MATRA PEMBARUAN
Jurnal Inovasi Kebijakan

ARTIKEL

Akuntabilitas dalam Kebijakan Perlindungan Data Pribadi di Indonesia

Belajar dari Korea Selatan dan Singapura

Accountability in Personal Data Protection Policy in Indonesia

Learning from South Korea and Singapore

Lailatul Badriah [1], **Dwiyanto Indiahono** [2], **Sukarso** [3]

[1, 2, 3] Magister Administrasi Publik, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Jenderal Soedirman, Purwokerto, Indonesia

badriatul.lailatul59@gmail.com

Abstrak: Artikel ini meneliti nilai akuntabilitas dalam kebijakan perlindungan data pribadi di Korea Selatan, Singapura, dan Indonesia dengan tujuan utama menjadi kerangka kerja inovasi bagi Indonesia. Penelitian ini menekankan komparasi strategi inovatif pada lima aspek: pendefinisian data pribadi yang dilindungi, mekanisme pengumpulan dan transfer data pribadi, mekanisme inovatif pelaporan pelanggaran data, dan mekanisme dalam memberikan sanksi serta kompensasi akibat pelanggaran data. Dengan metode kualitatif dan pendekatan *content analysis* terhadap *Personal Information Protection Act* (PIPA) Korea Selatan, *Personal Data Protection Act* (PDPA) Singapura, dan UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi milik Indonesia, menghasilkan temuan yang menggarisbawahi pentingnya inovasi kebijakan yang akuntabel guna memastikan perlindungan hak-hak individu dan memberdayakan lembaga otoritas perlindungan data pribadi. Implikasi utama ditujukan bagi Indonesia, di antaranya agar segera mengimplementasikan UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi, membentuk lembaga otoritas perlindungan data terpusat, dan mendorong *Public-Private Partnerships* untuk meningkatkan akuntabilitas dalam perlindungan data pribadi.

Abstract: *This article examines the value of accountability in personal data protection policies in South Korea, Singapore and Indonesia with the main objective of providing a framework for innovation for Indonesia. This research emphasizes the comparison of innovative strategies in five aspects: defining protected personal data, mechanisms for collecting and transferring personal data, innovative mechanisms for reporting data breaches, and mechanisms for providing sanctions and compensation for data breaches. Using a qualitative method and content analysis approach to South Korea's Personal Information Protection Act (PIPA), Singapore's Personal Data Protection Act (PDPA), and Indonesia's Law No. 27 of 2022 on Personal Data Protection, the findings underscore the importance of accountable policy innovation to ensure the protection of individual rights and empower the institution of personal data protection authorities. The main implications are for Indonesia to immediately implement Law No. 27 of 2022 on Personal Data Protection, establish a centralized data protection authority, and encourage Public-Private Partnerships to improve accountability in personal data protection.*

OPEN ACCESS

Sitasi: Badriah, L., Indiahono, D., & Sukarso, S. (2024). Akuntabilitas dalam Kebijakan Perlindungan Data Pribadi di Indonesia: Belajar dari Korea Selatan dan Singapura. *Matra Pembaruan: Jurnal Inovasi Kebijakan, 8*(2), 89-102. https://doi.org/10.21787/mp.8.2.2024.89-102

Dikirim: 26 Juni 2024
Diterima: 28 November 2024
Diterbitkan: 31 Desember 2024

Kata Kunci: Inovasi, Kebijakan, Akuntabilitas, Mekanisme Perlindungan, Data Pribadi.

Abstract: *innovation, policy, accountability, protection mechanisms, personal data.*

1. Pendahuluan

Akuntabilitas dalam perlindungan data pribadi merupakan wacana mengenai pentingnya data pribadi dan privasi, khususnya di era digital, yang terbentuk karena meningkatnya insiden pelanggaran data, kegiatan berbagi data yang tidak sah, dan pelanggaran privasi yang telah menimbulkan kekhawatiran tentang perlindungan data pribadi. Hal ini sehubungan dengan adanya minat yang lebih besar pada data pribadi yang dianggap sebagai bagian dari *cybercrime-security and criminology* secara lebih luas (Walters & Coghlan, 2019). Informasi pribadi yang diunggah ke media sosial, terutama informasi lokasi, akan menjadi informasi milik subjek analisis konsumen atau analisis bisnis, dan target pemantauan pemerintah (Boyd & Crawford, 2011). Data pribadi juga digunakan untuk mengatur kelompok sasaran iklan dari sudut pandang riset pemasaran, atau menjadi subjek analisis untuk menangkap mata-mata atau mencegah kejahatan dari sudut pandang keamanan nasional (Smith et al., 2012).

Tren privasi data global seperti *Personal Data Protection Regulation* (GDPR) di Uni Eropa telah menetapkan standar untuk akuntabilitas dan perlindungan data. Beberapa standar utama yang ditetapkan dalam GDPR Uni Eropa adalah: definisi data pribadi; memberikan berbagai hak kepada subjek data; pemrosesan data pribadi secara sah, adil, dan transparan; pemberitahuan pelanggaran data; penunjukkan Petugas Perlindungan Data; dan transfer data internasional dengan persyaratan yang ketat (European Union Agency for Fundamental Rights & Council of Europe, 2018).

Di samping itu, era administrasi publik digital juga membutuhkan pembangunan akuntabilitas yang berfokus pada tanggung jawab kolektif dan individu. Beberapa tantangan untuk mencapai akuntabilitas yang efektif dalam lingkungan kolektif ini, yaitu: mengenali dualitas tanggungjawab, mengatasi perubahan yang dipengaruhi TIK, risiko terhadap akuntabilitas, pembagian kerja dan akuntabilitas, dan dampak TIK pada akuntabilitas (Brown, 2013). Dengan demikian, untuk menyeimbangkan privasi individu dan akuntabilitas publik dalam berbagi data, diusulkan suatu pendekatan legal-teknis terpadu (Young et al., 2019), yang dapat berfungsi sebagai dasar kepercayaan data dalam berbagai konteks, sehingga memungkinkan lembaga pemerintah, peneliti, dan publik untuk mengakses data pribadi sambil memastikan privasi dan akuntabilitas.

Meski demikian, tantangan utama akuntabilitas dalam konteks *e-government* mencakup kompleksitas hubungan akuntabilitas yang beragam, ambiguitas dalam konsep akuntabilitas, dan potensi konflik tuntutan dari berbagai pemangku kepentingan (Al-Shbail & Aman, 2018). *E-Government* dapat meningkatkan kompleksitas hubungan akuntabilitas dengan memperkenalkan saluran komunikasi dan interaksi baru antara lembaga pemerintah dan masyarakat. Maka, *e-governance* yang akuntabel melibatkan jaminan 'akuntabilitas yang dirancang' untuk situs penyedia layanan pemerintah (Sharma et al., 2021)). Penelitian Sharma et al (2021) mengidentifikasi dimensi penting akuntabilitas yang dapat membantu mencapai hal tersebut ialah: transparansi, pengendalian, *responsibility*, daya tanggap, *liability*, keamanan, dan privasi.

Korea Selatan dan Singapura adalah salah dua negara yang telah menunjukkan kemajuan signifikan dalam pengembangan *e-government*. Korea Selatan adalah negara Asia terdepan dalam *e-government* yang telah memperlihatkan pengalaman transformasi dari lembaga pemerintahan yang tidak efisien menjadi penyedia layanan publik yang efisien melalui implementasi *e-government* (Kim et al., 2007). Sedang Singapura adalah satu-satunya negara di Asia Tenggara dengan *E-Government* Development Index (EGDI) tertinggi, bersaing dengan negara-negara maju seperti Eropa dan Amerika Serikat (Arief, 2023). Pemerintah Singapura dan Korea Selatan juga telah memiliki inisiatif untuk mempromosikan perlindungan data dan keamanan

siber dalam tata kelola digital, dimana pengelolaan data pribadi dan regulasi perlindungannya menjadi dasar bagi pengontrol data untuk mengembangkan kebijakan umum dan membuat keputusan yang signifikan bagi masyarakat (Hisbulloh, 2021; Sautunnida, 2018; Sinaga, 2020; Sloot, 2017; Yuniarti, 2019).

Kerangka kebijakan perlindungan data pribadi menjadi isu yang penting untuk dapat mengakomodasi kepentingan individu atas perlindungan privasi dan keamanan informasi, serta kepentingan negara dalam mengemban pelayanan publik melalui pemanfaatan data pribadi masyarakat (Rahman, 2021). Dalam upaya memperkuat implementasi kebijakan yang responsif dan efektif, inovasi telah menjadi kunci dalam optimalisasi perlindungan data pribadi di berbagai negara, termasuk Korea Selatan dan Singapura. Sedangkan, kebijakan data pribadi Indonesia ketika dibandingkan dengan Korea Selatan dan Singapura masih jauh belum optimal. Oleh karena itu, inovasi kebijakan perlindungan data pribadi menjadi salah satu urgensi dalam menghadapi kompleksnya tantangan era digital di Indonesia saat ini.

Kelemahan kebijakan perlindungan data pribadi di Indonesia dibandingkan dengan Korea Selatan dan Singapura tersebut mencakup belum diimplementasikannya UU Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi sehingga standar dan praktik keamanan data belum ada. Kesadaran dan pendidikan masyarakat Indonesia juga terbatas mengenai hak privasi data, belum adanya pengawas peraturan dan aktivitas pemrosesan data, serta potensi infrastruktur teknologi yang kurang berkembang untuk perlindungan data. Kelemahan-kelemahan ini dapat berkontribusi pada tingginya risiko pelanggaran data, perlindungan informasi pribadi yang tidak memadai, dan kurangnya mekanisme yang kuat untuk memastikan kepatuhan terhadap peraturan perlindungan data. Dengan demikian, penelitian ini akan memperlihatkan betapa mendesaknya kebutuhan Indonesia akan inovasi kebijakan perlindungan data pribadi yang akuntabel dalam menghadapi kompleksitas lingkungan digital yang terus berkembang. Fokus penelitian ini terletak pada: akuntabilitas pemenuhan hak-hak publik terkait perlindungan data pribadi di Korea Selatan, Singapura, dan Indonesia; akuntabilitas mekanisme perlindungan data pribadi di negara-negara tersebut; dan akuntabilitas kebijakan dalam menangani kasus-kasus pelanggaran data pribadi.

2. Metode

Penelitian ini menggunakan metode kualitatif dengan sumber data berupa dokumen, termasuk: *Singapore Personal Data Protection Act* (PDPA), The *Personal Information Protection Act* (PIPA), UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi, dan dokumen resmi lainnya yang relevan, sehingga teknik pengumpulan datanya ialah dokumentasi. Analisis data kemudian dilakukan menggunakan *Qualitative Content Analysis* (QCA), yaitu suatu metode untuk mendeskripsikan makna materi kualitatif secara sistematis (Schreier, 2012).

Dalam menganalisis dokumen kebijakan pada penelitian komparatif, QCA mengharuskan untuk 'menerjemahkan' semua makna dalam materi yang diminati ke dalam kategori pengkodean, serta mengklasifikasikan bagian-bagian materi secara berurutan menurut kategori-kategori pengkodean tersebut (Schreier, 2012). Lebih lanjut, penelitian ini menggunakan pendekatan hermeneutika untuk melakukan pemaknaan dan penafsiran dokumen kebijakan dari ketiga negara tersebut. Langkah-langkah dalam pendekatan ini meliputi: mempersiapkan studi, analisis, interpretasi, kontekstualisasi, dan presentasi (Nuyen, 1994).

3. Hasil dan Pembahasan

Melalui studi komparatif, penelitian ini mengeksplorasi lima aspek untuk dijadikan tolak ukur dalam penilaian keunggulan akuntabilitas kebijakan perlindungan data pribadi di ketiga negara. Masing-masing aspek tersebut kemudian memiliki sub-aspek untuk lebih memfokuskan pengukurannya. Lebih lanjut dapat diuraikan sebagai berikut:

Table 1. Aspek Penilaian Akuntabilitas Kebijakan Perlindungan Data Pribadi

Aspek	Sub-aspek
Definisi data pribadi yang dilindungi	Subjek, objek, dan latar belakang pendefinisian
Mekanisme pengumpulan data pribadi	Subjek, metode, dan media yang digunakan
Mekanisme transfer data pribadi	Subjek, metode, dan media yang digunakan
Mekanisme pelaporan pelanggaran perlindungan data pribadi	Subjek, metode, dan media pelaporan yang digunakan
Sanksi atas pelaanggaran perlindungan data pribadi	Subjek, jenis sanksi, dan garansi atau ganti rugi yang diberikan

3.1. Definisi Data Pribadi yang Dilindungi

Ketiga negara mendefinisikan data pribadi sebagai informasi terkait seseorang yang dapat diidentifikasi baik secara langsung maupun tidak langsung (perlu digabungkan atau dikombinasikan dengan informasi lain). Secara keseluruhan, definisi data pribadi di ketiga negara bertujuan untuk melindungi privasi, hak, dan martabat individu.

Table 2. Definisi Data Pribadi di Korea Selatan, Singapura, dan Indonesia

	Korea Selatan	Singapura	Indonesia
Istilah	Informasi pribadi	Data pribadi	Data pribadi
Definisi	Informasi apapun yang berkaitan dengan individu yang masih hidup	Data, baik benar atau tidak, tentang seseorang yang dapat diidentifikasi	Data yang dapat diidentifikasi secara langsung atau digabungkan dengan informasi lain melalui sistem elektronik atau nonelektronik

Pendefinisian data pribadi dalam PDPA, PIPA, dan UU No. 27 Tahun 2022 bertujuan untuk melindungi privasi, hak, dan martabat individu dengan mendefinisikan data pribadi sebagai informasi terkait individu yang dapat diidentifikasi secara langsung atau tidak langsung. PIPA Korea Selatan menggunakan terminologi “informasi pribadi” dan bukan “data pribadi” seperti Singapura dan Indonesia, serta menekankan kemudahan kombinasi dalam mendefinisikan data pribadi. PIPA juga berfokus pada individu yang masih hidup, serta menekankan kendali mereka atas bagaimana informasi pribadi mereka diproses. Hal ini berbeda dengan PDPA Singapura dan UU PDP Indonesia, yang tidak memasukkan konsep “kemudahan kombinasi” sebagai kriteria penentu data pribadi. Penetapan individu yang masih hidup dalam PIPA berarti bahwa cakupan informasi pribadi yang dilindungi undang-undang tidak mencakup individu yang telah meninggal. Hal ini menyoroti fokus pada individu yang masih hidup yang mempunyai hak untuk mengontrol bagaimana informasi pribadi mereka diproses.

Terminologi “benar atau tidak” adalah sorotan dalam konteks definisi data pribadi berdasarkan PDPA Singapura. Terminologi ini berarti bahwa data tersebut dianggap sebagai data pribadi, terlepas dari keakuratannya, bertolak belakang dengan definisi berdasarkan PIPA Korea Selatan yang menjadikan akurasi sebagai salah satu prinsip tujuan dan pendefinisian. Dengan demikian, PDPA mengakui bahwa data pribadi mencakup informasi faktual dan informasi yang berpotensi tidak akurat atau menyesatkan tentang seseorang. Maka, terlepas dari keakuratannya, PDPA memastikan bahwa individu dilindungi tidak hanya ketika datanya benar tetapi juga ketika berhadapan dengan data yang mungkin salah, selama data ini dapat digunakan

untuk mengidentifikasi individu dan masih berpotensi berdampak pada privasi dan hak individu.

Sedangkan terminologi "melalui sistem elektronik atau nonelektronik" dimiliki oleh definisi data pribadi dalam UU PDP Indonesia yang merujuk pada dua cara utama bagi data pribadi dapat diproses atau disimpan. Dengan mempertimbangkan dua metode pengolahan data ini, UU PDP mengatur standar perlindungan dan keamanan yang sama untuk data pribadi, terlepas cara pengolahan dan pemrosesan secara elektronik maupun nonelektronik.

Singapura, Korea Selatan, dan Indonesia telah menerapkan undang-undang perlindungan data pribadi yang mencakup serangkaian informasi di luar rincian data pribadi umum seperti nama lengkap, nomor registrasi nasional, informasi kontak, data biometrik, dan foto. Kategori data lainnya mencakup informasi sensitif, yang memerlukan pemrosesan khusus untuk memastikan keamanan dan perlindungan karena potensi dampaknya terhadap individu jika salah ditangani atau diungkapkan. Ada pula informasi yang disamarkan (*pseudonymized information*), yang diproses sedemikian rupa sehingga individu tidak dapat diidentifikasi tanpa informasi tambahan, sehingga mengurangi risiko akses tidak sah atau penyalahgunaan. Jenis data ini dapat digunakan untuk analisis statistik, penelitian ilmiah, pengarsipan, dan tujuan lainnya tanpa persetujuan eksplisit dari subjek data.

Prinsip-prinsip pendefinisian data pribadi di tiga negara bertujuan untuk melindungi privasi dan hak-hak individu sekaligus memastikan pemrosesan data pribadi yang tepat. Menurut PDPA Singapura, *Data Protection Officer* (DPO) yang bertanggung jawab harus mengambil langkah-langkah untuk memastikan kepatuhan terhadap kewajiban perlindungan data dan menunjukkan kemampuan mereka untuk melakukannya bila diperlukan. Akuntabilitas dalam kebijakan dan praktik perlindungan data menetapkan kerangka kerja dimana DPO bertanggung jawab untuk memenuhi hak-hak subjek data dan juga bertanggung jawab kepada Komisi Perlindungan Data Pribadi.

3.2. Mekanisme Pengumpulan Data Pribadi

Istilah pengumpulan data secara umum mengacu pada setiap tindakan atau serangkaian tindakan yang melaluinya, organisasi memperoleh kendali atas atau memiliki data pribadi (Personal Data Protection Commission Singapore, 2019). Persyaratan umum dalam mekanisme pengumpulan data pribadi di Singapura, Korea Selatan, dan Indonesia adalah untuk mendapatkan persetujuan eksplisit dari subjek data sebelum memproses data pribadi. Persetujuan eksplisit mengacu pada persetujuan yang jelas dan tidak ambigu dari subjek data mengenai pengumpulan dan pemrosesan data pribadi. UU No. 27 Tahun 2022 milik Indonesia merinci persetujuan yang sah, termasuk persetujuan tertulis atau tercatat secara eksplisit, memastikan keabsahan hukum untuk persetujuan elektronik dan nonelektronik. Jika persyaratan persetujuan tidak memenuhi ketentuan yang ditentukan dan tidak menyertakan persetujuan eksplisit yang sah, pemrosesan data dianggap batal secara hukum. Berbeda dengan Singapura dan Korea Selatan yang mengenal persetujuan tersirat, dimana persetujuan disimpulkan dari tindakan atau perilaku subjek data yang menunjukkan kesediaan untuk memberikan data pribadi untuk tujuan tertentu tanpa konfirmasi lisan atau tertulis secara eksplisit. Namun, di Korea Selatan, pengontrol data menanggung beban pembuktian dalam kasus pemrosesan informasi atau data pribadi tanpa persetujuan tertulis.

Selain itu, pengontrol data yang akuntabel juga berkewajiban memberikan pemberitahuan kepada subjek data tentang tujuan pengumpulan, penggunaan, dan pengungkapan data pribadi mereka. Tujuan pengumpulan ini harus memiliki batasan,

untuk memastikan bahwa organisasi hanya mengumpulkan, menggunakan, dan mengungkapkan data pribadi yang relevan dan untuk tujuan yang wajar.

Mekanisme pengumpulan data yang akuntabel dapat didukung oleh kebijakan keamanan TIK untuk perlindungan data. Mengembangkan dan menerapkan kebijakan keamanan TIK untuk perlindungan data memerlukan standar, kebijakan, dan prosedur yang mencakup kontrol akun dan akses, kebijakan pencadangan/retensi, dan kebijakan kata sandi. Pemerintah Korea Selatan telah melibatkan penggunaan sistem TIK yang inovatif seperti aplikasi isolasi mandiri dan diagnostik, pusat pemeriksaan *drive-through* dan *walk-in*, serta survei epidemiologi untuk mengumpulkan data pribadi guna merespons COVID-19 dan penyelidikan epidemiologi. Sistem respons COVID-19 ini disebut dengan model respon karantina 3P (*Preemptive, Prompt, dan Precise*) dan 3T (*Trace, Test, Treat*) plus P (*Participate*) (Ahn et al., 2020).

Personal Data Protection Commission (PDPC) Singapura mengeluarkan *"Advisories on Collection of Personal Data for COVID-19 Contact Tracing and Use of SafeEntry"* yang memberikan pedoman bagi setiap organisasi yang mengumpulkan data melalui *SafeEntry* (Personal Data Protection Commission Singapore, 2021a). Ketentuan ini menyatakan bahwa pengumpulan, penggunaan, dan pengungkapan data pribadi yang relevan oleh organisasi diperbolehkan selama perang melawan COVID-19 untuk pelacakan kontak dan tindakan respons lainnya (Alibeigi & Munir, 2023). Penelitian Alibeigi & Munir (2023) ini kemudian menunjukkan bahwa PDPA Singapura tidak berlaku bagi sektor publik. Hal ini karena ID pengguna yang seharusnya hanya boleh dideskripsi oleh Kementerian Kesehatan jika seseorang dinyatakan positif COVID-19, ternyata dapat diakses oleh Kepolisian Singapura untuk menyelidiki kejahatan serius (Han, 2021) dengan menggunakan kewenangan *Criminal Procedure Code* (CPC) atau KUHP mereka dan meminta pengguna mengunggah data pribadi aplikasi mereka untuk penyelidikan kriminal (Alibeigi & Munir, 2023). Oleh karena itu, aturan mengenai pemrosesan data pribadi oleh entitas publik di Singapura selanjutnya diatur oleh *The Government Instruction Manual on Infocomm Technology & Smart Systems Management* (IM on ICT&SS Management) (GovTech Singapore, 2024) dan *Public Sector* (*Governance*) *Act* (PSGA) 2018 (The Law Revision Commission, 2020).

Salah satu best practices dari kebijakan pengumpulan dan pengelolaan data pribadi

Gambar 1. Logo Sertifikat DPTM

Sumber: *Infocomm Media Development Authority, 2023*

Singapura adalah dengan membuat kerangka sertifikasi *Data Protection Trustmark* (DPTM). Logo DPTM ditampilkan oleh organisasi sebagai ciri bahwa mereka memiliki kebijakan dan praktik perlindungan data yang akuntabel untuk mengelola dan melindungi data pribadi pengguna dengan baik sesuai dengan kerangka sertifikasi (Personal Data Protection Commission Singapore, 2024).

3.3. Mekanisme Transfer Data Pribadi

Singapura, Korea Selatan, dan Indonesia memiliki mekanisme transfer data pribadi yang serupa, yang mewajibkan adanya persetujuan eksplisit dari subjek data sebelum data dibagikan kepada pihak ketiga. Persetujuan eksplisit, batasan tujuan, dan kewajiban pengontrol data untuk memberitahu subjek data tentang pemrosesan data pribadinya merupakan poin penting dalam mekanisme ini. Meski selanjutnya ketiga negara memiliki aturan khusus masing-masing pada praktiknya.

Ketiga negara membatasi transfer data pribadi ke luar negeri oleh organisasi atau pengontrol data jika organisasi tersebut melepaskan kendali langsung atas data tersebut. Jika data pribadi dimiliki atau dikendalikan oleh suatu organisasi, maka organisasi tersebut harus sepenuhnya melaksanakan kewajiban perlindungan data. Organisasi harus memastikan bahwa pihak ketiga yang menerima data memberikan perlindungan setara dengan yang diwajibkan oleh hukum. Dalam konteks transfer data, pengontrol data yang bertanggung jawab harus melakukan inventarisasi data, dan penilaian risiko, ketika data disusupi, tingkat risiko dapat ditentukan dengan mempertimbangkan tiga parameter dampak, yaitu: kerahasiaan, integritas, dan ketersediaan data. Organisasi didorong untuk mengandalkan kewajiban yang dapat ditegakkan secara hukum atau sertifikasi khusus dalam hubungannya dengan organisasi penerima, dimana persetujuan pribadi, kepentingan vital, atau kepentingan nasional juga dapat menjadi dasar transfer data.

3.4. Mekanisme Pelaporan Pelanggaran Data

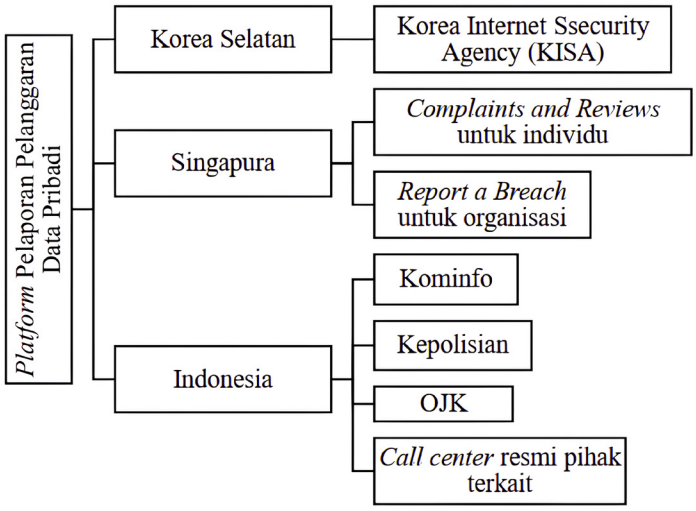
Mekanisme penanganan insiden pelanggaran data di Singapura, Indonesia, dan Korea Selatan diawali dengan memahami konsep pelanggaran data. Singapura menyebut pelanggaran data sebagai “insiden pelanggaran data”, dimana (“insiden”) mengacu pada insiden yang mengekspos data pribadi yang dimiliki atau berada di bawah kendali suatu organisasi terhadap risiko akses, pengumpulan, penggunaan, pengungkapan, penyalinan, modifikasi, pembuangan yang tidak sah, atau risiko serupa (Personal Data Protection Commission Singapore, 2022), dan Indonesia menyebutnya sebagai “Kegagalan Perlindungan Data Pribadi.” Keduanya mengacu pada situasi di mana terdapat pelanggaran kerahasiaan, integritas, dan ketersediaan data pribadi seseorang, termasuk aktivitas seperti penghancuran, kehilangan, perubahan, pengungkapan, atau akses tidak sah terhadap data pribadi yang dikirim, disimpan, atau diproses. Kegagalan perlindungan data pribadi menunjukkan ketidakmampuan untuk menjaga data individu, yang dapat diakibatkan oleh aktivitas jahat, kelalaian manusia, atau kesalahan sistem.

Standar pelaporan yang dimiliki oleh Personal Information Protection Commission (PIPC) Korea Selatan adalah didasarkan pada Pasal 34 PIPA, Pasal 39-4 PIPA, dan Pasal 39-4 Undang-Undang Penggunaan dan Perlindungan Informasi Kredit. Sedangkan rincian pelaporannya termasuk apakah individu yang terkena dampak telah diberitahu, daftar dan skala informasi pribadi yang diungkapkan, waktu dan laporan kecelakaan. Juga mengenai tindakan untuk meminimalkan kerusakan dan hasil, metode yang memungkinkan bagi individu yang terkena dampak untuk meminimalkan kerusakan dan proses bantuan yang tersedia, serta informasi kontak departemen dan personil yang bertanggung jawab.

Pelanggaran data yang memenuhi skala signifikan menurut Komisi Perlindungan Data Singapura adalah yang melibatkan data pribadi 500 orang atau lebih (Personal Data Protection Commission Singapore, 2019). Sebelum pemberitahuan pelanggaran data dilakukan, penilaian terhadap insiden/pelanggaran data wajib dilakukan guna

memastikan bahwa kondisi tersebut merupakan pelanggaran data yang dapat diberitahukan dalam waktu 30 hari kalender. Sedangkan mekanisme pelaporan kegagalan perlindungan data pribadi berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mencakup beberapa poin penting termasuk kewajiban pemberitahuan yang mewajibkan pengendali data untuk memberikan pemberitahuan tertulis dalam waktu 72 jam (3x24 jam) kepada subjek data dan otoritas terkait apabila terjadi kegagalan dalam perlindungan data pribadi (Pasal 46 ayat 1). Isi pemberitahuan ini harus mencakup rincian data pribadi yang diungkapkan, kapan dan bagaimana data pribadi tersebut diungkapkan, serta upaya yang dilakukan untuk mengatasi dan memulihkan pengungkapan tersebut (Pasal 46 ayat 2). Dalam keadaan tertentu, pengontrol data harus memberitahukan kepada publik tentang kegagalan dalam perlindungan data pribadi (Pasal 46 ayat 3). Istilah "dalam keadaan tertentu" mengacu pada situasi di mana kegagalan dalam perlindungan data pribadi mempunyai konsekuensi yang lebih luas dan signifikan bagi masyarakat umum, seperti gangguan terhadap layanan publik yang penting atau dampak serius terhadap kepentingan bersama.

Kebijakan pelaporan pelanggaran data di ketiga negara mengamanatkan bahwa setiap insiden pelanggaran data harus dilaporkan ke Komisi Perlindungan Data Pribadi dan individu yang terkena dampak setelah kejadian tersebut terkonfirmasi. Kriteria pemberitahuan didasarkan pada kerugian signifikan yang ditimbulkan pada individu yang terkena dampak, termasuk kerugian fisik, psikologis, emosional, ekonomi, keuangan, reputasi, atau kerugian lain yang dapat diidentifikasi akibat pelanggaran data.



Gambar 2. *Platform* Pelaporan Pelanggaran Data di Korea Selatan, Singapura, dan Indonesia

Sumber: *Hasil olahan peneliti*

Prinsip dan nilai akuntabilitas dalam menangani insiden pelanggaran data tidak hanya mencakup pelaporan pelanggaran tetapi juga mencakup pencegahan dan pengelolaan pelanggaran data (Personal Data Protection Commission Singapore, 2021b). Untuk mencegah pelanggaran data, organisasi harus menerapkan langkah-langkah keamanan yang kuat seperti enkripsi, kontrol akses, dan audit keamanan rutin untuk melindungi data pribadi. Mereka harus melatih pengontrol data tentang praktik perlindungan data terbaik dan meningkatkan kesadaran tentang pentingnya menjaga informasi pribadi. Mengembangkan dan memperbaharui rencana manajemen pelanggaran data secara berkala yang menguraikan prosedur untuk pencegahan, deteksi, dan respons terhadap pelanggaran sangatlah penting. Dalam mengelola pelanggaran data, organisasi harus bertindak cepat untuk mengatasi pelanggaran dan

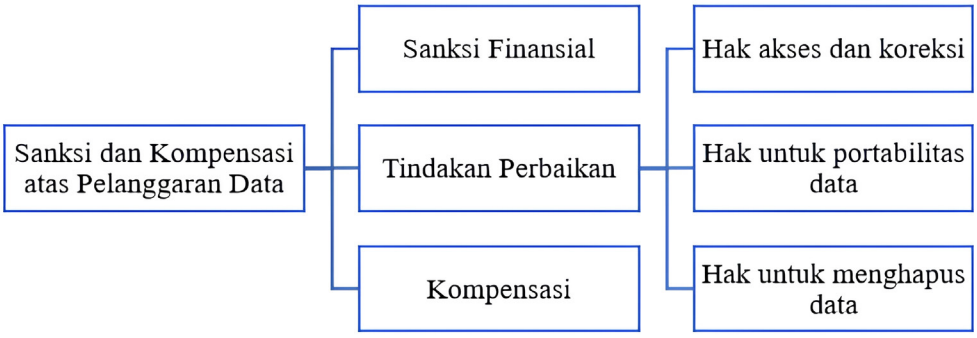
meminimalkan dampaknya dengan menerapkan langkah-langkah mitigasi, melakukan penilaian komprehensif untuk menentukan akar penyebab dan efektivitas tindakan pembendungan, dan mendokumentasikan semua langkah yang diambil untuk menilai dan merespons pelanggaran untuk memastikan kepatuhan terhadap pelanggaran data. pelanggaran kewajiban pemberitahuan.

3.5. Sanksi atas Pelanggaran Data

PIPA Korea Selatan mengatur penalti dan sanksi administratif bagi pelanggar data dalam Bagian 10 Pasal 70 sampai Pasal 76. Diantaranya ialah penjara hingga 10 tahun atau denda maksimal 100 juta won untuk pelanggaran seperti menyebabkan kesulitan besar pada pekerjaan lembaga publik dengan mengubah atau menghapus informasi pribadi, atau memperoleh dan memberikan informasi pribadi untuk tujuan mencari keuntungan (Pasal 70), dan denda administratif hingga 50 juta won untuk pelanggaran seperti mengumpulkan informasi pribadi tanpa izin atau gagal mendapatkan izin dari perwakilan hukum (Pasal 75).

Berdasarkan Pasal 48J PDPA, Singapura mengatur bahwa Komisi Perlindungan Data dapat mengenakan denda finansial hingga S$1 juta atau 10% dari omzet tahunan organisasi yang melakukan pelanggaran terhadap Ketentuan Perlindungan Data. Penentuan sanksi finansial ini dapat berdasarkan faktor-faktor seperti kerugian dan kesalahan, dampak proporsional dan efektifitas terhadap pelanggar, pengakuan dan kerjasama selama proses investigasi, dll (Personal Data Protection Commission Singapore, 2022). Denda administratif yang dapat dikenakan sebagai sanksi administratif atas pelanggaran ketentuan Undang-Undang Perlindungan Data Pribadi Indonesia diatur dalam Pasal 57. Besaran denda administratif ini tidak bersifat tetap, melainkan dapat mencapai maksimum 2 persen dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.

Di samping sanksi yang diberikan kepada pelanggar, subjek data yang terkena dampak pelanggaran data memiliki hak untuk: diberitahu jika data pribadinya telah dibocorkan secara sah, hak akses dan perbaikan, hak atas portabilitas data, hak untuk menghapus data yang dilanggar atau tidak lagi diperlukan, hak untuk mengajukan pengaduan, serta hak atas kompensasi yang dapat mencakup kerugian finansial, tekanan emosional, dsb.



Gambar 3. Sanksi, Tindakan Perbaikan, dan Kompensasi atas Pelanggaran Data

Sumber: *Hasil olahan peneliti*

Berdasarkan *Guide on Active Enforcement* Singapura, organisasi yang akuntabel dapat memilih untuk mengambil tindakan atau mempercepat keputusan penegakan hukum setelah mendeteksi insiden data dengan persetujuan dari Komisi Perlindungan Data. Organisasi yang secara proaktif mendeteksi dan merespons insiden data dengan cepat dapat mengajukan komitmen kepada Komisi Perlindungan Data untuk menerapkan rencana pemulihan. Pengakuan atas kesalahan secara sukarela dapat

dianggap sebagai faktor mitigasi yang kuat dalam kasus penegakan hukum dan dapat memberikan kesempatan bagi organisasi yang akuntabel untuk bertindak secara bermartabat.

3.6. Pembahasan

Secara keseluruhan, prinsip dasar utama dalam membentuk ketentuan-ketentuan perlindungan data pribadi adalah akuntabilitas. Prinsip ini mengacu pada pendekatan berbasis risiko dalam mengidentifikasi, memantau, dan menanggapi risiko di seluruh siklus hidup data. Maka, lembaga publik harus mampu menjelaskan setiap kebijakan yang telah ditentukan baik dari segi tujuan, alasan pengambilan keputusan, manfaat yang dihasilkan, dan berbagai macam dampak negatif yang mungkin disebabkan oleh setiap kebijakan yang telah atau akan diambil (Arsik & Lawelai, 2020). Akuntabilitas merupakan refleksi dari pemerintah ang memiliki misi yang jelas dan menarik serta berfokus pada kebutuhan masyarakat (Henry, 2015). Dengan demikian, lahirnya UU Perlindungan Data Pribadi seharusnya merupakan wujud kebijakan pemerintah yang akuntabel dan menjamin pencegahan penyelewengan kewenangan, serta dapat diarahkan pada pencapaian tujuan institusional dengan tingkat efisiensi, efektivitas, kejujuran, dan hasil yang seoptimal mungkin.

Berdasarkan kelima aspek penilaian akuntabilitas kebijakan perlindungan data pribadi yang digunakan dalam penelitian ini, Singapura dan Korea Selatan jelas lebih unggul daripada Indonesia. Dimensi akuntabiitas pemenuhan hak-hak publik dalam perlindungan data pribadi, dinilai dari kelima aspek, memperlihatkan efektivitas PDPA Singapura dan PIPA Korea Selatan dalam memberikan pedoman dan standar kebijakan yang jelas untuk dipatuhi oleh organisasi maupun individu dalam melindungi data pribadi. Dengan adanya dewan pengawas yang kuat serta mekanisme yang tepat memungkinkan para pengelola data di Korea Selatan dan Singapura memprioritaskan praktik perlindungan data, sehingga berpotensi terjaganya data pribadi individu sekaligus terpenuhinya hak-hak publik atas perlindung data pribadi.

Pemenuhan hak subjek data yang akuntabel dapat dilihat dari implementasi kebijakan terkait hak subjek data, termasuk pengumpulan data pribadi, perlakuan terhadap data pribadi, dan otonomi individu atas data pribadi. Subjek data mempunyai hak untuk meminta akses terhadap data dan informasi pribadinya, untuk memahami bagaimana data tersebut digunakan atau diungkapkan, dan untuk meminta transfer data ke pihak lain dalam format yang umum digunakan dan dapat dibaca mesin. Konsep dan nilai akuntabilitas juga memastikan bahwa individu sebagai subjek data dapat meminta akses terhadap data pribadi mereka yang disimpan atau dikendalikan oleh suatu organisasi, mengambil tindakan hukum terhadap pelanggaran data, dan mengajukan pengaduan kepada Komisi Perlindungan Data yang dapat meninjau atau menyelidiki perilaku dan kepatuhan DPO terhadap UU.

Dimensi akuntabiitas mekanisme perlindungan data pribadi menonjolkan praktik akuntabilitas Singapura dengan menekankan peran Komisi Perlindungan Data, pengontrol data, petugas perlindungan data, dan organisasi yang memanfaatkan data pribadi. Mekanisme perlindungan data pribadi yang akuntabel juga menekankan pentingnya aspek-aspek: 1) pendefinisian data pribadi yang dilindungi, 2) praktik pengumpulan data yang transparan, 3) mekanisme transfer data yang jelas, 4) mekanisme pelaporan pelanggaran terpusat, dan 5) penegakkan sanksi dan kompensasi atas pelanggaran data, untuk memastikan akuntabilitas dan penghormatan terhadap hak privasi individu.

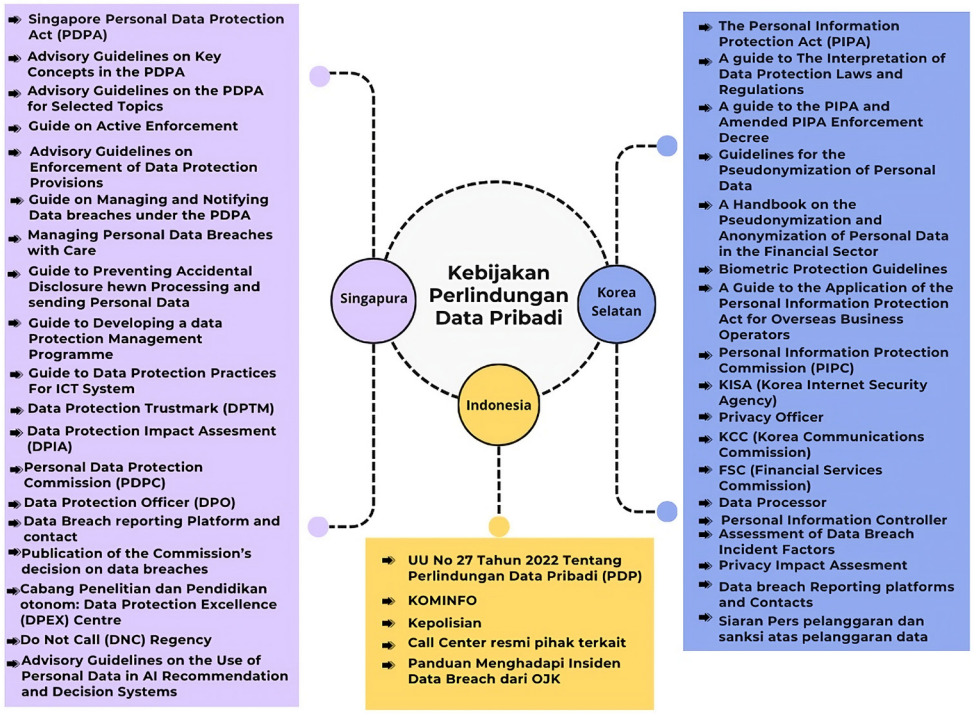
Dimensi akuntabilitas penanggulangan kasus pelanggaran data membuktikan betapa tidak akuntabelnya Indonesia dalam masalah ini. Indonesia tidak memiliki badan

pengawas yang tersentralisasi dan khusus, serupa PDPC Singapura dan PIPC serta *Internet Security Agency* (KISA) Korea Selatan. Hal ini mengakibatkan pelaporan juga pengelolaan pelanggaran data di Indonesia terfragmentasi dan melibatkan banyak entitas, yang berpotensi menyebabkan inkonsistensi juga keterlambatan dalam menangani insiden pelanggaran data. Terbukti dari kasus kebocoran data di Indonesia yang terus terjadi, seperti 149 kasus pada 2023 (Biro Hukum dan Komunikasi Publik BSSN, 2023), 311 kasus pada 2022 (Mustajab, 2023), hingga kasus serangan *ransomware* terhadap *server* Pusat Data Nasional (PDN) pada Juni 2024 ini. Dalam kasus PDN ini terdapat kritik terhadap keterlambatan dalam menetapkan aturan *backup* data setelah terjadinya serangan (Gatra, 2024), yang menunjukkan kurangnya kesiapan dalam menghadapi situasi krisis. Maka, faktor lain yang mempengaruhi buruknya akuntabilitas penanganan pelanggaran data di Indonesia adalah lemahnya sumber daya manusia (SDM) dan sistem TIK yang dimiliki.

SDM yang tidak memadai dalam hal keahlian dan kesadaran keamanan siber mengakibatkan kurangnya kesiapan untuk mencegah, mendeteksi, dan merespon peanggaran data secara efektif. Sedang sistem TIK yang ketinggalan zaman atau tidak memadai menciptakan kerentanan yang dapat dieksploitasi oleh pelaku kejahatan, sehingga meningkatkan kemunkinan keberhasilan serangan siber dan pelanggaran data. Meskipun tidak secara langsung menunjukkan buruknya sumber daya manusia, kasus ini menggarisbawahi pentingnya peningkatan kesadaran, pelatihan, dan keterampilan dalam bidang keamanan cyber di kalangan pihak terkait. Upaya untuk memperkuat sumber daya manusia dalam hal keamanan *cyber* menjadi krusial untuk mencegah dan merespons serangan *cyber* di masa depan.

Akuntabilitas Singapura dan Korea Selatan selanjutnya diperkuat dengan inovasi kebijakan perlindungan data masing-masing. Salah duanya adalah inovasi Singapura dengan memiliki *Data Protection Trustmark* (DPTM) untuk membantu organisasi dalam manajemen perlindungan data, juga pembentukan Program Manajemen Perlindungan Data yang dapat ditiru oleh Indonesia, yang sangat penting dalam menetapkan landasan kepatuhan perlindungan data bagi pengelola data. Landasan kepatuhan ini dapat dilakukan melalui empat langkah: 1) tata kelola dan penilaian risiko; 2) mengembangkan kebijakan perlindungan data dan praktik perlindungan data; 3) merancang proses untuk mengoperasionalkan kebijakan Manajemen Pelanggaran Data; dan 4) pemeliharaan (Jarmen, 2024). Sedang Korea Selatan memiliki kebijakan kolaborasi dengan berbagai lembaga terkait perlindungan data.

Lebih lanjut, perbedaan kebijakan perlindungan data pribadi yang dimiliki oleh Korea Selatan, Singapura, dan Indonesia secara lengkap ditampilkan dalam gambar berikut:



Gambar 4. Kebijakan Perlindungan Data Pribadi di Korea Selatan, Singapura, dan Indonesia

Sumber: *Hasil olahan peneliti*

4. Kesimpulan

Berdasarkan hasil dan pembahasan, Korea Selatan dan Singapura disimpulkan sebagai negara-negara yang akuntabel dalam perlindungan data pribadi, sementara Indonesia perlu segera mengimplementasikan UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Untuk meningkatkan akuntabilitas dalam perlindungan data, Indonesia harus merangkul inovasi dengan membentuk otoritas perlindungan data, memperkuat sumber daya manusia dan infrastruktur TIK, serta mengupayakan kolaborasi dengan mitra internasional untuk mengembangkan kebijakan perlindungan data yang efektif. Dengan mengambil langkah-langkah inovatif seperti yang dilakukan Korea Selatan dan Singapura, Indonesia dapat mengatasi kurangnya akuntabilitas dalam perlindungan data dan menjamin keamanan serta privasi data pribadi bagi setiap individu.

Penelitian ini mengakui adanya keterbatasan dalam metodologi yang digunakan sehingga untuk menangkap semua dimensi dari prlindungan data pribadi membutuhkan pendekatan yang lebih komprehensif. Terkait kompleksitas kebijakan perlindungan data juga menjadi tantangan untuk menciptakan pemahaman yang holistik dalam penelitian ini.

Keterbatasan penelitian ini mendorong implikasi akademis untuk penelitian masa depan mencakup: 1) fokus pada studi komparatif yang lebih komprehensif tentang persamaan dan perbedaan UU dan praktik perlindungan data; 2) penggunaan pendekatan metodologis yang lebih kuat seperti survei dan wawancara untuk mendapatkan pemahaman yang lebih mendalam; dan 3) kolaborasi interdisipliner dengan para ahli di bidang hukum, etika, teknologi, dan keamanan siber untuk memperoleh pemahaman holistik tentang tantangan dan inovasi perlindungan data pribadi yang akuntabel.

Ucapan Terima Kasih

Ucapan terima kasih terutama ditujukan kepada Bapak Prof. Dr. Dwiyanto Indiahono, M.Si., dan Bapak Dr. Sukarso, M.Si., serta Prodi Magister Administrasi Publik Universitas Jenderal Soedirman, sehingga selesainya penelitian Ini.

Referensi

Ahn, N. Y., Park, J. E., Lee, D. H., & Hong, P. C. (2020). Balancing Personal Privacy and Public Safety During COVID-19: The Case of South Korea. *IEEE Access, 8*, 171325–171333. https://doi.org/10.1109/ACCESS.2020.3025971

Al-Shbail, T., & Aman, A. (2018). E-government and Accountability: How to Mitigate The Disorders and Dysfunctions of Accountability Relationships. *Transforming Government: People, Process and Policy, 12*(2), 155–190. https://doi.org/10.1108/TG-09-2017-0057

Alibeigi, A., & Munir, A. B. (2023). Public Health Data and International Privacy Rules and Practices: A Case Study of Singapore. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 14149 LNCS*(November), 51–66. https://doi.org/10.1007/978-3-031-39841-4_4

Arief, V. (2023). E-Government di Asia Tenggara : Perbandingan Pengembangan E- Government di Singapura , Malaysia dan Indonesia. *Social Issues Quarterly, 1*(2), 345–362.

Arsik, S. F., & Lawelai, H. (2020). Penerapan Akuntabilitas, Efektivitas, Dan Transparansi Dalam Mewujudkan Good Governance: Studi Pemerintah Desa Banabungi. *Jurnal Studi Ilmu Pemerintahan, 1*(1), 1–7. https://doi.org/10.35326/jsip.v1i1.523

Biro Hukum dan Komunikasi Publik BSSN. (2023). *Rapat Dengar Pendapat BSSN Bersama Komisi I DPR*. BSSN.Go.Id. https://www.bssn.go.id/rapat-dengar-pendapat-bssn-bersama-komisi-i-dpr/

Blacklaws, C. (2018). Algorithms: Transparency and Accountability. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376*. https://doi.org/10.1098/rsta.2017.0351

Boch, A., Hohma, E., & Trauth, R. (2022). *Towards an Accountability Framework for AI: Ethical and Legal Considerations. July*. https://doi.org/10.13140/RG.2.2.10231.50086

Boyd, D., & Crawford, K. (2011). Six Provocations for Big Data - A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society (September 21, 2011). *SSRN Electronic Journal*, 1–17.

Brown, D. C. G. (2013). Accountability in a collectivized environment: From Glassco to digital public administration. *Canadian Public Administration, 56*(1), 47–69. https://doi.org/10.1111/capa.12003

European Union Agency for Fundamental Rights & Council of Europe. (2018). Handbook on European Data Protection Law. In *Publications Office of the European Union*. https://doi.org/10.2811/58814

Gatra, S. (2024). *Pusat Data Nasional Jebol: Menkominfo Mundur atau Dimaklumi?* Kompas.Com. https://nasional.kompas.com/read/2024/06/28/08212831/pusat-data-nasional-jebol-menkominfo-mundur-atau-dimaklumi?page=all

GovTech Singapore. (2024). *Instruction Manual for Infocomm Technology and Smart Systems (ICT&SS) Management*. Singapore Government Developer Portal. https://www.developer.tech.gov.sg/guidelines/standards-and-best-practices/instruction-manual-for-ict-ss-management.html

Han, K. (2021). *Broken Promises: How Singapore Lost Trust On Contact Tracing Privacy*. MIT Technology Review. https://www.technologyreview.com/2021/01/11/1016004/singapore-tracetogether-contact-tracing-police/

Henry, N. (2015). *Public Administration and Public Affairs* (Twelfth Ed). Routledge. https://doi.org/10.4324/9781315663067

Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi. *Jurnal Hukum, 37*(2), 119. https://doi.org/10.26532/jh.v37i2.16272

Infocomm Media Development Authority. (2023). *About the Data Protection Trustmark (DPTM)*. Infocomm Media Development Authority. https://www.imda.gov.sg/how-we-can-help/data-protection-trustmark-certification

Jarmen, S. (2024). *From Inception to Impact: Singapore's PDPA After Ten Years*. Straits Interactive. https://www.linkedin.com/pulse/from-inception-impact-singapores-pdpa-after-ten-years-djgdc

Kim, H. J., Pan, G., & Pan, S. L. (2007). *Managing IT-Enabled Transformation in The Public Sector: A Case Study on E-Government in South Korea. 24*, 338–352. https://doi.org/10.1016/j.giq.2006.09.007

Mustajab, R. (2023). *BSSN: Ada 311 Kasus Kebocoran Data di Indonesia pada 2022*. Dataindonesia. Id. https://dataindonesia.id/internet/detail/bssn-ada-311-kasus-kebocoran-data-di-indonesia-pada-2022

Nuyen, A. T. (1994). Interpretation and Understanding in Hermeneutics and Deconstruction. *Philosophy of the Social Sciences, 24*(4), 426–438.

Personal Data Protection Commission Singapore. (2019). *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*. June, 1–164.

Personal Data Protection Commission Singapore. (2021a). *Advisories on Collection of Personal Data for COVID-19 Contact Tracing and Use of SafeEntry*. Personal Data Protection Commission, Singapore. https://www.pdpc.gov.sg/help-and-resources/2021/05/advisory-on-collection-of-personal-data-for-covid-19-contact-tracing

Personal Data Protection Commission Singapore. (2021b). *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (Issue March).

Personal Data Protection Commission Singapore. (2022). *Guide on Active Enforcement* (Issue October).

Personal Data Protection Commission Singapore. (2024). *Share Your Personal Data with Care*. Personal Data Protection Commission, Singapore. https://www.pdpc.gov.sg/overview-of-pdpa/data-protection/individual/protecting-your-personal-data

Personal Information Protection Commission South Korea. (n.d.). *Reporting on Divulgence of Personal Information*. Pipa.Go.Kr. Retrieved April 3, 2024, from https://www.pipc.go.kr/eng/user/lgp/ntp/reportingDivulgence.do

Rahman, F. (2021). Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di Indonesia. *Jurnal Legislasi Indonesia, 18*(1), 81. https://doi.org/10.54629/jli.v18i1.736

Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum, 20*(2), 369–384. https://doi.org/10.24815/kanun.v20i2.11159

Schreier, M. (2012). *Qualitative Content Analysis in Practice* (1st ed.). SAGE Publications Ltd.

Sharma, S., Kar, A. K., & Gupta, M. P. (2021). Unpacking Digital Accountability: Ensuring efficient and answerable e-governance service delivery. *ACM International Conference Proceeding Series, October 2021*, 260–269. https://doi.org/10.1145/3494193.3494229

Sinaga, E. M. C. (2020). Formulasi Legislasi Perlindungan Data Pribadi. *Jurnal RechtVinding, 9*(2), 237–256.

Sloot, B. van der. (2017). *Privacy as Virtue : Moving Beyond the Individual in the Age of Big Data*. Intersentia.

Smith, M., Szongott, C., Henne, B., & Von Voigt, G. (2012). Big data privacy issues in public social media. *IEEE International Conference on Digital Ecosystems and Technologies*. https://doi.org/10.1109/DEST.2012.6227909

The Law Revision Commission. (2020). *Public Sector (Governance) Act 2018*. Singapore Statutes Online. https://sso.agc.gov.sg/Act/PSGA2018

Walters, R., & Coghlan, M. (2019). Data Protection and Artificial Intelligence Law: Europe Australia Singapore - An Actual or Perceived Dichotomy. *American Journal of Science, Engineering and Technology, 4*(4), 55. https://doi.org/10.11648/j.ajset.20190404.11

Young, M., Rodriguez, L., Keller, E., Sun, F., Sa, B., Whittington, J., & Howe, B. (2019). Beyond open vs. Closed: Balancing individual privacy and public accountability in data sharing. FAT* 2019 - Proceedings of the 2019 Conference on Fairness, Accountability, and Transparency, i, 191–200. https://doi.org/10.1145/3287560.3287577

Yuniarti, S. (2019). Perlindungan Hukum Data Pribadi Di Indonesia. Business Economic, Communication, and Social Sciences (BECOSS) Journal, 1(1), 147–154. https://doi.org/10.21512/becossjournal.v1i1.6030