BLOCKCHAIN: INOVASI PEMBARUAN DALAM SEKTOR PENGAMANAN *E-GOVERNMENT* DALAM MENINGKATKAN SISTEM AKUNTABILITAS PEMERINTAHAN DI INDONESIA

Blockchain: Innovation Update in E-Government Security Sector in Improving Government Accountability System in Indonesia

Fadil Isam Yusuf Endiputra[1], Adrian Pratama Nasution[2], Akbar Dwi Febrian[3]
Fakultas Hukum Universitas Gajah Mada
fadilisamyusufendiputra2005@ugm.ac.id

Abstrak: Akuntabilitas dalam perlindungan data pribadi menjadi krusial di tengah pesatnya perkembangan teknologi digital dan meningkatnya ancaman keamanan siber. Blockchain, sebagai teknologi terdesentralisasi yang mengedepankan imutabilitas, menghadirkan solusi inovatif untuk memastikan keamanan dan transparansi dalam pengelolaan data. Implementasi blockchain di Indonesia melibatkan tiga lembaga utama: Badan Siber dan Sandi Negara (BSSN), Pusat Data Nasional (PDN), dan Kementerian Komunikasi dan Informatika (Kominfo). BSSN bertanggung jawab dalam pengawasan keamanan siber, memastikan teknologi blockchain terlindungi dari serangan seperti 51% attack dan ransomware. Mereka mengembangkan protokol keamanan yang mutakhir untuk menjaga integritas data. PDN fokus pada manajemen data, memastikan bahwa data yang disimpan dalam blockchain tidak dapat dimanipulasi dan mematuhi prinsip imutabilitas. PDN juga merancang mekanisme pemusnahan data yang sesuai dengan standar teknologi blockchain. Di sisi lain, Kominfo berperan dalam merumuskan kerangka regulasi yang adaptif dan inklusif, bekerja sama dengan sektor publik, swasta, serta akademisi untuk mendorong adopsi blockchain secara luas. Dengan kolaborasi kuat antara BSSN, PDN, dan Kominfo, blockchain dapat menjadi pilar utama dalam memperkuat tata kelola e-government, meningkatkan efisiensi, keamanan, serta transparansi dalam pengelolaan data pribadi di Indonesia.
Kata Kunci: blockchain; e-government; sistem pengamanan

Abstract: *Accountability in personal data protection is crucial amidst the rapid development of digital technology and increasing cybersecurity threats. Blockchain, as a decentralized technology that prioritizes immutability, presents an innovative solution to ensure security and transparency in data management. The implementation of blockchain in Indonesia involves three main institutions: the National Cyber and Crypto Agency (BSSN), the National Data Center (PDN), and the Ministry of Communication and Informatics (Kominfo). BSSN is responsible for overseeing cybersecurity, ensuring that blockchain technology is protected from attacks such as 51% attacks and ransomware. They develop state-of-the-art security protocols to maintain data integrity. PDN focuses on data management, ensuring that data stored in the blockchain cannot be manipulated and complies with the principle of immutability. PDN also designs a data destruction mechanism that complies with blockchain technology standards. On the other hand, Kominfo plays a role in formulating an adaptive and inclusive regulatory framework, working with the public, private, and academic sectors to encourage widespread blockchain adoption. With strong*

collaboration between BSSN, PDN, and Kominfo, blockchain can become a main pillar in strengthening e-government governance, increasing efficiency, security, and transparency in personal data management in Indonesia.
Keywords: *blockchain; e-government; security system*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah mengantarkan dunia memasuki era digital yang ditandai dengan terbentuknya ruang siber atau *cyberspace*. *Cyberspace* merupakan ruang virtual yang tercipta dari interaksi antara jaringan komputer dan teknologi digital lainnya, yang memungkinkan pertukaran informasi dan komunikasi secara global tanpa batasan geografis.[1] Ruang ini tidak hanya menjadi medium untuk berkomunikasi dan bertukar informasi, tetapi juga menjadi *platform* bagi berbagai aktivitas ekonomi, sosial, politik, dan budaya. Namun, seiring dengan manfaat yang ditawarkan, *cyberspace* juga menghadirkan tantangan dan ancaman baru, seperti kejahatan siber, pelanggaran privasi, dan penyebaran informasi palsu (*hoax*), yang memerlukan perhatian serius dari pemerintah dan masyarakat. Indonesia merupakan negara yang menganut sistem welfare state yaitu pemerintah dianggap memegang peranan penting dalam menjamin kesejahteraan bagi setiap warga negaranya.[2]

Dalam konsep negara *welfare state*, pemerintah dapat melakukan *staatsbemoenis* yaitu sebuah wewenang untuk melakukan tindakan atau perbuatan yang dilakukan pemerintah untuk campur tangan dalam segala urusan lapangan kehidupan masyarakat. Artinya, pemerintah memiliki peranan penting untuk bertindak aktif dalam dinamika kehidupan bermasyarakat. Di Indonesia, pengelolaan *cyberspace* masih menghadapi berbagai tantangan signifikan. Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), pada tahun 2022, terdapat lebih dari 700 juta serangan siber yang terdeteksi, meningkat 28% dibanding tahun sebelumnya.[3] Salah satu insiden yang mencolok adalah peretasan sistem Kementerian Komunikasi dan Informatika (Kominfo) yang terjadi pada awal 2023, di mana data pribadi jutaan warga bocor.[4] Insiden ini menunjukkan kelemahan dalam sistem keamanan siber

[1] Yasraf Amir Piliang, "Masyarakat Informasi dan Digital: Teknologi Informasi dan Perubahan Sosial," *Jurnal Sosioteknologi* 27, no. 11 (2012): 143–56.
[2] Laurensius Arliman, "Partisipasi Masyarakat dalam Pembentukan Perundang-Undangan Untuk Mewujudkan Indonesia Sejahtera dalam Pandangan Teori Negara Kesejahteraan," *Jurnal Politik Pemerintahan* 10, no. 1 (2017): 59–72.
[3] Muhammad Prakoso Aji, "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)," *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 13, no. 2 (4 Januari 2023): 222–38, https://doi.org/10.22212/jp.v13i2.3299.
[4] Sigar P Berutu, Rizki, dan Heriyanti, *Digital Security*, vol. 1, 1 (Medan: UNPRI PRESS, 2024).

pemerintah, sekaligus menyoroti kurangnya kesiapan institusi pemerintah dalam menghadapi ancaman digital di era yang semakin canggih, termasuk yang melibatkan kecerdasan buatan yaitu *Artificial Intelligence* (AI). Dalam konsep negara *welfare state*, pemerintah dapat melakukan *staatsbemoenis* yaitu sebuah wewenang untuk melakukan tindakan atau perbuatan yang dilakukan pemerintah untuk campur tangan dalam segala urusan lapangan kehidupan masyarakat. Artinya, pemerintah memiliki peranan penting untuk bertindak aktif dalam dinamika kehidupan bermasyarakat. Selain itu, laporan dari *Global Cybersecurity Index* yang dikeluarkan oleh *International Telecommunication Union* (ITU) menempatkan Indonesia pada peringkat ke-24 dari 194 negara pada tahun 2022, menandakan bahwa masih ada banyak ruang untuk perbaikan dalam hal keamanan siber.[5] Hal ini diperburuk oleh fakta bahwa literasi digital di kalangan masyarakat masih rendah, dengan hanya 56,5% populasi yang memiliki pemahaman dasar tentang keamanan siber. Peretasan data pribadi dalam institusi pemerintahan berdampak luas bagi masyarakat, baik yang terdampak langsung maupun tidak.[6] Bagi yang terkena langsung, peretasan ini dapat menyebabkan penyalahgunaan informasi sensitif, seperti nomor identitas, data keuangan, atau rekam medis, yang dapat dimanfaatkan untuk pencurian identitas, penipuan, atau kejahatan finansial lainnya.

Sementara itu, bagi masyarakat secara keseluruhan, peretasan ini merusak kepercayaan terhadap pemerintah dan stabilitas sistem pelayanan publik. Ketidakmampuan pemerintah dalam menjaga keamanan data juga dapat mengganggu keamanan nasional, membuka celah bagi intervensi pihak asing, serta menimbulkan kepanikan di masyarakat, mengingat potensi data penting yang bocor bisa dimanfaatkan untuk manipulasi politik atau sosial. Ahli hukum administrasi negara dari luar negeri seperti Paul De Hert, seorang profesor di *Vrije Universiteit Brussel*, menyatakan bahwa pemerintah memiliki kewajiban yang sangat besar dalam melindungi data pribadi warganya, dengan standar keamanan yang harus setara atau bahkan melebihi sektor swasta.[7] Di Indonesia, ahli hukum administrasi negara, Prof. Philipus M. Hadjon, menegaskan bahwa pelindungan data pribadi adalah bagian dari tanggung jawab pemerintah dalam menjaga hak konstitusional warga negara. Hadjon berpendapat bahwa kelalaian dalam pelindungan data pribadi tidak hanya melanggar

[5] Yayat Popon Ruhiat, "Membangun Sistem Keamanan Siber Di Ibu Kota Nusantara (IKN) dalam Rangka Menunjang Pembangunan Nasional yang Berkelanjutan," *Lembaga Ketahanan Nasional Republik Indonesia*, 2023, 82–90.
[6] Irfan Naufal dan Ali Rokhman, "Analisis Ketahanan Data dan Keamanan Informasi dalam Manajemen Publik di Era Digital," *Jurnal Pemasaran Bisnis* 6, no. 3 (2024): 259–77.
[7] Serge Gutwirth dan Paul De Hert, "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power," *Direito Público* 18, no. 100 (27 Januari 2022), https://doi.org/10.11117/rdp.v18i100.6200.

hak privasi, tetapi juga meruntuhkan kepercayaan publik terhadap legitimasi pemerintah. Hal ini tentu membuat citra institusi pemerintah semakin buruk, sedangkan fasilitas negara merupakan suatu kewajiban negara yang harus dilaksanakan dalam rangka kebijakan pengaturan secara tertata dan sistematis agar tiap-tiap masyarakat tidak mengalami kesusahan terhadap kepentingan yang melibatkan informasi pribadi mereka. Salah satu teknologi yang dapat menunjang ini adalah *blockchain*. *Blockchain*, sebagai teknologi terdesentralisasi, menawarkan keamanan dan transparansi yang kuat dalam pengelolaan data pribadi. Teknologi ini mendukung tanggung jawab pemerintah dalam menjaga privasi warga, mengurangi risiko kebocoran, dan sebagai bentuk upaya pemerintah untuk kembali menaikkan kepercayaan publik terhadap sistem pelindungan data yang ada.

Penelitian ini memiliki relevansi penting dalam memperkuat tata kelola *cyberspace* di Indonesia yang berlandaskan prinsip-prinsip *good governance* khususnya prinsip akuntabilitas. Analisis dan rekomendasi yang disajikan dalam karya ini didasarkan pada dasar hukum yang kuat, seperti UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan UU No. 27 2022 pelindungan Data Pribadi (UU PDP) beserta peraturan pelaksananya, serta prinsip-prinsip Hukum Administrasi Negara (HAN) dan Asas-Asas Umum Pemerintahan yang Baik (AAUPB) yang menjadi landasan dalam membentuk kebijakan yang adil, transparan, dan efektif. Dengan demikian, penelitian ini tidak hanya memberikan landasan teoretis tetapi juga menawarkan solusi praktis yang dapat diaplikasikan oleh pemerintah untuk meningkatkan keamanan dan tata kelola *cyberspace* di Indonesia, sesuai dengan prinsip akuntabilitas dan kebutuhan negara dalam era digital yang terus berkembang.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif atau yuridis normatif. Metode hukum normatif adalah salah satu jenis metodologi penelitian hukum yang didasarkan pada analisis berbagai buku, dokumen resmi, dan data sekunder lainnya yang berguna untuk menyelesaikan permasalahan hukum.[8] Penelitian ini bertujuan untuk menemukan norma hukum penggunaan *blockchain* untuk sistem pengamanan *e-government* di Indonesia. Penelitian ini menggunakan pendekatan melalui pendekatan peraturan perundang-undangan (*statute approach*), pendekatan komparatif (*comparative approach*), dan pendekatan konseptual (*conceptual approach*). Pendekatan peraturan perundang-undangan atau statute

[8] Kornelius Benuf dan Muhamad Azhar, "Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer," *Gema Keadilan* 7, no. 1 (1 April 2020): 20–33, https://doi.org/10.14710/gk.2020.7504.

approach berfokus pada kajian terhadap berbagai aturan hukum yang relevan, baik yang telah berlaku maupun yang masih dalam bentuk rancangan. Pendekatan ini memungkinkan peneliti untuk memahami bagaimana peraturan tersebut terbentuk, diimplementasikan, serta dikaitkan dengan topik yang diteliti.

Sementara itu, pendekatan komparatif (*comparative approach*) digunakan untuk membandingkan peraturan atau konsep hukum dari berbagai sistem hukum atau negara yang berbeda. Melalui perbandingan ini, peneliti dapat mengevaluasi kelebihan dan kekurangan dari berbagai sistem hukum, sehingga dapat diambil pelajaran atau rekomendasi bagi perbaikan hukum nasional. Di samping itu, pendekatan konseptual (*conceptual approach*) digunakan untuk memahami konsep-konsep hukum yang mendasari suatu norma atau kebijakan, yang memungkinkan peneliti untuk menggali lebih dalam mengenai filosofi hukum yang menjadi landasan pembentukan aturan hukum tersebut. Pendekatan ini sangat penting untuk memberikan justifikasi ilmiah yang lebih mendalam terhadap topik yang sedang dikaji. Dengan menggabungkan ketiga pendekatan ini, penelitian dapat menghasilkan analisis yang lebih kaya dan beragam, serta memberikan rekomendasi yang lebih tepat sasaran dan didukung oleh teori serta praktik yang telah teruji.

ANALISIS DAN DISKUSI 1

Permasalahan Pelindungan Data Pribadi Secara Yuridis, Politis, Sosial dan Teknologi

Data pribadi menurut Peraturan Menteri Komunikasi dan Informatika Pasal 1 Angka 1 No. 20 Tahun 2016 Tentang perlindungan Data Pribadi dalam Sistem Elektronik bahwa "*Data pribadi merupakan data perorangan tertentu yang disimpan, dan dijaga kebenaran serta dilindungi kerahasiaannya*."[9] Sebagaimana diatur dalam Pasal 28 Huruf G Ayat (1) UUD 1945 yang menyatakan bahwa: "*Setiap orang berhak atas pelindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi*." Selain itu, hak privasi dari data pribadi juga diatur dalam Pasal 26 Ayat (1) UU No. 11 Tahun 2008 Sebagaimana telah diubah dengan UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), bahwa: "*Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan*." Meskipun banyaknya aturan perundang-undangan yang mengatur tentang perlindungan data pribadi di berbagai sektoral, nampaknya aturan tersebut

[9] CSA Teddy Lesmana, Eva Elis, dan Siti Hamimah, "Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia," *Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia* 3, no. 2 (2022): 1–6.

dinilai kurang komprehensif dan mengakomodir masyarakat dan masih bersifat sangat umum yang hanya menjelaskan tentang perlindungan. Seperti halnya diatur dalam Pasal 26 ayat (2) UU ITE yang berbunyi: "*Setiap orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang Undang ini*."

Berdasarkan ketentuan di atas, setiap orang yang merasa hak privasinya terganggu oleh orang lain, dapat mengajukan gugatan ke pengadilan. Namun ketentuan tersebut masih bersifat umum dan tidak spesifik sehingga tidak bisa. memberikan perlindungan data pribadi secara optimal. Secara yuridis, aturan tentang perlindungan data pribadi di Indonesia ini masih bersifat umum dan hanya menggambarkan secara umum tentang konsep perlindungan data pribadi yang belum terlalu komprehensif membahas secara holistik. Berbeda dengan Hukum Uni Eropa (EU), yang lebih menitikberatkan pada pengumpulan data pribadi yang lebih terintegrasi dan holistik yang tertuang dalam *General Data Protection Regulation* (GDPR). GDPR ini dengan tegas menyatakan setiap orang berdaulat atas perlindungan data pribadi masing-masing di hadapan pihak manapun di Uni Eropa (EU). Perbandingan yang signifikan antara hukum di Indonesia dengan hukum Uni Eropa adalah adanya beberapa kebijakan yang masih abu-abu atau tidak komprehensif dalam hukum Indonesia dibandingkan dengan hukum Uni Eropa.

Sementara itu, UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi belum diaturnya mengenai lembaga pengawas yang independen guna melaksanakan pengawasan perlindungan data pribadi. Hal ini akan berimplikasi terjadinya penyelewengan kepentingan yang mengarah ke *conflict of interest*. Tidak adanya badan pengawas yang independen tersebut dapat dilihat sebagai indikasi bahwa Indonesia tidak memenuhi persyaratan tingkat perlindungan yang memadai (*adequate level of protection*).[10] Di sisi lain, sebagaimana diatur dalam Pasal 53 GDPR, orang yang ditunjuk sebagai anggota otoritas pengawas perlindungan data pribadi harus memiliki kualifikasi, pengalaman, dan keterampilan yang relevan di bidang perlindungan data dan tidak dapat diberikan kepada orang atau masyarakat yang belum memiliki pengetahuan yang memadai di bidang digital. Apabila seseorang yang tidak kompeten ditunjuk sebagai anggota badan pengawas tersebut tentunya akan memberikan dampak yang merugikan bagi negara bahkan masyarakat luas. Oleh karena itu, agar terciptanya keamanan perlindungan data pribadi harus benar-benar dipegang dan diawasi oleh pihak yang berkompeten dan berpengalaman agar menciptakan stabilitas keamanan.

Di balik itu semua, fakta menyebutkan bahwa tingkat kesadaran masyarakat terhadap pentingnya perlindungan data pribadi ini yang masih rendah. Masih banyak

[10] Guswan Hakim, Oheo Kaimuddin Haris, dan Muthaharry Mohammad, "Analisis Perbandingan Hukum Mengenai Regulasi Perlindungan Data Pribadi Antara Uni Eropa dan Indonesia," *Halu Oleo Legal Research* 5, no. 2 (2023): 443–53.

masyarakat yang cenderung kurang peka terhadap keamanan data pribadi mereka dan bahkan acuh dengan resiko yang mungkin akan terjadi. Hal tersebut tentunya akan berimplikasi serius terhadap stabilitas keamanan data pribadi, seperti meningkatnya resiko kejahatan siber seperti pencurian data dan kebocoran data akibat belum optimalnya sistem pengamanan dan tingkat kesadaran dari masyarakat.[11] Selain itu, fakta di lapangan menunjukkan bahwa kebanyakan masyarakat tidak mengetahui adanya regulasi yang mengatur perlindungan data pribadi di Indonesia. Padahal, Undang-Undang Perlindungan Data Pribadi telah disahkan dan seharusnya menjadi pedoman bagi masyarakat dalam menjaga privasi mereka. Hal tersebut bisa terjadi karena faktor pengetahuan dari masyarakat tentang akses peraturan, teknologi dan informasi tersebut yang kurang. Dengan fenomena tersebut tentunya akan menghambat perkembangan teknologi digital yang ada di Indonesia.

ANALISIS DAN DISKUSI 2

Perbandingan Penerapan *Blockchain* di Negara Lain

Penggunaan *blockchain* saat ini dinilai efektif karena dapat mengamankan data dan meningkatkan efisiensi dibandingkan menggunakan teknologi konvensional lainnya. Beberapa negara sudah menggunakan *blockchain* untuk pengaman data pada sistem *e-government*. Penelitian ini mencoba mengkomparasikan konsep, potensi, dan keuntungan dengan tiga negara, yakni Estonia, Brazil, dan Guinea-Bissau. Alasan dipilih negara tersebut karena negara-negara tersebut sudah berhasil mengembangkan teknologi *blockchain* dalam sistem *e-goverment*-nya. Lalu, Estonia merupakan negara pelopor pertama memasukkan blockchain dalam sistem *e-government* mereka Selain itu, adanya karakteristik yang sama antara Indonesia dan Guinea-Bissau, yakni sama-sama negara masih rentan dan berkembang.

a. Estonia
   Estonia adalah salah satu negara pelopor dalam penerapan *blockchain* dalam sistem *e-government*. Sejak tahun 2008, Estonia telah mengintegrasikan teknologi ini ke dalam berbagai layanan publik, termasuk sistem identitas digital dan pendaftaran perusahaan. Dengan sistem *e-residency*, warga negara asing dapat mendaftar dan menjalankan bisnis di Estonia tanpa harus berada di negara tersebut. Hal ini menunjukkan bagaimana *blockchain* dapat mempermudah akses dan memperluas partisipasi dalam ekonomi global. Keberhasilan Estonia dalam menerapkan *blockchain* tidak lepas dari dukungan

[11] Syfa Tasya Zahwani dan Muhammad Irwan Padli Nasution, "Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital," *JoSES: Journal of Sharia Economics Scholar* 2, no. 2 (2023): 105–9.

pemerintah yang kuat dan kebijakan yang pro-teknologi. Estonia juga telah mengembangkan sistem keamanan siber yang canggih untuk melindungi data warganya.[12] Hal ini menjadikan Estonia sebagai contoh yang baik bagi negara-negara lain yang ingin mengadopsi teknologi *blockchain*.

b. Guinea-Bissau

Guinea Bissau adalah negara pertama di sub-Sahara Afrika yang menggunakan blockchain untuk *e-government* khususnya dalam mengelola gaji para pegawai, memperkuat transparansi fiskal, dan melindungi dari tata kelola yang rentan. Negara ini termasuk rentan dan menjadi salah satu negara dengan kemiskinan tertinggi di dunia dengan rasio 69.3% sehingga menjadi tantangan berat di penggunaan penggunaan blockchain di Guinea Bissau bisa meningkatkan akuntabilitas dan kepercayaan publik kepada pemerintah, hal ini dibuktikan saat penggunaan *blockchain* pada tahun 2020, 84 persen anggaran belanja Guinea-Bissau hanya dihabiskan untuk gaji pegawai. penggunaan *blockchain* terhadap pengelolaan gaji pegawai bisa menurunkan rasio beban gaji kepada pegawai menjadi 53 persen. Keberhasilan ini tak terlepas adanya kerja sama Guinea-Bissau dengan IMF, UNDP, Bank Pembangunan Afrika, dan Perusahaan Ernst and Young sebagai auditor.[13]

ANALISIS DAN DISKUSI 3

Regulasi untuk Mengintegrasikan *Blockchain* dalam Kerangka Hukum Indonesia

Indonesia telah memiliki beberapa instrumen hukum yang mengatur teknologi dan perlindungan data. Di antaranya, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi tonggak utama. UU ITE, meskipun berfungsi sebagai payung hukum untuk berbagai aktivitas digital, cenderung memiliki cakupan umum dan belum mengakomodasi spesifikasi teknologi *blockchain*, terutama dalam hal struktur desentralisasi dan transparansi publik yang menjadi inti dari teknologi tersebut. Langkah awal untuk perlindungan data, UU PDP diresmikan untuk menjawab kekhawatiran terkait penyalahgunaan data pribadi, menyusul tren peningkatan insiden kebocoran data di Indonesia. Sepanjang tahun

[12] Muhamad Fajar Putranto dkk., "Analisis Penerapan Blockchain dalam Penyelenggaraan Administrasi Pemerintahan dan Keuangan Negara Untuk Meningkatkan Kepastian dan Kepatuhan Hukum: Studi Kasus di Estonia," *Jurnal Pemandhu* 5, no. 2 (2024): 103–19.

[13] International Monetary Fund, "Guinea-Bissau: A Blockchain Platform to Strengthen Wage Bill Management Goes Live," *International Monetary Fund* (blog), 2024, https://www.imf.org/en/News/Articles/2024/05/29/pr-24188-guinea-bissau-a-blockchain-platform-to-strengthen-wage-bill-management-goes-live.

2022, Badan Siber dan Sandi Negara (BSSN) mencatat peningkatan serangan siber sebanyak 33% dibandingkan tahun sebelumnya, termasuk serangan terhadap Penyedia Data Nasional (PDN) yang melibatkan lebih dari 300 juta data sensitif warga negara. Sayangnya, regulasi yang ada belum sepenuhnya siap menghadapi teknologi seperti *blockchain* yang mengubah paradigma pengelolaan dan penyimpanan data.

Sistem *blockchain*, yang berbasis desentralisasi dan kriptografi, menghadirkan tantangan tersendiri dalam kerangka hukum yang masih mengandalkan model pengelolaan data tradisional, yaitu sistem berbasis server terpusat. Teknologi ini mendistribusikan pengelolaan data ke node-node yang tersebar, membuat kontrol dan pengawasan menjadi jauh lebih kompleks.[14] Misalnya, pengelolaan transaksi atau penyimpanan data dalam *blockchain* tidak dikendalikan oleh satu entitas tunggal, sehingga mempersulit identifikasi pelaku jika terjadi kebocoran atau manipulasi data. Hingga saat ini, Indonesia belum memiliki regulasi yang secara eksplisit mengatur tata kelola *blockchain*, khususnya yang menyangkut perlindungan data pribadi dan keamanan transaksi berbasis teknologi ini. Padahal, *blockchain* sudah mulai diadopsi dalam sektor-sektor vital, seperti perbankan, *fintech*, dan logistik. Integrasi *blockchain* ke dalam sistem pemerintahan juga semakin dekat, terutama dengan adanya wacana pemanfaatan teknologi ini dalam sistem Pemilu Elektronik yang sedang dirintis oleh Komisi Pemilihan Umum (KPU). Oleh karena itu, regulasi yang tepat sangat diperlukan untuk melindungi kepentingan publik dan menjaga keamanan data yang bersifat krusial.

Blockchain membawa karakteristik unik yang membuatnya berbeda dari sistem teknologi konvensional, terutama terkait dengan prinsip transparansi, desentralisasi, dan ketahanan terhadap manipulasi data. Namun, sifat-sifat ini juga menimbulkan tantangan besar bagi kerangka hukum yang ada.[15] Misalnya, UU PDP mengatur bahwa setiap individu memiliki hak untuk menghapus data pribadinya (*right to be forgotten*), tetapi dalam *blockchain*, data yang tersimpan dalam blok tidak bisa diubah atau dihapus, karena setiap blok terkait dengan blok sebelumnya melalui mekanisme enkripsi yang kompleks. Selain itu, teknologi *blockchain* menciptakan ekosistem di mana semua node dalam jaringan memiliki salinan data yang identik. Dalam konteks perlindungan data pribadi, ini menimbulkan masalah, karena data pribadi yang tersebar di berbagai node sulit dikontrol secara penuh. Setiap pelanggaran di satu node berpotensi menyebar ke seluruh jaringan. Oleh karena itu, pembaruan regulasi perlu memastikan bahwa hak privasi individu tetap terlindungi, tanpa mengabaikan

[14] Mikail Sidik Tuna, Refly Singal, dan Mario Mangowal, "Implementasi Blockchain dalam Lembaga Keuangan Perbankan," *Lex Administratum* 12, no. 5 (2024): 1–12.
[15] Agus Arwani dan Unggul Priyadi, "Eksplorasi Peran Teknologi Blockchain dalam Meningkatkan Transparansi dan Akuntabilitas dalam Keuangan Islam: Tinjauan Sistematis," *Jurnal Ekonomi Bisnis dan Manajemen* 2, no. 2 (4 Maret 2024): 23–37, https://doi.org/10.59024/jise.v2i2.653.

keunggulan teknologi *blockchain* dalam hal transparansi dan ketahanan terhadap manipulasi data. Di sektor keuangan, khususnya dengan berkembangnya industri aset kripto di Indonesia, Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti) mulai mengatur perdagangan aset kripto melalui Peraturan Bappebti Nomor 8 Tahun 2021. Meski demikian, regulasi ini masih terbatas pada aspek perdagangan dan belum mencakup potensi *blockchain* di sektor lain, seperti logistik, kesehatan, hingga pengelolaan data pemerintahan. Dari sini, jelas bahwa kebutuhan akan regulasi yang lebih komprehensif semakin mendesak.

Agar integrasi *blockchain* ke dalam sistem hukum di Indonesia dapat berjalan lancar dan aman, diperlukan beberapa langkah kebijakan yang teknis, spesifik, dan berbasis data. Berikut adalah beberapa rekomendasi kebijakan untuk mendukung penerapan *blockchain* dalam kerangka hukum Indonesia:

a. Penunjukan BSSN, PDN, dan Kementerian Komunikasi dan Informatika (Kominfo) sebagai Pengawas Teknologi *Blockchain*

Dalam struktur pengawasan teknologi *blockchain*, Badan Siber dan Sandi Negara (BSSN) harus berperan sebagai pengawas utama dalam hal keamanan siber dan pengelolaan infrastruktur teknologi *blockchain* di Indonesia. Sebab dalam UU No. 27 Tahun 2022 tentang Perlindungan data Pribadi belum adanya aturan yang memuat mengenai adanya lembaga pengawas independen yang bertugas untuk melakukan pengawasan perlindungan data pribadi. BSSN dapat bekerja sama dengan PDN dan Kominfo untuk memformulasikan standar teknis dan operasional bagi setiap implementasi *blockchain* di sektor publik maupun swasta. BSSN bertanggung jawab dalam pengembangan sistem keamanan siber yang tahan terhadap berbagai ancaman, seperti serangan 51% *attack* atau serangan *ransomware* yang bisa mengunci data dalam *blockchain*.[16] PDN harus bertanggung jawab dalam pengelolaan dan perlindungan data yang tersimpan di *blockchain*, memastikan kepatuhan terhadap UU PDP, serta menetapkan mekanisme pemusnahan data yang sesuai dengan prinsip-prinsip *blockchain*. Kominfo berperan dalam penyusunan kebijakan regulasi yang melibatkan berbagai *stakeholder*, termasuk pemerintah, sektor swasta, dan akademisi untuk menciptakan kerangka kerja blockchain yang sejalan dengan perkembangan teknologi global.

b. Penyusunan Standar Keamanan *Blockchain*

[16] Arinaldo Adma, Yusuf Marsel Surbakti, dan Puspita Sari, "Transformasi Sistem Pertahanan Siber Indonesia dengan BSSN Sebagai Poros & Motor Penggerak Menuju Angkatan Siber Mandiri di Masa Depan," *Jurnal Kajian Stratejik Ketahanan Nasional* 6, no. 1 (25 Juni 2023): 1–15, https://doi.org/10.7454/jkskn.v6i1.10077.

Berdasarkan data dari BSSN, serangan siber terhadap sistem digital di Indonesia meningkat pesat selama lima tahun terakhir.[17] Oleh karena itu, penerapan *blockchain* harus diiringi dengan standar keamanan yang ketat. Regulasi harus mewajibkan setiap entitas yang menggunakan *blockchain* untuk mematuhi standar enkripsi minimal yang mampu melindungi integritas data, mengimplementasikan protokol keamanan siber yang ketat, seperti penggunaan *multi-signature* untuk otorisasi transaksi dalam *blockchain*, guna meminimalisir risiko penipuan atau pencurian data. Menjalankan audit berkala terhadap sistem *blockchain* yang mereka gunakan, dengan melibatkan pihak ketiga independen yang memiliki kredibilitas dalam hal audit teknologi informasi.

c. Hak Akses dan Pemusnahan Data di Blockchain
Dalam konteks UU PDP, setiap individu memiliki hak untuk mengakses dan menghapus data pribadi yang dimiliki oleh suatu entitas. Namun, teknologi *blockchain* yang bersifat *immutable* membuat pemusnahan data menjadi tantangan tersendiri. Oleh karena itu, perlu disusun regulasi yang memungkinkan: Penerapan *smart contracts* yang dapat digunakan untuk mengontrol hak akses terhadap data pribadi dalam *blockchain*, sehingga individu memiliki kontrol penuh atas siapa yang dapat mengakses informasi mereka. Pengembangan mekanisme pemusnahan data yang sesuai dengan prinsip desentralisasi, misalnya dengan *redaction technology* yang mampu menghapus data tanpa merusak blok lainnya dalam *blockchain*.

Kesuksesan penerapan blockchain dalam sistem hukum Indonesia tidak hanya bergantung pada regulasi yang kuat, tetapi juga pada kolaborasi antar-lembaga yang efektif. Beberapa langkah kolaborasi yang dapat diambil adalah: pertama, kolaborasi antara Badan Siber dan Sandi Negara (BSSN), Pusat Data Nasional (PDN), Kementerian Komunikasi dan Informatika (Kominfo), serta sektor swasta yang telah mulai mengadopsi teknologi *blockchain* menjadi kunci dalam menciptakan ekosistem digital yang aman, terintegrasi, dan relevan dengan perkembangan teknologi terkini. Di Indonesia, sektor fintech seperti pembayaran digital, kontrak pintar, dan perbankan mulai mengadopsi *blockchain* dalam proses transaksi digital untuk meningkatkan keamanan dan efisiensi. Kolaborasi ini akan menguntungkan karena masing-masing pihak memiliki kekuatan yang berbeda. BSSN bertanggung jawab atas keamanan siber nasional, yang mencakup perlindungan terhadap ancaman serangan siber, termasuk dalam implementasi *blockchain*.

[17] Agus Haryanto dan Satya Muhammad Sutra, "Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020," *Global Political Studies Journal* 7, no. 1 (30 April 2023): 56–69, https://doi.org/10.34010/gpsjournal.v7i1.8141.

PDN mengelola infrastruktur data nasional yang mendukung penggunaan *blockchain* dalam skala yang lebih luas, seperti dalam pengelolaan data publik. Sementara itu, Kominfo sebagai regulator memiliki peran dalam merumuskan kebijakan dan regulasi yang adaptif, agar inovasi yang diadopsi sektor swasta tidak bertentangan dengan standar keamanan dan regulasi nasional. Dasar hukum yang relevan dalam kerjasama ini adalah Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur tentang perlindungan data pribadi, keamanan transaksi elektronik, dan kewenangan pemerintah dalam mengelola infrastruktur digital. Selain itu, Peraturan Presiden No. 133 Tahun 2017 tentang Keamanan Siber Nasional memperjelas peran BSSN dalam menjaga keamanan infrastruktur digital Indonesia. Kerjasama ini juga penting untuk merancang regulasi yang lebih spesifik mengenai *blockchain*, agar sesuai dengan kebutuhan industri dan perlindungan data.

Kedua, adanya partisipasi akademisi dan penelitian. Penelitian akademis dapat membantu memberikan pemahaman yang lebih dalam mengenai tantangan dan peluang implementasi blockchain dalam berbagai sektor, seperti tata kelola pemerintahan, keamanan data, hingga efisiensi pelayanan publik. Kolaborasi antara akademisi, pemerintah, dan sektor swasta juga dapat mengacu pada Peraturan Pemerintah No. 45 Tahun 2019 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE), yang mendorong penggunaan teknologi digital dalam pelayanan publik serta inovasi penelitian untuk mendukung tata kelola pemerintahan yang lebih baik. Dengan adanya kerjasama antara berbagai pihak serta kontribusi dari akademisi, implementasi *blockchain* di Indonesia diharapkan dapat memberikan dampak positif bagi keamanan dan tata kelola digital di berbagai sektor. Dasar hukum yang dapat digunakan sebagai rujukan adalah Undang-Undang No. 12 Tahun 2012 tentang Pendidikan Tinggi, yang mengamanatkan bahwa universitas harus berkontribusi dalam pengembangan teknologi dan ilmu pengetahuan yang bermanfaat bagi masyarakat.

PENUTUP

Implementasi teknologi *blockchain* dalam sektor *e-government* di Indonesia menawarkan berbagai potensi untuk meningkatkan keamanan dan akuntabilitas tata kelola pemerintahan. Seiring dengan pesatnya perkembangan teknologi digital, kebutuhan akan sistem yang dapat menjamin keamanan data dan transparansi menjadi semakin mendesak. Blockchain, dengan karakteristik desentralisasi dan keamanan yang tinggi, mampu menjawab tantangan ini dan memberikan landasan yang kuat bagi reformasi sistem *e-government* yang lebih efisien dan transparan. Namun, adopsi teknologi ini juga memerlukan kerangka kebijakan yang komprehensif

serta dukungan infrastruktur yang memadai. Dibutuhkan kolaborasi dan sinergitas antara pemerintah dan juga masyarakat demi berjalannya program ini. Kelemahan pada aspek hukum dan regulasi, seperti kurangnya standar keamanan yang jelas dan pengaturan mengenai tanggung jawab hukum dalam sistem desentralisasi, masih menjadi kendala utama yang perlu diatasi.

Oleh karena itu, diperlukan kolaborasi antara pemerintah, akademisi, dan sektor swasta untuk menciptakan kebijakan yang tepat serta mendorong penerapan *blockchain* yang lebih luas dalam berbagai aspek pemerintahan. Pada akhirnya, keberhasilan integrasi teknologi *blockchain* dalam *e-government* tidak hanya bergantung pada aspek teknis, tetapi juga pada kesiapan masyarakat dan pemerintah untuk beradaptasi dengan perubahan. Pendidikan dan sosialisasi mengenai pentingnya perlindungan data pribadi serta manfaat teknologi ini harus terus ditingkatkan. Dengan demikian, diharapkan Indonesia dapat mencapai tata kelola pemerintahan yang lebih transparan, akuntabel, dan responsif terhadap kebutuhan masyarakat di era digital.

DAFTAR PUSTAKA

Aji, Muhammad Prakoso. "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)." *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 13, no. 2 (4 Januari 2023): 222–38. https://doi.org/10.22212/jp.v13i2.3299.

Arinaldo Adma, Yusuf Marsel Surbakti, dan Puspita Sari. "Transformasi Sistem Pertahanan Siber Indonesia dengan BSSN Sebagai Poros & Motor Penggerak Menuju Angkatan Siber Mandiri di Masa Depan." *Jurnal Kajian Stratejik Ketahanan Nasional* 6, no. 1 (25 Juni 2023): 1–15. https://doi.org/10.7454/jkskn.v6i1.10077.

Arwani, Agus, dan Unggul Priyadi. "Eksplorasi Peran Teknologi Blockchain dalam Meningkatkan Transparansi dan Akuntabilitas dalam Keuangan Islam: Tinjauan Sistematis." *Jurnal Ekonomi Bisnis dan Manajemen* 2, no. 2 (4 Maret 2024): 23–37. https://doi.org/10.59024/jise.v2i2.653.

Benuf, Kornelius, dan Muhamad Azhar. "Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer." *Gema Keadilan* 7, no. 1 (1 April 2020): 20–33. https://doi.org/10.14710/gk.2020.7504.

CSA Teddy Lesmana, Eva Elis, dan Siti Hamimah. "Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia." *Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia* 3, no. 2 (2022): 1–6.

Gutwirth, Serge, dan Paul De Hert. "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power." *Direito Público* 18, no. 100 (27 Januari 2022). https://doi.org/10.11117/rdp.v18i100.6200.

Hakim, Guswan, Oheo Kaimuddin Haris, dan Muthaharry Mohammad. "Analisis Perbandingan Hukum Mengenai Regulasi Perlindungan Data Pribadi Antara Uni Eropa dan Indonesia." *Halu Oleo Legal Research* 5, no. 2 (2023): 443–53.

Haryanto, Agus, dan Satya Muhammad Sutra. "Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020." *Global Political Studies Journal* 7, no. 1 (30 April 2023): 56–69. https://doi.org/10.34010/gpsjournal.v7i1.8141.

International Monetary Fund. "Guinea-Bissau: A Blockchain Platform to Strengthen Wage Bill Management Goes Live." *International Monetary Fund* (blog), 2024. https://www.imf.org/en/News/Articles/2024/05/29/pr-24188-guinea-bissau-a-blockchain-platform- to-strengthen-wage-bill-management-goes-live.

Laurensius Arliman. "Partisipasi Masyarakat dalam Pembentukan Perundang-Undangan Untuk Mewujudkan Indonesia Sejahtera dalam Pandangan Teori Negara Kesejahteraan." *Jurnal Politik Pemerintahan* 10, no. 1 (2017): 59–72.

Naufal, Irfan, dan Ali Rokhman. "Analisis Ketahanan Data dan Keamanan Informasi dalam Manajemen Publik di Era Digital." *Jurnal Pemasaran Bisnis* 6, no. 3 (2024): 259–77.

Piliang, Yasraf Amir. "Masyarakat Informasi dan Digital: Teknologi Informasi dan Perubahan Sosial." *Jurnal Sosioteknologi* 27, no. 11 (2012): 143–56.

Putranto, Muhamad Fajar, Pandi Zulfikar, Mustofa Kamil, dan Hasnah Aziz. "Analisis Penerapan Blockchain dalam Penyelenggaraan Administrasi Pemerintahan dan Keuangan Negara Untuk Meningkatkan Kepastian dan Kepatuhan Hukum: Studi Kasus di Estonia." *Jurnal Pemandhu* 5, no. 2 (2024): 103–19.

Ruhiat, Yayat Popon. "Membangun Sistem Keamanan Siber Di Ibu Kota Nusantara (IKN) dalam Rangka Menunjang Pembangunan Nasional yang Berkelanjutan." *Lembaga Ketahanan Nasional Republik Indonesia*, 2023, 82–90.

Sigar P Berutu, Rizki, dan Heriyanti. *Digital Security*. Vol. 1. 1. Medan: UNPRI PRESS, 2024.

Tuna, Mikail Sidik, Refly Singal, dan Mario Mangowal. "Implementasi Blockchain dalam Lembaga Keuangan Perbankan." *Lex Administratum* 12, no. 5 (2024): 1–12.

Zahwani, Syfa Tasya, dan Muhammad Irwan Padli Nasution. "Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital." *JoSES: Journal of Sharia Economics Scholar* 2, no. 2 (2023): 105–9.