JPH Galunggung
Jurnal Penelitian Hukum Galunggung

ANALISIS PERBANDINGAN HUKUM PERLINDUNGAN DATA ANTARA INDONESIA DAN UNI EROPA: TINJAUAN KASUS CAMBRIDGE ANALYTICA

A COMPARATIVE LEGAL ANALYSIS OF DATA PROTECTION BETWEEN INDONESIA AND THE EUROPEAN UNION: A CASE STUDY OF CAMBRIDGE ANALYTICA

Ahmad Tarikh
Sekolah Tinggi Hukum Galunggung
ahmadtarikh22@gmail.com

Robi Assadul Bahri
Sekolah Tinggi Hukum Galunggung
robiassadulbahri@sthg.ac.id

Abstrak

Perkembangan teknologi informasi telah mendorong peningkatan pengumpulan dan pemrosesan data pribadi oleh berbagai entitas, termasuk korporasi dan pemerintah. Namun, pemanfaatan data pribadi tanpa pengawasan yang memadai menimbulkan persoalan hukum yang serius, sebagaimana terjadi dalam kasus Cambridge Analytica. Penelitian ini mengangkat permasalahan mengenai kesiapan sistem hukum Indonesia dalam menjamin perlindungan data pribadi, khususnya dalam aspek mekanisme transfer data lintas yurisdiksi, *binding corporate rules*, dan sistem sertifikasi pengendali data. Penelitian ini merupakan penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan komparatif. Sumber data terdiri dari regulasi primer, seperti GDPR dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta bahan sekunder berupa literatur dan dokumen resmi. Hasil penelitian menunjukkan bahwa GDPR memiliki struktur hukum yang lebih lengkap dalam menjamin akuntabilitas pengendali data, termasuk pengawasan independen oleh lembaga khusus. Sebaliknya, sistem hukum Indonesia masih menghadapi kekosongan teknis dalam pengaturan operasional, belum mengatur mekanisme transfer data secara rinci, dan belum memiliki otoritas pengawas independen. Oleh karena itu, perlu pembentukan lembaga independen serta penyusunan peraturan pelaksana yang menjabarkan prinsip-prinsip hukum agar perlindungan data pribadi di Indonesia dapat setara dengan standar internasional.

Kata kunci: Perlindungan Data Pribadi, GDPR, Cambridge Analytica

Abstract

The advancement of information technology has led to increased collection and processing of personal data by various entities, including corporations and governments. However, the use of personal data without proper legal oversight raises serious legal concerns, as exemplified by the Cambridge Analytica case. This study addresses the problem of Indonesia's legal preparedness in protecting personal data, particularly concerning cross-jurisdictional data transfers, Binding Corporate Rules, and data controller certification systems. This is a normative legal research employing statutory and comparative approaches. The sources include primary legal materials such as the GDPR and Indonesia's Law Number 27 of 2022 on Personal Data Protection, alongside secondary sources such as academic literature and official documents. The findings indicate that the GDPR provides a more comprehensive legal structure to ensure accountability of data controllers,

including oversight by an independent supervisory authority. In contrast, Indonesia's legal system still faces technical gaps, lacks detailed regulation on cross-border data transfers, and has yet to establish an independent supervisory body. Thus, there is a pressing need to establish an independent authority and develop implementing regulations that elaborate legal principles, in order to align Indonesia's personal data protection system with international standards.

Keywords: Personal Data Protection, GDPR, Cambridge Analytica

I. Pendahuluan

Perkembangan serta transformasi digital di dunia mengalami pertumbuhan sangat pesat. Berbagai layanan berbasis teknologi kini tersedia untuk memudahkan aktivitas sehari-hari masyarakat, seperti berbelanja, layanan transportasi digital hingga transaksi keuangan elektronik.[1] Aktivitas digital ini, secara tidak langsung mendorong peningkatan pengumpulan, pemrosesan dan pengiriman data-data pribadi pengguna oleh entitas, seperti perusahaan dan instansi pemerintahan. Namun, pengelolaan data pribadi tersebut, menghadirkan berbagai persoalan, terutama terkait kebocoran data, penyalahgunaan informasi, dan transfer data lintas yurisdiksi hukum negara.

Salah satu permasalahan pemrosesan data pribadi yang berdampak besar secara global adalah kasus Cambridge Analytica, dalam putusan *Federal Trade Commission* (FTC) pada 22 Juli 2019. Kasus ini bermula dari pengumpulan data oleh Aleksandr Kogan dan Alexander Nix melalui aplikasi "*This Is Your Digital Life*" yang dikembangkan oleh GSR App. Aplikasi tersebut memanfaatkan API Facebook yang memungkinkan akses terhadap data pengguna serta daftar teman mereka tanpa persetujuan eksplisit, sehingga melanggar prinsip *informed consent*[2] dan otorisasi pihak ketiga. Data yang dikumpulkan kemudian dikelola oleh Cambridge Analytica, anak perusahaan dari SCL dan digunakan untuk kepentingan politik, termasuk kampanye Donald Trump dan referendum Brexit. Seluruh pemrosesan data dilakukan tanpa dasar hukum yang sah dan tanpa kontrak legal seperti *standard contractual clauses* atau *binding corporate rules*, sehingga melanggar prinsip legalitas dan mengabaikan perlindungan atas transfer data antarnegara.

Ancaman penyalahgunaan data pribadi tidak hanya terjadi di tingkat global. Di Indonesia, insiden serupa juga terjadi, seperti pada kasus kebocoran data BPJS Kesehatan tahun 2021, yang data penduduk menyangkut informasi sensitif diduga terjual di forum

[1] Sofyan Mufti Prasetiyo, Rehan Gustiawan, Farhat, Fabian Rizzel Albani" Analisis Pertumbuhan Pengguna Internet di Indonesia" *Buletin Ilmiah Ilmu Komputer dan Multimedia,* Volume 2, No. 1, Juni Tahun 2024.

[2] Prinsip ini secara umum mempunyai arti persetujuan dari pihak terkait. Penggunaan prinsip ini sering digunakan di dunia kedokteran, yang mana mempunyai arti yaitu suatu aturan dimana setiap tindakan medik harus mendapatkan persetujuan dari pasien atau keluarga pasien.

daring. Permasalahan ini terjadi karena ketiadaan lembaga otoritatif khusus yang bertugas menjalankan pengawasan dan perlindungan data secara independen.[3]

Ketiadaan lembaga pengawas independen dan lemahnya sistem hukum pada saat itu memperkuat urgensi lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Namun, dalam beberapa penelitian telah menyoroti kesenjangan yang luas antara UU PDP dengan *General Data Protection Regulation* (GDPR), terutama dalam aspek penegakan hukum, dan ketiadaan lembaga pengawas yang kuat,[4] serta mekanisme perlindungan data yang belum optimal. UU PDP juga masih menunjukkan kekurangan dalam hal transparansi, akuntabilitas, serta sistematika regulasi yang belum sekomprehensif GDPR.[5]

Penelitian ini bertujuan untuk mengisi kesenjangan tersebut, dengan menganalisis bagaimana UU PDP merespons dinamika hukum global pasca skandal Cambridge Analytica. Fokus utama diarahkan pada sejauh mana pengaturan dalam GDPR terkait *binding corporate rules*, mekanisme transfer data lintas yurisdiksi, dan sistem sertifikasi telah diadopsi ke dalam kerangka UU PDP, serta implikasinya terhadap akuntabilitas dan kelembagaan pengendali data di Indonesia.

Meskipun sejumlah penelitian telah membahas perbandingan antara GDPR dan UU PDP, sebagian besar masih berfokus pada analisis normatif atau komparasi prinsip dasar perlindungan data secara umum. Kajian-kajian tersebut cenderung belum mengulas secara rinci aspek teknis operasional, seperti mekanisme transfer data lintas yurisdiksi, penerapan *binding corporate rules*, serta sistem sertifikasi pengendali data. Selain itu, evaluasi terhadap kesiapan kelembagaan dalam mendukung akuntabilitas pengendali data di Indonesia juga belum menjadi fokus utama dalam literatur yang ada.

Kebaruan dalam penelitian ini terletak pada penggunaan pendekatan studi kasus global, yaitu skandal Cambridge Analytica, sebagai kerangka evaluatif untuk menilai kesenjangan sistem hukum Indonesia terhadap standar internasional. Dengan menitikberatkan pada instrumen teknis, seperti *adequacy decision*, *binding corporate*

---

[3] Kominfo. *Pemeriksaan Dugaan Kebocoran Data BPJS Kesehatan.* 21 Oktober 2022. https:// www.kominfo.go.id/content/detail/34906/pemeriksaan-dugaan-kebocoran-data-bpjs-kesehatan/0/berita_ satker BPJS Kesehatan".

[4] Loso Judijanto, Nuryati Solapari, Irman Putra" An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia. *The Easta Journal Law and Human Rights*, Vol. 3, No. 01, October 2024.

[5] Muhammad Maleno, Andriana Kusumawati," Comparative Analysis of Indonesia's Personal Data Protection Law with the European Union and California Regulations to Identify Best Practices in Protecting Public Privacy Rights." *Indonesia Law Collage Association Law Journal*, Vol.3, No 2 December 2024.

rules, dan *certification mechanisms* dalam GDPR, penelitian ini memberikan kontribusi orisinal melalui usulan reformasi kelembagaan berupa pembentukan otoritas pengawas independen yang belum diatur secara eksplisit dalam UU PDP. Pendekatan ini memadukan analisis normatif dan struktural, guna menghasilkan rekomendasi kebijakan berbasis praktik global yang relevan dan aplikatif.

II. Metode Penelitian

Penelitian ini merupakan penelitian hukum normatif dengan menggunakan pendekatan perundang-undangan dan pendekatan komparatif. Pendekatan perundang-undangan digunakan untuk menganalisis isi dan struktur hukum yang berlaku,[6] sedangkan pendekatan komparatif digunakan untuk membandingkan prinsip-prinsip hukum[7] perlindungan data antara Indonesia dan Uni Eropa.

Sumber data dalam penelitian ini terdiri atas bahan hukum primer, yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, *General Data Protection Regulation* (GDPR), serta putusan *Federal Trade Commission* (FTC) terkait kasus Cambridge Analytica. Adapun bahan hukum sekunder, mencakup literatur ilmiah, jurnal, serta dokumen resmi yang relevan dengan topik perlindungan data pribadi dan tata kelola data lintas yurisdiksi.

Pengumpulan data dilakukan melalui studi kepustakaan terhadap bahan hukum primer dan sekunder tersebut. Selanjutnya, data dianalisis secara kualitatif dengan metode deduktif, yakni dengan menafsirkan dan membandingkan prinsip-prinsip hukum yang berlaku dalam sistem hukum Uni Eropa dan Indonesia. Analisis ini bertujuan untuk menilai sejauh mana prinsip-prinsip global dalam GDPR telah diadopsi ke dalam sistem perlindungan data nasional serta mengidentifikasi implikasinya terhadap akuntabilitas pengendali data di Indonesia.

III. Pembahasan

1. Asas-Asas Perlindungan Data: Kajian Filosofis dan Yuridis

Asas hukum merupakan fondasi utama dalam merancang kerangka hukum, karena asas menjadi inti dari peraturan dan pedoman dalam penerapan suatu hukum. Asas ini juga memberikan nilai-nilai fundamental yang menjadi dasar dalam penyelenggaraan

[6] Peter Mahmud Marzuki, *Penelitian Hukum,* Edisi Revisi, Jakarta: Prenadamedia:2005, hlm.136.
[7] *Ibid*. hlm 172.

hukum. Setiap negara memiliki asas fundamental yang berbeda, yang tercermin dalam sistem hukum masing-masing. Hal ini juga berlaku pada GDPR dan UU PDP. GDPR, sebagai instrumen hukum utama Uni Eropa dalam perlindungan data pribadi, mendasarkan prinsip-prinsipnya pada *Charter of Fundamental Rights of the European Union*. GDPR mengatur tujuh asas utama: *lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality;* dan *accountability*.[8] Asas fundamental ini dibangun berdasarkan *Charter of Fundamental Rights* Uni Eropa, yang menghormati hak-hak pribadi, termasuk hak atas kehidupan pribadi, keluarga, rumah, dan komunikasi. Selain asas, GDPR memperkenalkan sejumlah hak penting bagi individu sebagai subjek data,[9] seperti:

1. *Right to be Forgotten* (Hak untuk Dihapus): Individu memiliki hak untuk meminta penghapusan data pribadi mereka dalam kondisi tertentu.
2. *Right to Object* (Hak untuk Menentang): Individu dapat menentang pemrosesan data pribadi mereka.
3. *Right to Rectification* (Hak untuk Memperbaiki): Hak untuk mengubah atau memperbaiki data pribadi yang tidak akurat.
4. *Right to Portability* (Hak untuk Pindah): Individu dapat mentransfer data pribadi mereka dari satu penyedia layanan ke penyedia layanan lainnya.
5. *Right of Access* (Hak Akses): Individu berhak meminta transparansi tentang bagaimana data pribadi mereka diproses.
6. *Right to be Notified* (Hak untuk Diberitahu): Individu berhak diberitahu jika terjadi pelanggaran terhadap data pribadi mereka, termasuk pembobolan data.

Ketentuan ini membatasi otoritas entitas pengendali data, termasuk badan hukum seperti perusahaan, untuk memastikan bahwa pemrosesan data pribadi dilakukan secara sah, proporsional, dan bertanggung jawab serta memantau aktivitas data pengguna di area Uni Eropa. Pembatasan ini juga menjadi dasar pembentukan kebijakan teknis seperti *Corporate Binding Rules,* Transfer Lintas Yurisdiksi, dan Sistem Sertifikasi. Sementara itu, UU PDP di Indonesia memberikan perlindungan terhadap hak privasi yang juga dijamin dalam Pasal 28G Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD 1945)**,** yang menekankan pentingnya penghormatan terhadap hak asasi manusia dan

[8] Regulation (EU) 2016/679 Of the Europian Parliament and of the Council, Article 5.
[9] Michael L. Rustad, Thomas H. Koenig, "Towards A Global Data Privacy Standard" *Florida Law Review*, Volume. 71, Issue 2, Art. 3, 2019.

pembatasannya berdasarkan hukum. Indonesia telah menetapkan prinsip-prinsip dasar perlindungan data dalam Pasal 2 UU PDP, yang mencakup: perlindungan, kepastian hukum, kepentingan umum, kemanfaatan, kehati-hatian, keseimbangan, pertanggungjawaban, dan kerahasiaan. Salah satu bentuk penerapan asas ini, tercantum dalam Pasal 21 UU PDP yang memuat konsep *contractual consent*[10] yakni perjanjian eksplisit antara para pihak-pihak terkait mengenai penggunaan data pribadi untuk meminmalkan resiko penyalahgunaan yang bersifat vital.[11] Namun, UU PDP belum meciptakan pengaturan teknis terkait *Corporate Binding Rules*, Mekanisme Transfer Lintas Yurisdiksi dan sistem sertifikasi terhadap pengelolaan data. Kekosongan terhadap regulasi ini dapat membuka peluang terjadinya akses terhadap pemrosesan data secara ilegal, serta melemahkan kontrol hukum terhadap pengendali data. Oleh karena itu, dibutuhkan peraturan pelaksana yang dapat menjabarkan dan memperkuat implementasi asas-asas hukum tersebut dalam praktik, agar perlindungan data pribadi di Indonesia selaras dengan perkembangan global.

2. Mekanisme Transfer Data Lintas dan Instrumen Akuntabilitas

Pengaturan transfer data lintas yurisdiksi merupakan fondasi penting dalam kerangka hukum perlindungan pribadi. GDPR mengatur legalitas transfer data keluar wilayah Uni Eropa dalam Pasal 44 hingga Pasal 50.[12] Untuk dapat melakukan transfer data ke negara ketiga, negara tujuan diwajibkan memperoleh "*adequacy decision*" dari Komisi Eropa. Keputusan *adequacy* ini hanya diberikan kepada negara-negara yang sistem hukumnya memiliki prinsip perlindungan data yang setara dengan GDPR, antara lain: prinsip pembatasan tujuan (*purpose limitation*), kualitas data (*data quality*), dan akuntabilitas (*accountability*). Negara tujuan juga wajib menjamin pemenuhan hak-hak subjek secara utuh seperti, hak akses, hak koreksi, dan hak menolak pemrosesan. Selain itu, perlindungan tambahan *seperti standard contract clauses* dan *binding corporate rules*[13] sebagai bagian dari persyaratan kecukupan tersebut. Namun, jika suatu negara

[10] Masitoh Indriani, Annida Aqiila Putri, "Persetujuan Dinamis sebagai Sarana Optimalisasi Pelindungan Data Pribadi dan Hak atas Privasi" *Jurnal HAM*, Volume 14, No. 2, Agustus 2023.

[11] Rai Mantili, Putu Eka Trisna Dewi" Prinsip Kehati-Hatian Dalam Penyelenggaraan Sistem Elektronik Dalam Upaya Perlindungan Data Pribadi Di Indonesia" *Jurnal Aktual Justice*. Vol.5, No.2 Desember 2020.

[12] Jiménez-Gómez, Briseida Sofía, "Cross-Border Data Transfers Between the EU and the U.S.: A Transatlantic Dispute" *Santa Clara Journal of International Law*, Volume 19, Issues 2, 2021.

[13] Casalini, F. and J. López González., "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, No. 220, OECD Publishing, Paris, 2019.

tidak memperoleh *adequency decision*, pengendali data tetap dapat melakukan transfer data lintas yurisdiksi selama menerapkan mekanisme hukum lain yang sah, seperti penggunaan *Standard Contractual Clauses* sebagai persetujuan eksplisit dari subjek data.

Salah satu instrument akuntabiltas pengendali data dalam transfer data lintas yurisdiksi adalah *Binding Corporate Rules* (BCR). BCR dikembangkan sebagai kerangka hukum internal yang mengikat seluruh entitas dalam satu korporasi multinasional untuk memastikan pemrosesan data tetap sesuai dengan prinsip GDPR, bahkan ketika data dipindahkan ke negara yang tidak memiliki status *adequacy*.[14]

BCR diatur dalam Pasal 46 GDPR dan secara khusus diuraikan dalam Pasal 47 GDPR. Pengaturan ini mencakup ketentuan substansif seperti pengawasan internal dan independen, prosedur pelaporan pelanggaran, serta mekanisme remediasi bagi subjek data. Tujuan utamaBCR adalah membangun kekuatan hukum yang mengikat, baik secara internal maupun eksternal.

Secara internal, BCR diberlakukan kepada karyawan melalui kebijakan perusahaan dan didukung sanksi yang efektif. Sementara secara eksternal, BCR memberikan kedudukan hukum kepada subjek data sebagai pihak ketiga yang berhak menuntut kepatuhan atas BCR dihadapan otoritas perlindungan data dan/atau pengadilan. Subjek data juga memiliki hak untuk menuntut ganti rugi atas pelanggaran terhadap hak-hak pribadinya.[15]

Untuk memperkuat perlindungan hak-hak subjek data, GDPR mengatur sistem sertifikasi melalui Pasal 42 dan 43. Sistem ini berfungsi sebagai instrumen penilaian kepatuhan yang lembaga sertifikasi independen (*certifier*) dengan melibatkan badan hukum atau perusahaan sebagai kandidat penerima sertifikasi. Lembaga sertifikasi bertugas untuk memverifikasi kesesuaian praktik pemrosesan data dengan standar perlindungan yang berlaku.[16] Apabila kandidat memenuhi persyaratan, maka akan di terbitkan sertifikat dengan masa berlaku terbatas, maksima tiga tahun, dan dapat diperpanjang selama syarat tetap terpenuhi. Sebelum menerbitkan sertifikasi, badan sertifikasi terlebih dahulu memberi tahu otoritas pengawas nasional terkait serfikat tersebut. Otoritas pengawas berwenang untuk menolak jika ditemukan ketidaksesuaian

[14] Bianka Maksó" Binding Corporate Rules as a New Concept for Data Protection in Data Transfers" *MPI Studies on Intellectual Property and Competition Law*,2018.

[15] David Bender, Larry Ponemon," Binding Corporate Rules for Cross-Border Data Transfer" *Rutgers Journal of Law & Urban Policy*, Volume 3, No. 2,2006.

[16] Eric Lachaud, "Why the certification process defined in the General Data Protection Regulation cannot be successful", *Computer law & Security Review,* 2016.

dengan regulasi, semua fungsi pengawasan ini dilaksanakan oleh *Europian Data Protection Board*.

Europian Data Protection Board (EPDB) juga menekankan pentingnya pemisahan fungsi antara lembaga yang melakukan investigasi dan penegakan hukum. EPDB membuka kemungkinan pengaturan fleksibel bagi *Data Protection Authority* (DPA) seperti: melakukan penilaian dan penerbitan sendiri, merancang skema sertifikasi sendiri, merancang skema sertifikasi, melisensikan keselurhan proses kepada pihak ketiga yang terakreditasi sesuai dengan arahan dan petunjuk dari EPDB.[17] Langkah-langkah tersebut, bertujuan membentuk sistem pengawasan yang tepat terhadap pemerosesan data pribadi dan penyalahgunaan oleh entitas komersial si seperti yang terjadi dalam kasus Cambridge Analytica, yang menunjukan adanya kekosongan hukum terhadap pemeroresan data di area Uni Eropa sebelum GDPR diberlakukan secara penuh.

3. Studi Kasus: Skandal Cambridge Analytica dan Kerapuhan Sistem Privasi Global

Cambridge Analytica, LLC adalah sebuah perseroan terbatas yang didirikan di Delaware pada bulan Desember 2013, dengan kantor beralamat di 597 Fifth Avenue, Lantai 7, New York, NY 10017. Perusahaan ini merupakan bagian dari SCL Elections Limited, sebuah perusahaan swasta yang berbasis di Inggris, memiliki kepemilikan saham atas Cambridge Analytica.

Cambridge Analytica beroperasi sebagai perusahaan analisis data dan konsultan yang menyediakan layanan pemetaan profil pemilih dan strategi pemasaran, perusahaan ini memiliki citra sebagai entitas yang "netral secara politik." Cambridge Analytica dan SCL Elections menjalankan kegiatan usaha melalui jaringan perusahaan yang saling terkait, dengan kesamaan struktur kepemilikan, pejabat eksekutif, dan karyawan. Salah satu tokoh sentral dalam jaringan ini adalah Alexander Nix, yang menjabat sebagai CEO Cambridge Analytica sekaligus Kepala Eksekutif di SCL Elections.[18]

Peran Alexander Nix menjadi lebih signifikan setelah bergabungnya Aleksandr Kogan, seorang peneiti dan pengajar di Fakultas Psikologi, University of Cambridge, Inggris. Pada awal 2014, SCL Elections dan Cambridge Analytica menyadari bahwa data profil pengguna facebook dapat digunakan untuk mengidentifikasi karakteristik subjek

[17] Efstratios Koulierakis. "Certification as guidance for data protection by design", *International Review of Law, Computers & Technology,* Volume 38, No.2,17 [Oktober 2023].

[18] Federal Trade Commission, *In the Matter of Cambridge Analytica, LLC*, Docket No. 9383, before the Federal Trade Commission, United States of America, 2019.

data dengan menerapkan model Psychometric OCEAN yaitu *openess to experience, conscientiousness, extravesion, agreeableness,* dan *neuroticism*. Kemudian mengembangkan algoritma berdasarkan "*likes*" yang dianalisis semakin akurat dalam memprediksi kepribadian subjek, bahkan melebihi pemahaman lingkungan sosial mereka. Untuk memperoleh data tersebut, Cambridge Anakytica dan SNL menggunakan Graph API (v1) milik Facebook, yang memungkinkan pengembang mengakses profil subjek data dan daftar teman mereka, meskipun pengguna tidak secara langsung menggunakan aplikasi atau situs milik Facebook. Karena celah keamanan ini, pada April 2014, Facebook meluncurkan *Graph API* versi 2 yang membatasi akses terhadap data teman pengguna yang tidak memberikan izin eksplisit. Namun, Cambridge Analytica dan SCL Elections tetap memanfaatkan versi awal (*Graph API v1*) yang memiliki regulasi lebih longgar terhadap akses data. Dengan pemanfaatan algoritma prediktif yang canggih serta celah dalam regulasi akses data Facebook, data yang dikumpulkan oleh Cambridge Analytica dan SCL Elections kemudian digunakan untuk kepentingan kampanye politik klien mereka di Amerika Serikat.

Dampak Kasus Cambridge Analytica Terhadap Perkembangan Regulasi Perlindungan Data

Kasus Cambridge Analytica tidak hanya menjadi skandal penyalahgunaan data terbesar dalam sejarah platform media sosial, tetapi juga menjadi titik balik yang signifikan dalam perkembangan regulasi global mengenai perlindungan data pribadi, terutama di Uni Eropa. Skandal ini, mendorong Parlemen Eropa untuk memanggil pendiri Facebook dalam sidang Komite Kebebasan Sipil dan mempercepat penguatan kerangka hukum yang telah dirancang melalui Regulasi Perlindungan Data Umum atau *General Data Protection Regulation* (GDPR) No. 679/2016.[19]

Prinsip-prinsip utama yang ditekankan dalam GDPR meliputi: *lawfulness, fairness, and transparency*; *purpose limitation*; *data minimization*; *accuracy*; *storage limitation*; *integrity and confidentiality*; serta *accountability*. Prinsip-prinsip tersebut, mengikat sistem perlindungan data di Eropa dan menjadi pembaruan dari ketentuan yang

[19] Federica Casarosa, "Tansnational Collective Actioms for Cross Border Data Protection Violation", *Internet Policy Review,* Vol 9, No3, (September 2020).

sebelumnya diatur dalam *EU Data Protection Directive* 95/46/EC (1995) dan *OECD Privacy Guidelines* (1980).[20]

Meskipun dasar hak atas privasi telah diakui dalam berbagai instrumen internasional, seperti *International Covenant on Civil and Political Rights* dan *European Convention on Human Rights*, permasalahan implementasi tetap muncul, khususnya mengenai definisi pengendali data, batasan akses, serta cakupan data sensitif yang berkaitan dengan kehidupan pribadi seseorang.[21] Hingga Kasus Cambridge Analytica terjadi, menekankan urgensinya perlindungan terhadap data pribadi terutama terhadap kewajiban pengendali data yang meminimalisir perusahaan dalam menggunakan data yang pada akhirnya memunculkan principal mengatur mekanisme transfer data *adequacy decision* chapter 5 (article 44-50) memastikan untuk kelayakan negara dalam menjamin keamanan data, Corporate Binding yang diatur dalam article 46 dan 47 yang mengikat perusahaan dalam pengolahan mengenai data *rules*, dan *certified system* sebagai mekanisme penilaian terhadap perusahaan secara berkala sebagai pengelola data.

4. Evaluasi Kelemahan Undang-Undang Perlindungan Data Pribadi dalam Konteks Regulasi Global

Kerangka perlindungan hukum data pribadi di Indonesia berakar pada konstitusi, yaitu Pasal 28G UUD 1945, yang kemudian diperluas melalui UU PDP. Pasal 3 UU PDP menetapkan tujuh asas perlindungan data: perlindungan, kepastian hukum, kepentingan umum, kemanfaatan, kehati-hatian, keseimbangan, pertanggungjawaban, dan kerahasiaan. Berdasarkan asas-asas ini, UU PDP mengklasifikasikan informasi menjadi dua kategori utama: informasi vital (*concern information*) dan informasi umum.[22]

Perlindungan informasi vital menjadi fokus utama, di mana setiap pemrosesan data wajib diawali dengan perjanjian kerahasiaan yang mencantumkan standar kontrak sesuai Pasal 20–22 UU PDP. Selain itu, Pasal 15 UU PDP mengatur pengecualian akses data pribadi untuk kepentingan negara dan keamanan, penegakan hukum, penyelenggaraan negara, pengawasan jasa keuangan, serta penelitian statistik dan ilmiah. Namun, semua pengecualian ini dibatasi oleh prosedur ketat yang diatur dalam undang-undang tersebut.

---

[20] Peter Starchon, Thomas Pikulik. "GDPR Principles in Data Protection Encourage Pseudonymization Through Most Popular and Full-Personalized Devices- Mobile Phones" *Prodcedia Computer Science*, (Mei 2019).

[21] Lee A. Bygrave, "Privacy and Data Protection in an International Perspective*, in* Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics", *Scandinavian Studies in Law*, 2002.

[22] Muhammad Saiful Rizal, "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia", *Jurnal Cakrawala Hukum,* (Desember 2019).

Di sisi lain, meskipun subjek data memiliki hak penuh atas data mereka termasuk hak koreksi dan hak penghapusan, masih terdapat kekurangan dalam mekanisme kontrol dan pengawasan terhadap perusahaan selaku pengendali data. Ketiadaan lembaga pengawas independen membuat implementasi asas akuntabilitas dan transparansi pada praktik pengelolaan data belum optimal.[23]

Kesenjangan Teknis Undang-Undang Pelindungan Data Terhadap Mekanisme Global (*Adequecy Decision, Binding Corporate Rules* dan *Certified*)

Pengawasan terhadap pengelolaan data oleh perusahaan penyedia layanan digital di Indonesia, masih memerlukan kontrol yang lebih ketat, terutama terhadap informasi yang dimanfaatkan untuk kepentingan komersial. Meskipun Pasal 2 UU PDP telah menetapkan klasifikasi spesifik atas jenis data pribadi yang sebelumnya belum diatur secara rinci dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang mana implementasinya masih belum mencakup mekanisme perlindungan data lintas yurisdiksi secara komprehensif.

Hak atas data pribadi dipertegas dalam Pasal 5 UU PDP, dan kewajiban transparansi bagi pengendali data ditegaskan dalam Pasal 21 UU PDP. Namun, dalam sistem hukum internasional, seperti GDPR Uni Eropa (EU Regulation 679/2016), prinsip transparansi dikembangkan lebih lanjut melalui instrumen BCR dan *certification mechanisms*. Bahkan, perusahaan dari luar yurisdiksi Uni Eropa diwajibkan untuk memenuhi ketentuan *adequacy decision* agar dapat melakukan transfer data secara sah ke wilayah Uni Eropa.

UU PDP memang mengatur bahwa pengendali data (*data controller*) yang ingin mentransfer data pribadi ke luar negeri wajib mendapatkan persetujuan tertulis dari subjek data. Selain itu, negara tujuan transfer harus memiliki regulasi yang setara atau lebih tinggi dibandingkan UU PDP. Namun, hingga saat ini belum terdapat parameter atau standar penilaian yang tegas untuk menentukan kesetaraan tersebut. Berbeda dengan GDPR, *adequacy decision* ditetapkan oleh Komisi Eropa melalui proses penilaian komprehensif yang mempertimbangkan keberadaan *standard contractual clauses*, serta prinsip dasar seperti *purpose limitation*, *data quality*, dan *accountability*.[24] Hingga kini, mekanisme transfer data lintas yurisdiksi dalam hukum Indonesia masih berada dalam

[23] Eri Satriana dan Dewi Kania Sugiharti, "Implementasi Perlindungan Data Pribadi di Indonesia," *Jurnal Ilmu Hukum,* Vol 10, No.1 (2022).

[24] Graham Greenleaf, "Global Data Privacy Laws 2023: Expansion, Enforcement, and Approaches," *Privacy Laws & Business International Report*, no. 186 (2023), pg. 10–14.

Rancangan Peraturan Pemerintah yang akan menjadi turunan dari UU PDP. Instrumen seperti *binding corporate rules* Pasal 46–47 GDPR dan *certified systems* Pasal 42–43 GDPR yang berfungsi sebagai mekanisme audit internal dan eksternal belum dikenal atau diadopsi secara eksplisit dalam sistem hukum nasional.

Di wilayah Uni Eropa, pengawasan terhadap pemrosesan data dilakukan oleh *European Data Protection Board* (EDPB),[25] sebuah lembaga independen yang memiliki kewenangan penuh untuk menegakkan kepatuhan terhadap GDPR. Sementara itu, di Indonesia, fungsi pengawasan berada di bawah Kementerian Komunikasi dan Informatika (Kemenkominfo) yang berada di bawah kekuasaan eksekutif dan belum bersifat independen. Perbedaan struktur kelembagaan ini, menimbulkan kesenjangan pengawasan yang signifikan. Lemahnya sistem pengawasan di Indonesia dapat menjadi hambatan dalam memperoleh *adequacy decision* dari Uni Eropa, yang pada akhirnya dapat mempersulit kerja sama transfer data lintas negara dan berdampak pada sektor ekonomi digital nasional.

Urgensi Pembaharuan Undang-Undang Perlindungan Data Indonesia

Pembaruan UU PDP merupakan kebutuhan mendesak untuk memperkuat pengelolaan dan pemrosesan data pribadi secara nasional. UU PDP belum sepenuhnya mengenal tingkat perlindungan yang memadai (*adequate level of protection*) bagi warga negaranya.[26] sebagaimana dipersyaratkan dalam standar internasional seperti yang ditetapkan dalam GDPR Uni Eropa.

Ketiadaan pengaturan teknis terkait instrumen seperti *binding corporate rules*, *adequacy decision*, dan *certified system* dalam UU PDP, menempatkan Indonesia pada posisi yang berisiko diisolasi dari ekosistem data global. Hal ini membuka celah terjadinya akses dan pemanfaatan data secara masif oleh entitas hukum yang tidak sah untuk kepentingan komersial, tanpa mekanisme akuntabilitas yang kuat. Selain itu, UU PDP tidak memberikan definisi eksplisit mengenai pembobolan data (*data breach*) maupun mekanisme tanggap darurat apabila terjadi pelanggaran terhadap keamanan data. UU PDP juga belum mengatur secara rinci sanksi atau kompensasi bagi subjek data yang

[25] Lokke Moerel, Corien Prins, "Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things," *SSRN Electronic Journal* (2016).

[26] Elza Aulia," Analisis Pasal 56 dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi dari Perspektif Kepastian Hukum", *Unnes Law Review*, Vol 7, No.1, (September 2024).

dirugikan.[27] Fungsi pengawasan terhadap perlindungan data diserahkan sepenuhnya kepada Kemenkominfo, yang secara struktural berada di bawah kekuasaan eksekutif dan belum bersifat independen.

Hal ini sangat berbeda dengan sistem di Uni Eropa, di mana pengawasan dilakukan oleh EDPB, sebuah lembaga independen yang memiliki kewenangan penuh dalam memastikan kepatuhan pengendali data terhadap GDPR. Keberadaan lembaga seperti EDPB memungkinkan optimalisasi penerapan instrumen seperti *binding corporate rules* dan *certified systems*, serta mendorong akuntabilitas dan kepercayaan dalam ekosistem data. Oleh karena itu, adopsi prinsip-prinsip perlindungan data internasional serta pengaturan teknis yang kuat dalam hal transfer data dan pengawasan terhadap pelaku usaha merupakan kebutuhan strategis. Langkah ini diperlukan untuk menjaga kedaulatan negara atas data pribadi warga, sekaligus memastikan bahwa hak-hak subjek data tetap terlindungi secara efektif dalam sistem hukum nasional.

IV. Penutup

Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia perlu dikaji ulang untuk mengadopsi model hukum yang lebih efektif dalam mengatur pemrosesan data pribadi oleh badan hukum, baik swasta maupun publik. Pasca skandal besar seperti Cambridge Analytica, kebutuhan akan batasan hukum yang tegas mengenai transfer data, pengawasan terhadap korporasi, dan kelayakan pengelolaan data menjadi semakin mendesak. Untuk menjawab tantangan tersebut, Indonesia memerlukan sistem hukum yang lebih siap secara sistematis, seperti yang ditunjukkan oleh *General Data Protection Regulation* (GDPR). GDPR telah menetapkan instrumen teknis yang komprehensif seperti *adequacy decision, binding corporate rules*, dan *certification scheme* sebagai respon langsung terhadap permasalahan lintas yurisdiksi yang diungkap dalam kasus Cambridge Analytica. Secara kelembagaan, GDPR juga memiliki struktur yang lebih kuat melalui keberadaan lembaga independen seperti *European Data Protection Board* (EDPB) yang mengawasi pemrosesan data secara objektif dan terpisah dari otoritas eksekutif.

Di sisi lain, meskipun UU PDP Indonesia telah mengenal konsep-konsep seperti *standard contractual clauses* sebagaimana dalam GDPR, namun masih terdapat

[27] Budi Agus Riswandi, Alif Muhammad Ghifari, "Protecting Our Mosts Valuable Personal Data: A Comparison of Transborder Data Flow Laws in the European Union, United Kingdom, And Indonesia", *Prophetic Law Review,* Vol.5. No. 2. (Desember 2023).

kesenjangan substansial dalam aspek transfer data lintas yurisdiksi, khususnya pada Pasal 50 UU PDP. Belum terdapat batasan tegas mengenai standar kelayakan negara penerima data, tidak dikenalnya mekanisme *binding corporate rules* sebagai bentuk pengawasan internal perusahaan, serta belum diatur sistem sertifikasi sebagai penjamin kepatuhan pengendali data terhadap prinsip-prinsip perlindungan. Oleh karena itu, pembaruan regulasi di Indonesia menjadi sangat penting, tidak hanya untuk memperkuat sistem pengawasan, tetapi juga untuk mengisi kekosongan hukum dan teknis yang masih ada. Pemerintah perlu mempertimbangkan pembentukan Lembaga Pengawas Independen di luar struktur Kementerian Komunikasi dan Informatika, sebagaimana diterapkan di Uni Eropa melalui EDPB. Selain itu, dibutuhkan regulasi turunan yang memperjelas prosedur, batas yurisdiksi, serta instrumen-instrumen teknis dalam pemrosesan data. Penguatan regulasi dan kelembagaan merupakan langkah strategis untuk membangun sistem perlindungan data pribadi yang efektif, akuntabel, dan setara dengan standar global yang telah diterapkan di berbagai yurisdiksi maju.

Daftar Pustaka

Buku

Peter Mahmud Marzuki, *Penelitian Hukum Edisi Revisi*, Jakarta: Prenadamedia:2005,

Jurnal

Bianka Maksó "Binding Corporate Rules as a New Concept for Data Protection in Data Transfers" *MPI Studies on Intellectual Property and Competition Law*, 2018.

Budi Agus Riswandi, Alif Muhammad Ghifari, "Protecting Our Mosts Valuable Personal Data: A Comparison of Transborder Data Flow Laws in the European Union, United Kingdom, And Indonesia", *Prophetic Law Review*, Vol.5, No.2. (Desember 2023).

Casalini, F. and J. López González, "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers,* No. 220, OECD Publishing, Paris, 2019.

David Bender, Larry Ponemon, "Binding Corporate Rules for Cross-Border Data Transfer" *Rutgers Journal of Law & Urban Policy*, Volume 3, No. 2, 2006.

Eri Satriana dan Dewi Kania Sugiharti, "Implementasi Perlindungan Data Pribadi di Indonesia," *Jurnal Ilmu Hukum*, Vol 10, No.1 (2022).

Eric Lachaud, "Why the certification process defined in the General Data Protection Regulation cannot be successful", *Computer law & Security Review*, 2016.

Efstratios Koulierakis. "Certification as Guidance for Data Protection by Design", *International Review of Law, Computers & Technology*, Volume 38, No.2, [17 Oktober 2023].

Elza Aulia, "Analisis Pasal 56 dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi dari Perspektif Kepastian Hukum", U*nnes Law Review*, Vol 7, No.1, (September 2024).

Federica Casarosa, "Tansnational Collective Actioms for Cross Border Data Protection Violation", *Internet Policy Review*, Vol 9, No3, (September 2020).

Graham Greenleaf, "Global Data Privacy Laws 2023: Expansion, Enforcement, and Approaches," *Privacy Laws & Business International Report*, No. 186 (2023).

Jiménez-Gómez, Briseida Sofía, "Cross-Border Data Transfers Between the EU and the U.S.: A Transatlantic Dispute" *Santa Clara Journal of International Law*, Volume 19, Issues 2, 2021.

Lee A. Bygrave, "Privacy and Data Protection in an International Perspective*, in* Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics", *Scandinavian Studies in Law*,2002.

Lokke Moerel, Corien Prins, "Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things," *SSRN Electronic Journal* (2016).

Loso Judijanto, Nuryati Solapari, Irman Putra, "An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia." *The Easta Journal Law and Human Rights,* Vol. 3, No. 01, October 2024.

Masitoh Indriani, Annida Aqiila Putri, "Persetujuan Dinamis sebagai Sarana Optimalisasi Pelindungan Data Pribadi dan Hak atas Privasi", *Jurnal HAM*, Volume 14, No. 2, Agustus 2023.

Michael L. Rustad, Thomas H. Koenig, "Towards A Global Data Privacy Standard", *Florida Law Review*, Volume. 71, Issue 2, Art. 3, 2019.

Muhammad Saiful Rizal, "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia", *Jurnal Cakrawala Hukum*, (Desember 2019).

Muhammad Maleno, Andriana Kusumawati, "Comparative Analysis of Indonesia's Personal Data Protection Law with the European Union and California Regulations to Identify Best Practices in Protecting Public Privacy Rights." *Indonesia Law Collage Association Law Journal,* Vol.3, No 2 December 2024.

Peter Starchon, Thomas Pikulik, "GDPR Principles in Data Protection Encourage Pseudonymization Through Most Popular and Full-Personalized Devices- Mobile Phones" *Prodcedia Computer Science*, (Mei 2019).

Rai Mantili, Putu Eka Trisna Dewi, "Prinsip Kehati-Hatian Dalam Penyelenggaraan Sistem Elektronik Dalam Upaya Perlindungan Data Pribadi Di Indonesia" *Jurnal Aktual Justice,* Vol.5, No.2 Desember 2020.

Sofyan Mufti Prasetiyo, Rehan Gustiawan, Farhat, Fabian Rizzel Albani, "Analisis Pertumbuhan Pengguna Internet di Indonesia" *Buletin Ilmiah Ilmu Komputer dan Multimedia,* Volume 2, No. 1, Juni Tahun 2024

Website

Kominfo. “Pemeriksaan Dugaan Kebocoran Data BPJS Kesehatan”. Diakses pada tanggal 21 Oktober 2022. Tersedia pada https:// www.kominfo.go.id/content/detail/34906/ pemeriksaan-dugaan-kebocoran-data-bpjs-kesehatan/0/berita_satker BPJS Kesehatan