Hal ini merugikan masyarakat sebagai pemilik data pribadi.

Perbedaan berikutnya berkaitan dengan penegakan hukum atas penyebaran data pribadi yang melibatkan pihak swasta. Singapura memberikan sanksi administratif yang sangat berat kepada korporasi yang lalai melindungi data subjek, termasuk denda mencapai 10% dari pendapatan tahunan bagi perusahaan besar. Indonesia baru mengenal model sanksi administratif ini setelah hadirnya UU PDP, namun mekanisme implementasinya masih sangat bergantung pada pembentukan lembaga otoritatif yang hingga kini belum memiliki kewenangan setara PDPC. Di sisi lain, penegakan hukum pidana di Indonesia masih lebih mengandalkan aparat penegak hukum konvensional seperti Polri dan Kejaksaan. Sementara itu, Singapura memadukan mekanisme administratif dan pidana secara proporsional sehingga penegakan dilakukan secara teknis, cepat, dan responsif terhadap perkembangan insiden siber. Hal ini memberikan rasa aman yang lebih tinggi bagi korban pelanggaran data.

Dalam hal penyebaran data pribadi melalui media massa, Indonesia cenderung menekankan aspek larangan dan sanksi, sebagaimana tercantum dalam Pasal 27 ayat (1) serta Pasal 36 UU ITE yang mengatur ancaman pidana bagi pelaku. Namun, UU ITE tidak memberikan batasan teknis yang memadai untuk mengatur tanggung jawab platform media massa atau media daring apabila terjadi kebocoran karena kelalaian internal. UU PDP mulai menambal kekosongan tersebut, tetapi masih memerlukan banyak peraturan turunan. Sebaliknya, PDPA secara langsung mengatur tanggung jawab organisasi, baik media, penyedia platform, maupun pemegang data yang bertindak lalai. Model tanggung jawab korporasi ini menciptakan jaminan lebih komprehensif bagi korban, terutama ketika penyebaran data terjadi tanpa persetujuan yang sah. Perbandingan ini menunjukkan tingkat kedewasaan sistem hukum yang berbeda di antara kedua negara.

Perbandingan juga dapat dilihat dari kewajiban pelaporan insiden kebocoran data (data breach notification). Di Singapura, kewajiban ini bersifat wajib untuk setiap organisasi yang mengalami insiden signifikan, dan laporan harus disampaikan kepada PDPC dalam waktu 72 jam. Kewajiban ini menciptakan transparansi serta memudahkan investigasi sejak tahap awal. Di Indonesia, kewajiban pelaporan sudah dimasukkan ke dalam UU PDP, tetapi implementasi teknisnya masih menunggu peraturan lanjutan, sehingga efektivitasnya belum terukur. Ketidakhadiran mekanisme pelaporan yang cepat membuat banyak kasus penyebaran data pribadi di Indonesia sulit ditangani secara tepat waktu. Dari sudut pandang korban, hal ini menunda pemulihan hak dan akses terhadap keadilan. Perbedaan ini menunjukkan bahwa Singapura unggul dalam aspek responsiveness.

Dalam menilai efektivitas mekanisme pengawasan, terlihat bahwa Singapura lebih menekankan aspek proaktif melalui kebijakan audit berkelanjutan terhadap organisasi yang mengelola data pribadi. PDPC secara berkala melakukan pemeriksaan kepatuhan terhadap perusahaan-perusahaan yang dianggap memiliki risiko tinggi, seperti sektor kesehatan, keuangan, dan telekomunikasi. Di Indonesia, mekanisme audit kepatuhan berdasarkan UU PDP masih bersifat parsial dan belum dilakukan secara menyeluruh terhadap seluruh organisasi. Ketika audit dilakukan, ia sering bersifat reaktif, yaitu setelah pelanggaran terjadi. Pendekatan reaktif ini menyebabkan lemahnya deteksi pelanggaran sebelum menimbulkan kerugian besar pada korban. Jika Indonesia ingin memperkuat jaminan keamanan data pribadi, pola pengawasan perlu bergeser menjadi proaktif seperti di Singapura, dengan audit berkala yang menekankan mitigasi risiko.

Lingkup yurisdiksi merupakan aspek lain yang memberikan perbedaan mencolok. PDPA Singapura berlaku terhadap organisasi luar negeri yang memproses data milik individu di Singapura, meskipun organisasi tersebut tidak berkedudukan di Singapura. Pendekatan extraterritorial ini memperkuat perlindungan warga Singapura terhadap ancaman global. UU PDP Indonesia belum sepenuhnya menerapkan kewenangan extraterritorial sehingga sering kali sulit menindak organisasi luar negeri yang memproses data warga negara Indonesia tanpa konsen yang sah. Dalam ekosistem digital yang tidak mengenal batas negara, yurisdiksi extraterritorial menjadi alat penting untuk menjaga keamanan data pribadi. Indonesia perlu mengadopsi model serupa agar dapat memberikan perlindungan hukum yang setara dengan standar internasional.

Secara keseluruhan, perbandingan sistem hukum Indonesia dan Singapura dalam penyelesaian perkara penyebaran data pribadi menunjukkan bahwa efektivitas perlindungan korban sangat dipengaruhi oleh integrasi antar-aspek regulatif, administratif, dan teknis. Singapura telah membangun ekosistem perlindungan data yang matang, sedangkan Indonesia masih dalam proses menyempurnakan kerangka hukumnya. Hasil analisis ini menegaskan bahwa pembaruan legislasi, perbaikan tata kelola, serta peningkatan kapasitas aparat penegak hukum merupakan langkah penting untuk memastikan perlindungan data pribadi yang efektif dan memberikan rasa aman serta keadilan bagi korban di Indonesia. Dengan adopsi kebijakan yang tepat, Indonesia dapat mencapai tingkat perlindungan yang setara dengan praktik terbaik internasional.

D. Kesimpulan

Berdasarkan hasil penelitian perbandingan mengenai penyelesaian perkara dan sistem pembuktian penyebaran data pribadi di Indonesia dan Singapura, dapat disimpulkan bahwa kedua negara memiliki komitmen yang sama dalam melindungi data pribadi sebagai bagian dari hak privasi individu di era digital. Namun demikian, perbedaan pendekatan regulatif, kelembagaan, serta mekanisme penegakan hukum menyebabkan tingkat efektivitas perlindungan data pribadi di masing-masing negara berbeda secara signifikan.

Dalam menjawab rumusan masalah pertama, penelitian ini menunjukkan bahwa penyelesaian perkara penyebaran data pribadi di Indonesia dan Singapura memiliki karakteristik yang berbeda. Di Indonesia, sebelum lahirnya Undang-Undang Perlindungan Data Pribadi (UU PDP), penyelesaian perkara penyebaran data pribadi lebih banyak bergantung pada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang berorientasi pada pendekatan penal. Akibatnya, perlindungan terhadap korban sering kali terhambat oleh proses pidana yang panjang dan kompleks. Kehadiran UU PDP pada tahun 2022 memperluas mekanisme penyelesaian perkara melalui jalur administratif dan perdata, namun efektivitasnya masih terbatas karena lembaga pengawas data pribadi belum sepenuhnya terbentuk dan operasional.

Sebaliknya, Singapura melalui Personal Data Protection Act (PDPA) telah menyediakan mekanisme penyelesaian perkara yang lebih terintegrasi dan efektif. Penyelesaian pelanggaran data pribadi tidak semata-mata ditempuh melalui jalur pidana, melainkan lebih menekankan mekanisme administratif yang dijalankan oleh Personal Data Protection Commission (PDPC). PDPC memiliki kewenangan luas untuk melakukan pengawasan, investigasi, serta menjatuhkan sanksi administratif seperti denda, perintah korektif, dan enforcement directions. Mekanisme ini memberikan perlindungan yang lebih cepat dan responsif bagi korban, sekaligus menciptakan kepastian hukum bagi pelaku usaha. Dengan demikian, dari aspek penyelesaian perkara, sistem Singapura dinilai lebih efektif dan berorientasi pada pemulihan hak subjek data.

Terkait rumusan masalah kedua mengenai sistem pembuktian, penelitian ini menemukan bahwa Indonesia masih menghadapi berbagai kendala dalam pembuktian perkara penyebaran data pribadi. Meskipun UU ITE telah mengakui alat bukti elektronik sebagai alat bukti yang sah dan UU PDP memperkuat dasar pertanggungjawaban pengendali data, proses pembuktian tetap sangat bergantung pada hukum acara pidana dan perdata yang bersifat formalistik. Tantangan utama muncul dalam aspek autentikasi, integritas, dan penelusuran bukti digital, yang sering kali menyulitkan korban untuk membuktikan adanya pelanggaran data pribadi secara efektif.

Di Singapura, sistem pembuktian dinilai lebih mapan dan adaptif terhadap perkembangan teknologi informasi. Pengaturan dalam Evidence Act memperkuat kedudukan bukti digital,

sementara PDPC memiliki kewenangan administratif untuk mengumpulkan, menilai, dan menggunakan bukti elektronik dalam proses penegakan hukum. Beban pembuktian yang lebih proporsional serta dukungan standar teknis investigasi siber menjadikan proses pembuktian lebih efisien dan tidak sepenuhnya membebani korban. Dengan demikian, sistem pembuktian di Singapura lebih mampu menjawab tantangan pembuktian dalam perkara penyebaran data pribadi di era digital.

Secara keseluruhan, hasil penelitian menunjukkan bahwa Singapura unggul dalam aspek efektivitas penyelesaian perkara dan sistem pembuktian karena didukung oleh regulasi yang terintegrasi dan kelembagaan pengawas yang kuat. Sementara itu, Indonesia telah berada pada jalur pembaruan hukum yang tepat melalui pembentukan UU PDP, namun masih memerlukan penguatan kelembagaan, harmonisasi regulasi, serta peningkatan kapasitas penegak hukum agar perlindungan data pribadi dapat terlaksana secara optimal.

E. Referensi

- Personal Data Protection Commission Singapura.
- Asshiddiqie, J. (2018). Pengantar ilmu hukum tata negara. Jakarta: RajaGrafindo Persada.
- Budhijanto, D. (2010). Cyber law: Perlindungan hukum terhadap kejahatan dunia maya. Bandung: Refika Aditama.
- Computer Misuse Act 1993 (CMA) dirancang untuk mengatasi kejahatan siber.
- Gustryan, & Hoesein. (2025). Peran Undang-Undang ITE dan UU PDP dalam perlindungan data dan privasi di era ekonomi digital. *Jurnal Minfo Polgan*.
https://jdih.tanjungpinangkota.go.id/data_file/3201/Pengaturan%20Perlindungan%20Data%20Pribadi%20di%20Indonesia%20Perspektif%20Teori%20Keadilan%20Bermartabat.pdf
- Latumahina, R. E. (2014). Aspek hukum perlindungan data pribadi di dunia maya. *Jurnal Gema Aktualita*, 3(2).
- Marzuki, P. M. (2008). Pengantar ilmu hukum. Jakarta: Kencana.
- Nonet, P., & Selznick, P. (1978). *Law and society in transition: Toward responsive law*. New York, NY: Harper & Row.
- Nusamedia. (2020). Pengaturan perlindungan data pribadi di Indonesia perspektif teori keadilan bermartabat. Diakses 27 Desember 2024, dari PDPC Annual Report (setiap tahun relevan dengan konteks implementasi)
- Personal Data Protection Act 2012 (PDPA) mengatur perlindungan data pribadi di Singapura, Rahardjo, S. (2014). Ilmu hukum. Bandung: Citra Aditya Bakti.
- Ramli, A. M. (2021). Tantangan penegakan hukum UU ITE. *Jurnal Legislasi Indonesia*, 18(2), 145–160.
- Setiowati, I. (2022). Analisis yuridis penerapan sanksi pidana bagi pelaku judi online melalui informasi dan transaksi elektronik (Proposal tesis). Universitas Esa Unggul, Jakarta.
- Singapura. Personal Data Protection (Amendment) Act 2020.
- Singapura. Personal Data Protection (Enforcement) Regulations.
- Singapura. Personal Data Protection (Notification of Data Breaches) Regulations. PDPC.
- Singapura. Personal Data Protection Act 2012 (PDPA).
- Sunggono, B. (2003). Metodologi penelitian hukum. Jakarta: Raja Grafindo Persada.
- Sutanto, H. (2020). Pembuktian alat bukti elektronik dalam perkara pidana. *Jurnal Hukum dan Peradilan*, 9(1), 55–72.
- Warsita, B. (2011). Landasan teori dan teknologi informasi dalam pengembangan teknologi pembelajaran. *Jurnal Teknodik*, 15(1). Diakses 23 Mei 2024.