

KEBIJAKAN VERIFIKASI BIOMETRIK DAN PERLINDUNGAN HAK KONSTITUSIONAL DALAM PERSPEKTIF KONSTITUSIONALISME DIGITAL DI INDONESIA

M.Yasin al Arif

Fakultas Syariah, UIN Raden Intan Lampung, Indonesia
myasinalarif@radenintan.ac.id

Diajukan: 14 Oktober 2025 | Diterima: 5 November 2025 | Diterbitkan: 10 Maret 2026

Abstrak

Perkembangan teknologi digital telah mengubah cara negara menjalankan fungsi pemerintahan dan pengawasan terhadap warga negara. Salah satu manifestasinya adalah kebijakan verifikasi biometrik yang direncanakan oleh Kementerian Komunikasi dan Digital (Komdigi) untuk memperkuat keamanan digital dan menekan penyebaran konten negatif. Namun, kebijakan ini menimbulkan persoalan konstitusional serius karena berpotensi melanggar hak privasi, kebebasan berekspresi, dan rasa aman warga negara yang dijamin dalam Pasal 28F, 28G, dan 28I UUD 1945. Penelitian ini bertujuan untuk menganalisis kebijakan verifikasi biometrik Komdigi dalam perspektif *digital constitutionalism* dengan menggunakan tiga uji konstitusionalitas, yaitu legalitas, tujuan sah, dan proporsionalitas. Jenis penelitian ini adalah penelitian hukum normatif dengan pendekatan konseptual, perundang-undangan, perbandingan, dan kasus. Data penelitian diperoleh dari bahan hukum primer (peraturan perundang-undangan dan putusan pengadilan), sekunder (buku, jurnal, laporan penelitian), dan tersier (kamus serta panduan internasional). Hasil analisis menunjukkan bahwa kebijakan verifikasi biometrik Komdigi belum memenuhi syarat konstitusional, terutama karena ketiadaan dasar hukum eksplisit, otoritas pengawas independen, dan mekanisme *data protection impact assessment* (DPIA). Penelitian ini menawarkan model *constitutional-by-design biometric governance* yang mengintegrasikan prinsip *digital constitutionalism*, perlindungan hak konstitusional, dan akuntabilitas algoritmik, serta menekankan pentingnya penguatan Komisi Perlindungan Data Pribadi sebagai lembaga pengawas independen.

Kata Kunci: Konstitusionalisme Digital, Verifikasi Biometrik, Hak Konstitusional, Proporsionalitas, Tata Kelola Data.

Abstract

The rapid development of digital technology has transformed the way states exercise governance and surveillance over citizens. One manifestation of this transformation is the biometric verification policy planned by Indonesia's Ministry of Communication and Digital (Komdigi), intended to strengthen digital security and counter online misinformation. However, this policy raises significant constitutional concerns as it potentially violates



2025 Proceeding APHTN-HAN

This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License

citizens' rights to privacy, freedom of expression, and personal security as guaranteed under Articles 28F, 28G, and 28I of the 1945 Constitution. This study analyzes Komdigi's biometric verification policy through the lens of digital constitutionalism by applying three constitutional tests: legality, legitimate aim, and proportionality. The research employs a normative legal method with conceptual, statutory, comparative, and case approaches. Data were collected from primary legal materials (legislation and court decisions), secondary sources (books, journal articles, and reports), and tertiary materials (legal dictionaries and international guidelines). The findings reveal that Komdigi's biometric verification policy fails to meet constitutional standards due to the absence of explicit legal foundations, an independent supervisory authority, and a mandatory data protection impact assessment (DPIA). This article proposes a constitutional-by-design biometric governance model integrating principles of digital constitutionalism, constitutional rights protection, and algorithmic accountability, emphasizing the need to strengthen the Personal Data Protection Commission as an independent oversight body.

Keywords: *Digital Constitutionalism, Biometric Verification, Constitutional Rights, Proportionality, Data Governance.*

I. PENDAHULUAN

A. Latar belakang

Perkembangan teknologi digital dalam satu dekade terakhir telah mengubah cara negara mengelola pemerintahan dan melakukan pengawasan terhadap warga negara. Salah satu bentuk nyata transformasi tersebut adalah penggunaan teknologi biometrik – seperti pengenalan wajah (*facial recognition*), sidik jari, dan pemindaian iris mata – yang kini menjadi bagian penting dalam sistem identitas digital di banyak negara.¹ Teknologi ini diadopsi dengan alasan efisiensi dan keamanan karena mampu mempercepat proses verifikasi identitas serta mencegah penipuan digital. Namun, di balik manfaat tersebut, biometrik menyimpan potensi ancaman terhadap hak-hak dasar manusia, khususnya privasi, otonomi personal, dan kebebasan berekspresi. Karena data biometrik bersifat permanen dan tidak dapat diganti, penyalahgunaannya dapat menciptakan bentuk pengawasan struktural (*structural surveillance*) yang sulit dikontrol.²

Dalam konteks tersebut, muncul paradigma baru dalam hukum tata negara yang dikenal sebagai *digital constitutionalism*. Konsep ini menegaskan bahwa kekuasaan digital – baik yang dijalankan oleh negara maupun korporasi teknologi – harus tunduk pada prinsip-prinsip konstitusional seperti *rule of law*, perlindungan hak-hak fundamental, dan *checks and balances*.³ *Digital constitutionalism* hadir sebagai

¹ Mark Simonitis, "Note: Facial Recognition Technology And The Constitution," *Notre Dame Journal on Emerging Technologies* 2, no. 2 (2021), <https://scholarship.law.nd.edu/ndlsjet/vol2/iss2/5>.

² Michael Odden, "Biometric Crisis: Legal Challenges to Biometric Identification Initiatives," *Wisconsin International Law Journal* 39, no. 2 (2022): 365–90.

³ Edoardo Celeste, "Digital Constitutionalism, EU Digital Sovereignty Ambitions and the Role of the European Declaration on Digital Rights," dalam *New Directions in Digitalisation Perspectives from EU Competition Law and the Charter of Fundamental Rights*, vol. 13 (European Union and its

upaya untuk menegaskan kembali supremasi konstitusi di tengah ekspansi kekuasaan digital yang kian dominan, sekaligus sebagai mekanisme normatif untuk memastikan bahwa inovasi teknologi tidak melanggar batas-batas konstitusional negara demokrasi.

Diskursus global ini menemukan relevansinya di Indonesia seiring rencana Kementerian Komunikasi dan Digital (Komdigi) tahun 2025 yang akan menerapkan kebijakan verifikasi biometrik bagi pengguna media sosial dan layanan digital.⁴ Kebijakan ini diklaim bertujuan menekan penyebaran hoaks dan ujaran kebencian serta memperkuat keamanan siber nasional. Namun, sejumlah akademisi dan organisasi masyarakat sipil menilai kebijakan ini berpotensi melanggar hak-hak konstitusional warga, seperti hak atas privasi (Pasal 28G UUD 1945), kebebasan berekspresi (Pasal 28F), dan perlindungan data pribadi. Kekhawatiran ini semakin beralasan karena meskipun UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah disahkan, otoritas pengawas independen sebagaimana diamanatkan undang-undang belum dibentuk. Akibatnya, tidak ada mekanisme pengawasan yang efektif terhadap pengumpulan dan pemrosesan data biometrik warga.

Kondisi ini menyingkap kesenjangan antara kemajuan teknologi dan perlindungan hak konstitusional. Beberapa penelitian sebelumnya, seperti Asokawati⁵ dan Muh. Aqil al Naufal,⁶ juga mengonfirmasi lemahnya kerangka hukum nasional dalam menjamin praktik perlindungan data biometrik sehingga rawan untuk dieksploitasi. Sementara itu, kajian internasional oleh De Gregorio⁷ dan Pollicino⁸ menunjukkan pentingnya *constitutional anchoring* terhadap kebijakan digital agar tidak berkembang menjadi alat kekuasaan yang otoriter.

Kesenjangan konseptual dan normatif ini menimbulkan persoalan mendasar bagi hukum tata negara Indonesia: sejauh mana penggunaan kekuasaan digital oleh negara dapat tetap sejalan dengan prinsip-prinsip konstitusionalisme. Hingga kini, penelitian di Indonesia cenderung membahas perlindungan data pribadi dari sudut pandang keamanan siber, bukan dari perspektif konstitusionalisme digital. Karena itu, penelitian ini menempati posisi kebaruan (*novelty*) dengan memadukan

Neighbours in a Globalized World, 2025); Giovanni De Gregorio dan Roxana Radu, "Digital Constitutionalism in the New Era of Internet Governance," *International Journal of Law and Information Technology* 30, no. 1 (2022): 68–87, <https://doi.org/10.1093/ijlit/eaac004>.

⁴ Dhelly Ramadhon Tambunan, "Komdigi Siapkan Verifikasi Biometrik Untuk Akun Digital," Rri.Co.Id - Portal Berita Terpercaya, diakses 13 Oktober 2025, <https://rri.co.id/lain-lain/1849375/komdigi-siapkan-verifikasi-biometrik-untuk-akun-digital>.

⁵ Ainunnisa Rezky Asokawati, "Perlindungan Data Biometrik Dalam Sektor Perbankan Di Indonesia Dan Amerika Serikat," *Legal Standing: Jurnal Ilmu Hukum* 8, no. 3a (2024): 895–907, <https://doi.org/10.24269/lis.v8i3a.10775>.

⁶ Muh Aqil Al Naufal H.s dan Imam Fadhil Nugraha, "Worldcoin Dan Ancaman Privasi Biometrik: Tinjauan Cyber Ethics Dalam Konteks Regulasi Digital Indonesia," *Triwikrama: Jurnal Ilmu Sosial* 8, no. 9 (2025): 1–10, <https://doi.org/10.9963/cv8e1274>.

⁷ Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*, Cambridge Studies in European Law and Policy (Cambridge University Press, 2022), <https://doi.org/10.1017/9781009071215>.

⁸ Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet A Road Towards Digital Constitutionalism?* (Hart Publishing, 2021).

teori *digital constitutionalism* dan teori perlindungan hak konstitusional untuk menyusun kerangka konstitusional minimal bagi kebijakan verifikasi biometrik di Indonesia. Tujuan utama penelitian ini adalah menganalisis kesesuaian kebijakan verifikasi biometrik Komdigi dengan prinsip-prinsip konstitusionalisme digital, menilai legalitas serta proporsionalitas kebijakan tersebut, dan merumuskan model *constitutional-by-design biometric governance* yang menjamin supremasi konstitusi dalam tata kelola teknologi digital.

B. Rumusan Masalah

Berangkat dari uraian latar belakang di atas, maka rumusan masalah dalam penelitian ini adalah

1. Bagaimana prinsip-prinsip *digital constitutionalism* dapat digunakan sebagai paradigma hukum tata negara untuk membatasi dan mengawasi kekuasaan digital negara dalam kebijakan verifikasi biometrik?
2. Sejauh mana kerangka hukum dan konstitusional di Indonesia mampu menjamin perlindungan hak konstitusional warga terhadap penerapan kebijakan biometrik?
3. Bagaimana membangun model *constitutional-by-design biometric governance* yang menjamin supremasi konstitusi, akuntabilitas algoritmik, dan perlindungan hak digital warga negara di Indonesia?

C. Metode Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif. Penelitian hukum normatif dipilih karena isu yang dikaji dalam artikel ini tidak bersifat empiris, melainkan konseptual dan normatif, yaitu berfokus pada pengujian kesesuaian kebijakan verifikasi biometrik Komdigi dengan prinsip-prinsip konstitusional dalam kerangka *digital constitutionalism*.

Pendekatan yang digunakan meliputi empat pendekatan utama: pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*) dan pendekatan perbandingan (*comparative approach*). Pendekatan perundang-undangan digunakan untuk menelaah berbagai ketentuan hukum nasional yang relevan dengan isu perlindungan data pribadi dan hak konstitusional, seperti Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD 1945), khususnya Pasal 28F, 28G, dan 28I tentang hak atas privasi, rasa aman, dan kebebasan berekspresi. Selain itu, digunakan juga UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai kerangka hukum utama yang mengatur pemrosesan data pribadi di Indonesia. Pendekatan konseptual digunakan untuk menganalisis teori dan doktrin hukum yang relevan, terutama teori *digital constitutionalism*, *constitutional limitation of power*, *proportionality principle*, dan *algorithmic accountability* yang menjadi landasan normatif dalam menilai sejauh mana kekuasaan negara dalam ruang digital harus dibatasi oleh konstitusi. Sementara itu, pendekatan perbandingan digunakan untuk melihat praktik tata kelola data biometrik di negara lain sebagai cerminan penerapan prinsip konstitusional dalam konteks digital. Dalam hal ini, penelitian ini membandingkan pengaturan di Uni

Eropa melalui *General Data Protection Regulation (GDPR)*, di India melalui putusan *Justice K.S. Puttaswamy v. Union of India (Aadhaar Case, 2018)*.

Data yang digunakan dalam penelitian ini sepenuhnya bersifat sekunder, karena penelitian ini tidak melakukan pengumpulan data lapangan. Data sekunder diperoleh melalui studi kepustakaan (*library research*) dengan menelaah dan menganalisis berbagai sumber hukum yang relevan. Sumber data sekunder tersebut terdiri dari bahan hukum primer, sekunder, dan tersier. Bahan hukum primer mencakup seluruh peraturan perundang-undangan yang memiliki kekuatan mengikat, antara lain UUD 1945, UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Di samping itu, penelitian ini juga menggunakan bahan hukum primer internasional, seperti *General Data Protection Regulation (GDPR)* Uni Eropa, *Biometric Information Privacy Act (BIPA)* Illinois, dan putusan-putusan pengadilan internasional yang mengatur perlindungan data biometrik dan hak privasi.

Adapun bahan hukum sekunder terdiri dari buku, jurnal ilmiah, artikel akademik, dan laporan penelitian yang memberikan penjelasan dan interpretasi terhadap bahan hukum primer. Metode pengumpulan data dilakukan melalui penelusuran literatur dan dokumentasi hukum, di mana penulis mengidentifikasi dan menginventarisasi sumber hukum yang relevan, kemudian mengklasifikasikannya berdasarkan tingkat kekuatan hukum dan relevansinya terhadap masalah penelitian. Analisis data dilakukan secara kualitatif-normatif, yaitu dengan menafsirkan norma-norma hukum untuk menemukan kesesuaian antara teori, asas, dan praktik kebijakan. Analisis dilakukan dalam tiga tahap: pertama, deskriptif-analitis, yaitu menguraikan ketentuan hukum nasional dan internasional yang terkait dengan tata kelola data biometric.

II. PEMBAHASAN

A. Konstitusionalisme Digital dan Pembatasan Kekuasaan Negara dalam Tata Kelola Biometrik

Perkembangan teknologi digital dalam dekade terakhir telah mengubah cara kekuasaan negara dijalankan dan dikontrol. Dalam konteks masyarakat modern yang semakin terhubung melalui jaringan data, algoritma, dan sistem otomatisasi, kekuasaan tidak lagi semata-mata dijalankan melalui perangkat institusional tradisional seperti eksekutif, legislatif, atau yudikatif, tetapi juga melalui desain teknologi dan infrastruktur digital. Fenomena ini menimbulkan bentuk kekuasaan baru yang disebut oleh Giovanni De Gregorio sebagai *digital power* – yakni kekuasaan yang dijalankan melalui data, kode, dan algoritma yang beroperasi dalam ruang siber tanpa batas geografis.⁹ Menurutnya, munculnya kekuasaan digital tersebut menggeser kebutuhan mendesak bagi hukum konstitusi modern untuk beradaptasi dengan realitas baru di mana keputusan penting, yang berdampak langsung pada hak-hak warga negara, diambil bukan lagi oleh manusia, tetapi oleh sistem teknologi yang didesain dan dijalankan secara otomatis. Dalam kondisi ini, *digital*

⁹ Giovanni De Gregorio, "The rise of digital constitutionalism in the European Union," *International Journal of Constitutional Law* 19, no. 1 (2021): 41–70, <https://doi.org/10.1093/icon/moab001>.

constitutionalism hadir sebagai paradigma normatif baru yang bertujuan untuk mengembalikan supremasi konstitusi dalam mengontrol kekuasaan di ruang digital.

De Gregorio menegaskan bahwa *digital constitutionalism* merupakan suatu gerakan normatif yang berupaya menundukkan kekuasaan digital pada nilai-nilai dasar konstitusional seperti *rule of law*, *accountability*, *fundamental rights*, dan *checks and balances*.¹⁰ Prinsip *rule of law* dalam konteks digital menuntut agar setiap bentuk penggunaan teknologi oleh negara harus berlandaskan hukum yang jelas, dapat dipertanggungjawabkan, dan terbuka untuk diuji secara publik. Oreste Pollicino menyoroti bahwa tantangan utama *rule of law* di era digital adalah bagaimana menjamin agar keputusan yang dihasilkan oleh algoritma tidak menjadi bentuk kekuasaan yang tersembunyi (*hidden power*) yang bebas dari mekanisme pengawasan hukum.¹¹ Menurut Pollicino, diperlukan inovasi hukum konstitusional yang memungkinkan munculnya hak-hak baru seperti *right to explanation* (hak untuk mendapatkan penjelasan atas keputusan algoritmik) dan *algorithmic transparency* (transparansi terhadap logika sistem) agar warga tetap dapat menuntut pertanggungjawaban atas kebijakan digital yang menyangkut kepentingan publik.¹²

Selain *rule of law*, prinsip *accountability* menjadi elemen kunci dalam memastikan bahwa kekuasaan digital tidak berkembang tanpa kontrol. Edoardo Celeste menulis bahwa *accountability* dalam era digital harus dipahami secara luas, tidak hanya sebagai tanggung jawab hukum, tetapi juga tanggung jawab etis dan institusional dalam merancang sistem teknologi yang sejalan dengan nilai-nilai hak asasi manusia.¹³ Akuntabilitas digital menuntut agar setiap kebijakan berbasis teknologi, termasuk kebijakan verifikasi biometrik, disertai dengan *impact assessment* yang jelas, mekanisme pengawasan independen, dan saluran pengaduan (*effective remedy*) yang mudah diakses oleh publik. Celeste menegaskan bahwa tanpa akuntabilitas yang nyata, negara digital dapat berubah menjadi entitas yang tidak tersentuh oleh hukum, sehingga melanggar prinsip dasar demokrasi konstitusional.

Prinsip ketiga dalam konstitusionalisme digital adalah perlindungan terhadap *fundamental rights*. Zuiderveen Borgesius mengemukakan bahwa hak-hak dasar yang diakui oleh konstitusi, seperti hak atas privasi, kebebasan berekspresi, dan perlindungan dari diskriminasi, kini harus ditafsirkan ulang agar relevan dengan konteks digital.¹⁴ Dalam dunia yang diatur oleh data, pelanggaran terhadap hak-hak dasar tidak lagi dilakukan secara fisik, tetapi melalui pemrosesan informasi yang tidak transparan, penyalahgunaan data pribadi, atau pengawasan massal yang melampaui batas proporsionalitas. Oleh karena itu, hak-hak konstitusional klasik

¹⁰ Giovanni De Gregorio, "The rise of digital constitutionalism in the European Union," *International Journal of Constitutional Law* 19, no. 1 (2021): 56–64, <https://doi.org/10.1093/icon/moab001>.

¹¹ Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet A Road Towards Digital Constitutionalism?*

¹² Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet A Road Towards Digital Constitutionalism?*, 199.

¹³ "Digital Constitutionalism, EU Digital Sovereignty Ambitions and the Role of the European Declaration on Digital Rights," 269.

¹⁴ Frederik J. Zuiderveen Borgesius, "Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence," *The International Journal of Human Rights* 24, no. 10 (2020): 1572–93, <https://doi.org/10.1080/13642987.2020.1743976>.

seperti hak atas privasi kini berkembang menjadi *digital rights*—hak untuk mengontrol data pribadi, hak untuk tidak diawasi secara sewenang-wenang, dan hak untuk menikmati kebebasan berekspresi di ruang digital tanpa ancaman atau sensor algoritmik.

Prinsip terakhir adalah *checks and balances*, yaitu mekanisme untuk mencegah penyalahgunaan kekuasaan digital baik oleh negara maupun oleh entitas swasta yang memiliki kendali atas data publik. Pollicino menegaskan bahwa di era digital, mekanisme *checks and balances* harus diperluas tidak hanya mencakup hubungan antara cabang eksekutif, legislatif, yudikatif, tetapi juga melibatkan lembaga pengawas independen seperti komisi perlindungan data pribadi, otoritas etika digital, dan mekanisme audit teknologi.¹⁵ Tanpa kontrol semacam ini, kekuasaan digital negara akan berpotensi menjadi otoriter karena mampu mengawasi, mengontrol, dan memprofilkan warganya dengan tingkat presisi yang belum pernah ada sebelumnya dalam sejarah hukum tata negara.

Keempat prinsip tersebut menunjukkan bahwa *digital constitutionalism* bukan sekadar teori hukum yang abstrak, melainkan kerangka normatif yang dapat digunakan untuk menilai legitimasi dan konstitusionalitas kebijakan digital suatu negara. Pergeseran paradigma dari *law governing technology* menuju *constitution governing technology* menandai perubahan mendasar dalam cara kita memahami hubungan antara hukum dan teknologi. Jika sebelumnya hukum hanya berfungsi mengatur bagaimana teknologi digunakan, maka kini konstitusi harus berfungsi mengatur bagaimana teknologi dirancang dan dijalankan agar sesuai dengan nilai-nilai konstitusional.

Dalam konteks Indonesia, prinsip-prinsip konstitusionalisme digital dapat ditemukan cerminnya dalam ketentuan Pasal 28A sampai dengan Pasal 28J Undang-Undang Dasar 1945 yang mengatur tentang hak asasi manusia. Beberapa pasal kunci dapat dijadikan dasar untuk membingkai perlindungan hak-hak digital. Pasal 28F menjamin *hak setiap orang untuk berkomunikasi dan memperoleh informasi serta untuk mengembangkan diri melalui teknologi informasi*, yang berarti kebebasan berekspresi digital dijamin secara konstitusional, termasuk hak untuk mengakses dan berbagi informasi di ruang digital tanpa diskriminasi. Pasal 28G ayat (1) menegaskan *hak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda, serta hak atas rasa aman dan perlindungan dari ancaman ketakutan*. Ketentuan ini menjadi dasar normatif bagi hak atas privasi digital, termasuk perlindungan terhadap penyalahgunaan data biometrik dan praktik pengawasan massal oleh negara. Sementara itu, Pasal 28I ayat (1) menjamin *hak untuk bebas dari perlakuan diskriminatif dan hak atas pengakuan serta perlindungan hukum yang adil*, yang relevan untuk mencegah bias algoritmik dan diskriminasi teknologi dalam penggunaan sistem biometrik. Terakhir, Pasal 28J ayat (2) menegaskan bahwa pembatasan terhadap hak-hak asasi manusia hanya dapat dilakukan dengan undang-undang, dan semata-mata untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain, moral, ketertiban umum, dan keamanan nasional. Pasal ini memberikan dasar bagi

¹⁵ Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet A Road Towards Digital Constitutionalism?*

penerapan *proportionality test* dalam menilai apakah kebijakan digital seperti verifikasi biometrik sah secara konstitusional atau justru melampaui batas yang diperbolehkan.

Dari perspektif hak-hak konstitusional tersebut, *digital rights* seperti hak atas privasi, hak atas rasa aman, hak atas kebebasan berekspresi, dan hak atas perlindungan dari penyalahgunaan kekuasaan merupakan turunan langsung dari prinsip-prinsip yang tertuang dalam Pasal 28 UUD 1945. Dalam praktiknya, hak-hak ini memerlukan perlindungan baru di ruang digital. Hak atas privasi harus melindungi individu dari pengumpulan data biometrik tanpa persetujuan; hak atas kebebasan berekspresi harus memastikan bahwa verifikasi identitas digital tidak digunakan untuk membungkam suara kritis; hak atas rasa aman harus menjamin bahwa data biometrik disimpan dengan aman dan tidak disalahgunakan; sedangkan hak atas perlindungan dari penyalahgunaan kekuasaan harus memastikan adanya mekanisme pengawasan independen terhadap setiap kebijakan digital negara.

Dalam konteks kebijakan verifikasi biometrik yang direncanakan oleh Komdigi, prinsip konstitusionalisme digital menjadi alat analisis normatif yang krusial. Pertanyaan mendasarnya bukan hanya apakah kebijakan tersebut efektif secara teknis, tetapi apakah ia konsisten dengan prinsip-prinsip konstitusi yang membatasi kekuasaan negara. Kebijakan yang mengharuskan setiap warga untuk diverifikasi melalui data biometrik berisiko memperluas kekuasaan pengawasan negara ke tingkat yang belum pernah terjadi sebelumnya. Jika dilakukan tanpa dasar hukum yang jelas, tanpa batas tujuan yang tegas, dan tanpa mekanisme akuntabilitas, maka kebijakan tersebut dapat melanggar *rule of law* serta hak konstitusional warga yang dijamin dalam UUD 1945. Selain itu, ketiadaan lembaga pengawas independen terhadap data biometrik menimbulkan persoalan serius terhadap prinsip *accountability* dan *checks and balances* dalam pemerintahan digital.

Dengan demikian, *digital constitutionalism* bukan hanya konsep teoretis, tetapi menjadi parameter substantif untuk menilai sejauh mana kebijakan biometrik negara menghormati prinsip *constitutional limitation of power*—yaitu prinsip bahwa kekuasaan negara, dalam bentuk apa pun, termasuk kekuasaan digital, harus dibatasi oleh konstitusi. Jika kebijakan verifikasi biometrik dijalankan tanpa memperhatikan prinsip-prinsip ini, maka negara berisiko melakukan ekspansi kekuasaan digital yang melanggar hak-hak dasar warga negara. Oleh sebab itu, setiap kebijakan teknologi informasi, khususnya yang melibatkan data biometrik, harus diletakkan dalam kerangka *constitution governing technology*, bukan semata-mata *law governing technology*. Dalam kerangka itulah supremasi konstitusi tetap terjaga di era digital, memastikan bahwa teknologi menjadi alat bagi demokrasi, bukan sebaliknya — alat kekuasaan yang membatasi kebebasan warga negara.

B. Kerangka Hukum dan Konstitusional Pengaturan Data Biometrik di Indonesia: Antara Perlindungan dan Pengawasan

Dalam sistem ketatanegaraan Indonesia, perlindungan data pribadi—termasuk biometrik—memiliki dasar normatif yang kuat dalam Bab XA UUD 1945 tentang Hak Asasi Manusia, meskipun istilah *data pribadi* tidak disebut secara eksplisit. Pasal

28F menjamin hak setiap orang “untuk berkomunikasi dan memperoleh informasi serta untuk mengembangkan diri melalui teknologi informasi,” yang pada konteks digital mencakup hak untuk mengontrol data pribadi yang digunakan dalam komunikasi publik. Pasal 28G ayat (1) menegaskan hak atas perlindungan diri pribadi, kehormatan, martabat, dan rasa aman dari ancaman ketakutan—sebuah jaminan konstitusional terhadap invasi privasi melalui verifikasi digital. Sementara Pasal 28I ayat (1) menjamin perlindungan dan kepastian hukum yang adil, relevan untuk mencegah diskriminasi algoritmik dalam kebijakan berbasis biometrik. Dengan demikian, hak atas privasi dan kebebasan berekspresi dalam UUD 1945 merupakan *derivative rights* dari hak asasi klasik yang kini menemukan relevansinya di era digital.¹⁶

Konsep tersebut sejalan dengan prinsip *digital constitutionalism*, yakni pandangan bahwa kekuasaan digital negara harus tunduk pada prinsip *rule of law*, akuntabilitas, dan perlindungan hak asasi. Menurut Giovanni De Gregorio, *digital constitutionalism* menuntut negara untuk tidak hanya menjamin hak warga di ruang digital, tetapi juga membatasi kekuasaan teknologi agar tidak bertransformasi menjadi alat pengawasan struktural.¹⁷ Dalam kerangka yang sama, Pollicino menekankan bahwa konstitusionalisme digital adalah upaya memperluas logika *checks and balances* terhadap bentuk kekuasaan baru yang bersumber dari algoritma dan data³. Oleh karena itu, kebijakan biometrik negara harus diuji melalui tiga kriteria konstitusional: legalitas, tujuan sah, dan proporsionalitas.

Dalam konteks hukum positif, UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan tonggak awal rezim hukum perlindungan data di Indonesia. UU ini mengakui data pribadi sebagai “setiap data tentang seseorang yang teridentifikasi atau dapat diidentifikasi,”¹⁸ termasuk karakteristik fisik seseorang yang mencakup data biometrik. Namun, tidak seperti *General Data Protection Regulation* (GDPR) Uni Eropa—khususnya Pasal 9, yang menetapkan data biometrik sebagai *special category data* dengan perlindungan berlapis—UU PDP belum memberikan kategori perlindungan khusus bagi data biometrik.¹⁹ Hal ini menimbulkan celah hukum karena biometrik memiliki sifat permanen, tidak dapat diubah, dan berpotensi disalahgunakan untuk *mass surveillance*.

Selain itu, UU PDP mengandung tiga lapisan perlindungan hukum: (1) prinsip perlindungan data (transparansi, akuntabilitas, dan pembatasan tujuan), (2) kewajiban pengendali dan prosesor data, dan (3) hak subjek data, seperti hak akses, perbaikan, dan penghapusan data.²⁰ Namun secara kelembagaan, mandat

¹⁶ Nur Azizah Qurrotuaini, “Hak Privasi Sebagai Hak Konstitusional Di Era Digital: Kajian Yuridis Dalam Perspektif Hukum Siber,” *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 2 (2024): 235–54, <https://doi.org/10.14421/a9d95k61>.

¹⁷ Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet A Road Towards Digital Constitutionalism?*

¹⁸ UU No. 27 Tahun 2022.

¹⁹ General Data Protection Regulation (GDPR).

²⁰ Seven Media Technology, “Artikel - JDIIH - Kota Semarang,” Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi : Menjaga Keamanan Dan Privasi Data Warga Negara, <http://jdiih.semarangkota.go.id/artikel/view/undang-undang-nomor-27-tahun-2022-tentang-pelindungan-data-pribadi-pdp-menjaga-keamanan-dan-privasi-data-warga-negara>.

pembentukan otoritas pengawas independen dalam Pasal 58–60 UU PDP belum terealisasi hingga kini, menyebabkan *regulatory vacuum* dalam mekanisme pengawasan dan penegakan hukum.²¹

Lebih jauh, mekanisme *Data Protection Impact Assessment* (DPIA), yang dalam sistem hukum Eropa diwajibkan untuk setiap kegiatan pemrosesan berisiko tinggi seperti verifikasi biometrik, belum diatur secara jelas di Indonesia.²² Ketiadaan DPIA menyebabkan kebijakan seperti rencana verifikasi biometrik Komdigi (Kementerian Komunikasi dan Digital) berada di area abu-abu hukum (*grey zone*), tanpa batasan eksplisit mengenai tujuan, mekanisme pemrosesan, serta bentuk pertanggungjawaban publik.

Keterbatasan regulatif ini diperburuk oleh fragmentasi hukum antara UU PDP, UU ITE, dan UU Administrasi Pemerintahan. UU ITE memberi legitimasi terhadap pemrosesan data elektronik oleh pemerintah, namun tidak mengatur secara substantif privasi biometrik. Situasi ini menandakan bahwa tata kelola hukum digital di Indonesia belum terintegrasi dalam satu *constitutional framework* yang solid sehingga masih bersifat sectoral.

Jika dibandingkan secara internasional, sistem hukum Indonesia masih tertinggal dalam aspek perlindungan dan akuntabilitas. Di India, Mahkamah Agung melalui putusan *Justice K.S. Puttaswamy v. Union of India* (2018) menegaskan bahwa sistem identitas biometrik nasional (*Aadhaar*) hanya konstitusional jika memenuhi prinsip proporsionalitas dan tidak digunakan untuk pengawasan massal.²³ Sementara di Amerika Serikat, negara bagian Illinois melalui Biometric Information Privacy Act (BIPA) mewajibkan *informed consent* tertulis sebelum pengumpulan data biometrik dan memberi *private right of action* bagi warga yang dirugikan.²⁴

Dengan demikian, secara konstitusional dan normatif, Indonesia berada di persimpangan antara *perlindungan dan pengawasan*. Di satu sisi, UU PDP telah meletakkan fondasi pengakuan hak atas data pribadi sebagai hak konstitusional; namun di sisi lain, ketiadaan otoritas independen dan mekanisme akuntabilitas yang kuat berpotensi menjadikan kebijakan biometrik sebagai alat ekspansi kekuasaan digital negara. Oleh karena itu, diperlukan *reformulasi hukum* yang menjadikan setiap kebijakan biometrik *constitutional-by-design*, tunduk pada prinsip transparansi, proporsionalitas, dan supremasi konstitusi.

C. Analisis Konstitusional atas Kebijakan Verifikasi Biometrik Komdigi: Uji Legalitas, Tujuan Sah, dan Proporsionalitas

Dalam hukum tata negara, pembatasan terhadap hak konstitusional warga negara hanya sah jika memenuhi tiga uji konstitusionalitas, yakni *legalitas (legality)*, *tujuan sah*

²¹ Caecilia Mediana, "Lembaga Pengawas Nihil, Jutaan Data Pribadi Masyarakat Bocor Terus," Kompas.id, 9 Juni 2025, <https://www.kompas.id/artikel/dua-tahun-uu-pdp-berlaku-lembaga-pengawas-tak-kunjung-hadir>.

²² Fitri Novia Heriani, "Memahami Data Protection Impact Assessments Dalam Perlindungan Data Pribadi," hukumonline.com, <https://www.hukumonline.com/berita/a/memahami-data-protection-impact-assessments-dalam-perlindungan-data-pribadi-lt667615ca09b2e/>.

²³ Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors.

²⁴ Illinois Biometric Information Privacy Act (BIPA).

(*legitimate aim*), dan *proporsionalitas* (*proportionality*).²⁵ Uji ini merupakan turunan dari prinsip *rule of law* yang melarang tindakan sewenang-wenang (*non-arbitrariness*) serta menjamin bahwa setiap penggunaan kekuasaan negara tetap berada dalam batas konstitusi. Dalam konteks rencana kebijakan verifikasi biometrik oleh Kementerian Komunikasi dan Digital (Komdigi), penerapan tiga uji tersebut menjadi penting untuk menilai sejauh mana negara menjalankan kekuasaan digital secara sah, berimbang, dan tidak melanggar hak asasi warga negara.

Prinsip *legality* mensyaratkan bahwa setiap pembatasan terhadap hak asasi harus memiliki dasar hukum formal yang jelas, baik dalam bentuk undang-undang maupun peraturan pelaksanaannya, serta substansi hukum yang dapat dipertanggungjawabkan secara konstitusional.²⁶ Dalam konteks Indonesia, rencana kebijakan verifikasi biometrik Komdigi belum memiliki dasar hukum eksplisit yang diatur dalam UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU PDP hanya mengatur prinsip umum perlindungan data pribadi, tanpa memberikan mandat langsung bagi kementerian untuk memaksa warga menyerahkan data biometrik sebagai syarat penggunaan media sosial. Kondisi ini bertentangan dengan prinsip *rule by law*, karena kebijakan administratif yang mempengaruhi hak konstitusional tidak boleh lahir dari diskresi eksekutif semata.

Dari perspektif *legality*, kebijakan ini juga menimbulkan problem substansial karena tidak disertai mekanisme *Data Protection Impact Assessment* (DPIA) sebagai prasyarat uji kelayakan hukum dan etis terhadap pemrosesan data berisiko tinggi. Dalam standar internasional, DPIA merupakan instrumen wajib sebagaimana diatur dalam GDPR Pasal 35 untuk memastikan setiap kebijakan digital telah diuji terhadap dampaknya bagi hak-hak individu.²⁷ Dengan tidak adanya mekanisme serupa di Indonesia, kebijakan Komdigi berpotensi melanggar asas kepastian hukum (Pasal 28I ayat (1) UUD 1945) dan prinsip *participation* yang menuntut transparansi serta partisipasi publik dalam proses perumusan kebijakan digital.

Uji kedua adalah *legitimate aim*, yang menilai apakah pembatasan hak warga negara benar-benar dilakukan untuk tujuan sah sesuai prinsip konstitusi, seperti menjaga keamanan nasional, ketertiban umum, atau melindungi hak orang lain. Dalam argumentasi Komdigi, kebijakan verifikasi biometrik ditujukan untuk mengatasi penyebaran hoaks, ujaran kebencian, dan penyalahgunaan akun anonim yang dianggap mengancam ruang digital nasional. Tujuan ini tampak sah secara formal, namun permasalahan muncul ketika kebijakan tersebut memperluas fungsi negara dari regulator menjadi pengawas digital permanen (*surveillance state*).²⁸

Dalam konteks Indonesia, tujuan sah kebijakan publik harus selaras dengan Pasal 28J ayat (2) UUD 1945, yang mensyaratkan pembatasan hak hanya

²⁵ Sri Yuliana, "Harmonisasi Regulasi Digital Dengan Prinsip Kebebasan Berpendapat Dalam Negara Hukum Indonesia," *RIO LAW JURNAL* 6, no. 2 (2025): 713-30, <https://doi.org/10.36355/rlj.v6i2.1777>; Putusan MK Nomor 89/PUU-XXIII/2025, 37.

²⁶ Yuliana, "Harmonisasi Regulasi Digital Dengan Prinsip Kebebasan Berpendapat Dalam Negara Hukum Indonesia."

²⁷ General Data Protection Regulation (GDPR).

²⁸ "Ancaman Penguatan State Surveillance dalam Layanan Digital Pemerintahan," ELSAM, <https://www.elsam.or.id/teknologi-dan-ham/ancaman-penguatan-state-surveillance-dalam-layanan-digital-pemerintahan>.

dapat dilakukan untuk menjamin pengakuan dan penghormatan terhadap hak orang lain serta memenuhi tuntutan moral, nilai agama, keamanan, dan ketertiban umum. Namun, Komdigi tidak menguraikan secara rinci bagaimana kebijakan verifikasi biometrik ini memenuhi prinsip tersebut, baik dari sisi rasionalitas maupun proporsionalitas tujuannya. Dengan demikian, kebijakan ini berpotensi melanggar prinsip *constitutional clarity* sebagaimana ditegaskan oleh European Court of Human Rights (ECHR) dalam perkara *S. and Marper v. United Kingdom* (2008), di mana penyimpanan data biometrik individu tanpa tujuan sah yang terukur dinyatakan melanggar *Article 8 European Convention on Human Rights* tentang hak atas privasi.²⁹

Uji ketiga, *proportionality*, mengharuskan adanya keseimbangan antara pembatasan hak dengan manfaat publik yang ingin dicapai. Uji ini meliputi tiga tahapan: *suitability test* (apakah kebijakan sesuai untuk mencapai tujuannya), *necessity test* (apakah tidak ada cara lain yang kurang membatasi hak), dan *balancing test* (apakah manfaat publik lebih besar daripada kerugian terhadap hak individu). Dalam konteks kebijakan Komdigi, kewajiban verifikasi biometrik bagi seluruh pengguna media digital tidak memenuhi prinsip *necessity* karena tidak dibuktikan bahwa langkah ini merupakan satu-satunya cara untuk mengurangi disinformasi atau penyalahgunaan identitas. Negara memiliki alternatif yang lebih *less intrusive*, seperti peningkatan literasi digital, penguatan moderasi konten, dan optimalisasi sistem *two-step verification* yang tidak melibatkan data biometrik sensitive.

Dari perspektif risiko konstitusional, kebijakan verifikasi biometrik Komdigi menghadirkan setidaknya tiga ancaman. Pertama, potensi pengumpulan massal data biometrik tanpa *informed consent*, karena warga tidak memiliki pilihan lain selain tunduk pada kebijakan negara untuk mengakses layanan digital. Kedua, risiko penggunaan data untuk *profiling* politik atau ekonomi, yang dapat mengancam prinsip netralitas digital dan kebebasan berpendapat. Ketiga, risiko kebocoran data akibat lemahnya sistem keamanan dan ketiadaan mekanisme kompensasi (*remedy mechanism*) jika pelanggaran terjadi.

Dengan menimbang ketiga uji konstitusional tersebut, dapat dikatakan bahwa kebijakan verifikasi biometrik Komdigi belum memenuhi prinsip konstitusionalitas digital. Ia lemah dari sisi *legal basis*, ambigu dalam *legitimate aim*, dan gagal dalam uji *proportionality*. Untuk itu, diperlukan penerapan digital proportionality test yang lebih komprehensif di Indonesia, mencakup kejelasan dasar hukum, pembatasan tujuan, dan analisis dampak terhadap hak konstitusional warga sebelum kebijakan teknologi dijalankan. Hanya dengan cara demikian, supremasi konstitusi dapat tetap dijaga di tengah perkembangan teknologi biometrik yang kian meluas.

D. Menuju Kerangka Tata Kelola Biometrik Berbasis Konstitusi untuk Indonesia

Membangun tata kelola biometrik yang selaras dengan prinsip konstitusionalisme digital menuntut suatu model yang tidak hanya memprioritaskan efisiensi administratif, tetapi juga memastikan supremasi konstitusi dalam setiap lapisan desain kebijakan teknologi. Dalam paradigma ini, hukum tidak lagi sekadar mengatur

²⁹ *S. and Marper v. the United Kingdom*, 30562/04, 30566/04 (ECtHR [GC] 4 Desember 2008), <https://hudoc.echr.coe.int/fre?i=001-90051>.

penggunaan teknologi, melainkan menjadi mekanisme konstitusional yang mengontrol arah dan batas kekuasaan digital negara. Hal ini sebagaimana ditegaskan oleh De Gregorio bahwa *digital constitutionalism* berfungsi sebagai “arsitektur nilai” untuk menyeimbangkan antara inovasi teknologi dan perlindungan hak asasi manusia dalam masyarakat algoritmik.³⁰ Dengan demikian, tata kelola biometrik yang *constitutional-by-design* perlu menggabungkan tiga fondasi utama: (1) prinsip *digital constitutionalism*, (2) prinsip perlindungan hak konstitusional, dan (3) prinsip *algorithmic accountability*.

a. Prinsip-Prinsip Dasar dalam *Constitutional-by-Design Biometric Governance*

Pertama, prinsip *digital constitutionalism* menuntut agar kekuasaan digital tunduk pada empat sendi utama: *rule of law digital*, *accountability*, *rights protection*, dan *checks and balances*. Prinsip *rule of law digital* memastikan bahwa setiap kebijakan teknologi, termasuk verifikasi biometrik, memiliki dasar hukum yang jelas dan dapat dipertanggungjawabkan secara publik². *Accountability* menegaskan bahwa negara tidak hanya berkewajiban mematuhi hukum, tetapi juga harus transparan dalam menjelaskan cara algoritma bekerja dan bagaimana data warga digunakan. *Rights protection*, sebagaimana dikemukakan oleh Celeste, menuntut negara untuk menafsirkan kembali hak konstitusional klasik – seperti hak privasi, kebebasan berekspresi, dan rasa aman – ke dalam konteks ruang digital.³¹ Artinya, setiap sistem biometrik harus dirancang dengan prinsip “*rights by design*”, bukan sekadar “*compliance by law*”.

Kedua, prinsip perlindungan hak konstitusional menuntut integrasi tiga uji yang telah dibahas sebelumnya – legalitas, proporsionalitas, dan *due process*. Dalam konteks tata kelola biometrik, *due process* tidak hanya berarti perlindungan prosedural terhadap warga, tetapi juga kewajiban negara untuk melakukan konsultasi publik, penilaian dampak (*impact assessment*), serta menyediakan mekanisme keberatan dan pemulihan (*effective remedy*).

Ketiga, prinsip *algorithmic accountability* menjadi unsur baru yang krusial dalam tata kelola biometrik. Prinsip ini mencakup tiga pilar: *transparency* (keterbukaan logika algoritmik), *auditability* (kemampuan diaudit oleh lembaga independen), dan *explainability* (kemampuan menjelaskan keputusan yang dihasilkan sistem otomatis). Seperti dikemukakan oleh Zuiderveen Borgesius (2023), algoritma yang digunakan oleh negara harus dapat diaudit untuk mencegah bias sistemik, diskriminasi, atau penyalahgunaan data.³² Prinsip ini tidak hanya penting untuk memastikan akuntabilitas teknologi, tetapi juga untuk menghindari terjadinya bentuk baru kekuasaan negara yang tersembunyi di balik logika algoritmik. Dengan demikian, tata kelola biometrik yang berbasis konstitusi harus memastikan adanya pengawasan lintas-otoritas yang memungkinkan *technological power* tunduk pada *constitutional scrutiny*.

³⁰ De Gregorio dan Radu, “Digital Constitutionalism in the New Era of Internet Governance.”

³¹ “Digital Constitutionalism, EU Digital Sovereignty Ambitions and the Role of the European Declaration on Digital Rights.”

³² Zuiderveen Borgesius, “Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence,” 1583.

b. Desain Kelembagaan: *Penguatan Oversight Body* dan Mekanisme Partisipatif

Secara kelembagaan, model *constitutional-by-design biometric governance* bagi Indonesia menuntut adanya penguatan otoritas pengawas independen sebagai *constitutional oversight body*. Lembaga yang paling relevan untuk peran ini adalah Komisi Perlindungan Data Pribadi (KPDP), sebagaimana diamanatkan oleh UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Namun, untuk menjadikan KPDP sejajar dengan lembaga pengawas di yurisdiksi maju, diperlukan perluasan mandat konstitusional dan otonomi kelembagaan. KPDP seharusnya diberi kewenangan konstitusional eksplisit untuk: (1) melakukan *pre-approval* terhadap setiap kebijakan digital berisiko tinggi, termasuk verifikasi biometrik; (2) melakukan audit terhadap lembaga publik maupun privat yang memproses data biometrik; dan (3) mengeluarkan sanksi administratif berupa pemberhentian penggunaan verifikasi biometrik.

Praktik pengawasan serupa dapat ditemukan di Uni Eropa, di mana *Data Protection Authorities* (DPA) seperti CNIL (Prancis) atau ICO (Inggris) memiliki otonomi penuh untuk melakukan audit dan penegakan sanksi terhadap kebijakan digital pemerintah.³³ Sementara di Kanada, lembaga *Office of the Privacy Commissioner* (OPC) diberi kewenangan untuk menilai *privacy impact assessment* terhadap setiap kebijakan pemerintah federal yang melibatkan teknologi pengenalan wajah.³⁴ Di Australia, *Office of the Australian Information Commissioner* (OAIC) memiliki mandat konstitusional untuk memastikan bahwa setiap kebijakan publik yang menggunakan biometrik memenuhi uji *necessity and proportionality*. Model kelembagaan ini menunjukkan bahwa tata kelola biometrik yang berakar pada konstitusionalisme digital harus berorientasi pada independence, transparency, dan enforceability.

III. KESIMPULAN

Kebijakan verifikasi biometrik yang direncanakan oleh Kementerian Komunikasi dan Digital (Komdigi) mencerminkan dilema antara kepentingan keamanan digital dan perlindungan hak konstitusional warga negara. Berdasarkan hasil analisis, kebijakan ini belum memenuhi prinsip konstitusionalitas sebagaimana diatur dalam Pasal 28F, 28G, dan 28I UUD 1945, karena belum memiliki dasar hukum yang jelas, belum diawasi oleh lembaga independen, dan belum menerapkan mekanisme *data protection impact assessment* (DPIA) yang memadai. Melalui pendekatan *digital constitutionalism*, penelitian ini menegaskan bahwa setiap kebijakan digital negara harus tunduk pada prinsip *rule of law, accountability*, dan *rights protection* yang menjadi inti dari pembatasan kekuasaan negara di ruang digital. Sebagai alternatif, penelitian ini mengusulkan model *constitutional-by-design biometric governance* yang menempatkan hak konstitusional warga negara sebagai pusat desain kebijakan teknologi,

³³ "Annual Report: CNIL's Achievements and Key Actions in 2024," <https://www.cnil.fr/en/annual-report-2024>.

³⁴ Office of the Privacy Commissioner of Canada, "OPC's Guide to the Privacy Impact Assessment Process," 13 Oktober 2011, https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/.

memperkuat peran Komisi Perlindungan Data Pribadi (KPPD) sebagai pengawas independen, serta memastikan setiap sistem digital negara diuji berdasarkan asas legalitas, tujuan sah, dan proporsionalitas.

DAFTAR PUSTAKA

- "Annual Report: CNIL's Achievements and Key Actions in 2024." <https://www.cnil.fr/en/annual-report-2024>.
- Asokawati, Ainunnisa Rezky. "Perlindungan Data Biometrik Dalam Sektor Perbankan Di Indonesia Dan Amerika Serikat." *Legal Standing: Jurnal Ilmu Hukum* 8, no. 3a (2024): 895–907. <https://doi.org/10.24269/ls.v8i3a.10775>.
- Canada, Office of the Privacy Commissioner of. "OPC's Guide to the Privacy Impact Assessment Process." 13 Oktober 2011. https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/.
- De Gregorio, Giovanni, dan Roxana Radu. "Digital Constitutionalism in the New Era of Internet Governance." *International Journal of Law and Information Technology* 30, no. 1 (2022): 68–87. <https://doi.org/10.1093/ijlit/eaac004>.
- De Gregorio, Giovanni. "The rise of digital constitutionalism in the European Union." *International Journal of Constitutional Law* 19, no. 1 (2021): 41–70. <https://doi.org/10.1093/icon/moab001>.
- De Gregorio, Giovanni. *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*. Cambridge Studies in European Law and Policy. Cambridge University Press, 2022. <https://doi.org/10.1017/9781009071215>.
- Edoardo Celeste. "Digital Constitutionalism, EU Digital Sovereignty Ambitions and the Role of the European Declaration on Digital Rights." Dalam *New Directions in Digitalisation Perspectives from EU Competition Law and the Charter of Fundamental Rights*, vol. 13. European Union and its Neighbours in a Globalized World, 2024
- ELSAM. "Ancaman Penguatan State Surveillance dalam Layanan Digital Pemerintahan." <https://www.elsam.or.id/teknologi-dan-ham/ancaman-penguatan-state-surveillance-dalam-layanan-digital-pemerintahan>.
- General Data Protection Regulation (GDPR).
- H.s, Muh Aqil Al Naufal, dan Imam Fadhil Nugraha. "Worldcoin Dan Ancaman Privasi Biometrik: Tinjauan Cyber Ethics Dalam Konteks Regulasi Digital Indonesia." *Triwikrama: Jurnal Ilmu Sosial* 8, no. 9 (2025): 1–10. <https://doi.org/10.9963/cv8e1274>.
- Heriani, Fitri Novia. "Memahami Data Protection Impact Assessments Dalam Perlindungan Data Pribadi." [hukumonline.com. https://www.hukumonline.com/berita/a/memahami-data-protection-impact-assessments-dalam-perlindungan-data-pribadi-lt667615ca09b2e/](https://www.hukumonline.com/berita/a/memahami-data-protection-impact-assessments-dalam-perlindungan-data-pribadi-lt667615ca09b2e/).
- Illinois Biometric Information Privacy Act (BIPA).
- Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors.
- Michael Odden. "Biometric Crisis: Legal Challenges to Biometric Identification Initiatives." *Wisconsin International Law Journal* 39, no. 2 (2022): 365–90.

- Mediana, Caecilia, "Lembaga Pengawas Nihil, Jutaan Data Pribadi Masyarakat Bocor Terus." Kompas.id, 9 Juni 2025. <https://www.kompas.id/artikel/dua-tahun-uu-pdp-berlaku-lembaga-pengawas-tak-kunjung-hadir>.
- Oreste Pollicino. *Judicial Protection of Fundamental Rights on the Internet A Road Towards Digital Constitutionalism?* Hart Publishing, 2021.
- Putusan MK Nomor 89/PUU-XXIII/2025.
- Qurrotuaini, Nur Azizah. "Hak Privasi Sebagai Hak Konstitusional Di Era Digital: Kajian Yuridis Dalam Perspektif Hukum Siber." *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 2 (2024): 235-54. <https://doi.org/10.14421/a9d95k61>.
- S. and Marper v. the United Kingdom, 30562/04, 30566/04 (ECtHR [GC] 4 Desember 2008). <https://hudoc.echr.coe.int/fre?i=001-90051>.
- Simonitis, Mark. "Note: Facial Recognition Technology And The Constitution." *Notre Dame Journal on Emerging Technologies* 2, no. 2 (2021). <https://scholarship.law.nd.edu/ndlsjet/vol2/iss2/5>.
- Tambunan, Dhelly Ramadhon. "Komdigi Siapkan Verifikasi Biometrik Untuk Akun Digital." Rri.Co.Id - Portal Berita Terpercaya. Diakses 13 Oktober 2025. <https://rri.co.id/lain-lain/1849375/komdigi-siapkan-verifikasi-biometrik-untuk-akun-digital>.
- Technology, Seven Media. "Artikel - JDIH - Kota Semarang." Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi : Menjaga Keamanan Dan Privasi Data Warga Negara. <http://jdih.semarangkota.go.id/artikel/view/undang-undang-nomor-27-tahun-2022-tentang-pelindungan-data-pribadi-pdp-menjaga-keamanan-dan-privasi-data-warga-negara>.
- UU No. 27 Tahun 2022.
- Yuliana, Sri. "Harmonisasi Regulasi Digital Dengan Prinsip Kebebasan Berpendapat Dalam Negara Hukum Indonesia." *RIO LAW JURNAL* 6, no. 2 (2025): 713-30. <https://doi.org/10.36355/rlj.v6i2.1777>.
- Zuiderveen Borgesius, Frederik J. "Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence." *The International Journal of Human Rights* 24, no. 10 (2020): 1572-93. <https://doi.org/10.1080/13642987.2020.1743976>.