

Rekonstruksi Yurisprudensi Mahkamah Konstitusi di Era Pengawasan Data

Ismet Hadi

Program Studi Ilmu Hukum Universitas Muhammadiyah Gorontalo

Email: ismethadi@umgo.ac.id

Abstract

Digital transformation has accelerated data-driven governance, enabling public authorities to collect, store, link, and analyze personal data at scale. In this environment, privacy harms are increasingly systemic: they stem not only from isolated intrusions but also from institutional design choices, procedural gaps, and power asymmetries between individuals and data-controlling entities. This article reconstructs Indonesia's Constitutional Court (Mahkamah Konstitusi, MK) jurisprudence on privacy and personal data protection to (i) map the evolution of constitutional standards, (ii) assess argumentative consistency across key rulings, and (iii) formulate a reform agenda for data governance compatible with democratic rule-of-law principles. Methodologically, the study is doctrinal and case-based, combining close reading of judgments with normative analysis. It clusters MK decisions into three domains: (a) wiretapping and communications interception; (b) the acquisition of electronic evidence; and (c) personal data protection after the enactment of the Personal Data Protection Act (UU PDP). The findings indicate a shift from an infringement-based approach—focused on whether a specific interference is lawful—toward a governance-based approach that evaluates whether legal frameworks provide adequate safeguards through system architecture, oversight, and accountability mechanisms. Decision No. 5/PUU-VIII/2010 strengthens the legality principle by requiring wiretapping powers to be grounded in statute. Decision No. 20/PUU-XIV/2016 embeds due process by conditioning evidentiary validity on lawful data acquisition. Decision No. 151/PUU-XXII/2024 affirms personal data protection as a constitutional interest that demands risk-based governance, independent supervision, and enforceable accountability. Building on these trends, the article proposes a set of Minimum Constitutional Safeguards (MCS) as an operational checklist: clear legal basis, purpose limitation, data minimization, storage/retention limits, logging and auditability, independent supervisory authority, and accessible remedies. Practically, the study recommends harmonizing fragmented sectoral regulations, strengthening the independence of the data protection supervisor, and mainstreaming privacy-by-design and algorithmic transparency so that MK's constitutional signals translate into effective protections in Indonesia's digital ecosystem.

Keywords: Digital Privacy; Data Surveillance; Constitutional Court; Personal Data Protection; Constitutional Safeguards

Abstrak

Transformasi digital mendorong negara mengelola layanan publik berbasis data, tetapi sekaligus memperluas kapasitas pengawasan melalui pengumpulan, interkoneksi, dan analitik data pribadi. Dalam lanskap data-driven governance, risiko pelanggaran privasi tidak lagi bersifat insidental, melainkan sistemik: lahir dari desain prosedur, arsitektur kelembagaan, serta relasi kuasa yang timpang antara warga dan institusi pengendali data. Artikel ini merekonstruksi yurisprudensi Mahkamah Konstitusi (MK) Indonesia dalam isu privasi dan perlindungan data, dengan tujuan memetakan evolusi standar konstitusional, menguji konsistensi argumentasi, dan merumuskan agenda reformasi tata kelola data yang sejalan dengan prinsip negara hukum. Metode penelitian bersifat yuridis-normatif dengan pendekatan putusan (case-based) dan analisis doktrinal, berfokus pada tiga klaster: (i) penyadapan dan intersepsi komunikasi; (ii) perolehan serta keabsahan alat bukti elektronik; dan (iii) perlindungan data pribadi pasca-berlakunya UU PDP. Hasil analisis menunjukkan pergeseran dari pendekatan infringement-based—yang menilai sah/tidaknya tindakan pembatasan hak—menuju pendekatan governance-based yang menilai kecukupan desain sistem, prosedur, dan pengawasan. Putusan No. 5/PUU-VIII/2010 menegaskan asas legalitas: kewenangan penyadapan harus diatur oleh undang-undang. Putusan No. 20/PUU-XIV/2016 menguatkan due process dengan mensyaratkan perolehan bukti elektronik secara sah. Putusan No. 151/PUU-XXII/2024 mengafirmasi perlindungan data pribadi sebagai hak konstitusional yang memerlukan akuntabilitas, pengawasan independen, dan pendekatan berbasis risiko. Artikel ini merumuskan Minimum Constitutional Safeguards (MCS) sebagai daftar periksa normatif: dasar hukum yang jelas, pembatasan tujuan, minimisasi data, batas retensi, audit/logging, otoritas pengawas independen, serta mekanisme pemulihan yang efektif. Implikasinya ialah perlunya harmonisasi regulasi sektoral, penguatan institusi pengawas, dan internalisasi prinsip privacy-by-design agar yurisprudensi MK bertransformasi menjadi perlindungan yang operasional dalam ekosistem digital Indonesia. Selain memperkuat hak atas rasa aman (Pasal 28G ayat (1)), MK menautkan privasi dengan kepastian hukum (Pasal 28D ayat (1)) dan kerangka pembatasan (Pasal 28J ayat (2)). Temuan ini menegaskan privasi digital berkelindan dengan kebebasan berekspresi dan risiko diskriminasi berbasis profilisasi. Karena itu, reformasi perlu mencakup penilaian dampak perlindungan data, transparansi algoritmik, dan literasi hak konstitusional.

Kata Kunci: Privasi Digital; Pengawasan Data; Mahkamah Konstitusi; Pelindungan Data Pribadi; Safeguards Konstitusional

A. Pendahuluan

Transformasi digital global dalam dua dekade terakhir telah menciptakan perubahan fundamental dalam interaksi antara negara dan warga negara. Dalam era *data-driven governance*, negara kini memiliki akses dan kemampuan yang sangat besar untuk mengumpulkan, menyimpan, mengolah, dan menginterkoneksi data pribadi warganya (Gstrein & Beaulieu, 2022). Informasi tidak hanya menjadi instrumen birokrasi, melainkan juga menjadi sumber kekuasaan baru. Proses

pengawasan yang sebelumnya bersifat manual dan berbasis tindakan kini bergeser menjadi sistemik, otomatis, dan berlangsung secara terus-menerus tanpa disadari oleh subjek yang diawasi (Lynskey, 2023).

Dalam konteks tersebut, hak atas privasi muncul sebagai hak yang rentan tergerus oleh teknologi dan kebijakan. Privasi tidak lagi semata-mata menyangkut hak atas "ketersendirian" (*the right to be let alone*), tetapi bergeser menjadi hak untuk mengendalikan informasi pribadi (*informational self-determination*) serta membatasi kekuasaan negara atas data (Dalla Corte, 2022). Dengan kata lain, ancaman terhadap privasi dalam era digital bukan hanya muncul dari pelanggaran langsung, tetapi juga dari *power asymmetry* antara individu dan institusi pengumpul data. Sehingga, hak atas privasi perlu didekati tidak hanya sebagai hak sipil individual, melainkan sebagai hak konstitusional yang bersifat struktural dan sistemik (Celeste, 2022).

Hak atas privasi memiliki fondasi filosofis yang kuat dalam pemikiran hak asasi manusia. Dalam filsafat hukum natural, hak ini berakar pada pengakuan atas martabat manusia dan kebebasan individu untuk mengatur ruang hidupnya. Dalam perspektif hukum positif, hak atas privasi dikonstruksikan sebagai bagian dari kebebasan pribadi dan jaminan perlindungan terhadap penyalahgunaan kekuasaan. Pendekatan *rights-limitation* menekankan bahwa pembatasan atas hak ini harus memenuhi prinsip legalitas (didasarkan pada hukum), keniscayaan (diperlukan untuk tujuan sah), proporsionalitas (tidak berlebihan), dan adanya pengawasan serta remedi (Rojaszczak, 2021).

Dalam perkembangan yurisprudensi di berbagai negara, hak atas privasi telah berkembang dari prinsip moral menjadi norma hukum yang dapat ditegakkan. Mahkamah di berbagai yurisdiksi seperti *Court of Justice of the European Union* (CJEU), Mahkamah Agung Amerika Serikat, dan Mahkamah Konstitusi Jerman telah memperluas cakupan dan perlindungan atas hak ini, terutama dalam konteks pengawasan elektronik dan pengolahan data. Di Indonesia, perkembangan tersebut belum sepenuhnya tercermin dalam sistem hukum, mengingat belum adanya pengakuan eksplisit terhadap hak atas privasi dalam UUD 1945.

UUD 1945 tidak memuat istilah *privacy* secara eksplisit. Tidak ditemukan istilah "hak atas privasi" baik dalam batang tubuh maupun penjelasan konstitusi.

Meski demikian, Mahkamah Konstitusi telah memberikan kontribusi besar dalam konstruksi yuridis terhadap hak ini melalui interpretasi sistematis terhadap norma-norma yang ada. Pasal 28G ayat (1) tentang perlindungan terhadap diri pribadi dan rasa aman, serta Pasal 28D ayat (1) tentang kepastian hukum dan perlindungan yang sama di hadapan hukum, menjadi dasar utama dalam pembentukan doktrin konstitusional mengenai privasi. Ditambah, Pasal 28J ayat (2) menyediakan kerangka pembatasan yang berbasis proporsionalitas dan kepentingan umum.

Pada beberapa putusan, Mahkamah Konstitusi mengembangkan doktrin bahwa tindakan penyadapan, intersepsi, dan pengumpulan data pribadi oleh negara merupakan bentuk pembatasan hak konstitusional yang harus memenuhi uji legalitas, keniscayaan, dan proporsionalitas. Salah satu putusan penting adalah Putusan MK No. 5/PUU-VIII/2010, yang menyatakan bahwa kewenangan penyadapan hanya dapat diberikan melalui undang-undang, bukan melalui peraturan pelaksana. Putusan ini memperkuat prinsip bahwa intervensi negara terhadap privasi individu harus memiliki dasar hukum yang jelas dan pembatasan yang terukur.

Mahkamah juga menunjukkan konsistensi dalam menilai legalitas alat bukti elektronik, seperti terlihat dalam Putusan No. 20/PUU-XIV/2016. Mahkamah menyatakan bahwa bukti elektronik hanya sah jika diperoleh secara sah, menekankan prinsip *due process* sebagai bagian dari perlindungan hak atas privasi dalam proses hukum. Dalam hal ini, Mahkamah tidak hanya memperluas perlindungan terhadap data pribadi, tetapi juga menghubungkannya dengan hak atas peradilan yang adil. Ini menunjukkan bahwa privasi memiliki aspek procedural dan substansial yang saling melengkapi.

Putusan Mahkamah terbaru, No. 151/PUU-XXII/2024, memberikan arah baru dengan mengafirmasi bahwa perlindungan data pribadi merupakan bagian dari hak konstitusional yang memerlukan tata kelola yang efektif. Mahkamah memperkenalkan pendekatan berbasis risiko dan akuntabilitas dalam pengelolaan data. Ini menandai transisi dari pendekatan yang reaktif menjadi pendekatan yang preventif dan *proactive*, di mana desain sistem dan kelembagaan menjadi fokus utama perlindungan hak konstitusional.

Dalam konteks kelembagaan, Mahkamah telah mengisi kekosongan normatif melalui pendekatan interpretatif yang progresif. Namun, keterbatasan tetap ada karena posisi Mahkamah sebagai lembaga yudisial yang hanya dapat menilai konstusionalitas norma dan tidak dapat menggantikan fungsi legislator. Oleh karena itu, keterpaduan antara legislasi, penegakan hukum, dan desain kelembagaan menjadi syarat mutlak agar perlindungan hak atas privasi dapat berjalan secara efektif.

Berbagai tantangan muncul dalam praktik perlindungan privasi digital di Indonesia. Pertama, belum adanya otoritas pengawas independen yang mengawasi pelaksanaan UU PDP. Kedua, masih terdapat fragmentasi dalam regulasi yang menyangkut pengumpulan, pengolahan, dan penyimpanan data di sektor-sektor yang berbeda. Ketiga, rendahnya literasi data dan kesadaran privasi di kalangan birokrasi dan masyarakat juga memperlemah upaya perlindungan konstitusional terhadap privasi.

Dalam menghadapi tantangan tersebut, diperlukan pemahaman yang integratif antara teori hak asasi manusia, hukum tata negara, dan tata kelola teknologi informasi. Hak atas privasi tidak cukup dilihat sebagai *negative liberty* yang hanya menuntut non-intervensi negara, tetapi juga sebagai *positive obligation* yang memerlukan tindakan aktif dari negara untuk melindungi dan memberdayakan individu dalam mengendalikan informasi pribadinya. Pandangan ini sejalan dengan prinsip *dignity-based constitutionalism* yang menempatkan manusia sebagai pusat dari sistem hukum dan kebijakan publik (Gonzalez Fuster, 2014).

Lebih jauh, pendekatan *data justice* dan *algorithmic accountability* juga mulai relevan dalam diskursus perlindungan konstitusional. Ketika sistem digital dan algoritma digunakan dalam layanan publik, pemrosesan data tidak lagi bersifat netral, melainkan menghasilkan keputusan yang berdampak nyata terhadap kehidupan warga negara. Dalam konteks ini, hak atas privasi juga harus mencakup hak untuk mengetahui bagaimana data digunakan, diproses, dan dibagikan oleh institusi publik.

Kesimpulannya, perlindungan konstitusional terhadap hak atas privasi di Indonesia berada dalam proses pembentukan yang dinamis. Mahkamah Konstitusi telah memainkan peran penting dalam membangun kerangka normatif melalui interpretasi terhadap norma-norma yang ada. Namun, dibutuhkan langkah strategis dan

reformasi legislasi untuk memastikan bahwa hak atas privasi digital tidak hanya diakui secara yuridis, tetapi juga diimplementasikan secara efektif dalam sistem hukum nasional.

B. Hasil Penelitian dan Pembahasan

1. Yurisprudensi Mahkamah Konstitusi Menuju Tata Kelola Data

Perlindungan konstitusional terhadap hak atas privasi dalam konteks digital di Indonesia dibentuk secara bertahap melalui konstruksi yurisprudensial Mahkamah Konstitusi (MK). Putusan-putusan MK yang relevan menunjukkan adanya evolusi penting: dari semula berfokus pada keabsahan penyadapan dan alat bukti elektronik, menuju pembentukan kerangka tata kelola data yang lebih sistemik, berbasis risiko, dan berorientasi pada akuntabilitas lembaga. Pergeseran ini menandai transisi dari pendekatan yang bersifat *infringement-based* sekadar menilai sah atau tidaknya suatu tindakan yang membatasi hak menuju pendekatan *governance-based* yang menilai bagaimana sistem, prosedur, dan kelembagaan dirancang untuk mencegah pelanggaran sejak awal (Fitriani, 2022; Gstrein & Beaulieu, 2022).

Secara metodologis, yurisprudensi MK dalam isu privasi digital dapat dipetakan ke dalam tiga klaster besar. Pertama, klaster penyadapan dan intersepsi komunikasi, yang antara lain mencakup pengujian kewenangan lembaga penegak hukum melakukan penyadapan dalam perkara tindak pidana tertentu. Kedua, klaster perolehan dan keabsahan alat bukti elektronik, yang menelaah hubungan antara cara memperoleh data dengan prinsip *due process of law* dan hak atas peradilan yang adil. Ketiga, klaster perlindungan data pribadi setelah lahirnya Undang-Undang Pelindungan Data Pribadi (UU PDP), yang fokus pada desain kelembagaan, kewenangan otoritas pengawas, dan prinsip-prinsip tata kelola data yang sesuai dengan standar hak asasi manusia (Lynskey, 2023; Shahrullah et al., 2024).

Dalam putusan-putusan awal yang berkaitan dengan penyadapan, seperti Putusan No. 5/PUU-VIII/2010, MK menegaskan bahwa tindakan penyadapan merupakan bentuk pembatasan hak konstitusional, khususnya hak atas privasi dan rasa aman sebagaimana dijamin Pasal 28G ayat (1) UUD 1945. Oleh karena itu, tindakan tersebut hanya dapat dibenarkan apabila diatur secara tegas oleh undang-undang, bukan sekadar oleh peraturan pelaksana atau kebijakan administratif. Argumentasi ini sejalan dengan prinsip legalitas (*legality principle*) dalam hukum tata negara, yang

menempatkan konstitusi dan undang-undang sebagai sumber legitimasi utama pembatasan hak (Asshiddiqie, 2019; Yuliandri, 2007). Dengan demikian, MK menggariskan bahwa setiap intervensi terhadap komunikasi privat harus jelas dasar hukumnya, ruang lingkupnya, serta mekanisme pengawasannya.

Dimensi lain tampak dalam Putusan No. 20/PUU-XIV/2016 yang berkaitan dengan alat bukti elektronik. Dalam perkara ini, Mahkamah menegaskan bahwa bukti elektronik hanya sah dan dapat digunakan dalam proses peradilan apabila diperoleh dengan cara yang sah. Dengan kata lain, tidak cukup bahwa bukti tersebut relevan secara materiil; cara perolehannya pun harus sesuai dengan hukum dan menjunjung tinggi hak-hak terdakwa. Pendekatan ini mencerminkan integrasi prinsip *due process* ke dalam doktrin perolehan bukti digital, serta menunjukkan bahwa pelanggaran privasi dalam proses perolehan data dapat berdampak pada eksklusi bukti tersebut dari persidangan (Mahdy et al., 2025; Nurjihad, 2021). Di sini, hak atas privasi tidak hanya diposisikan sebagai hak substantif, tetapi juga sebagai elemen prosedural yang melekat pada hak atas peradilan yang adil.

Seiring dengan meningkatnya ketergantungan negara dan sektor swasta pada pengolahan data pribadi, MK mulai bergerak dari fokus pada tindakan intersepsi individual menuju penilaian terhadap desain sistemik tata kelola data. Momentum pentingnya adalah pengujian terhadap ketentuan dalam UU PDP yang berujung pada Putusan No. 151/PUU-XXII/2024. Dalam putusan ini, Mahkamah tidak hanya menilai apakah norma tertentu bertentangan dengan UUD 1945, tetapi juga menelaah apakah arsitektur kelembagaan dan mekanisme pengawasan yang dirancang UU PDP sudah memadai untuk menjamin perlindungan hak konstitusional atas data pribadi (Lubis, 2022).

Hak atas privasi digital dipahami sebagai hak yang tak dapat direalisasikan hanya melalui larangan formal, tetapi memerlukan *governance structure* yang konkret. Mahkamah menekankan pentingnya keberadaan otoritas pengawas data yang independen, keberadaan pejabat perlindungan data (*data protection officer*), kewajiban *logging* dan audit atas aktivitas pemrosesan data, serta mekanisme pengaduan dan pemulihan yang dapat diakses warga negara. Dengan demikian, MK memperluas cakupan perlindungan privasi dari sekadar relasi antara individu dan negara, menjadi relasi yang melibatkan aktor-aktor lain, termasuk badan usaha dan penyelenggara sistem elektronik (Bennett & Raab, 2020; Lynskey, 2023).

Pergeseran ini turut merefleksikan internalisasi prinsip-prinsip *data protection* internasional ke dalam tafsir konstitusi nasional. Konsep-konsep seperti *purpose limitation*, *data minimization*, *storage limitation*, dan *accountability* yang berkembang dalam rezim hukum Uni Eropa dan standar internasional lainnya, mulai tampak pengaruhnya dalam pertimbangan hukum MK, meskipun tidak selalu disebutkan secara eksplisit (De Gregorio & Radu, 2022; Gonzalez Fuster, 2014). MK menafsirkan Pasal 28G ayat (1) dan Pasal 28J ayat (2) UUD 1945 secara evolutif, sehingga hak atas privasi dan pembatasannya dapat menjawab tantangan baru yang dihadirkan oleh teknologi digital dan *algorithmic governance*.

Selain itu, pola argumentasi MK menunjukkan bahwa privasi digital tidak lagi dipandang sebagai hak yang berdiri terpisah, tetapi berkaitan erat dengan hak-hak lain seperti kebebasan berekspresi, hak atas informasi, dan hak atas non-diskriminasi. Misalnya, dalam diskursus mengenai penggunaan data pribadi untuk profilisasi, *scoring*, atau penyaringan penerima layanan publik, terdapat risiko diskriminasi sistemik yang hanya dapat ditangkap jika privasi dipahami sebagai bagian dari kerangka keadilan sosial (*social justice*) yang lebih luas (Gellert, 2018; Gstrein & Beaulieu, 2022). Pada konteks ini, yurisprudensi MK membuka peluang untuk pengembangan lebih lanjut konsep *data justice* dalam perspektif hukum tata negara Indonesia.

Meskipun MK telah melangkah maju dalam mengartikulasikan standar konstitusional perlindungan privasi digital, masih terdapat sejumlah celah. Pertama, argumentasi mengenai asas proporsionalitas belum selalu dirumuskan dalam bentuk uji tiga langkah yang eksplisit (kecocokan, keniscayaan, dan keseimbangan). Kedua, tolok ukur mengenai independensi pengawasan belum dioperasionalkan secara rinci, misalnya terkait dengan standar pendanaan, pengangkatan, atau mekanisme akuntabilitas lembaga pengawas data. Ketiga, mekanisme pemulihan bagi korban pelanggaran privasi digital masih banyak bergantung pada pengaturan sektoral dan belum sepenuhnya didorong menjadi bagian dari hak prosedural yang dijamin konstitusi (Faiz, 2021; Ridwan, 2022).

Sejumlah keterbatasan ini menunjukkan bahwa yurisprudensi MK perlu dibaca tidak hanya sebagai jawaban final, tetapi sebagai *normative trajectory* yang mengarahkan pembentukan kebijakan publik. Putusan-putusan MK dapat dipahami

sebagai *constitutional signaling* bagi pembentuk undang-undang dan pemerintah untuk memperbaiki kerangka regulasi dan kelembagaan. Dalam konteks ini, pendekatan *governance-based* yang dikembangkan Mahkamah menuntut penyusunan kebijakan yang lebih peka terhadap risiko, berbasis bukti, dan selalu mengutamakan perlindungan hak asasi sebagai parameter utama legitimasi kekuasaan (Bennett & Raab, 2020).

Dengan demikian yurisprudensi MK telah bergerak dari pengujian unit tindakan (misalnya satu kewenangan penyadapan) menuju pengujian desain sistem (misalnya tata kelola perlindungan data secara menyeluruh). Pergeseran ini mencerminkan pemahaman bahwa pelanggaran privasi di era digital umumnya tidak terjadi melalui satu tindakan tunggal, melainkan melalui desain sistem informasi yang tidak adil, kurang transparan, dan tidak akuntabel. MK merespons hal ini dengan mengaitkan hak atas privasi dengan kebutuhan akan arsitektur tata kelola data yang *pro-privacy by design* dan *accountability by design*.

Dalam perspektif hukum tata negara, perkembangan tersebut mengukuhkan posisi MK sebagai *constitutional guardian* yang tidak hanya menjaga teks konstitusi, tetapi juga menafsirkan nilai-nilainya dalam menghadapi perkembangan teknologi yang cepat. Yurisprudensi privasi digital MK menjembatani kesenjangan antara norma konstitusional yang relatif umum dengan realitas pengawasan digital yang kompleks. Dari sini, terlihat bahwa perlindungan konstitusional privasi tidak dapat lagi dipahami sebatas doktrin abstrak, melainkan harus diartikulasikan dalam bentuk standar, prosedur, dan institusi yang konkret.

2. Implikasi Normatif dan Agenda Reformasi

Mahkamah Konstitusi (MK) pada pembahasan diatas menunjukkan bahwa pendekatan konstitusional terhadap privasi digital di Indonesia telah bergerak dari sekadar penafsiran deklaratif menuju pembentukan standar substantif yang operasional. Putusan-putusan terkait penyadapan, alat bukti elektronik, dan perlindungan data pribadi membentuk semacam *constitutional grammar* baru tentang bagaimana hak atas privasi harus dipahami, dibatasi, dan dijamin dalam ekosistem *data-driven governance*. Dari perspektif hukum tata negara, perkembangan ini tidak dapat berhenti pada tataran yudisial; ia menuntut perubahan dalam desain legislasi, kelembagaan, dan mekanisme pemulihan hak.

Pertama, dari sisi konstitusi tertulis, terdapat argumen kuat mengenai pentingnya pengakuan eksplisit hak atas privasi sebagai hak konstitusional di Indonesia. Ketiadaan rumusan *privacy* dalam batang tubuh maupun penjelasan UUD 1945 menyebabkan doktrin privasi berkembang terutama melalui konstruksi Mahkamah Konstitusi, yang bertumpu pada penafsiran Pasal 28G ayat (1), 28D ayat (1), dan 28J ayat (2). Meskipun pendekatan ini memungkinkan fleksibilitas, ia juga menyimpan ketidakpastian normatif, terutama ketika pembentuk undang-undang atau aparat penegak hukum memiliki pemahaman yang terbatas tentang cakupan privasi digital (Wahyudi, 2020). Dalam konteks ini, wacana amandemen terbatas atau pembentukan undang-undang organik yang secara eksplisit mengafirmasi hak atas privasi sebagai hak konstitusional sebagaimana praktik di banyak negara layak dipertimbangkan (Asshiddiqie, 2019; Faiz, 2021).

Kedua, dari sisi legislasi sektoral, fragmentasi pengaturan yang menyentuh privasi digital menjadi salah satu persoalan utama. Berbagai undang-undang mulai dari UU ITE, UU Telekomunikasi, UU Intelijen, hingga regulasi sektoral di bidang keuangan, kesehatan, dan kependudukan memberikan kewenangan pengumpulan, pemrosesan, dan pertukaran data tanpa selalu disertai standar minimal perlindungan yang konsisten. Di banyak titik, terdapat tumpang tindih, celah, bahkan kontradiksi antara satu regulasi dengan regulasi lainnya (Ridwan, 2022). UU PDP memang menghadirkan kerangka umum perlindungan data pribadi, namun tanpa harmonisasi sistemik dan *sunset clause* terhadap ketentuan sektoral yang bertentangan, maka risiko inkonsistensi tetap tinggi (Fitriani, 2022; Lubis, 2022).

Dalam perspektif *Minimum Constitutional Safeguards* (MCS), harmonisasi tersebut tidak hanya menyangkut konsistensi redaksional, tetapi juga penyeragaman standar substantif: misalnya, keharusan adanya dasar hukum yang jelas untuk setiap bentuk pemrosesan data; penentuan tujuan yang spesifik (*purpose limitation*); pengaturan batas waktu penyimpanan (*storage limitation*); kewajiban *logging* dan audit; serta mekanisme pengawasan independen dan pemulihan yang efektif. Standar-standar ini sejalan dengan prinsip-prinsip *data protection* global, namun dalam konteks Indonesia harus diterjemahkan ke dalam instrumen hukum yang realistis, memperhitungkan kapasitas kelembagaan, dan tetap berpijak pada nilai-nilai Pancasila serta konsep negara hukum demokratis (De Gregorio & Radu, 2022; Gellert, 2018).

Ketiga, pada tataran kelembagaan, agenda reformasi tak terelakkan terkait dengan desain dan penguatan otoritas pengawas perlindungan data pribadi. Putusan MK, khususnya terkait UU PDP, telah memberi sinyal bahwa perlindungan data pribadi tidak dapat diserahkan semata kepada mekanisme pengaturan diri (*self-regulation*) oleh pelaku usaha atau pengelola sistem elektronik. Diperlukan lembaga pengawas yang independen, memiliki mandat yang jelas, kewenangan investigatif yang memadai, serta terlindung dari intervensi politik jangka pendek (Bennett & Raab, 2020; Lubis, 2022). Dalam desain kelembagaan seperti ini, prinsip *accountability* bukan hanya dituntut dari pengendali data, tetapi juga dari lembaga pengawas itu sendiri.

Reformasi kelembagaan juga menuntut penataan ulang hubungan antar lembaga yang selama ini memiliki kewenangan parsial atas isu privasi dan data misalnya, antara kementerian teknis, lembaga intelijen, aparat penegak hukum, dan otoritas sektoral di bidang keuangan maupun telekomunikasi. Tanpa kejelasan tata hubungan kewenangan, koordinasi dan pengawasan saling silang berpotensi melemahkan perlindungan hak warga negara. Di sini, panduan dari Mahkamah Konstitusi mengenai prinsip non-delegasi, kejelasan kewenangan, dan kebutuhan pengawasan eksternal dapat dijadikan acuan bagi perancangan ulang struktur kelembagaan (Asshiddiqie, 2019; Faiz, 2021).

Keempat, agenda reformasi yang tidak kalah pentingnya adalah penguatan mekanisme pemulihan (*remedies*). Yurisprudensi MK menunjukkan kesadaran akan pentingnya *due process* dalam konteks privasi digital, terutama ketika pelanggaran hak terjadi melalui pengumpulan atau penggunaan data yang melampaui batas kewenangan. Namun, dalam praktik, akses warga negara terhadap sarana pemulihan baik litigasi maupun non-litigasi sering kali terkendala oleh biaya, informasi yang timpang, dan ketiadaan jalur penyelesaian sengketa yang cepat, sederhana, dan terjangkau (Harding, 2021). Oleh karena itu, agenda reformasi harus memasukkan penguatan mekanisme pengaduan administratif, prosedur *class action* atau *public interest litigation*, serta skema ganti rugi dan pemulihan non-material yang lebih progresif (Gstrein & Beaulieu, 2022; Mahdy et al., 2025).

Kelima, dari sisi budaya hukum (*legal culture*), perlindungan privasi digital tidak akan efektif tanpa peningkatan literasi hak konstitusional di kalangan aparat dan masyarakat. Banyak praktik pengumpulan data yang invasif berlangsung bukan

hanya karena lemahnya regulasi, tetapi juga karena anggapan bahwa data adalah sumber informasi yang bebas diolah selama bermanfaat bagi efektivitas birokrasi atau profit ekonomi. Padahal, dalam paradigma hak asasi manusia, data pribadi harus dipandang sebagai perpanjangan dari martabat dan otonomi individu, bukan sekadar komoditas (Gonzalez Fuster, 2014; Lynskey, 2023). Di sini, pendidikan hukum dan pelatihan teknis bagi pejabat publik, hakim, dan aparat penegak hukum menjadi bagian integral dari agenda reformasi.

Seluruh agenda tersebut berkelindan dengan peran MK sebagai *constitutional guardian*. Mahkamah tidak hanya menjaga teks konstitusi, tetapi juga menafsirkan nilai-nilai dasarnya di tengah perubahan teknologi yang cepat dan sering kali tidak diantisipasi oleh pembentuk konstitusi. Putusan-putusan tentang privasi digital memperlihatkan bagaimana Mahkamah menggunakan prinsip-prinsip umum UUD 1945 seperti martabat manusia, negara hukum, dan keadilan sosial untuk mengisi kekosongan normatif dalam menghadapi pengawasan digital dan tata kelola data berskala besar (Celeste, 2022; Ridwan, 2022).

Secara normatif, *Minimum Constitutional Safeguards* yang disarikan dari yurisprudensi MK menawarkan kerangka yang dapat diadopsi tidak hanya oleh pembentuk undang-undang, tetapi juga oleh lembaga eksekutif dan yudikatif. Bagi legislator, MCS dapat dijadikan daftar pemeriksaan (*checklist*) dalam merancang dan merevisi undang-undang yang menyentuh pengumpulan dan pemrosesan data, baik di sektor keamanan nasional, layanan publik digital, maupun ekonomi digital. Bagi lembaga eksekutif, MCS memberikan panduan untuk menata prosedur internal, melakukan penilaian dampak perlindungan data (*data protection impact assessment*), dan menyusun standar operasional yang *privacy-friendly*. Sedangkan bagi pengadilan, MCS dapat berfungsi sebagai set kriteria dalam menguji konstitusionalitas tindakan maupun kebijakan yang berimplikasi pada privasi digital (Bennett & Raab, 2020; Gellert, 2018).

C. Hasil Penelitian dan Pembahasan

1. Yurisprudensi Mahkamah Konstitusi Menuju Tata Kelola Data

Perlindungan konstitusional terhadap hak atas privasi dalam konteks digital di Indonesia dibentuk secara bertahap melalui konstruksi yurisprudensial

Mahkamah Konstitusi (MK). Putusan-putusan MK yang relevan menunjukkan adanya evolusi penting: dari semula berfokus pada keabsahan penyadapan dan alat bukti elektronik, menuju pembentukan kerangka tata kelola data yang lebih sistemik, berbasis risiko, dan berorientasi pada akuntabilitas lembaga. Pergeseran ini menandai transisi dari pendekatan yang bersifat *infringement-based* sekadar menilai sah atau tidaknya suatu tindakan yang membatasi hak menuju pendekatan *governance-based* yang menilai bagaimana sistem, prosedur, dan kelembagaan dirancang untuk mencegah pelanggaran sejak awal (Fitriani, 2022; Gstrein & Beaulieu, 2022).

Secara metodologis, yurisprudensi MK dalam isu privasi digital dapat dipetakan ke dalam tiga klaster besar. Pertama, klaster penyadapan dan intersepsi komunikasi, yang antara lain mencakup pengujian kewenangan lembaga penegak hukum melakukan penyadapan dalam perkara tindak pidana tertentu. Kedua, klaster perolehan dan keabsahan alat bukti elektronik, yang menelaah hubungan antara cara memperoleh data dengan prinsip *due process of law* dan hak atas peradilan yang adil. Ketiga, klaster perlindungan data pribadi setelah lahirnya Undang-Undang Pelindungan Data Pribadi (UU PDP), yang fokus pada desain kelembagaan, kewenangan otoritas pengawas, dan prinsip-prinsip tata kelola data yang sesuai dengan standar hak asasi manusia (Lynskey, 2023; Shahrullah et al., 2024).

Dalam putusan-putusan awal yang berkaitan dengan penyadapan, seperti Putusan No. 5/PUU-VIII/2010, MK menegaskan bahwa tindakan penyadapan merupakan bentuk pembatasan hak konstitusional, khususnya hak atas privasi dan rasa aman sebagaimana dijamin Pasal 28G ayat (1) UUD 1945. Oleh karena itu, tindakan tersebut hanya dapat dibenarkan apabila diatur secara tegas oleh undang-undang, bukan sekadar oleh peraturan pelaksana atau kebijakan administratif. Argumentasi ini sejalan dengan prinsip legalitas (*legality principle*) dalam hukum tata negara, yang menempatkan konstitusi dan undang-undang sebagai sumber legitimasi utama pembatasan hak (Asshiddiqie, 2019; Yuliandri, 2007). Dengan demikian, MK menggariskan bahwa setiap intervensi terhadap komunikasi privat harus jelas dasar hukumnya, ruang lingkupnya, serta mekanisme pengawasannya.

Dimensi lain tampak dalam Putusan No. 20/PUU-XIV/2016 yang berkaitan dengan alat bukti elektronik. Dalam perkara ini, Mahkamah menegaskan bahwa bukti elektronik hanya sah dan dapat digunakan dalam proses peradilan apabila diperoleh dengan cara yang sah. Dengan kata lain, tidak cukup bahwa bukti tersebut

relevan secara materiil; cara perolehannya pun harus sesuai dengan hukum dan menjunjung tinggi hak-hak terdakwa. Pendekatan ini mencerminkan integrasi prinsip *due process* ke dalam doktrin perolehan bukti digital, serta menunjukkan bahwa pelanggaran privasi dalam proses perolehan data dapat berdampak pada eksklusivitas bukti tersebut dari persidangan (Mahdy et al., 2025; Nurjihad, 2021). Di sini, hak atas privasi tidak hanya diposisikan sebagai hak substantif, tetapi juga sebagai elemen prosedural yang melekat pada hak atas peradilan yang adil.

Seiring dengan meningkatnya ketergantungan negara dan sektor swasta pada pengolahan data pribadi, MK mulai bergerak dari fokus pada tindakan intersepsi individual menuju penilaian terhadap desain sistemik tata kelola data. Momentum pentingnya adalah pengujian terhadap ketentuan dalam UU PDP yang berujung pada Putusan No. 151/PUU-XXII/2024. Dalam putusan ini, Mahkamah tidak hanya menilai apakah norma tertentu bertentangan dengan UUD 1945, tetapi juga menelaah apakah arsitektur kelembagaan dan mekanisme pengawasan yang dirancang UU PDP sudah memadai untuk menjamin perlindungan hak konstitusional atas data pribadi (Lubis, 2022).

Hak atas privasi digital dipahami sebagai hak yang tak dapat direalisasikan hanya melalui larangan formal, tetapi memerlukan *governance structure* yang konkret. Mahkamah menekankan pentingnya keberadaan otoritas pengawas data yang independen, keberadaan pejabat perlindungan data (*data protection officer*), kewajiban *logging* dan audit atas aktivitas pemrosesan data, serta mekanisme pengaduan dan pemulihan yang dapat diakses warga negara. Dengan demikian, MK memperluas cakupan perlindungan privasi dari sekadar relasi antara individu dan negara, menjadi relasi yang melibatkan aktor-aktor lain, termasuk badan usaha dan penyelenggara sistem elektronik (Bennett & Raab, 2020; Lynskey, 2023).

Pergeseran ini turut merefleksikan internalisasi prinsip-prinsip *data protection* internasional ke dalam tafsir konstitusi nasional. Konsep-konsep seperti *purpose limitation*, *data minimization*, *storage limitation*, dan *accountability* yang berkembang dalam rezim hukum Uni Eropa dan standar internasional lainnya, mulai tampak pengaruhnya dalam pertimbangan hukum MK, meskipun tidak selalu disebutkan secara eksplisit (De Gregorio & Radu, 2022; Gonzalez Fuster, 2014). MK menafsirkan Pasal 28G ayat (1) dan Pasal 28J ayat (2) UUD 1945 secara evolutif, sehingga hak

atas privasi dan pembatasannya dapat menjawab tantangan baru yang dihadirkan oleh teknologi digital dan *algorithmic governance*.

Selain itu, pola argumentasi MK menunjukkan bahwa privasi digital tidak lagi dipandang sebagai hak yang berdiri terpisah, tetapi berkaitan erat dengan hak-hak lain seperti kebebasan berekspresi, hak atas informasi, dan hak atas non-diskriminasi. Misalnya, dalam diskursus mengenai penggunaan data pribadi untuk profilisasi, *scoring*, atau penyaringan penerima layanan publik, terdapat risiko diskriminasi sistemik yang hanya dapat ditangkap jika privasi dipahami sebagai bagian dari kerangka keadilan sosial (*social justice*) yang lebih luas (Gellert, 2018; Gstrein & Beaulieu, 2022). Pada konteks ini, yurisprudensi MK membuka peluang untuk pengembangan lebih lanjut konsep *data justice* dalam perspektif hukum tata negara Indonesia.

Meskipun MK telah melangkah maju dalam mengartikulasikan standar konstitusional perlindungan privasi digital, masih terdapat sejumlah celah. Pertama, argumentasi mengenai asas proporsionalitas belum selalu dirumuskan dalam bentuk uji tiga langkah yang eksplisit (kecocokan, keniscayaan, dan keseimbangan). Kedua, tolok ukur mengenai independensi pengawasan belum dioperasionalkan secara rinci, misalnya terkait dengan standar pendanaan, pengangkatan, atau mekanisme akuntabilitas lembaga pengawas data. Ketiga, mekanisme pemulihan bagi korban pelanggaran privasi digital masih banyak bergantung pada pengaturan sektoral dan belum sepenuhnya didorong menjadi bagian dari hak prosedural yang dijamin konstitusi (Faiz, 2021; Ridwan, 2022).

Sejumlah keterbatasan ini menunjukkan bahwa yurisprudensi MK perlu dibaca tidak hanya sebagai jawaban final, tetapi sebagai *normative trajectory* yang mengarahkan pembentukan kebijakan publik. Putusan-putusan MK dapat dipahami sebagai *constitutional signaling* bagi pembentuk undang-undang dan pemerintah untuk memperbaiki kerangka regulasi dan kelembagaan. Dalam konteks ini, pendekatan *governance-based* yang dikembangkan Mahkamah menuntut penyusunan kebijakan yang lebih peka terhadap risiko, berbasis bukti, dan selalu mengutamakan perlindungan hak asasi sebagai parameter utama legitimasi kekuasaan (Bennett & Raab, 2020).

Dengan demikian yurisprudensi MK telah bergerak dari pengujian unit tindakan (misalnya satu kewenangan penyadapan) menuju pengujian desain sistem (misalnya tata kelola perlindungan data secara menyeluruh). Pergeseran ini mencerminkan pemahaman bahwa pelanggaran privasi di era digital umumnya tidak terjadi melalui satu tindakan tunggal, melainkan melalui desain sistem informasi yang tidak adil, kurang transparan, dan tidak akuntabel. MK merespons hal ini dengan mengaitkan hak atas privasi dengan kebutuhan akan arsitektur tata kelola data yang *pro-privacy by design* dan *accountability by design*.

Dalam perspektif hukum tata negara, perkembangan tersebut mengukuhkan posisi MK sebagai *constitutional guardian* yang tidak hanya menjaga teks konstitusi, tetapi juga menafsirkan nilai-nilainya dalam menghadapi perkembangan teknologi yang cepat. Yurisprudensi privasi digital MK menjembatani kesenjangan antara norma konstitusional yang relatif umum dengan realitas pengawasan digital yang kompleks. Dari sini, terlihat bahwa perlindungan konstitusional privasi tidak dapat lagi dipahami sebatas doktrin abstrak, melainkan harus diartikulasikan dalam bentuk standar, prosedur, dan institusi yang konkret.

2. Implikasi Normatif dan Agenda Reformasi

Mahkamah Konstitusi (MK) pada pembahasan diatas menunjukkan bahwa pendekatan konstitusional terhadap privasi digital di Indonesia telah bergerak dari sekadar penafsiran deklaratif menuju pembentukan standar substantif yang operasional. Putusan-putusan terkait penyadapan, alat bukti elektronik, dan perlindungan data pribadi membentuk semacam *constitutional grammar* baru tentang bagaimana hak atas privasi harus dipahami, dibatasi, dan dijamin dalam ekosistem *data-driven governance*. Dari perspektif hukum tata negara, perkembangan ini tidak dapat berhenti pada tataran yudisial; ia menuntut perubahan dalam desain legislasi, kelembagaan, dan mekanisme pemulihan hak.

Pertama, dari sisi konstitusi tertulis, terdapat argumen kuat mengenai pentingnya pengakuan eksplisit hak atas privasi sebagai hak konstitusional di Indonesia. Ketidadaan rumusan *privacy* dalam batang tubuh maupun penjelasan UUD 1945 menyebabkan doktrin privasi berkembang terutama melalui konstruksi Mahkamah Konstitusi, yang bertumpu pada penafsiran Pasal 28G ayat (1), 28D ayat (1), dan 28J ayat (2). Meskipun pendekatan ini memungkinkan fleksibilitas, ia juga menyimpan

ketidakpastian normatif, terutama ketika pembentuk undang-undang atau aparat penegak hukum memiliki pemahaman yang terbatas tentang cakupan privasi digital (Wahyudi, 2020). Dalam konteks ini, wacana amandemen terbatas atau pembentukan undang-undang organik yang secara eksplisit mengafirmasi hak atas privasi sebagai hak konstitusional sebagaimana praktik di banyak negara layak dipertimbangkan (Asshiddiqie, 2019; Faiz, 2021).

Kedua, dari sisi legislasi sektoral, fragmentasi pengaturan yang menyentuh privasi digital menjadi salah satu persoalan utama. Berbagai undang-undang mulai dari UU ITE, UU Telekomunikasi, UU Intelijen, hingga regulasi sektoral di bidang keuangan, kesehatan, dan kependudukan memberikan kewenangan pengumpulan, pemrosesan, dan pertukaran data tanpa selalu disertai standar minimal perlindungan yang konsisten. Di banyak titik, terdapat tumpang tindih, celah, bahkan kontradiksi antara satu regulasi dengan regulasi lainnya (Ridwan, 2022). UU PDP memang menghadirkan kerangka umum perlindungan data pribadi, namun tanpa harmonisasi sistemik dan *sunset clause* terhadap ketentuan sektoral yang bertentangan, maka risiko inkonsistensi tetap tinggi (Fitriani, 2022; Lubis, 2022).

Dalam perspektif *Minimum Constitutional Safeguards* (MCS), harmonisasi tersebut tidak hanya menyangkut konsistensi redaksional, tetapi juga penyeragaman standar substantif: misalnya, keharusan adanya dasar hukum yang jelas untuk setiap bentuk pemrosesan data; penentuan tujuan yang spesifik (*purpose limitation*); pengaturan batas waktu penyimpanan (*storage limitation*); kewajiban *logging* dan audit; serta mekanisme pengawasan independen dan pemulihan yang efektif. Standar-standar ini sejalan dengan prinsip-prinsip *data protection* global, namun dalam konteks Indonesia harus diterjemahkan ke dalam instrumen hukum yang realistis, memperhitungkan kapasitas kelembagaan, dan tetap berpijak pada nilai-nilai Pancasila serta konsep negara hukum demokratis (De Gregorio & Radu, 2022; Gellert, 2018).

Ketiga, pada tataran kelembagaan, agenda reformasi tak terelakkan terkait dengan desain dan penguatan otoritas pengawas perlindungan data pribadi. Putusan MK, khususnya terkait UU PDP, telah memberi sinyal bahwa perlindungan data pribadi tidak dapat diserahkan semata kepada mekanisme pengaturan diri (*self-regulation*) oleh pelaku usaha atau pengelola sistem elektronik. Diperlukan lembaga pengawas yang independen, memiliki mandat yang jelas, kewenangan investigatif

yang memadai, serta terlindung dari intervensi politik jangka pendek (Bennett & Raab, 2020; Lubis, 2022). Dalam desain kelembagaan seperti ini, prinsip *accountability* bukan hanya dituntut dari pengendali data, tetapi juga dari lembaga pengawas itu sendiri.

Reformasi kelembagaan juga menuntut penataan ulang hubungan antar lembaga yang selama ini memiliki kewenangan parsial atas isu privasi dan data misalnya, antara kementerian teknis, lembaga intelijen, aparat penegak hukum, dan otoritas sektoral di bidang keuangan maupun telekomunikasi. Tanpa kejelasan tata hubungan kewenangan, koordinasi dan pengawasan saling silang berpotensi melemahkan perlindungan hak warga negara. Di sini, panduan dari Mahkamah Konstitusi mengenai prinsip non-delegasi, kejelasan kewenangan, dan kebutuhan pengawasan eksternal dapat dijadikan acuan bagi perancangan ulang struktur kelembagaan (Asshiddiqie, 2019; Faiz, 2021).

Keempat, agenda reformasi yang tidak kalah pentingnya adalah penguatan mekanisme pemulihan (*remedies*). Yurisprudensi MK menunjukkan kesadaran akan pentingnya *due process* dalam konteks privasi digital, terutama ketika pelanggaran hak terjadi melalui pengumpulan atau penggunaan data yang melampaui batas kewenangan. Namun, dalam praktik, akses warga negara terhadap sarana pemulihan baik litigasi maupun non-litigasi sering kali terkendala oleh biaya, informasi yang timpang, dan ketiadaan jalur penyelesaian sengketa yang cepat, sederhana, dan terjangkau (Harding, 2021). Oleh karena itu, agenda reformasi harus memasukkan penguatan mekanisme pengaduan administratif, prosedur *class action* atau *public interest litigation*, serta skema ganti rugi dan pemulihan non-material yang lebih progresif (Gstrein & Beaulieu, 2022; Mahdy et al., 2025).

Kelima, dari sisi budaya hukum (*legal culture*), perlindungan privasi digital tidak akan efektif tanpa peningkatan literasi hak konstitusional di kalangan aparat dan masyarakat. Banyak praktik pengumpulan data yang invasif berlangsung bukan hanya karena lemahnya regulasi, tetapi juga karena anggapan bahwa data adalah sumber informasi yang bebas diolah selama bermanfaat bagi efektivitas birokrasi atau profit ekonomi. Padahal, dalam paradigma hak asasi manusia, data pribadi harus dipandang sebagai perpanjangan dari martabat dan otonomi individu, bukan sekadar komoditas (Gonzalez Fuster, 2014; Lynskey, 2023). Di sini, pendidikan

hukum dan pelatihan teknis bagi pejabat publik, hakim, dan aparat penegak hukum menjadi bagian integral dari agenda reformasi.

Seluruh agenda tersebut berkelindan dengan peran MK sebagai *constitutional guardian*. Mahkamah tidak hanya menjaga teks konstitusi, tetapi juga menafsirkan nilai-nilai dasarnya di tengah perubahan teknologi yang cepat dan sering kali tidak diantisipasi oleh pembentuk konstitusi. Putusan-putusan tentang privasi digital memperlihatkan bagaimana Mahkamah menggunakan prinsip-prinsip umum UUD 1945 seperti martabat manusia, negara hukum, dan keadilan sosial untuk mengisi kekosongan normatif dalam menghadapi pengawasan digital dan tata kelola data berskala besar (Celeste, 2022; Ridwan, 2022).

Secara normatif, *Minimum Constitutional Safeguards* yang disarikan dari yurisprudensi MK menawarkan kerangka yang dapat diadopsi tidak hanya oleh pembentuk undang-undang, tetapi juga oleh lembaga eksekutif dan yudikatif. Bagi legislator, MCS dapat dijadikan daftar periksa (*checklist*) dalam merancang dan merevisi undang-undang yang menyentuh pengumpulan dan pemrosesan data, baik di sektor keamanan nasional, layanan publik digital, maupun ekonomi digital. Bagi lembaga eksekutif, MCS memberikan panduan untuk menata prosedur internal, melakukan penilaian dampak perlindungan data (*data protection impact assessment*), dan menyusun standar operasional yang *privacy-friendly*. Sedangkan bagi pengadilan, MCS dapat berfungsi sebagai set kriteria dalam menguji konstitusionalitas tindakan maupun kebijakan yang berimplikasi pada privasi digital (Bennett & Raab, 2020; Gellert, 2018).

D. Penutup

Era digital telah menggeser lanskap hubungan antara negara dan warga negara ke ruang yang sangat ditandai oleh data dan algoritma. Dalam konteks ini, hak atas privasi tidak lagi dapat dipahami sebagai hak pinggiran, melainkan sebagai salah satu pilar utama perlindungan konstitusional yang memastikan bahwa kekuasaan informasi tidak digunakan secara sewenang-wenang. Yurisprudensi Mahkamah Konstitusi Indonesia menunjukkan bahwa perlindungan terhadap privasi digital sedang dibentuk melalui serangkaian putusan yang menjembatani teks UUD 1945 dengan tantangan *data-driven governance*.

Melalui analisis atas putusan-putusan kunci, terlihat bahwa Mahkamah secara bertahap membangun standar tentang legalitas, keniscayaan, proporsionalitas, pengawasan independen, jaminan prosedural, dan mekanisme pemulihan. Standar-standar tersebut kemudian dikonsolidasikan dalam bentuk *Minimum Constitutional Safeguards* yang dapat berfungsi sebagai rujukan normatif bagi semua aktor negara. Dengan demikian, perlindungan privasi digital tidak lagi bergantung pada niat baik lembaga semata, tetapi ditopang oleh doktrin konstitusional yang lebih terstruktur.

Artikel ini menegaskan bahwa agenda ke depan adalah menerjemahkan standar-standar konstitusional tersebut ke dalam reformasi legislasi, penguatan kelembagaan, dan pengembangan mekanisme pemulihan yang efektif. Upaya tersebut harus disertai peningkatan literasi hak konstitusional, transparansi tata kelola data, dan partisipasi publik dalam perumusan kebijakan digital. Hanya dengan cara demikian konstitusionalisme Indonesia dapat bertahan dan berkembang dalam menghadapi risiko struktural yang ditimbulkan oleh pengawasan digital dan pengolahan data berskala besar.

Dengan kata lain, perlindungan konstitusional atas hak privasi digital tidak boleh berhenti pada putusan Mahkamah Konstitusi. Ia harus menjadi kerangka kerja hidup yang menuntun kerja legislator, pemerintah, dan lembaga penegak hukum dalam setiap kebijakan yang menyentuh data pribadi warga negara. Jika hal ini terwujud, maka Indonesia dapat membangun ekosistem digital yang tidak hanya efisien dan inovatif, tetapi juga adil, manusiawi, dan setia pada nilai-nilai konstitusi.

E. Daftar Pustaka

- Asshiddiqie, J. (2019). *Hukum Konstitusi dan Mahkamah Konstitusi*. Konstitusi Press.
- Bennett, C. J., & Raab, C. D. (2020). *The governance of privacy: Policy instruments in global perspective* (3rd ed.). MIT Press.
- Celeste, E. (2022). *Digital Constitutionalism: The Role of Internet Bills of Rights*. Routledge. <https://doi.org/10.4324/9781003256908>
- Dalla Corte, L. (2022). On proportionality in the data protection jurisprudence of the CJEU. *International Data Privacy Law*, 12(4), 259–275. <https://doi.org/10.1093/idpl/ipac014>
- De Gregorio, G., & Radu, R. (2022). Digital constitutionalism in the new era of Internet governance. *International Journal of Law and Information Technology*, 30(1), 68–87. <https://doi.org/10.1093/ijlit/eaac004>

- Faiz, P. M. (2021). *Reformasi kelembagaan dalam hukum tata negara Indonesia*. Rajawali Pers.
- Fitriani, E. (2022). *Perlindungan data pribadi dalam perspektif hukum tata negara*. Genta Publishing.
- Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review*, 34(2), 279–288. <https://doi.org/10.1016/j.clsr.2017.12.002>
- Gonzalez Fuster, G. (2014). *The emergence of personal data protection as a fundamental right of the EU*. Springer.
- Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy & Technology*, 35(1), 3. <https://doi.org/10.1007/s13347-022-00497-4>
- Harding, R. (2021). *Privacy and data protection law: The rights of individuals in the digital age*. Oxford University Press.
- Lubis, Y. C. (2022). *Desain lembaga pengawas perlindungan data pribadi: Kajian komparatif dan konstitusional*. Refika Aditama.
- Lynskey, O. (2023). Complete and Effective Data Protection. *Current Legal Problems*, 76(1), 297–344. <https://doi.org/10.1093/clp/cuad009>
- MAHDY, M., Hartiwiningsih, H., & Isharyanto, I. (2025). Wiretapping Law in Indonesia; *Asian Journal of Human Services*, 28(0), 242–272. <https://doi.org/10.14391/ajhs.28.242>
- Mahdy, W., Hartiwiningsih, H., Isharyanto, I., & Sobirov, M. (2025). Reformulation of Wiretapping Regulations Based on Criminal Justice Reform: Lessons from the United States and United Kingdom. *Indonesian Journal of Crime and Criminal Justice*, 3(1). <https://doi.org/10.60712/ijccj.v3i1.193>
- Nurjihad, A. (2021). *Hukum acara konstitusi dan pembuktian digital*. Sinar Grafika.
- Ridwan, M. (2022). *Konstitusi digital dan reformasi tata kelola informasi*. Rajawali Pers.
- Rojszczak, M. (2021). Surveillance, Legal Restraints and Dismantling Democracy: Lessons from Poland. *Democracy and Security*, 17(1), 1–29. <https://doi.org/10.1080/17419166.2020.1841367>
- Shahrullah, R. S., Park, J., & Irwansyah, I. (2024). Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment. *Hasanuddin Law Review*, 10(1), 1. <https://doi.org/10.20956/halrev.v10i1.5016>
- Yuliandri. (2007). *Asas-asas Pembentukan Peraturan Perundang-undangan yang Baik dalam Rangka Pembuatan undang-undang Berkelanjutan* [Disertasi]. Universitas Airlangga.