

DIALEKTIKA KEAMANAN SIBER TERHADAP PELINDUNGAN DATA PRIBADI ATAS ALGORITMA MEDIA SOSIAL

(The Dialectics of Cybersecurity in the Protection of Personal Data within Social Media Algorithms)

Apri Listiyanto, Tatok Sudjiarto, Armunanto Hutahaean

Program Magister Hukum, Universitas Kristen Indonesia

Kampus Diponegoro - Jl.Diponegoro No. 84-86, Jakarta Pusat

Email: japra.bphn@gmail.com

Abstrak

Upaya melindungi data pribadi dari penyalahgunaan yang terjadi pada ruang media sosial tentu merupakan bagian dari tanggung jawab negara di dalam mengambil peran untuk melindungi warganya dari berbagai jenis kejahatan yang terjadi di dunia *cyber*, oleh sebab itu keamanan *cyber* telah menjadi isu yang semakin mendesak dalam era digital saat ini. Adanya algoritma tertentu terhadap kebiasaan yang kita lakukan pada beberapa platform media sosial yang selalu digunakan akan menciptakan basis data profil pribadi seseorang, hal inilah yang memicu dialektika antara perlindungan data pribadi yang memiliki hak privasi dengan penggunaan algoritma oleh platform dalam mengenali profil kebiasaan dari penggunaannya. Terhadap latar belakang tersebut, tulisan ini berupaya menggali penggunaan sistem algoritma pengenalan profil pengguna internet oleh platform media sosial dan yang harus dilakukan dalam mengantisipasi penyalahgunaan data pribadi terhadap sistem algoritma tersebut. Dengan menggunakan metode penelitian yuridis normatif melalui pendekatan legal, diketahui bahwa keamanan sistem informasi merupakan aset yang harus dilindungi keamanannya dan merupakan tanggung jawab negara dalam melindungi warganya dari berbagai jenis kejahatan yang terjadi di dunia *cyber* dan perlu dibangun usaha memajukan literasi digital terhadap seluruh lapisan pengguna media sosial, hal ini untuk meminimalisir dampak negatif yang tidak diharapkan dari penggunaan media sosial.

Kata Kunci: Perlindungan Data Pribadi, Media Sosial, Hukum Siber

Abstract

Efforts to protect personal data from misuse within the realm of social media (digital networks) are undeniably part of the State's responsibility in safeguarding its citizens from various forms of cybercrime. Consequently, cybersecurity has emerged as an increasingly urgent issue in today's digital era. The presence of specific algorithms that track user behaviour across social media platforms contributes to the creation of personal data profiles. This condition triggers a dialectic between the right to personal data protection and privacy, and the use of algorithms by platforms to identify users' behavioural patterns. Against this background, this paper seeks to explore the use of profiling algorithms by social media platforms and the necessary measures to anticipate the misuse of personal data in such systems. Employing normative juridical research through a legal approach, it is found that information system security is a critical asset that must be protected, and it is the duty of the State to shield its citizens from various forms of cybercrime. Furthermore, efforts must be made to advance digital literacy among all layers of social media users to minimize the unintended negative impacts of social media usage.

Keywords: Personal data protection, social media, cyber law

A. Pendahuluan

Perkembangan arus informasi baik yang dipancarkan maupun yang diterima pada saat ini telah mengalami perkembangan pesat dan signifikan. Berbagai platform penyebarluasan informasi dengan berbagai ragam media (media sosial) menunjukkan bahwa batasan terhadap penyebarluasan informasi sudah tidak lagi mengalami hambatan ruang dan waktu. Akses kebutuhan terhadap ragam informasi pun tersedia, baik yang gratis (*free of charge*) maupun yang berbiaya. Jika dilihat dari ragam media sosial yang tersedia maka terdapat beberapa jenis layanan yang disediakan, seperti:¹

- a. Media Blog, merupakan jenis layanan untuk mengunggah jurnal pribadi melalui media internet. Media ini memiliki fungsi untuk membagikan catatan atau pandangan penggunanya tentang berbagai isu tertentu. Pengguna media sosial jenis ini biasanya disebut sebagai narablog atau blogger. Contoh media sosial layanan blog yaitu seperti: WordPress, Blogger.
- b. Jejaring sosial, merupakan jenis layanan yang memiliki fungsi sebagai wadah yang mampu menampung secara virtual sebagai tempat berkumpulnya banyak orang untuk saling bersosialisasi. Dalam layanan ini, pengguna biasanya saling mengirim pesan, informasi, foto, hingga video. Contoh media sosial layanan jejaring sosial adalah Facebook, Instagram, dan LinkedIn.
- c. Mikro Blog, disebut juga dengan *microblogging*. Memiliki fungsi yang hampir sama dengan blog, tetapi jenis media sosial ini menyajikan halaman yang lebih ringkas.

Hal ini membuat layanan mikro blog memiliki kecepatan yang lebih baik dibandingkan layanan blog. Salah satu contoh layanan blog mikro adalah Twitter.

- d. Media Sharing, merupakan layanan yang memiliki tujuan utama untuk berbagi konten media seperti foto, audio, atau video terhadap para anggotanya. Salah satu contoh lain dari layanan berbagi media, yaitu Youtube, Instagram, Flickr, Tiktok dan lain sebagainya.
- e. Kolaborasi konten, merupakan layanan dimana semua orang dapat memberikan informasi terhadap objek yang sama, dan digunakan untuk membuat pengguna saling mengajak pengguna yang lain untuk menciptakan suatu kontribusi. Tidak hanya mengajak, dalam layanan kolaborasi ini, pengguna biasanya diperbolehkan untuk membuat konten sekaligus melakukan koreksi terhadap isi konten dari 'anggota' dari situs tersebut, salah satu contoh layanan kontribusi yang paling populer saat ini adalah Wikipedia.
- f. Marketplace, digunakan sebagai media atau sarana jual beli melalui platform digital, yang mana antara penjual dan pembeli dipertemukan dalam ruang digital yang tidak lagi menghadirkan toko fisik sebagai ruang jual beli yang dilakukan, contoh dari layanan ini adalah Tokopedia, Shopee, Blibli, Lazada dan lain sebagainya.

Dari ragam media sosial tersebut tentu terdapat implikasi baik yang bersifat yuridis maupun non yuridis, tidak terkecuali terhadap data pribadi yang juga menjadi salah satu objek informasi, yang terhadap penyalahgunaan data

¹ Nandy, Pengertian Media Sosial, Sejarah, Fungsi, Jenis, Manfaat dan perkembangannya, <https://www.gramedia.com/literasi/pengertian-media-sosial/>, diakses 6 April 2025

pribadi tersebut termasuk dalam jenis kejahatan siber (*cyber crime*).

Jika melihat dari substansi yang terdapat pada data pribadi sesungguhnya berbagai informasi yang terkandung, baik tersirat maupun tersurat merupakan hak milik dari setiap orang, yang berarti hak tersebut harus diakui dan dilindungi sebagai sebuah hak konstitusional, sebagaimana disebutkan pada UUD NRI Tahun 1945 mencakup 40 hak warga negara. Salah satunya adalah hak atas perlindungan diri pribadi. Hak tersebut diatur pada Pasal 28 G Ayat (1) dengan garis besar bahwa warga negara berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang di bawah kekuasaannya. Pasal tersebut mengasumsikan hak pribadi adalah hak milik. Tetapi dengan berkembangnya teknologi informasi dan komunikasi, seharusnya hak pribadi tidak hanya diartikan sebagai hak milik. Hak pribadi seharusnya juga diakui sebagai hak privasi.² Hal ini sesuai dengan tujuan dari pembentukan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yaitu untuk menjamin hak warga negara atas perlindungan diri pribadi dan menumbuhkan

kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya perlindungan data pribadi.³

Upaya melindungi data pribadi dari penyalahgunaan yang terjadi pada ruang media sosial (*digital network*) tentu merupakan bagian dari tanggung jawab negara di dalam mengambil peran untuk melindungi warganya dari berbagai jenis kejahatan yang terjadi di dunia *cyber*,⁴ oleh sebab itu keamanan *cyber* telah menjadi isu yang semakin mendesak dalam era digital saat ini. Dalam beberapa tahun terakhir diketahui adanya peningkatan jumlah dan kompleksitas serangan *cyber* yang mengancam sistem komputer dan data di seluruh dunia. Serangan seperti pencurian data, serangan *malware*, peretasan, dan serangan DDoS telah menyebabkan kerugian finansial yang signifikan, kerusakan reputasi, dan gangguan pada operasi bisnis.⁵

Berdasarkan data dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet di Indonesia pada tahun 2024 mencapai 221.563.479 jiwa dari total populasi 278.696.200 jiwa, yang menunjukkan tingkat penetrasi internet mencapai 79,5%,

² Sekaring Ayumeida Kusnadi dan Andy Usmina Wijaya, *Perlindungan Hukum Data Pribadi Sebagai Hak Privasi*, JA: Jurnal Al-Wasath 2 No.1: 19-32, Journal homepage: <https://journal.unusia.ac.id/index.php/alwasath/index>, DOI: 10.47776/alwasath.v2i1.127.

³ Lihat pertimbangan menimbang Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

⁴ Dunia Cyber atau dalam istilah Indonesia dikenal dengan dunia maya (atau disebut juga ruang siber atau mayantara; bahasa Inggris: *cyberspace*) merupakan sebuah media elektronik dalam jaringan komputer yang banyak dipakai untuk keperluan komunikasi satu arah maupun timbal-balik secara *online* (terhubung langsung). Kata "*cyberspace*" (dari *cybernetics* dan *space*) berasal dan pertama kali diperkenalkan oleh penulis novel fiksi ilmiah, William Gibson dalam buku ceritanya, "*Burning Chrome*", 1982 dan menjadi populer pada novel berikutnya, *Neuromancer*, 1984 yang menyebutkan bahwa: *Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding.* Jadi secara singkat kita dapat menyebutkan bahwa Cyber Crime adalah kejahatan yang terjadi di dunia siber. Lihat dalam Edy Susanto, dkk, *Manajemen Keamanan Cyber di Era Digital*, Jurnal Bisnis dan Kewirausahaan (Journal of Business and Entrepreneurship) Vol. 11, No. 1 Mei 2023, e-ISSN: 2685-6255; p-ISSN: 2302-4119, Hal 23-33 doi: <https://doi.org/10.46273/job&e.v11i1.365>

⁵ Edy Susanto, dkk, *Ibid*, hlm 24.

jika dilihat penggunaan internet berdasarkan gender di Indonesia banyak bersumber dari laki-laki 50,7% dan untuk perempuan 49,1%, sementara dari segi umur, orang yang berselancar di dunia maya ini mayoritas adalah Gen Z (kelahiran 1997-2012) sebanyak 34,40%. Lalu, berusia generasi milenial (kelahiran 1981-1996) sebanyak 30,62%. kemudian berikutnya, Gen X (kelahiran 1965-1980) sebanyak 18,98%, Post Gen Z (kelahiran kurang dari 2023) sebanyak 9,17%, baby boomers (kelahiran 1946-1964) sebanyak 6,58% dan pre boomer (kelahiran 1945 sebanyak 0,24%. Berdasarkan data di atas menunjukkan bahwa negara tidak boleh abai terhadap perkembangan dunia *cyber* yang terjadi di tengah-tengah kehidupan masyarakat, termasuk di dalam melindungi dari adanya kejahatan ataupun penyalahgunaan terhadap data pribadi seseorang.

Hal menarik yang menjadi dialektika adalah perbincangan atas kemajuan teknologi yang memungkinkan mengenali kebiasaan ataupun profil dari pengguna internet yang ada, yang kemudian akan menjadi basis data yang dapat diolah dan mampu mengekstrasi berbagai kepentingan. Selanjutnya berbagai platform akan menyediakan konten sesuai dengan kebiasaan yang pengguna lakukan tanpa adanya persetujuan pengguna. Melalui algoritma tertentu, kebiasaan yang dilakukan pada beberapa platform media sosial yang sering digunakan akan menciptakan basis data profil pribadi seseorang, sebagai contoh pada pengguna Instagram ataupun Youtube ketika pengguna melakukan pencarian (*search*) untuk gambar atau video tertentu dan hal tersebut dilakukan berulang, maka Instagram dan Youtube akan mampu mengenali kebutuhannya.

Melalui algoritma yang digunakan tersebut, berbagai konten serupa/sejenis akan disajikan oleh platform tersebut tanpa harus meminta persetujuan dari penggunanya, hal inilah yang memicu dialektika antara perlindungan data pribadi yang memiliki hak privasi dengan penggunaan algoritma oleh platform dalam mengenali profil kebiasaan dari penggunanya.

Dengan latar belakang tersebut, tulisan ini akan mencoba mengelaborasi berbagai ketentuan secara normatif terhadap perlindungan data pribadi yang di dalamnya terdapat hak privasi dengan penggunaan algoritma pengenalan profil pengguna oleh platform media sosial. Hal ini dilakukan untuk menjawab apakah penggunaan sistem algoritma pengenalan profil pengguna internet oleh platform media sosial tidak bertentangan dengan peraturan perundang-undangan terkait perlindungan data pribadi, dan apa yang harus dilakukan dalam mengantisipasi penyalahgunaan data pribadi terhadap sistem algoritma pengenalan profil pengguna internet oleh platform media sosial.

B. Metode Penelitian

Pada penelitian ini penulis menggunakan metode penelitian yuridis normatif yang bersifat doktrinal, hal ini berangkat dari upaya menjawab masalah yang terkait dengan penggunaan algoritma pada platform media sosial yang kemudian dengan melandaskan pada aturan yang berlaku digunakan sebagai pisau analisa termasuk pendapat pakar maupun referensi yang dibutuhkan dalam menjawab persoalan dimaksud, oleh sebab itu penelitian ini bersifat preskriptif di dalam ilmu hukum.⁶ Pada penelitian ini data yang digunakan adalah

⁶ Muhaimin, *Metode Penelitian Hukum* (Mataram: Mataram University Press, 2020).

data sekunder yang diperoleh melalui bahan-bahan kepustakaan.⁷ Data-data tersebut kemudian dianalisa dengan pendekatan pendekatan asas-asas hukum dan peraturan perundang-undangan untuk memecahkan pokok permasalahan yang diangkat.

C. Pembahasan

1. Kedudukan Hak Pelindungan Data Pribadi

Data pribadi secara umum dimaknai sebagai informasi yang melekat pada diri pribadi seseorang yang digunakan untuk mengidentifikasi profil individu yang dimiliki satu orang dan membedakan dengan orang lain. Melihat makna tersebut tentu kita dapat mengatakan bahwa data pribadi akan selalu melekat dan tidak terpisahkan dari diri seseorang dan orang tersebut memiliki kuasa penuh atas data pribadi yang dimilikinya. Memahami data pribadi sebagai suatu hak, beberapa tokoh mengklasifikasikannya sebagai suatu hak privasi, seperti Mulligan, Koopman, & Doty⁸ yang berpendapat bahwa privasi adalah “konsep solusi untuk masalah yang kami tidak yakin bagaimana menyele-

saikannya; dan konsepsi tandingan adalah usulan saingan untuk menyelesaikannya atau untuk melakukan yang terbaik, dalam hal ini mengingat bahwa masalahnya tidak dapat dipecahkan”,⁹ sedangkan beberapa tokoh lain melihat hak privasi adalah gagasan yang sulit untuk didefinisikan,¹⁰ hal ini disampaikan oleh Adam D. Moore, dengan melihat semua konsep privasi yang saling bersaing ini, beberapa orang berpendapat bahwa tidak ada konsep privasi yang menyeluruh, melainkan beberapa konsep inti berbeda yang telah disatukan.¹¹

Memaknai data pribadi sebagai hak privasi merupakan hal yang skeptis sebagaimana dikemukakan Judith Jarvis Thomson. Menurut Thomson, *privacy* adalah gagasan yang sulit untuk didefinisikan. Mungkin hal yang paling nampak tentang hak privasi adalah bahwa tidak ada orang yang memiliki ide yang jelas tentang hal tersebut.¹²

Perdebatan tentang *right to privacy*, di Eropa dan Amerika Serikat, menurut Daniel J. Solove¹³ setidaknya memunculkan enam konsepsi *privacy* yang berkembang dan mewarnai pemikiran tentang hak atas *privacy*. Keenam konsepsi tersebut adalah:

-
- ⁷ Mukti Fajar ND and Yulianto Achmad, *Dualisme Penelitian Hukum, Normatif & Empiris* (Yogyakarta: Pustaka Pelajar, 2010).
- ⁸ Deirdre K. Mulligan¹, Colin Koopman² and Nick Doty, “Privacy is an Essentially Contested Concept: a Multidimensional Analytic for Mapping Privacy. *Phil. Trans. R. Soc. A* 374: 2016.0118.
- ⁹ Pendapat Mulligan, Koopman, & Doty menggunakan pemikiran Waldron yang mengatakan “essentially contested concepts can be ‘solution-concept(s)’ as well as ‘achievement-concept(s)’”. Waldron menganalisis konsep Demokrasi dalam kerangka “essentially contested concepts” yang dikemukakan Gallei. Waldron J, dalam “Is the rule of law an essentially contested concept (in Florida)?” *Law Philos.* 21 2002 ,137–164. Lihat lebih jauh dalam Wahyudi Djafar dan M. Jodi Santoso, *PERLINDUNGAN DATA PRIBADI: Konsep, Instrumen, dan Prinsipnya*, Lembaga Studi dan Advokasi Masyarakat (ELSAM), dengan dukungan dari Australian Government Department of Foreign Affairs and Trade (DFAT), 2019.
- ¹⁰ Adam D. Moore, “Privacy”, *Library Hi Tech*, Vol. 25, pp. 58-78, 2007 (available at: <http://ssrn.com/abstract=1980871>)
- ¹¹ Adam D. Moore, “Privacy: Its Meaning and Value”, *American Philosophical Quarterly*, Volume 40, Number 3, July 2003 (215-227).
- ¹² Judith Jarvis Thomson, “The Right to Privacy”, *Philosophy and Public Affairs*, Vol. 4, No. 4 (Summer, 1975), pp. 295-314.
- ¹³ Daniel J. Solove, “Conceptualizing Privacy”, *California Law Review*, Vol. 90, Issue 4 Article 2, 2002, [p.1087-1155].

- a. *right to privacy* dikonsepsikan sebagai *the right to be let alone*, atau hak untuk dibiarkan sendiri. Konsepsi ini dipopulerkan oleh Samuel Warren dan Louis Brandeis yang mengadopsi gagasan hakim Thomas Cooley dalam tulisannya *Treatise on the Law of Torts* (1880). Hal ini menjadi tonggak munculnya pemikiran hukum privasi modern dan memengaruhi pemikiran dan praktik hukum di Amerika dan Eropa.
- b. *right to privacy* dikonsepsikan sebagai *limited access to the self*, atau akses terbatas pada diri. Konsep ini menekankan pada keinginan individu untuk menyembunyikan diri dan terpisah dari yang lain. Akan tetapi, konsepsi akses terbatas bukan kesendirian (*solitude*) pengasingan, atau penarikan diri dari orang lain. Kesendirian adalah komponen dari konsepsi akses terbatas serta konsepsi hak untuk dibiarkan sendiri.
- c. *right to privacy* dikonsepsikan sebagai *secrecy* (kerahasiaan), dalam hal ini maksudnya adalah penyembunyian hal-hal tertentu dari orang lain. Salah satu pemahaman privasi yang paling umum adalah bahwa kerahasiaan itu merupakan kerahasiaan hal-hal tertentu.
- d. *right to privacy* dikonsepsikan sebagai *Control Over Personal Information*. Salah satu teori privasi yang paling dominan adalah kontrol atas informasi pribadi.
- e. *right to privacy* dikonsepsikan sebagai *Personhood*, atau perlindungan kepribadian, individualitas, dan martabat. Teori privasi ini dibangun berdasarkan gagasan Warren dan Brandeis tentang "kepribadian yang tidak dapat diganggu gugat." Menurut pandangan ini, privasi melindungi kepribadian dan tindakan otonom.

f. *right to privacy* dikonsepsikan sebagai *intimacy*, atau kontrol atas akses terbatas hubungan seseorang atau aspek kehidupan. Teori ini mengakui bahwa privasi tidak hanya penting untuk penciptaan diri individu, tetapi juga untuk hubungan manusia.

Berangkat dari pemaknaan data pribadi sebagai hak privasi di atas dengan berbagai pandangan tokoh tersebut, kita perlu juga melihat dalam konteks hubungan kenegaraan, baik antar warga negara, maupun badan hukum publik dan privat, yang mana data pribadi merupakan entitas yang melekat pada diri seorang warga negara yang memiliki hak dan kewajiban.

Mendudukan data pribadi setiap warga negara, maka penting melihat data pribadi tersebut sebagai bagian dari hak konstitusional warga negara, yaitu hak yang dijamin oleh undang-undang, artinya terhadap hak tersebut berimplikasi pada kewajiban konstitusional negara untuk melindungi hak warga negaranya. Dalam UUD NRI Tahun 1945 hak warga negara mencakup 40 jenis, salah satunya adalah hak atas perlindungan diri pribadi. Hak tersebut diatur pada Pasal 28 G Ayat (1) dengan garis besar bahwa warga negara berhak atas perlindungan diri pribadi. Selain itu, terdapat beberapa aturan, baik yang diterbitkan oleh Negara Indonesia, maupun yang berasal dari konvensi asing. Untuk aturan yang berasal dari luar (asing) sebagai berikut:

Konvensi/Regulasi	Wilayah Cakupan	Sifat Hukum	Prinsip Utama	Pengaruh ke Indonesia
Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – Dewan Eropa) Tahun 1981	Eropa (+ negara non-Eropa)	Binding	Perlindungan individu terhadap pemrosesan otomatis data pribadi	Diadopsi dalam spirit UU PDP
General Data Protection Regulation (GDPR) – Uni Eropa (2016, berlaku 2018)	Uni Eropa (global efektif)	Binding	Konsen eksplisit, hak atas data, akuntabilitas, portabilitas data	Jadi referensi utama dalam penyusunan UU PDP
OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980, diperbarui 2013)	Negara anggota OECD	Non Binding	8 Prinsip perlindungan privasi (<i>collection limitation, dsb</i>)	Memberikan dasar moral dan teknis
APEC Privacy Framework (2004)	Asia-Pasifik	Non Binding	Fokus pada arus data lintas batas dan perlindungan berbasis pasar	Menginspirasi pendekatan regional ASEAN dan RI

Adapun untuk aturan yang diterbitkan oleh Negara Indonesia antara lain sebagai berikut:

- Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, merupakan regulasi utama dan pertama yang khusus mengatur perlindungan data pribadi secara komprehensif. Undang-undang ini berlaku efektif penuh mulai tahun 2024 setelah masa transisi 2 tahun.
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-Undang Nomor 19 Tahun 2016, undang-undang ini mengakui perlindungan data pribadi dalam sistem elektronik, terutama dalam Pasal 26 ayat (1) yang menyebutkan penggunaan informasi pribadi harus atas persetujuan yang bersangkutan.
- Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Pemerintah

ini menjabarkan lebih lanjut prinsip dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang di dalamnya terdapat pengaturan terhadap kewajiban penyelenggara sistem elektronik (PSE) untuk: menyediakan perlindungan data pribadi, menyusun kebijakan privasi, dan melakukan pengamanan data.

- Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Peraturan ini lahir sebelum disahkannya UU PDP, peraturan ini menjadi dasar utama dalam pembentukan UU PDP yang di dalamnya terdapat pengaturan terkait definisi data pribadi, hak subjek data, dan kewajiban penyelenggara sistem elektronik.

Berdasarkan beberapa rujukan pengaturan di atas, negara dalam struktur ketatanegaraan memiliki kewajiban konstitusional untuk melindungi seluruh warga negara termasuk perlindungan atas data pribadi. Hal ini selaras dengan kewajiban konstitusional negara yang tertuang dalam Pembukaan Alinea Ke 4 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUDNRI 1945) yang menyatakan bahwa negara wajib melindungi segenap bangsa Indonesia dalam meningkatkan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan melaksanakan ketertiban dunia berdasar kemerdekaan, perdamaian dunia serta keadilan sosial.

2. Upaya Perlindungan Data Pribadi terhadap Sistem Algoritma Media Sosial

Media sosial yang memanfaatkan jaringan internet memungkinkan setiap orang membangun dan menyebarluaskan profil pribadi nya secara cepat dan luas, melalui *Internet of Things* (IoT) maka penyebaran informasi akan diteruskan secara dinamis melalui infrastruktur jaringan global dengan konfigurasi yang dapat diatur sesuai kebutuhan setiap platform media sosial. Oleh sebab itu, melalui IoT berarti kemampuan untuk membuat segala sesuatu di sekitar kita mulai dari mesin, perangkat, ponsel, dan mobil bahkan (kota dan jalan) dapat terhubung ke internet dengan perilaku yang cerdas dan dengan mempertimbangkan keberadaan jenis otonomi dan privasi.¹⁴

Data yang terkumpul yang diperoleh dari platform media sosial kemudian akan dianalisis,

ditafsirkan dan dipahami. Menurut Boyd, data yang diperoleh dari situs jejaring sosial adalah layanan berbasis web akan menghimpun data profil individu baik yang bersifat publik atau semi-publik ke dalam sistem, kemudian kemampuan untuk mengartikulasikan daftar pengguna lain dengan siapa mereka dapat berbagi koneksi, serta melihat dan mencari daftar koneksi mereka dan yang dibuat oleh orang lain dalam sistem. Lebih jauh, Kaplan dan Haenlein mendefinisikan media sosial sebagai “sekelompok aplikasi berbasis Internet yang dibangun di atas fondasi ideologis dan teknologi Web 2.0, dan memungkinkan pembuatan dan pertukaran konten yang dibuat pengguna”.¹⁵

Namun penggunaan algoritma pengumpulan dan pengolahan data tersebut juga memiliki dampak terhadap hak privasi seorang pengguna. Sebagai contoh, media sosial seperti Instagram, Facebook, TikTok, dan X (Twitter) kini bukan hanya berupa platform berbagi, melainkan juga alat pengumpulan dan pengolahan data pribadi melalui algoritma canggih. Algoritma ini memproses jejak digital untuk menyusun konten personalisasi, yang sering kali mengabaikan aspek privasi pengguna. Di sisi lain, aspek keamanan siber menjadi kebutuhan krusial untuk mencegah kebocoran dan penyalahgunaan data. Ketegangan antara kebutuhan keamanan siber dan perlindungan data pribadi inilah yang membentuk dialektika dalam era digital ini.

Keamanan sistem informasi merupakan aset yang harus dilindungi keamanannya. Keamanan secara umum diartikan sebagai “*quality or state of being secure to be free from danger*”.¹⁶ Hal

¹⁴ Mesra Betty Yel dan Mahyuddin K. M. Nasution, Keamanan Informasi Data Pribadi pada Media Sosial, Jurnal Informatika Kaputama (JIK), Vol. 6 No. 1, Januari 2022.

¹⁵ Mesra Betty Yel dan Mahyuddin K. M. Nasution *Ibid*, Hlm. 94.

¹⁶ Mesra Betty Yel dan Mahyuddin K. M. Nasution, *Ibid*, Hlm. 95.

tersebut berlaku juga terhadap keamanan siber yang bertujuan untuk melindungi sistem dari pihak ketiga, namun sering kali yang terjadi adalah adanya pengabaian terhadap bagaimana data tersebut diproses secara internal oleh penyedia platform. Hal inilah yang menimbulkan persoalan perlindungan hukum terhadap pengolahan data pribadi oleh penyedia platform.

Contoh kasus yang fenomenal dan menjadi salah satu skandal pelanggaran data pribadi terbesar dalam sejarah digital modern adalah kasus Cambridge Analytica. Kasus ini bermula dari tes kepribadian melalui platform Facebook bernama "This Is Your Digital Life" yang memberikan hasil setelah pengguna memberikan akses ke profil pribadi dan daftar teman mereka. Kuis ini diikuti oleh sekitar 270.000 pengguna secara langsung yang mengakses aplikasi ini, namun, karena kebijakan Facebook saat itu, data teman dari pengguna tersebut juga ikut terambil, sehingga total data pribadi sekitar 87 juta pengguna Facebook berhasil dikumpulkan tanpa persetujuan eksplisit. Data yang terkumpul oleh Dr. Aleksandr Kogan, seorang peneliti dari Universitas tidak hanya digunakan untuk riset akademik, tetapi dijual ke perusahaan konsultan politik Cambridge Analytica, yang mana perusahaan ini menggunakan data tersebut untuk membangun profil psikografis dari jutaan orang dan menargetkan iklan politik personal secara strategis yang digunakan untuk membantu kampanye Donald Trump dalam pemilu 2016. Dengan menggunakan iklan spesifik/target berdasarkan data pengguna Facebook, mereka mencoba memengaruhi opini pemilih di negara-negara bagian yang "swing". Skandal tersebut kemudian terbongkar oleh Christopher Wylie, yang merupakan

mantan karyawan Cambridge Analytica, bahwa telah terjadi praktik pembocoran data kepada media. Facebook sebagai platform media sosial menerima kecaman internasional karena kelalaian dalam melindungi data pengguna, akibat kelalaian tersebut Facebook didenda \$5 miliar oleh Federal Trade Commission (FTC). Ini merupakan denda terbesar terhadap perusahaan teknologi kala itu. Selanjutnya Negara Inggris melalui ICO (Information Commissioner's Office) juga mengenakan denda terhadap Facebook sebesar £500.000. Contoh kasus ini secara jelas menunjukkan pentingnya perlindungan data pribadi terhadap penggunaan algoritma untuk pengumpulan dan pengolahan data yang dilakukan oleh platform media sosial, yang secara langsung maupun tidak langsung berdampak terhadap hak privasi seorang pengguna layanan media sosial.

Jika melihat relasi penggunaan teknologi pada platform media sosial dengan uraian kasus di atas maka sesungguhnya terdapat teknologi pengenalan informasi yang mampu mengenali kebiasaan pengguna internet yang dikenal sebagai sistem berbasis *User Behavior Analytics* (UBA) atau *User Profiling System*. Sistem ini memanfaatkan berbagai metode untuk menganalisis, mempelajari, dan memprediksi pola perilaku pengguna saat menggunakan internet. Terdapat beberapa karakteristik sistem yang digunakan untuk mengenali kebiasaan pengguna internet yaitu:

- a. User Behavior Analytics (UBA), yaitu dengan menggunakan data historis perilaku pengguna untuk mendeteksi pola normal dan anomali, sistem ini banyak digunakan dalam bidang *cybersecurity* dan *personalization*. Adapun contoh dari penerapan sistem ini yaitu dengan penyesuaian konten rekomendasi seperti yang terdapat pada

platform YouTube, TikTok, Netflix, dan lainnya.

- b. Machine Learning-Based Recommendation System, yaitu sistem yang mempelajari riwayat pencarian, klik, pembelian, dan interaksi pengguna untuk merekomendasikan konten atau produk, contoh penerapan sistem ini dilakukan oleh e-commerce seperti Shopee, Tokopedia, dan *market place* lainnya, serta platform hiburan, contohnya Netflix yang merekomendasikan film berdasarkan tontonan sebelumnya, dan Spotify yang menyusun playlist "Discover Weekly" sesuai kebiasaan mendengar pengguna.
- c. Big Data Analytics Platform, yaitu sistem yang mampu menggabungkan data dari berbagai sumber: situs web, aplikasi, media sosial, hingga perangkat IoT. Hal ini memungkinkan perusahaan menganalisis pola konsumsi internet secara masif.
- d. AI-Powered Digital Assistants, berupa sistem yang mampu memberi pendampingan sesuai yang dibutuhkan oleh penggunanya seperti Google Assistant, Siri, atau Alexa, yang bisa belajar dari aktivitas pengguna untuk menyesuaikan respons, contohnya adalah menyediakan informasi cuaca, jadwal, atau berita sesuai kebiasaan pengguna.

Dengan hadirnya teknologi di atas, terdapat ketegangan hubungan yang memunculkan dialektika kemudahan pengolahan data dengan hak privasi yang terdapat pada pengguna layanan media sosial. Kemudian pertanyaan lanjutannya adalah apakah penggunaan sistem algoritma pengenalan profil pengguna internet oleh platform media sosial tidak bertentangan dengan peraturan perundang-undangan

yang ada, atau telah memberikan jaminan perlindungan hukum bagi penggunanya.

Menjawab hal tersebut dapat merujuk pada ketentuan yang terdapat dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, yang menyatakan bahwa subjek data berhak mendapatkan segala informasi yang berkaitan dengan pemanfaatan data pribadi yang dimilikinya oleh platform media sosial. Hal ini sebagaimana diatur Pada Pasal 5 yang menyebutkan: "*Subjek Data Pribadi berhak mendapatkan Informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan Data Pribadi, dan akuntabilitas pihak yang meminta Data Pribadi.*"

Selain akuntabilitas pemanfaatan data, hal yang terpenting adalah pemahaman terhadap pemrosesan data pribadi yang digunakan oleh berbagai platform. Hal ini akan memengaruhi maksud dan tujuan yang dihasilkan oleh algoritma itu sendiri, mulai dari mengumpulkan, menganalisis, dan memanfaatkan data pengguna yang menggunakan model algoritmik untuk berbagai tujuan, mulai dari personalisasi konten hingga periklanan tertarget. Oleh sebab itu, penting untuk melindungi subjek data pribadi dari pemrosesan algoritma yang tidak sesuai dengan tujuan yang disepakati, dan Undang-Undang Pelindungan Data Pribadi telah mengaturnya pada Pasal 8, yang menyatakan bahwa: "*Subjek Data Pribadi berhak untuk mengakhiri pemrosesan, menghapus, dan/atau memusnahkan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan*". Dan subjek pribadi juga dapat menarik persetujuan pemanfaatan data yang telah dia setujui bersama platform media sosial, hal ini juga telah dijamin oleh Undang-Undang Pelindungan Data Pribadi sebagaimana diatur

pada Pasal 9, yaitu: *“Subjek Data Pribadi berhak menarik kembali persetujuan pemrosesan Data Pribadi tentang dirinya yang telah diberikan kepada Pengendali Data Pribadi”*.

Dari beberapa ketentuan di atas, dapat diketahui bahwa undang-undang telah menjamin secara hukum terkait dengan kuasa pengendalian atas data pribadi yang diberikan oleh pengguna media sosial, sehingga terkait dengan informasi yang diberikan oleh pengguna media sosial bersifat sukarela.

Meskipun negara menjamin adanya perlindungan data pribadi dan kuasa atas pengendalian data ada di tangan pengguna di dalam memberikan atau tidak memberikan data informasi, namun yang menjadi persoalan adalah: (1) apakah seluruh pengguna media sosial memahami hal tersebut; (2) apakah semua yang tercantum dalam klausul persetujuan penggunaan aplikasi dan implikasi penggunaan data pribadi di media sosial dipahami oleh pengguna media sosial; dan (3) apakah kecakapan batas usia dalam persetujuan tersebut sudah memenuhi ketentuan peraturan perundang-undangan. Pertanyaan-pertanyaan tersebut tentu membutuhkan pengaturan lebih lanjut dari sekedar pengakuan atas kuasa penggunaan data pribadi yang dijamin oleh peraturan.

Negara melalui Undang-Undang Pelindungan Data Pribadi memang juga mengatur hal terkait keberatan atas pada pemrosesan data secara otomatis, sebagaimana disebutkan dalam Pasal 10 ayat (1) yang menyebutkan: *“Subjek Data Pribadi berhak untuk mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis, termasuk pemfilan, yang menimbulkan akibat hukum atau berdampak signifikan pada Subjek Data Pribadi”* serta subjek data juga dapat

memberikan batasan dalam pemrosesan data sebagaimana disebutkan pada Pasal 11, yaitu: *“Subjek Data Pribadi berhak menunda atau membatasi pemrosesan Data Pribadi secara sesuai dengan tujuan pemrosesan Data Pribadi”*. Terhadap pelanggaran hukum yang terjadi, pihak subjek data juga berhak menggugat sebagaimana disebutkan pada Pasal 12 ayat (1), yaitu: *“Subjek Data Pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan”*.

Namun ketentuan di atas menunjukkan bahwa upaya yang diberikan oleh negara bersifat *“berhak mengajukan keberatan”* atau *“berhak menunda atau membatasi pemrosesan”* atau *“berhak menggugat dan menerima ganti rugi”* yang seluruhnya bersifat stelsel pasif, artinya negara tidak terlibat aktif dalam memberikan perlindungan atas pemrosesan data otomatis, hal tersebut sepenuhnya diserahkan oleh pengguna media sosial.

Terkait dengan pemanfaatan data pribadi pengguna media sosial oleh penyedia platform dengan menggunakan algoritma secara otomatis, akan berdampak terhadap hak privasi yang ada pada data tersebut. Algoritma akan bekerja optimal dengan mendapat akses pada data besar (*big data*). Oleh karena itu, berbagai platform digital (seperti media sosial, e-commerce, dan aplikasi lainnya) secara terus-menerus akan mengumpulkan data pribadi pengguna: mulai dari lokasi, kebiasaan klik, minat, hingga interaksi sosial. Hal ini menyebabkan hak privasi terganggu karena pengguna sering kali tidak menyadari sejauh mana data mereka dikumpulkan dan digunakan.

Dengan data yang dikumpulkan, algoritma dapat membuat profil psikografis pengguna,

bahkan mampu memprediksi keputusan dan preferensi pengguna, sehingga akan mengarah pada risiko "manipulasi perilaku", terutama dalam iklan politik, pemasaran, atau rekomendasi konten yang memengaruhi pilihan individu secara tidak sadar. Algoritma, terutama yang berbasis *artificial intelligent* atau *machine learning*, sering kali bersifat "*black box*" artinya proses kerja dan hasilnya tidak sepenuhnya dapat diakses atau dipahami oleh publik, hal ini tentu menimbulkan kekhawatiran tentang siapa yang mengontrol data dan bagaimana keputusan otomatis dibuat, yang dapat berdampak pada pelanggaran privasi tanpa diketahui.

Terbatasnya pengaturan dan perlindungan yang diberikan negara terhadap pengguna media sosial atas penyerahan data pribadi sebelum menggunakan media sosial tersebut, maka hal yang perlu dibangun terhadap pengguna media sosial adalah kemauan membaca dan memahami syarat persetujuan penggunaan layanan media sosial, yang di dalamnya terdapat klausula terkait penggunaan dan pemanfaatan data pribadi pengguna.

Penggunaan dan pemanfaatan media sosial juga harus sesuai peruntukannya, baik cakap umur dan juga cakap bertindak. Hal ini karena layanan aplikasi media sosial yang diberikan bersifat satu arah dan tidak mengenali secara materiil kecakapan penggunaannya, penyedia aplikasi hanya menyediakan klausula baku yang dapat disetujui atau tidak disetujui oleh penggunaannya. Oleh sebab itu, kecakapan pengguna media sosial menjadi tanggung jawab bersama, baik negara melalui berbagai literasi digital, juga masyarakat ataupun keluarga di dalam mengawasi penggunaan media sosial oleh seorang anak.

Selain pemahaman literasi digital kepada seluruh lapisan pengguna media sosial,

hal penting yang perlu menjadi perhatian adalah "Keterbukaan Algoritma". Maksudnya adalah memberikan prinsip bahwa proses, struktur, dan hasil dari algoritma (terutama yang digunakan dalam sistem otomatis atau kecerdasan buatan) harus dapat dipahami, diawasi, dan dipertanggungjawabkan oleh publik atau otoritas yang berwenang, seperti bagaimana data dikumpulkan, bagaimana algoritma bekerja, dan bagaimana rekomendasi hasil algoritma disediakan. Oleh sebab itu, dibutuhkan audit sistem media sosial secara berkala sebagai proses evaluasi yang menyeluruh terhadap sistem, kebijakan, algoritma, serta praktik penggunaan data pada platform media sosial, yang dilakukan secara teratur guna menjamin keamanan sistem, dan menunjukkan adanya kepatuhan terhadap hukum terhadap perlindungan hak privasi pengguna.

D. Penutup

Hak atas perlindungan diri pribadi sesungguhnya telah menjadi bagian perlindungan yang diatur oleh konstitusi tertinggi melalui UUDNRI Tahun 1945. Hak tersebut diatur pada Pasal 28 G Ayat (1) yang secara umum warga negara berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang di bawah kekuasaannya. Upaya melindungi data pribadi dari penyalahgunaan yang terjadi pada ruang sosial media (*digital network*) tentu merupakan bagian dari tugas negara di dalam mengambil peran untuk melindungi warganya dari berbagai jenis kejahatan yang terjadi di dunia *cyber*.

Penggunaan algoritma dalam pengumpulan dan pengolahan data memiliki dampak terhadap hak privasi seorang pengguna, algoritma yang canggih akan memproses jejak digital untuk menyusun konten personalisasi,

hal ini sering kali mengabaikan aspek privasi pengguna. Oleh sebab itu, keamanan sistem informasi merupakan aset yang harus dilindungi keamanannya sebagai *"quality or state of being secure to be free from danger"*.

Meskipun negara menjamin adanya perlindungan data pribadi dan kuasa atas pengendalian data berada di tangan pengguna di dalam memberikan atau tidak memberikan data informasi dibutuhkan, pengaturan lebih lanjut dari sekedar pengakuan atas kuasa penggunaan data pribadi dijamin oleh peraturan. Saat ini perlindungan data pribadi terhadap pemrosesan data otomatis melalui algoritma masih bersifat stelsel pasif, artinya negara tidak terlibat aktif dalam memberikan perlindungan atas pemrosesan data otomatis, yang hal tersebut sepenuhnya diserahkan oleh pengguna media sosial.

Penting bagi negara dan masyarakat secara bersama membangun literasi digital terhadap seluruh lapisan pengguna media sosial, hal ini untuk meminimalisir dampak negatif yang tidak diharapkan dari penggunaan media sosial. Hal ini mengingat terbatasnya pengaturan dan perlindungan yang diberikan negara terhadap pengguna media sosial atas penyerahan data pribadi sebelum menggunakan media sosial tersebut. Selanjutnya hal penting yang juga perlu dibangun terhadap pengguna media sosial adalah kemauan membaca dan memahami syarat persetujuan penggunaan layanan media sosial.

Penting juga untuk dibangun keterbukaan algoritma yang akan membuka ruang informasi terhadap proses, struktur, dan hasil dari algoritma (terutama yang digunakan dalam sistem otomatis atau kecerdasan buatan). Dibutuhkan juga audit sistem media sosial secara berkala untuk menjamin keamanan

sistem dan menunjukkan adanya kepatuhan terhadap hukum terhadap perlindungan hak privasi pengguna.

DAFTAR PUSTAKA

Buku

- John Rawls, *A Theory of Justice*, Cambridge, Massachusetts: Harvard University Press, 1971.
- Nagel, Thomas. *The View from Nowhere*. Oxford: Oxford University Press, 1986

Jurnal

- Adam D. Moore, "Privacy", *Library Hi Tech*, Vol. 25, 2007 (available at: <http://ssrn.com/abstract=1980871>)
- Daniel J. Solove, "Conceptualizing Privacy", *California Law Review*, Vol. 90, Issue 4 Article 2, 2002.
- Deirdre K. Mulligan¹, Colin Koopman² and Nick Doty, "Privacy is an Essentially Contested Concept: a Multidimensional Analytic for Mapping Privacy. *Phil. Trans. R. Soc. A* 374: 2016.0118.
- Edy Susanto, dkk, Manajemen Keamanan Cyber di Era Digital, *Jurnal Bisnis dan Kewirausahaan (Journal of Business and Entrepreneurship)* Vol. 11, No. 1 Mei 2023, e-ISSN: 2685-6255; p-ISSN: 2302-4119
- Gallei. Waldron J, "Is the rule of law an essentially contested concept (in Florida)?" *Law Philos.* 21 2002.
- Judithj Arvis Thomson, "The Right to Privacy", *Philosophy and Public Affairs*, Vol. 4, No. 4 (Summer, 1975)
- Mesra Betty Yel dan Mahyuddin K. M. Nasution, Keamanan Informasi Data Pribadi Pada Media Sosial, *Jurnal Informatika Kaputama (JIK)*, Vol. 6 No. 1, Januari 2022.
- Nandy, Pengertian Media Sosial, Sejarah, Fungsi, Jenis, Manfaat dan perkembangannya, <https://www.gramedia.com/literasi/pengertian-media-sosial/>, diakses 6 April 2025
- Sekaring Ayumeida Kusnadi dan Andy Usmina Wijaya, Perlindungan Hukum Data Pribadi Sebagai Hak Privasi, *JA: Jurnal Al-Wasath* 2 No.1
- Wahyudi Djafar dan M. Jodi Santoso, Perlindungan Data Pribadi: Konsep, Instrumen, dan

Prinsipnya, Lembaga Studi dan Advokasi Masyarakat (ELSAM), dengan dukungan dari Australian Government Department of Foreign Affairs and Trade (DFAT), 2019.

Peraturan

Undang-Undang Nomor 27 Tahun 2022 tentang
Pelindungan Data Pribadi