Dr. Kurniawan Tri Wibowo, S.H., M.H. | Dr. Muhammad Alfian Dj, M.H.
Dr. Abdul Karim, S.T., M.M. | Dr. Abdul Karim, S.H., M.I.Kom.
Rizki Syafril, S.H.I, M.Si. | Dr. Ma'rifah, S.H., M.H.
Dr. H. Muhammad Syaukani, S.T., S.H., M.Cs, M.Kom.
Moh. Muniri, S.H., M.Kn.

HUKUM DIGITAL

DAN PRIVASI DATA

Editor:
Dr. H. Muhammad Syaukani, S.T., S.H., M.Cs., M.Kom.

Dr. Kurniawan Tri Wibowo, S.H., M.H., Dr. Muhammad Alfian Dj, M.H., Dr. Abdul Karim, S.T., M.M., Dr. Abdul Karim, S.H., M.I.Kom., Rizki Syafril, S.H.I, M.Si., Dr. Ma'rifah, S.H., M.H., Dr. H. Muhammad Syaukani, S.T., S.H., M.Cs., M.Kom., Moh. Muniri, S.H., M.Kn.

HUKUM DIGITAL DAN PRIVASI DATA

Editor:
Dr. H. Muhammad Syaukani, S.T., S.H., M.Cs., M.Kom.

Penerbit CV. Al-Haramain Lombok
1446 H/ 2025 M

HUKUM DIGITAL DAN PRIVASI DATA

Penulis: Dr. Kurniawan Tri Wibowo, S.H., M.H., Dr. Muhammad Alfian Dj, M.H., Dr. Abdul Karim, S.T., M.M., Dr. Abdul Karim, S.H., M.I.Kom., Rizki Syafril, S.H.I, M.Si., Dr. Ma'rifah, S.H., M.H., Dr. H. Muhammad Syaukani, S.T., S.H., M.Cs, M.Kom., Moh. Muniri, S.H., M.Kn.
Editor: Dr. H. Muhammad Syaukani, S.T., S.H., M.Cs, M.Kom.
Desain Sampul: Tim Al-Haramain Lombok
Proofreader: Tim Al-Haramain Lombok
Lay Out: Tim Al-Haramain Lombok
Cetakan Pertama: Rajab 1446 H/Januari 2025 M

Penerbit CV. Al-Haramain Lombok
Jl. Gunung Tambora, Mataram, NTB.
alharamainlombok.com
085-338-949-261 (WA)
Penerbit Al-Haramain Lombok (FB)
alharamainlombok1437@gmail.com
Anggota IKAPI (012/NTB/2022)

1446/ 2025, vi + 171 hlm. 15,5 x 23 cm

ISBN: 978-634-7095-05-3

KATA PENGANTAR

Segala puji bagi Tuhan semesta alam, yang telah memberikan rahmat, nikmat, dan hidayah-Nya, sehingga kita dapat bersama-sama menyelesaikan buku ini dengan penuh semangat dan dedikasi. Dengan rasa syukur yang mendalam, kami persembahkan buku ini sebagai kontribusi pemikiran dalam memahami hukum dalam perspektif digitalisasi dan privasi data.

Buku dengan judul "Hukum Digital dan Privasi Data" ini disusun untuk memberikan wawasan mendalam tentang isu-isu hukum yang berkaitan dengan perkembangan pesat teknologi digital, khususnya mengenai privasi data dalam konteks global yang semakin terhubung. Ditulis oleh tujuh orang praktisi pendidikan dan hukum yang memiliki pengetahuan serta pengalaman mumpuni di bidangnya, buku ini menawarkan analisis kritis mengenai tantangan hukum yang muncul seiring dengan pemanfaatan teknologi digital yang semakin luas. Dalam setiap bab, para penulis berbagi pandangan yang didasarkan pada pemahaman hukum yang mendalam, serta perspektif yang berbasis pada praktik nyata dalam menghadapi dinamika dunia digital.

Di era digital yang serba cepat ini, privasi data menjadi salah satu isu yang paling relevan dan penting untuk diperhatikan. Buku ini menyelami berbagai dimensi hukum yang terkait dengan pengelolaan dan perlindungan data pribadi, baik dari sudut pandang regulasi nasional maupun internasional. Dengan pertumbuhan pesat teknologi seperti internet of things (IoT), kecerdasan buatan (AI), dan media sosial, perlindungan data pribadi kini menghadapi tantangan yang jauh lebih kompleks daripada sebelumnya. Para penulis berusaha mengurai dengan

jelas bagaimana hukum dapat mengimbangi perkembangan teknologi tanpa mengesampingkan hak privasi individu.

Melalui bab-bab yang disusun secara sistematis, pembaca akan diperkenalkan pada konsep-konsep hukum digital yang fundamental, seperti hak atas privasi, perlindungan data pribadi, dan prinsip-prinsip dasar dalam peraturan perundang-undangan yang mengatur penggunaan data digital. Buku ini juga mengangkat berbagai peraturan yang relevan, seperti Regulasi Perlindungan Data Umum Uni Eropa (GDPR) dan kebijakan serupa di berbagai negara, serta tantangan yang dihadapi dalam implementasinya. Di samping itu, buku ini juga membahas potensi ancaman terhadap privasi data akibat penyalahgunaan informasi digital, serta langkah-langkah preventif yang dapat diambil untuk melindungi data pribadi di dunia maya.

Diharapkan bahwa buku ini akan menjadi referensi yang bermanfaat bagi berbagai kalangan, baik bagi praktisi hukum, pendidik, maupun masyarakat umum yang ingin memahami lebih dalam tentang pentingnya perlindungan data pribadi dalam konteks hukum digital. Dengan kontribusi penulis yang beragam dan perspektif yang berimbang, buku ini tidak hanya sekadar membahas teori-teori hukum, tetapi juga memberikan panduan praktis yang dapat diterapkan dalam menghadapi tantangan hukum di dunia digital. Semoga buku ini dapat membuka pemahaman baru serta memberikan solusi bagi pengelolaan hukum dan privasi data yang lebih baik di masa depan.

Salam Editor,

DAFTAR ISI

BAB 1

PENGENALAN HUKUM DIGITAL DAN PRIVASI DATA

Dr. Kurniawan Tri Wibowo, S.H., M.H.

(Universitas Islam Negeri Prof. Saifudin Zuhri Purwokerto)

A. Definisi dan Ruang Lingkup Hukum Digital

Secara mendasar, istilah "digital" merujuk pada teknologi yang memproses data dalam bentuk angka biner, yaitu 0 dan 1. [1] Kata "digital" sendiri berasal dari bahasa Yunani *digitus*, yang berarti jari jemari, mencerminkan fungsi awal manusia dalam menghitung menggunakan jari, yang kemudian diadaptasi menjadi dasar sistem perhitungan modern.[2] Konsep ini telah mengalami transformasi besar seiring dengan perkembangan teknologi, dari sekadar alat bantu perhitungan menjadi sistem teknologi kompleks yang mendominasi berbagai aspek kehidupan manusia.

Rafael Capurro, seorang filsuf teknologi, menekankan pentingnya memikirkan kembali ontologi dan etika di era digital, seiring dengan perubahan paradigma yang dibawa oleh teknik digital. Revolusi digital tidak hanya membuka peluang besar dalam efisiensi dan inovasi, tetapi juga menimbulkan tantangan seperti ancaman kejahatan siber dan pelanggaran privasi. Oleh karena itu, hukum digital bertujuan untuk menciptakan keseimbangan antara manfaat dan risiko yang muncul akibat penggunaan teknologi digital. [3]

Kemajuan teknologi mengakibatkan konsep digital tidak hanya

---

[1] Muhamad Danuri, *Perkembangan Dan Transformasi Teknologi Digital*, Jurnal Infokam Nomor II Th. XV/SEPTEMBER/2019, hal. 119

[2] Amitabh Bhattacharya, 2013, *Digital communication. (14 print)*. (New Delhi: McGraw Hill publication, hal. 1-30.

[3] Rafael Capurro, 2017, *Homo Digitalis. Beiträge zur Ontologie, Anthropologie und Ethik der gitilaen Technik*, Springer VS, Wiesbaden, page. 34

terbatas pada pengolahan angka, tetapi juga mencakup kemampuan untuk menyimpan, mengirim, dan mengolah informasi dalam berbagai bentuk, seperti teks, suara, dan gambar. Perkembangan ini memungkinkan terciptanya perangkat pintar, jaringan internet global, dan aplikasi yang telah mengubah cara manusia bekerja, berkomunikasi, dan hidup sehari-hari. Dengan kemajuan teknologi informasi dan komunikasi yang pesat, manusia telah menyaksikan transformasi luar biasa dalam hampir setiap aspek kehidupan. Revolusi ini memiliki dua sisi yang sama-sama kuat: sisi positif yang penuh dengan potensi dan kemungkinan, serta sisi negatif yang mengandung tantangan dan risiko yang serius.[4]

Saat ini aktivitas manusia banyak memanfaatkan sistem digital. Mulai dari berbelanja harian sampai tagihan bulanan juga menggunakan sistem digital. Hal ini menimbulkan tantangan dan risiko tersebut yang harus diatur oleh hukum. "Hukum Digital" merujuk pada serangkaian hukum dan regulasi yang mengatur perilaku dan transaksi di dunia digital yang melibatkan teknologi informasi, internet, dan segala bentuk komunikasi elektronik. Ini mencakup bidang hukum yang berkaitan dengan keamanan siber, privasi data, hak kekayaan intelektual, bisnis elektronik, dan isu-isu hukum lainnya yang berkaitan dengan dunia digital.[5]

Spesialisasi Hukum Digital memberikan pemahaman menyeluruh tentang kerangka hukum yang membentuk ekonomi digital. Mahasiswa akan mempelajari keamanan siber, kejahatan siber, hak kekayaan intelektual, perlindungan data, dan etika AI.[6] Radchenko dan Gorbunov membedakan unsur-unsur hukum digital berikut: hak konstruksi negara digital dan administrasi publik, hak cipta atas entitas digital, hukum

---

[4] Yopie Indra Pribadi, *Telaah Kritis Revolusi Digital : Sindrom Ketidaksadaran Pengguna Internet dalam era Kapitalisme Surveilans*, https://disdukcapil.pontianak.go.id/telaah-kritis-revolusi-digital--sindrom-ketidaksadaran-pengguna-internet-dalam-era-kapitalisme-surveilans-ditulis-oleh-yopie-indra-pribadi

[5]Agus Wibowo, 2023, Hukum di Era Globalisasi Digital, Yayasan Prima Agus bekerjasama dengan Universitas Sains & Teknologi Komputer (Universitas STEKOM), Semarang, hal. i

[6] Digital Law ath, *Explore the World of Digital Law,* https://digi-dcl.com/digital-law

perangkat lunak, hak atas uang digital, transaksi, sengketa, dan lainnya.[7] Linlay James menyatakan bahwa, Hukum digital mengakui tanggung jawab elektronik individu atas tindakan dan perbuatannya, terlepas dari instrumentasi etis atau tidak etisnya. Hukum digital sering kali didorong oleh hubungan kontraktual dari perjanjian daring antara individu dan bisnis. Salah satu bagian penting dari Hukum digital adalah privasi data dan pelanggaran tindakan perlindungan data.[8]

Hukum digital mencerminkan realitas bahwa hampir semua aktivitas manusia, mulai dari bisnis, hiburan, hingga komunikasi, kini semakin bergantung pada teknologi digital dan internet. Perkembangan teknologi ini telah menciptakan ruang maya tanpa batas geografis, sehingga regulasi hukum digital harus bersifat lintas batas dan berorientasi global untuk mengatasi tantangan yang timbul. Tantangan tersebut mencakup berbagai isu, seperti perlindungan data pribadi, keamanan siber, dan hak kekayaan intelektual, yang memerlukan pendekatan kolaboratif antarnegara.

Setiap negara atau wilayah memiliki kerangka hukum yang berbeda sesuai dengan kebutuhan lokal dan budaya hukum masing-masing, ada upaya global untuk menyelaraskan peraturan di beberapa aspek kunci. Kesepakatan internasional dan penerapan standar global sangat penting untuk menciptakan tata kelola digital yang harmonis, adil, dan mampu mengimbangi dinamika perkembangan teknologi yang pesat.Ruang lingkup hukum digital sangat luas, mencakup berbagai aspek yang terkait dengan penggunaan teknologi dalam kehidupan manusia. Hukum ini meliputi pengaturan transaksi elektronik, hak cipta digital, keamanan data, dan privasi pengguna.

Dalam era digital, aspek perlindungan data pribadi menjadi salah satu fokus utama hukum digital. Informasi dalam bentuk data numerik sering kali diproses, disimpan, dan dibagikan tanpa sepengetahuan

---

[7] Radchenko, M. Y., & Gorbunov, V. P. (2000). Digital law of the future [Digital law of the future]. The Second All-Russian Conference "Law and the Internet: Theory and Practice". https://ifap.ru/pi/02/r03.htm

[8]Linlay James, Digital Law, https://linleyjames.co.uk/digital-law/#:~:text=Digital%20law%20recognises%20an%20individuals,protect%20themselves%20from%20digital%20exploitation.

pemiliknya, yang dapat menimbulkan potensi penyalahgunaan. Revolusi digital telah mempercepat terjadinya transformasi ekonomi digital, di mana transaksi berbasis teknologi menjadi semakin umum. Namun, kemudahan ini diiringi oleh ancaman serius, seperti pencurian identitas, pelanggaran privasi, dan serangan siber. Untuk mengatasi tantangan tersebut, hukum digital memberikan kerangka aturan yang memastikan data pengguna dilindungi dan hak-hak mereka dihormati.

Revolusi digital juga memengaruhi aspek hukum terkait hak kekayaan intelektual, terutama dalam konteks distribusi dan konsumsi karya kreatif. Dalam dunia digital, reproduksi dan distribusi karya seni, musik, dan film menjadi lebih mudah, tetapi sering kali tanpa izin pemilik hak cipta. Hal ini menimbulkan dilema antara kemudahan akses dan perlindungan hak cipta. Hukum digital memainkan peran penting dalam menetapkan aturan mengenai perlindungan hak cipta digital untuk mencegah pelanggaran serta memastikan para kreator mendapatkan hak mereka. Regulasi ini menjadi semakin penting seiring dengan berkembangnya platform digital seperti media sosial dan layanan streaming.

Selain itu, hukum digital juga mencakup aspek keamanan siber yang bertujuan melindungi infrastruktur digital dari ancaman dan serangan. Serangan siber seperti peretasan, *malware*, dan *ransomware* menjadi ancaman serius bagi individu, perusahaan, dan negara. Dalam hal ini, hukum digital bertujuan untuk memberikan perlindungan hukum terhadap korban serta memberikan sanksi kepada pelaku kejahatan siber. Keamanan digital tidak hanya berhubungan dengan teknologi, tetapi juga memerlukan pendekatan etik dan strategis untuk memastikan ruang digital yang aman dan terpercaya.

Ruang lingkup hukum digital juga merambah pada pengaturan etika penggunaan teknologi digital dalam interaksi sosial dan ekonomi. Teknologi digital telah menciptakan realitas baru seperti media sosial, yang menjadi platform utama komunikasi dan informasi. Namun, penggunaan media sosial juga memunculkan isu-isu seperti hoaks, ujaran kebencian, dan penyalahgunaan platform. Hukum digital bertugas mengatur agar teknologi ini digunakan secara bertanggung jawab, dengan memberikan batasan pada perilaku yang melanggar norma

hukum dan sosial. Regulasi yang jelas dan tegas diperlukan untuk menjaga keseimbangan antara kebebasan berekspresi dan perlindungan masyarakat.

Hukum digital juga berperan dalam mendukung pembangunan ekonomi digital yang berkelanjutan. Di era ini, banyak sektor ekonomi yang bergantung pada teknologi digital, termasuk *e-commerce, fintech, metaverse* dan *blockchain*. Regulasi yang mendukung pertumbuhan ekonomi digital tanpa mengorbankan keamanan dan keadilan menjadi fokus utama hukum digital. Dengan memberikan kepastian hukum, regulasi ini dapat mendorong inovasi sekaligus melindungi kepentingan konsumen dan pelaku usaha. Keberadaan hukum digital yang kokoh menjadi kunci untuk menciptakan lingkungan bisnis yang sehat dan kompetitif.

B. Konseptualisasi Hukum Digital

Apabila dilihat dari definisinya konsep digital pada dasarnya memiliki konsep yang luas, yang merujuk pada teknologi yang memproses data dalam bentuk angka biner, yaitu 0 dan 1. Konsep ini digunakan oleh system computer, internet bahkan dunia siber. Dengan demikian hukum digital juga tidak lepas dari konsep-konsep hukum lainnya seperti *Internet law* dan *cyber law*. Bahkan Maxim I. Inozemtsev menyatakan bahwa, dalam lingkungan akademis, konsep "hukum internet" masih lebih mapan dibandingkan konsep "hukum digital".[9]

Di negara-negara Eropa dan AS, "*Internet law*" telah menjadi disiplin akademis. Hukum ini pertama kali muncul pada tahun 1991[10], meskipun sebagian besar peraturan hukum yang relevan dibuat jauh setelahnya.[11] Ilmu hukum secara bertahap menguasai bidang baru hubungan masyarakat, yang dibentuk di ruang internet, seiring dengan perkembangan ruang ini sendiri. Oleh karena itu, publikasi ilmiah paling otoritatif tentang isu-isu umum tantangan digital muncul sejak tahun

[9] Maxim I. Inozemtsev, *Digital law: The Pursuit Of Certainty*, Digital Law Journal, 2(1), 8–28. https://doi.org/10.38044/2686-9136-2021-2-1-8-28

[10] Goldman, E. (2008). *Teaching cyberlaw*. Saint Louis University Law Journal, 52(3), 749–764.

[11] Edwards, L., & Waelde, C. (Eds.). (2009). *Law and the Internet*. Bloomsbury Publishing.

1990-an.[12]

Internet law adalah cabang hukum yang secara spesifik mengatur aktivitas yang terjadi dalam ruang lingkup internet. Hukum ini mencakup berbagai aspek seperti nama domain, *e-commerce*, perlindungan data, dan kejahatan yang terjadi di platform online, seperti penipuan dalam transaksi digital. Karena internet adalah jaringan global, hukum ini seringkali membutuhkan kerjasama internasional untuk mengatur penggunaannya secara efektif. Fokus utamanya adalah memastikan bahwa aktivitas di internet berjalan sesuai dengan aturan yang berlaku, baik di tingkat lokal maupun global, termasuk perlindungan hak cipta untuk konten digital yang diunggah di *platform online*.

Asal usul *Internet law* dapat ditelusuri kembali ke kebangkitan Internet dan perkembangan teknologi komunikasi elektronik. Hukum komunikasi elektronik awal difokuskan pada transmisi dan pemrosesan informasi elektronik, dengan tujuan utama melindungi privasi dan keamanan komunikasi. Pada tahun 1986, Amerika Serikat mengesahkan Undang-Undang Privasi Komunikasi Elektronik, yang memberikan perlindungan hukum untuk privasi dan keamanan komunikasi elektronik. Selain itu, dengan mempopulerkan Internet, negara-negara telah memperkenalkan hukum dan peraturan yang relevan, seperti "Undang-Undang Layanan Informasi dan Komunikasi" Jerman dan "Langkah-Langkah Manajemen Layanan Informasi Internet" Tiongkok untuk mengatur transmisi informasi jaringan dan pengoperasian layanan Internet.[13]

Internet law menghadapi banyak tantangan, termasuk perlindungan privasi data, penanggulangan kejahatan dunia maya, perlindungan hak cipta, dan sebagainya. Untuk mengatasi tantangan ini, negara-negara perlu memperkuat legislasi dan regulasi, mendorong kerja sama internasional, dan bersama-sama mengatasi tantangan hukum *cyberspace*.[14]

---

[12] Marsden, C. T. (Ed.). (2000). *Regulating the global information society* (Vol. 2). Psychology Press.

[13] Zongqi Li, *The Evolution of Internet Law in The Digital Age*, International Journal of Education and Humanities ISSN: 2770-6702 | Vol. 13, No. 2, 2024, hal. 124

[14] Reidenberg, J. R., & De Hert, P. (Eds.). (2019). Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection. Oxford, UK

Perkembangan teknologi jaringan komputer global atau internet telah menciptakan dunia baru yang dinamakan *cyberspace*.[15] Sebuah dunia baru yang berbasis komputer dan menawarkan berbagai kemudahan seperti *browsing, chating, e-mail, e-commerce, e-shopping,* dan kemudahan lainnya.

Pengertian *cyberspace* tidak terbatas pada dunia yang tercipta ketika terjadi hubungan melalui internet. Setidak-tidaknya dengan memperhatikan definisi melalui internet tentang *cyberspace* dari John Perry Barlow, *cyberspace* lebih luas dari sekedar melalui internet. Ketika kita sedang menelepon atau membaca buku, ada ruang yang muncul (juga dinamakan *cyberspace* oleh Barlow), tetapi ruang yang tercipta itu tidak mungkin untuk berinteraksi secara *real time*.[16]

Anonimitas di ruang siber menciptakan tantangan besar bagi penegakan hukum, karena mengaburkan identitas pelaku dan membuat pelacakan aktivitas ilegal menjadi jauh lebih sulit.[17] "Regulasi hukum seringkali tertinggal dari perkembangan teknologi, menciptakan celah yang dimanfaatkan oleh pelaku kejahatan dunia maya.[18] Perkembangan dunia maya menciptakan adanya *cyberlaw*. *Cyber law* yaitu Hukum yang mengatur aktivitas di dunia maya (kejahatan dunia maya melalui jaringan internet).[19]

Cyber law memiliki cakupan yang lebih luas dibandingkan *Internet law*, karena mencakup seluruh aktivitas yang terjadi di dunia maya, baik di internet maupun jaringan komputer lainnya. Hukum ini berfokus pada isu-isu yang berhubungan dengan keamanan siber, seperti perlindungan terhadap serangan siber, pencurian data, dan pelanggaran privasi. *Cyber law* juga mencakup regulasi terhadap penggunaan perangkat keras dan perangkat lunak yang terhubung dalam jaringan, termasuk pengaturan terkait malware, hacking, dan bentuk kejahatan siber lainnya. Tujuan utama *Cyber law* adalah menciptakan lingkungan digital yang aman bagi individu, organisasi, dan negara.

---

15 Agus Raharjo, 2002, *Cyber Crime*, Citra Aditya, Bandung, hal. 91

16 *Ibid.,* hal. 92

17 Lawrence Lessig, 1999. *Code: And Other Laws of Cyberspace,* NY: Basic Books, New York, hal. 157

18 *Ibid.,* hal. 127

19 Widodo, 2013, *Hukum Pidana di Bidang teknologi Informasi (cybercrime law) : Telaah Teoritik dan Bedah Kasus*, Yogyakarta, hal. 15

Digital law adalah konsep hukum yang lebih luas dan mencakup tidak hanya internet dan dunia maya, tetapi juga segala bentuk teknologi digital yang memengaruhi kehidupan manusia. Ini mencakup pengaturan penggunaan perangkat pintar, kecerdasan buatan, blockchain, hingga teknologi realitas virtual. Digital law berfokus pada regulasi yang berkaitan dengan hak cipta digital, perlindungan data, transaksi elektronik, serta dampak sosial dari teknologi digital, seperti etika penggunaan teknologi dan pengaruhnya terhadap hak asasi manusia. Digital law bertujuan menciptakan kerangka hukum yang holistik untuk mengatur interaksi manusia dengan teknologi digital secara menyeluruh.

Perbedaan signifikan antara *Internet law*, cyber law, dan digital law terletak pada ruang lingkup dan fokus pengaturannya. *Internet law* secara eksklusif membahas aspek hukum dari aktivitas yang terjadi di internet, sedangkan *Cyber law* mencakup seluruh interaksi dan ancaman yang terjadi dalam jaringan komputer, baik online maupun offline. Digital law, di sisi lain, memiliki cakupan yang jauh lebih luas, mencakup berbagai teknologi digital yang tidak selalu terkait dengan internet, seperti perangkat lunak berbasis blockchain atau algoritma kecerdasan buatan.

Seiring dengan pesatnya perkembangan teknologi, digital law atau hukum digital menjadi lebih relevan karena mampu menjangkau lebih banyak aspek yang tidak tercakup oleh *Internet law* atau cyber law. Misalnya, pengaturan terkait kendaraan otonom, sistem pembayaran berbasis cryptocurrency, dan etika kecerdasan buatan menjadi fokus utama digital law. Sementara itu, *Internet law* tetap relevan untuk mengatur transaksi online dan konten digital, serta *Cyber law* penting untuk menangani ancaman keamanan di dunia maya. Perbedaan ini menunjukkan bagaimana ketiga cabang hukum tersebut saling melengkapi dalam mengatur teknologi modern.

Secara ontologis, hukum digital lahir sebagai respons terhadap perubahan mendasar dalam cara manusia berinteraksi, bertransaksi, dan mengelola informasi di era teknologi. Hakikat hukum digital adalah sebagai alat untuk mengatur aktivitas manusia yang melibatkan teknologi digital, seperti internet, kecerdasan buatan, blockchain, dan perangkat pintar. Hukum digital mencerminkan kebutuhan untuk mengatasi

masalah yang muncul akibat perkembangan teknologi, termasuk tantangan dalam melindungi privasi, keamanan, dan hak asasi manusia. Dengan demikian, ontologi hukum digital didasarkan pada kenyataan bahwa teknologi digital telah menjadi bagian integral dari kehidupan manusia, yang memerlukan pengaturan hukum yang khusus dan relevan.

Pengetahuan hukum digital berasal dari pengamatan dan analisis terhadap fenomena digital, seperti interaksi online, transaksi elektronik, dan ancaman siber. Proses epistemologis melibatkan pendekatan interdisipliner yang menggabungkan ilmu hukum, teknologi informasi, etika, dan ekonomi. Sumber-sumber pengetahuan hukum digital meliputi penelitian akademik, yurisprudensi, dan kebijakan internasional terkait teknologi. Pengetahuan ini terus berkembang seiring dengan kemajuan teknologi dan perubahan kebutuhan masyarakat, yang berarti hukum digital harus bersifat adaptif dan berbasis bukti. Epistemologi hukum digital berfokus pada bagaimana pengetahuan tentang hukum digital dibangun, diperoleh, dan divalidasi.

Aksiologi hukum digital berkaitan dengan nilai-nilai yang ingin dicapai melalui penerapan hukum ini. Secara aksiologis, hukum digital bertujuan untuk menciptakan keadilan, keamanan, dan keteraturan dalam penggunaan teknologi digital. Nilai utama yang ingin dicapai mencakup perlindungan privasi, keadilan dalam akses terhadap teknologi, perlindungan terhadap pelanggaran hak kekayaan intelektual, dan penciptaan ruang digital yang aman dan inklusif. Selain itu, hukum digital juga bertujuan untuk mengatur inovasi teknologi yang bertanggung jawab secara sosial. Dengan kata lain, hukum digital memiliki fungsi instrumental untuk mendukung kehidupan yang lebih baik di era digital, dengan mengintegrasikan nilai-nilai etis dan sosial dalam pengaturannya.

Ketiga aspek ini saling terkait dalam membangun dan mengembangkan hukum digital. Ontologi memberikan dasar keberadaan hukum digital, yaitu sebagai respons terhadap kebutuhan pengaturan di era teknologi. Epistemologi menyediakan cara untuk memahami dan mengembangkan hukum digital berdasarkan pengetahuan empiris dan teoritis. Sementara itu, aksiologi memastikan bahwa hukum digital diterapkan untuk mencapai tujuan-tujuan yang bernilai, seperti keadilan,

keamanan, dan kesejahteraan masyarakat. Kombinasi ketiga aspek ini memungkinkan hukum digital untuk tetap relevan, adaptif, dan bermakna dalam menghadapi tantangan era teknologi.

C. Pentingnya Perlindungan Data dalam Era Digital

Kemajuan pesat teknologi informasi membawa dampak signifikan pada berbagai aktivitas masyarakat. Namun, di balik perkembangan teknologi digital yang semakin maju, muncul berbagai tantangan, terutama yang berkaitan dengan perlindungan data pribadi. Salah satu masalah utama adalah adanya celah keamanan pada situs-situs perusahaan maupun instansi pemerintah, yang sering kali dimanfaatkan oleh peretas atau hacker untuk mencuri data pribadi masyarakat.

Hak privasi terhadap data pribadi merupakan salah satu hak mendasar yang berperan penting dalam melindungi martabat manusia dan menjadi landasan bagi berbagai hak asasi manusia lainnya. Menurut Danrivanto Budhijanto, hak privasi sebagai bagian dari hak asasi manusia mencakup perlindungan terhadap hak-hak pribadi atau privat. Perlindungan ini memiliki banyak manfaat, seperti memperkuat nilai-nilai kemanusiaan, mempererat hubungan antara individu dan masyarakat, meningkatkan otonomi pribadi untuk mengontrol dan menentukan kepentingan, serta mendorong toleransi dan menghindari diskriminasi. Selain itu, perlindungan hak privasi juga berfungsi untuk membatasi penyalahgunaan kekuasaan oleh pemerintah.[20]

Perlindungan data pribadi dalam menjamin keamanan privasi masyarakat Indonesia saat ini masih belum optimal. Hal ini tercermin dari banyaknya kasus pelanggaran dan penyalahgunaan data pribadi yang terus terjadi, seiring dengan pesatnya pertumbuhan penggunaan platform digital yang belum diimbangi dengan perlindungan hukum yang memadai. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) baru saja meluncurkan survei bertajuk Penetrasi Internet Indonesia 2024. Riset itu mengungkap kalau warga RI rawan menjadi korban kasus keamanan data digital selama tahun 2024. Kebocoran data pribadi.

[20] Danrivanto Budhijanto, 2010, *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi: Regulasi & Konvergensi*, PT. Refika Aditama, Bandung, hal. 4

Pencurian data pribadi memiliki persentase 20,97 persen, meningkat dari 7,96 persen di tahun 2023.[21]

Banyaknya kasus kebocoran data pribadi yang terjadi menunjukkan bahwa hak privasi warga negara Indonesia sangat rentan terhadap penyalahgunaan, yang dapat menyebabkan kerugian bagi masyarakat. Selain itu, pelanggaran terhadap data pribadi tidak hanya disebabkan oleh kebocoran data semata, tetapi juga oleh pengolahan data pribadi yang dilakukan secara tidak bertanggung jawab.[22]

Di Indonesia, perlindungan data yang buruk telah mengakibatkan peretasan dan kebocoran data yang meluas. Peristiwa hukum seperti ini merupakan suatu bentuk kejahatan di dunia maya, seperti peretasan (hacking) media sosial dan cracking (pembajakan), sehingga mengarah pada pelanggaran data pribadi, pemerasan, hingga terjadinya penipuan online. Perlu diketahui bahwa, transaksi timbul akibat adanya suatu hubungan hukum yang dilindungi oleh hukum baik yang disengaja maupun tidak disengaja.[23]

Perlindungan data pribadi yang bersifat khusus akan dapat memperkokoh posisi dari Indonesia sebagai tempat pusat.berbisnis dan investasi terpercaya dan menciptakan suatu lingkungan yang kondusif untuk pertumbuhan manajemen. investasi yang dipercaya dan dapat menciptakan lingkungan yang baik untuk pertumbuhan manajemen data global pada industri pengolahan data seperti komputasi awan untuk berkembang di Indonesia.[24]

Indonesia saat ini telah memiliki sumber hukum perlindungan data pribadi. Undang-Undang Republik Indonesia Nomor 27 Tahun 2022

---

[21] Dicky Prastya, *Riset: Orang Indonesia Rawan Jadi Korban Penipuan Online dan Kebocoran Data di 2024*, https://www.suara.com/tekno/2024/02/01/093231/riset-orang-indonesia-rawan-jadi-korban-penipuan-online-dan-kebocoran-data-di-2024

[22] Teddy Lesmana, dkk, *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| Vol. 3| No. 2| 2022, hal. 2

[23] Albert Lodewyk Sentosa Siahaan, *Urgensi Perlindungan Data Pribadi Di Platform Marketplace Terhadap Kemajuan Teknologi*, Majalah Hukum Nasional Volume 52 Nomor 2 Tahun 2022, hal. 211

[24] Erlina.Maria Christin Sinaga, *Formulasi.Legislasi Perlindungan.Data Pribadi Dalam Revolusi.Industri* 4.0, Jurnal Rechtsvinding, Vol. 9, No. 2, tahun 2020, hal. 239

Tentang Pelindungan Data Pribadi diundangkan pada 17 Oktober 2022. Pelindungan Data Pribadi merupakan kebutuhan untuk melindungi hak individu di dalam masyarakat sehubungan dengan pemrosesan Data Pribadi baik yang dilakukan secara elektronik dan nonelektronik menggunakan perangkat olah data. Pelindungan yang memadai atas Data Pribadi akan mampu memberikan kepercayaan masyarakat untuk menyediakan Data Pribadi guna berbagai kepentingan masyarakat yang lebih besar tanpa disalahgunakan atau melanggar hak pribadinya.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi menciptakan keseimbangan antara hak individu dan masyarakat yang diwakili kepentingannya oleh negara. Pengaturan tentang Pelindungan Data Pribadi ini akan memberikan kontribusi yang besar terhadap terciptanya ketertiban dan kemajuan dalam masyarakat informasi. Pengaturan Data Pribadi bertujuan antara lain melindungi dan menjamin hak dasar warga negara terkait dengan pelindungan diri pribadi, menjamin masyarakat untuk mendapatkan pelayanan dari Korporasi, Badan Publik, Organisasi Internasional, dan Pemerintah, mendorong pertumbuhan ekonomi digital dan industri teknologi informasi dan komunikasi, dan mendukung peningkatan daya saing industri dalam negeri.

D. Perkembangan Hukum Digital Global

Perkembangan hukum digital global merupakan respons langsung terhadap revolusi teknologi informasi dan komunikasi yang telah mengubah cara manusia berinteraksi, bekerja, dan bertransaksi. Dalam era digital, berbagai aspek kehidupan, seperti perdagangan internasional, privasi data, keamanan siber, dan hak kekayaan intelektual, telah terintegrasi dengan teknologi digital. Hal ini menuntut adanya kerangka hukum yang dapat mengatur aktivitas di dunia maya secara global.

Pada awalnya, hukum digital lebih banyak dikembangkan di tingkat nasional, seperti penerapan Electronic Communications Privacy Act di Amerika Serikat atau Peraturan Perlindungan Data Umum (GDPR) di Uni Eropa. Namun, karena aktivitas digital bersifat lintas negara, maka diperlukan regulasi global untuk menjawab tantangan yang bersifat transnasional, seperti kejahatan siber, perlindungan data lintas

negara, dan transaksi elektronik internasional. Contoh nyata upaya global adalah Konvensi Budapest tentang Kejahatan Siber, yang menjadi standar internasional pertama untuk memerangi kejahatan digital.

Dalam beberapa tahun terakhir, banyak negara mulai memperluas regulasi mereka untuk mencakup isu-isu digital yang spesifik, seperti perlindungan data pribadi dan keamanan jaringan. Di tingkat internasional, organisasi seperti *United Nations Commission on International Trade Law* (UNCITRAL) telah mengembangkan panduan hukum untuk memfasilitasi perdagangan elektronik lintas negara. Sementara itu, organisasi seperti Internet Governance Forum (IGF) menyediakan platform dialog antara pemerintah, sektor swasta, dan masyarakat sipil untuk membahas isu-isu global yang berkaitan dengan internet.

Namun, perkembangan hukum digital global tidak lepas dari tantangan. Salah satu tantangan terbesar adalah adanya kesenjangan regulasi antara negara maju dan negara berkembang. Negara maju cenderung memiliki regulasi yang lebih komprehensif dan infrastruktur digital yang lebih mapan, sementara banyak negara berkembang masih berusaha mengejar ketertinggalan di bidang teknologi dan regulasi. Selain itu, konflik geopolitik juga dapat menghambat upaya untuk menciptakan standar global yang seragam.

Meskipun begitu, ada tren yang menunjukkan peningkatan kolaborasi antarnegara dalam menyusun kerangka hukum digital global. Inisiatif seperti *Asia-Pacific Economic Cooperation* (APEC) *Cross-Border Privacy Rules System* menunjukkan bagaimana kawasan tertentu dapat bekerja sama untuk menciptakan standar perlindungan data yang konsisten. Selain itu, kolaborasi antara sektor publik dan swasta juga menjadi kunci penting dalam menghadapi tantangan hukum digital global.

Dalam era yang semakin terhubung ini, hukum digital global tidak hanya bertujuan untuk mengatur, tetapi juga untuk melindungi dan memfasilitasi aktivitas digital. Kerangka hukum yang kuat dan inklusif dapat menciptakan kepercayaan dalam ekosistem digital, memastikan keamanan dan keadilan, serta mendorong inovasi yang bermanfaat bagi masyarakat global. Ke depannya, hukum digital global akan terus

berkembang untuk menjawab tantangan baru yang dihadirkan oleh kemajuan teknologi, seperti kecerdasan buatan, *blockchain, metaverse* dan *internet of things* (IoT).

E. Referensi

Danuri, Muhamad. 2019. "Perkembangan Dan Transformasi Teknologi Digital." Jurnal Infokam Nomor II Th. XV/September/2019.

Bhattacharya, Amitabh. 2013. *Digital Communication*. New Delhi: McGraw Hill Publication.

Capurro, Rafael. 2017. *Homo Digitalis: Beiträge zur Ontologie, Anthropologie und Ethik der digitalen Technik*. Springer VS, Wiesbaden.

Pribadi, Yopie Indra. "Telaah Kritis Revolusi Digital: Sindrom Ketidaksadaran Pengguna Internet dalam Era Kapitalisme Surveilans." https://disdukcapil.pontianak.go.id/telaah-kritis-revolusi-digital--sindrom-ketidaksadaran-pengguna-internet-dalam-era-kapitalisme-surveilans-ditulis-oleh-yopie-indra-pribadi

Wibowo, Agus. 2023. *Hukum di Era Globalisasi Digital*. Yayasan Prima Agus bekerjasama dengan Universitas Sains & Teknologi Komputer (Universitas STEKOM), Semarang.

Digital Law Ath. "Explore the World of Digital Law." https://digi-dcl.com/digital-law

Radchenko, M. Y., & Gorbunov, V. P. 2000. "Digital Law of the Future." *The Second All-Russian Conference "Law and the Internet: Theory and Practice"*. https://ifap.ru/pi/02/r03.htm

James, Linlay. "Digital Law." https://linleyjames.co.uk/digital-law/#:~:text=Digital%20law%20recognises%20an%20individuals.protect%20themselves%20from%20digital%20exploitation

Inozemtsev, Maxim I. 2021. "Digital Law: The Pursuit of Certainty." *Digital Law Journal*, 2(1), 8–28. https://doi.org/10.38044/2686-9136-2021-2-1-8-28

Goldman, Eric. 2008. "Teaching Cyberlaw." *Saint Louis University Law Journal*, 52(3), 749–764.

Edwards, Lilian, & Waelde, Charlotte (Eds.). 2009. *Law and the Internet*. Bloomsbury Publishing.

Marsden, Christopher T. (Ed.). 2000. *Regulating the Global Information Society* (Vol. 2). Psychology Press.

Li, Zongqi. 2024. "The Evolution of Internet Law in The Digital Age." *International Journal of Education and Humanities*, Vol. 13, No. 2.

Reidenberg, Joel R., & De Hert, Paul (Eds.). 2019. *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Oxford, UK.

Raharjo, Agus. 2002. *Cyber Crime*. Citra Aditya, Bandung.

Lessig, Lawrence. 1999. *Code: And Other Laws of Cyberspace*. New York: Basic Books.

Widodo. 2013. *Hukum Pidana di Bidang Teknologi Informasi (Cybercrime Law): Telaah Teoritik dan Bedah Kasus*. Yogyakarta.

Budhijanto, Danrivanto. 2010. *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi: Regulasi & Konvergensi*. PT Refika Aditama, Bandung.

Prastya, Dicky. 2024. "*Riset: Orang Indonesia Rawan Jadi Korban Penipuan Online dan Kebocoran Data."* https://www.suara.com/tekno/2024/02/01/093231/riset-orang-indonesia-rawan-jadi-korban-penipuan-online-dan-kebocoran-data-di-2024

Lesmana, Teddy, et al. 2022. "*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, Vol. 3, No. 2.

Siahaan, Albert Lodewyk Sentosa. 2022. "*Urgensi Perlindungan Data Pribadi di Platform Marketplace Terhadap Kemajuan Teknologi."* Majalah Hukum Nasional, Volume 52, Nomor 2.

Sinaga, Erlina Maria Christin. 2020. "Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0." *Jurnal Rechtsvinding*, Vol. 9, No. 2.

BAB 2

KONSEP DAN PRINSIP PRIVASI DATA: MENEGAKKAN HAK WARGA NEGARA DI ERA DIGITAL

Dr. Muhammad Alfian Dj, M.H.

Madrasah Muallimin Muhammadiyah Yogyakarta

A. Pengertian Perlindungan Data

Perlindungan data pribadi adalah upaya dilakukan untuk menjaga keamanan dan privasi informasi pribadi seseorang agar tidak disalahgunakan oleh pihak yang tidak berwenang. Data pribadi bisa mencakup berbagai jenis informasi yang dapat mengidentifikasi individu, seperti nama, alamat, nomor telepon, data finansial, data medis, hingga riwayat transaksi. Mengingat pentingnya data ini dalam kehidupan sehari-hari, baik untuk kepentingan pribadi, bisnis, maupun pemerintahan.[25]

Undang undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi menyebutkan Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau non elektronik.[26]

Perlindungan data pribadi bukan hanya mengenai pengamanan fisik dari ancaman luar, tetapi juga terkait dengan cara data tersebut dikumpulkan, diproses, dan dibagikan oleh organisasi atau pihak yang mengumpulkannya. Perlindungan data pribadi ditujukan untuk menjamin hak warga negara atas perlindungan diri pribadi. Dalam dunia yang semakin terhubung di era digital, informasi pribadi seseorang dapat

[25] "Ketahui Berbagai Jenis Data Pribadi Yang Harus Kamu Jaga," *Eraspace*, 2024.

[26] Pemerintah Pusat Indonesia, "Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi" (2022), Pasal 1 ayat 1.

dengan mudah diakses dan disebarluaskan. Tanpa perlindungan yang tepat, data pribadi bisa jatuh ke tangan yang salah dan disalahgunakan.

Perlindungan data pribadi bukan hanya sekadar masalah keamanan teknis, tetapi juga menyangkut hak dasar setiap individu untuk menjaga dan mengontrol informasi pribadi mereka sesuai dengan kehendak mereka. Pasal 1 Undang undang Undang undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi menegaskan Perlindungan data adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data Pribadi guna menjamin hak konstitusi subyek Data Pribadi.[27]

B. Prinsip-prinsip Perlindungan Data Pribadi

1. Esensi Perlindungan Data Diri

Perlindungan hukum merupakan suatu hal yang dilindungi sebagai subyek hukum melalui peraturan perundang-undangan yang berlaku dan dipaksakan pelaksanaannya dengan adanya sanksi yang diberikan. Perlindungan hukum dapat dibedakan menjadi dua, yaitu perlindungan preventif dan represif.[28]

Pentingnya regulasi perlindungan data pribadi semakin terasa seiring dengan berkembangnya teknologi digital yang memungkinkan akses yang sangat cepat terhadap berbagai informasi pribadi. Setiap hari, tiap individu bisa menghasilkan data dalam jumlah besar, baik melalui interaksi di media sosial, transaksi online, hingga penggunaan aplikasi digital.

Perlindungan data pribadi menjadi tugas pemerintah Indonesia untuk dinatanya dengan melahirkan aturan yang menjamin terpenuhinya hak konstitusional seluruh warga negaranya. Kriteria ideal dari instrumen hukum terkait perlindungan data pribadi yakni: 1) berkarakter internasional serta 2) mengandung elemen perekat antara individu dan masyarakat dalam taraf ekonomi.[29]

---

[27] *Ibid*, Pasal 1 ayat 2.

[28] Muchsin, *Perlindungan Dan Kepastian Hukum Bagi Investor Di Indonesia* (Surakarta: Universitas Sebelas Maret, 2003), hlm. 14.

[29] Sinta Dewi Rosadi and Garry Gumelar Pratama, "Urgensi Perlindungan Data

Perlindungan data pribadi tidak hanya berkaitan dengan keamanan informasi, tetapi juga dengan hak asasi manusia. Dalam konteks ini, UUD 1945 Pasal 28 G ayat 1 dan Pasal 28 H ayat 4 menegaskan bahwa setiap orang berhak untuk mendapatkan perlindungan terhadap diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya.[30]

Dalam banyak kasus, kebocoran atau penyalahgunaan data pribadi dapat menimbulkan dampak yang sangat merugikan, seperti pencurian identitas, penipuan finansial, atau bahkan manipulasi informasi. Regulasi yang memadai akan memberikan rasa aman kepada individu bahwa data pribadi mereka akan diproses dan digunakan secara sah, transparan, dan bertanggung jawab.

Perlindungan data pribadi memiliki dampak positif terhadap keberlanjutan dan integritas sistem hukum itu sendiri. Negara yang memiliki regulasi perlindungan data pribadi yang kuat akan menunjukkan komitmen untuk menegakkan hak asasi manusia dan menjaga keseimbangan antara kemajuan teknologi dan hak privasi individu. Regulasi yang memadai juga dapat mencegah eksploitasi data pribadi yang merugikan banyak pihak, baik individu, perusahaan, maupun masyarakat luas.

2. Kebocoran data Pribadi

Kebocoran data pribadi adalah masalah yang semakin meresahkan di era digital, dan frekuensinya terus meningkat dalam beberapa tahun terakhir. Sepanjang Januari hingga September 2022, tercatat sudah tujuh kebocoran data yang berskala besar, yang melibatkan berbagai sektor penting, mulai dari lembaga keuangan, rumah sakit, hingga perusahaan besar. Misalnya, pada awal Januari 2022.

Kebocoran data besar menimpa Bank Indonesia, di mana 200 komputer terinfeksi peretas dan menyebabkan 52 ribu dokumen nasabah terbuka untuk umum. Kebocoran data ini bukan hanya

---

Privasi Dalam Era Ekonomi Digital Di Indonesia," *Veritas et Justitia* 4, no. 1 (2018): 88–110, https://doi.org/http://doi.org/10.25123/vej.2916.

[30] Undang undang dasar 1945

merugikan nasabah yang datanya bocor, tetapi juga mengganggu kepercayaan publik terhadap sistem keamanan data yang ada.[31]

Pada bulan yang sama, sebuah rumah sakit mengalami kebocoran data sebesar 720 GB yang berisi informasi sensitif seperti nama pasien, foto, hasil tes COVID-19, hingga hasil pindai X-ray.[32] Kebocoran data di sektor kesehatan ini sangat berbahaya, karena data medis adalah salah satu informasi paling sensitif yang dimiliki seseorang. Pengungkapan data medis tanpa izin dapat mengakibatkan dampak negatif, baik bagi pasien yang datanya bocor, maupun bagi institusi yang seharusnya menjaga kerahasiaan informasi tersebut.

Di bulan Agustus 2022, kebocoran data besar lainnya terjadi dengan bocornya data 21.000 perusahaan di Indonesia, termasuk laporan keuangan dan dokumen-dokumen penting lainnya. Pada bulan yang sama, 26,7 juta data pelanggan IndiHome juga bocor ke publik.

Peristiwa kebocoran data yang semakin sering terjadi tidak hanya melibatkan sektor swasta, tetapi juga instansi pemerintah. Salah satu yang paling menggemparkan adalah kebocoran data yang dilakukan oleh peretas bernama Bjorka. Pada tahun 2022, Bjorka mengaku memiliki 1,3 miliar data hasil registrasi SIM Card dan 105 juta data penduduk yang diperoleh dari Komisi Pemilihan Umum (KPU). Tidak hanya itu, Bjorka juga mengklaim telah mengakses dokumen rahasia milik Badan Intelijen Negara (BIN) dan mengancam untuk membocorkan data MyPertamina serta dokumen rahasia Presiden RI, Joko Widodo. Kejadian ini menunjukkan betapa rentannya data yang dimiliki oleh negara, dan bagaimana kebocoran data ini bisa menimbulkan ancaman serius terhadap stabilitas nasional. [33]

---

[31] Moh Khory Alfarizi, "Pakar Jelaskan Dampak Kebocoran Data Milik Bank Indonesia," *Tempo.Com*, 2022.

[32] Desy Setyowati, "Ahli IT Ungkap Bahaya Jika Benar Jutaan Data Pasien Bocor," *Katadata.Co.Id*, 2022.

[33] "10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-Ramai Bantah Baca Artikel CNN Indonesia '10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-Ramai Bantah' Selengkapnya Di Sini: Https://Www.Cnnindonesia.Com/Teknologi/20221230125430-192-894094/10-

Kejadian-kejadian tersebut memperlihatkan pentingnya keberadaan regulasi yang tegas untuk melindungi data pribadi, terutama data sensitif yang terkait dengan identitas dan kesehatan. Tanpa adanya aturan yang jelas, pihak yang tidak bertanggung jawab akan dengan mudah memanfaatkan data pribadi untuk kepentingan pribadi atau kelompok tertentu.

Perlindungan data pribadi yang baik tidak hanya melindungi individu dari potensi kerugian atau ancaman keamanan, tetapi juga mencegah penyalahgunaan data oleh pihak-pihak yang tidak bertanggung jawab. Negara harus hadir untuk memastikan bahwa data pribadi yang dimiliki oleh warganya diperlakukan dengan bijak dan aman, serta tidak disalahgunakan oleh siapapun

Kebocoran data yang melibatkan lembaga pemerintah dan perusahaan besar menunjukkan bahwa upaya perlindungan data selama ini masih belum cukup efektif. Keamanan data harus menjadi prioritas utama bagi seluruh pihak yang terlibat, baik itu pemerintah, perusahaan, maupun individu.

Kehadiran negara dalam menjamin perlindungan data pribadi menjadi mutlak diperlukan. Negara harus menjadi fasilitator yang memastikan bahwa data pribadi setiap warganya dilindungi dengan baik, melalui regulasi yang jelas dan pengawasan yang ketat. Tanpa perlindungan yang memadai, kebocoran data akan terus menjadi ancaman serius yang dapat merusak kehidupan pribadi, sosial, dan ekonomi individu.

Keamanan data pribadi merupakan tanggung jawab bersama antara negara, sektor swasta, dan individu. Negara harus hadir dengan kebijakan dan regulasi yang tegas, perusahaan harus memastikan bahwa data konsumen dilindungi dengan baik, dan individu harus lebih sadar akan pentingnya menjaga privasi data mereka. Dengan langkah-langkah tersebut, diharapkan kebocoran data dapat diminimalkan dan kepercayaan masyarakat terhadap penggunaan teknologi digital dapat terus berkembang.

Kasus-," *CNN Indonesia*, 2022.

C. Privasi data Versus Keamanan Data

Perbedaan antara privasi data dan keamanan data seringkali membingungkan karena keduanya saling terkait, namun memiliki fokus yang berbeda dalam hal perlindungan data pribadi. Keamanan data mengacu pada serangkaian langkah, protokol, dan teknologi yang diterapkan untuk melindungi data dari ancaman eksternal, seperti pencurian, perusakan, atau akses yang tidak sah.

Keamanan bertujuan untuk memastikan kerahasiaan, integritas, dan ketersediaan data dalam setiap tahap siklus hidup data, mulai dari pengumpulan, pemrosesan, hingga penyimpanan dan penghapusan. Dengan adanya pengamanan yang baik, organisasi dapat mengurangi risiko pelanggaran data, serangan siber, dan ancaman lainnya yang dapat merugikan reputasi dan integritas data.

Tiga tujuan utama dari keamanan data adalah pertama, kerahasiaan yang memastikan bahwa hanya pihak yang berwenang yang dapat mengakses data sensitif. Kedua, integritas, yang bertujuan untuk menjaga data tetap akurat dan konsisten, serta mencegah perubahan yang tidak sah. Ketiga, ketersediaan, yang menjamin bahwa data dapat diakses oleh pihak yang sah kapan saja diperlukan. Pengamanan ini melibatkan berbagai metode teknis seperti enkripsi data, otentikasi dua faktor, dan firewalls, yang semuanya berfungsi untuk menjaga data dari ancaman yang datang dari luar organisasi.[34]

Privasi data lebih menekankan pada hak individu untuk mengontrol bagaimana informasi pribadi mereka dikumpulkan, digunakan, dibagikan, dan disimpan. Ini lebih berfokus pada aspek etika dan hukum dalam penanganan data pribadi, sehingga individu memiliki otonomi atas informasi yang mereka miliki. Privasi data mengatur bagaimana perusahaan atau organisasi dapat mengakses, menggunakan, dan mengungkapkan informasi pribadi yang dikumpulkan dari individu. Privasi data bertujuan untuk memastikan bahwa data tersebut hanya digunakan untuk tujuan yang sah dan dengan izin yang jelas dari individu

[34] Security Lit Limited, "Apa Tiga Tujuan Keamanan Siber?," Medium, 2023, https://securitylit.medium.com/what-are-the-three-goals-of-cybersecurity-6ec5499fe61.

yang bersangkutan.

Peraturan privasi data seringkali melibatkan aspek yang berkaitan dengan pengumpulan persetujuan dari individu. Sebagai contoh, organisasi harus mendapatkan izin yang tegas dari individu sebelum mengumpulkan dan memproses data pribadi mereka. Hal ini tercermin dalam peraturan seperti General Data Protection Regulation (GDPR) yang diberlakukan di Eropa atau California Consumer Privacy Act (CCPA) di Amerika Serikat. Kedua peraturan ini menetapkan bahwa data pribadi hanya dapat digunakan untuk tujuan yang jelas dan terbatas, serta memastikan bahwa individu memiliki hak untuk mengetahui bagaimana data mereka diproses, serta hak untuk mengoreksi atau menghapus data pribadi mereka jika diinginkan.[35]

Transparansi adalah elemen penting dalam privasi data. Organisasi harus dengan jelas menginformasikan kepada individu mengenai data apa saja yang akan dikumpulkan, bagaimana data tersebut akan digunakan, dan apakah data tersebut akan dijual atau dibagikan kepada pihak ketiga. Transparansi ini sangat penting untuk membangun kepercayaan antara organisasi dan konsumen. Tanpa transparansi yang memadai, individu mungkin merasa data pribadi mereka digunakan secara tidak adil atau tidak sesuai dengan harapan mereka.

Privasi data juga mengharuskan organisasi untuk mematuhi prinsip batasan tujuan. Artinya, data pribadi yang dikumpulkan harus digunakan hanya untuk tujuan yang spesifik dan dinyatakan sejak awal. Misalnya, jika data pribadi dikumpulkan untuk tujuan tertentu, seperti untuk keperluan pemasaran, organisasi tidak boleh menggunakannya untuk tujuan lain tanpa persetujuan lebih lanjut dari individu tersebut. Prinsip ini membantu mencegah penyalahgunaan data pribadi dan memastikan bahwa data hanya diproses sesuai dengan apa yang telah disetujui.

Peraturan terkait privasi data dan keamanan data seringkali berjalan beriringan, namun keduanya memiliki fokus yang berbeda. Keamanan data lebih menitikberatkan pada perlindungan terhadap ancaman yang dapat merusak data, sementara privasi data berkaitan

[35] "Apa Itu GDPR?," IBM, 2018.

dengan bagaimana data tersebut diperlakukan dan dibagikan oleh organisasi. Meski begitu, keduanya memiliki tujuan yang sama, yaitu untuk melindungi hak individu dan memastikan bahwa data pribadi tidak jatuh ke tangan yang salah, baik itu karena tindakan pihak ketiga yang tidak sah maupun karena penyalahgunaan oleh pihak yang mengelola data tersebut.

Pada konteks regulasi global, banyak negara atau wilayah memiliki peraturan yang menggabungkan kedua konsep ini untuk memastikan bahwa data pribadi individu terlindungi dengan cara yang sah dan efektif. Sebagai contoh, GDPR di Eropa tidak hanya mengatur bagaimana data pribadi harus diamankan, tetapi juga bagaimana data tersebut harus dikelola dan dibagikan oleh perusahaan. Organisasi yang melanggar ketentuan privasi dan keamanan ini dapat dikenakan denda yang besar. Dengan demikian, meskipun privasi dan keamanan data memiliki pendekatan yang berbeda, keduanya harus berjalan seiring untuk memastikan perlindungan maksimal terhadap data pribadi dalam era digital ini.

Secara keseluruhan, perbedaan antara privasi data dan keamanan data terletak pada fokus mereka: keamanan data berfokus pada perlindungan fisik data, sedangkan privasi data berfokus pada hak individu dan pengelolaan data pribadi secara sah. Meski demikian, keduanya saling melengkapi dan sangat diperlukan untuk memberikan perlindungan yang maksimal bagi data pribadi, baik itu dalam konteks individu, organisasi, maupun dalam lingkup hukum dan regulasi yang berlaku.

D. Perlindungan Data Merupakan Hak Asasi Manusia

Perlindungan data pribadi berhubungan dengan konsep privasi. Konsep privasi adalah gagasan untuk menjaga integritas dan martabat pribadi. Hak privasi merupakan kemampuan individu untuk menentukan siapa yang memegang informasi tentang mereka dan bagaimana informasi tersebut digunakan.[36]

[36] Wahyudi Djafar and Asep Komarudin, *Perlindungan Hak Atas Privasi Di Internet- Beberapa Penjelasan Kunci* (Jakarta: ELSAM, 2014), hlm. 2.

Perlindungan data pribadi sebagai hak asasi manusia telah menjadi isu yang semakin penting di seluruh dunia, terutama dalam konteks kemajuan teknologi digital yang pesat. Seiring dengan penggunaan telepon seluler, internet, dan platform digital lainnya, informasi pribadi yang dulu dianggap hanya milik individu kini sering kali tersebar luas di dunia maya. Setiap orang memiliki hak untuk menjaga privasinya, yang mencakup kendali penuh atas data pribadi mereka. Dalam hal ini, perlindungan data pribadi menjadi bagian integral dari hak asasi manusia, karena data pribadi adalah informasi yang dapat memengaruhi kehidupan individu, baik dari segi pribadi, sosial, maupun ekonomi.

Hak Privasi merupakan salah satu hak yang melekat pada diri setiap orang. Hak Privasi merupakan martabat setiap orang yang harus dilindungi. Data pribadi adalah data yang berkenaan dengan ciri seseorang, nama, umur, jenis kelmin, pendidikan, pekerjaan, alamat, dan kedudukan dalam keluarga.[37]

Allan Westin menyatakan privasi pribadi adalah hak individu, kelompok, atau lembaga untuk memutuskan apakah informasi tentang mereka akan dikomunikasikan atau dibagikan kepada pihak lain. Definisi ini, yang dikenal sebagai *information privacy*, menekankan pentingnya kontrol atas data pribadi, sehingga individu dapat menentukan bagaimana data mereka digunakan[38]. Perlindungan data pribadi menjadi jaminan bahwa informasi pribadi tidak akan diproses tanpa izin atau disalahgunakan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, hak untuk mengontrol data pribadi juga mencakup hak untuk menolak pengumpulan atau penggunaan data oleh pihak ketiga.

Perlindungan data pribadi telah diakui sebagai hak asasi manusia yang fundamental oleh banyak negara. Pengumpulan dan penyebarluasan data pribadi merupakan pelanggaran terhadap privasi. Konsep ini mencakup hak individu untuk mendapatkan pengamanan

---

[37] Dararida Fandra Fandra Mahira, Emilda Yofita, and Lisa Nur Azizah, "Consumer Protection System (CPS): Sistem Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept," *Legislatif* 3, no. 2 (2020).

[38] Menurut Alan Westin: Privacy is the claim of individuals, group or institution to determine for themselves when, how, and to what extent information about them is communicated to others dalam, Allan Westin, Alan F. Westin, Privacy and Freedom, London, 1967, hlm. 7

terhadap data mereka serta untuk memperoleh pembenaran atau perbaikan jika data tersebut disalahgunakan. Beberapa negara bahkan mengakui perlindungan data sebagai hak konstitusional dalam bentuk *habeas data*, yang memberikan perlindungan hukum kepada individu atas hak untuk mengakses, mengoreksi, dan melindungi data pribadi mereka.[39]

Negara-negara seperti Albania, Armenia, Filipina, Timor Leste, Kolombia, dan Argentina, meskipun memiliki sejarah dan budaya yang berbeda, telah mengakui peran perlindungan data sebagai bagian dari proses demokrasi dan hak individu untuk menjaga privasi mereka. Data pribadi merupakan suatu aset atau komoditas bernilai ekonomi tinggi.[40]

Sebagai contoh, negara-negara yang memiliki hak habeas data memberikan individu hak untuk mengajukan tuntutan atau memperoleh perbaikan jika data pribadi mereka disalahgunakan, yang mempertegas pentingnya regulasi perlindungan data dalam sistem hukum negara. Pengakuan terhadap hak perlindungan data pribadi ini semakin diperkuat dengan adopsi undang-undang perlindungan data pribadi di berbagai negara.

Regulasi ini tidak hanya bertujuan untuk melindungi informasi pribadi, tetapi juga untuk menjamin bahwa data tersebut tidak akan dipergunakan untuk tujuan yang merugikan individu, seperti dalam kasus penyalahgunaan data untuk penipuan, pencurian identitas, atau eksploitasi ekonomi.

Masalah terkait penyalahgunaan data pribadi semakin sering muncul seiring dengan meningkatnya jumlah pengguna teknologi digital.[41] Sejumlah kasus kebocoran data pribadi, terutama yang melibatkan individu atau kelompok rentan, semakin menguatkan wacana perlunya peraturan hukum yang jelas dan tegas mengenai perlindungan

---

[39] Ananthia Ayu D, Titis Anindyajati, and Abdul Ghoffar, "Perlindungan Hak Privasi Atas Data Diri Di Era Ekonomi Digital" (Jakarta, 2019).

[40] Edmon Makarim, *Kompilasi Hukum Telematika* (Jakarta: PT. Raja Grafindo Perkasa, 2003), hlm. 3.

[41] Ervina Chintia et al., "Kasus Kejahatan Siber Yang Paling Banyak Terjadi Di Indonesia Dan Penanganannya," *JJIEET (Journal Information Engineering and Educational Technology)* 2, no. 2 (2018).

data pribadi. Penyalahgunaan data pribadi oleh pihak yang tidak berwenang tidak hanya melanggar privasi, tetapi juga dapat menimbulkan kerugian besar bagi individu, seperti dalam kasus penipuan atau tindak kriminal yang menggunakan data pribadi sebagai alat. Dalam kasus yang lebih serius, penyalahgunaan data pribadi dapat merusak reputasi seseorang, merugikan keuangan, bahkan merusak hubungan sosial.

Pentingnya perlindungan data pribadi juga berhubungan erat dengan peningkatan kesadaran global mengenai pentingnya hak privasi di era digital. Perlindungan data pribadi tidak hanya berbicara tentang menghindari kebocoran informasi, tetapi juga tentang memberikan hak kepada individu untuk mengontrol bagaimana dan siapa yang dapat mengakses data mereka.

Seiring dengan meningkatnya ketergantungan terhadap internet, media sosial, dan aplikasi digital, data pribadi menjadi komoditas yang sangat berharga dan sering dipergunakan untuk tujuan bisnis, pemasaran, atau bahkan pengawasan. Tanpa regulasi yang jelas, data pribadi dapat dengan mudah jatuh ke tangan yang salah dan disalahgunakan untuk kepentingan yang tidak sah.

Sebagai aset atau komoditas yang bernilai tinggi, data pribadi harus dilindungi dengan berbagai mekanisme yang memastikan bahwa informasi tersebut hanya digunakan untuk tujuan yang sah dan transparan. Oleh karena itu, regulasi yang ketat sangat diperlukan untuk mengatur pengumpulan, penggunaan, dan penyebarluasan data pribadi. Undang-undang perlindungan data pribadi, seperti General Data Protection Regulation (GDPR) di Uni Eropa dan Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia, bertujuan untuk memberikan hak yang jelas kepada individu atas data pribadi mereka. Hal ini mencakup kewajiban bagi perusahaan atau organisasi untuk memperoleh persetujuan yang jelas sebelum mengumpulkan data pribadi dan memberikan individu hak untuk mengakses, mengoreksi, atau menghapus data mereka.

Di Indonesia, Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan pada 2022 memberikan dasar hukum bagi

perlindungan data pribadi sebagai hak asasi manusia. UU ini memberikan masyarakat Indonesia kejelasan dan keamanan terkait pengelolaan data pribadi mereka, dengan ketentuan yang mengharuskan organisasi atau perusahaan yang mengumpulkan data untuk mematuhi prinsip perlindungan data pribadi yang ketat. UU PDP ini bertujuan untuk mencegah penyalahgunaan data pribadi yang dapat merugikan individu, serta menjamin transparansi dan akuntabilitas dalam pengelolaan data pribadi oleh pihak ketiga.

Selain perlindungan melalui regulasi, penting bagi masyarakat untuk memiliki pemahaman yang baik mengenai hak atas data pribadi mereka. Pendidikan mengenai privasi dan perlindungan data pribadi perlu diberikan sejak dini agar individu dapat mengerti betul hak-hak mereka dalam dunia digital. Dengan meningkatnya pemahaman ini, diharapkan masyarakat dapat lebih sadar dalam melindungi data pribadi mereka sendiri dan menghindari berbagai potensi ancaman yang mungkin muncul akibat pengumpulan atau penyebarluasan data secara tidak sah.

Pentingnya perlindungan data pribadi sebagai hak asasi manusia juga menjadi sangat relevan dalam konteks globalisasi dan integrasi teknologi yang terus berkembang. Masyarakat digital saat ini tidak hanya berinteraksi dengan individu atau perusahaan dalam negeri, tetapi juga dengan entitas internasional.[42] Dengan adanya standar perlindungan data pribadi yang kuat, negara-negara dapat memastikan bahwa data yang dipertukarkan antar negara tetap terjaga dengan baik dan tidak disalahgunakan. Oleh karena itu, pengakuan terhadap perlindungan data pribadi sebagai hak asasi manusia mendukung terciptanya ekosistem yang aman dan saling menghormati dalam era digital global.

Dengan adanya perlindungan data pribadi yang kuat dan diakui sebagai hak asasi manusia, individu tidak hanya memiliki kendali atas informasi pribadi mereka, tetapi juga dapat merasakan rasa aman dalam berinteraksi dengan dunia digital. Negara-negara yang telah mengadopsi perlindungan data pribadi dalam konstitusi mereka menunjukkan komitmen untuk menjaga hak-hak warga negaranya di dunia digital.

[42] Aptika, "Pentingnya Pelindungan Data Pribadi Di Era Digital," *Kominfo*, 2021.

Oleh karena itu, penting bagi negara-negara di seluruh dunia, termasuk Indonesia, untuk terus memperkuat regulasi perlindungan data pribadi, guna memastikan bahwa hak atas privasi tetap terjaga di tengah pesatnya perkembangan teknologi.

E. Regulasi dan Kebijakan Privasi Data

1. Peraturan Privasi Data negara Asean

Pengaturan hukum perlindungan data pribadi merupakan aspek yang semakin penting dalam dunia yang semakin terhubung secara digital. Di tingkat global, banyak negara yang telah menyadari pentingnya untuk mengatur penggunaan data pribadi agar tidak disalahgunakan, dan negara-negara di kawasan Asia Tenggara (ASEAN) pun tidak terkecuali. Perlindungan data pribadi memiliki tujuan untuk menjaga hak privasi individu, memberikan kendali kepada setiap orang atas data pribadi mereka, serta mencegah penyalahgunaan informasi pribadi yang dapat merugikan. Pengaturan ini sangat diperlukan dalam rangka menghormati kehidupan pribadi seseorang (the liberty to live in private), sebagaimana yang ditekankan dalam prinsip perlindungan data pribadi.

Beberapa negara di ASEAN, seperti Singapura, Malaysia, Thailand, dan Filipina, telah terlebih dahulu mengesahkan peraturan atau undang-undang yang mengatur perlindungan data pribadi. Singapura misalnya, melalui Personal Data Protection Act (PDPA) yang disahkan pada tahun 2012, telah menjadikan negara ini sebagai pelopor di kawasan ASEAN dalam hal pengaturan perlindungan data pribadi. PDPA Singapura dirancang untuk memberikan perlindungan terhadap data pribadi individu, dan memberikan sanksi yang tegas bagi perusahaan yang melanggar ketentuan terkait pengelolaan data pribadi. Dalam hal ini, Singapura menempatkan pengelolaan data pribadi di bawah pengawasan Personal Data Protection Commission (PDPC).

Melalui Personal Data Protection Act 2010, Malaysia membentuk Komite Penasihat Perlindungan Data Pribadi yang bertugas menerima laporan jika terjadi penyalahgunaan dan

pemindah-tanganan data pribadi secara melawan hukum.[43] Undang-undang ini mengatur tentang pengumpulan, penyimpanan, pemrosesan, dan pengungkapan data pribadi oleh organisasi di Malaysia.

Aturan dari Personal Data Protection Act 2010, ini bertujuan untuk mengatur pengolahan data pribadi oleh pengguna data dalam konteks transaksi komersial, dengan maksud menjaga kepentingan subjek data itu. Hal ini dicapai dengan memastikan bahwa persetujuan dari subjek data diperoleh sebelum pengolahan data pribadi serta memberikan data dengan subjek hak untuk mengakses, benar dan juga kontrol pengolahan data pribadi mereka.[44]

Thailand, pada tahun 2019, mengesahkan Personal Data Protection Act (PDPA) yang lebih komprehensif. PDPA Thailand mengatur pengelolaan data pribadi oleh pihak yang memproses data, termasuk perusahaan, lembaga pemerintah, dan individu. Undang-undang ini mengadopsi prinsip-prinsip dasar perlindungan data pribadi yang sejalan dengan standar internasional, seperti yang ada dalam General Data Protection Regulation (GDPR) di Uni Eropa. PDPA Thailand juga memberikan hak kepada individu untuk meminta penghapusan data pribadi mereka dan memberikan transparansi dalam pengumpulan data pribadi, serta menetapkan sanksi bagi yang melanggar.[45]

Tujuan utama dari pengaturan hukum perlindungan data pribadi di negara-negara ASEAN adalah untuk memberikan alternatif perlindungan hak privasi manusia yang semakin penting di era digital.[46] Dengan perkembangan teknologi yang pesat, pengumpulan dan penggunaan data pribadi semakin meluas. Oleh karena itu, perlindungan hukum yang jelas dan tegas sangat diperlukan untuk

---

[43] MS Rizal, "Perbandingan Perlindungan Data Pribadi Indonesia Dan Malysia," *Jurnal Cakrawala Hukum*, 2019, https://doi.org/DOI: https://doi.org/10.26905/idjch.v10i2.3349. 218-227.

[44] *Ibid.*

[45] Robb Hiscock, "Panduan Utama Untuk Kepatuhan Terhadap PDPA Thailand," *Onetrust*, 2022.

[46] Kadek Rima Anggen Suari, "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia," *Jurnal Analisis Hukum* 1 (6AD).

memastikan bahwa data pribadi individu tidak jatuh ke tangan yang salah, dan bahwa individu memiliki kendali penuh atas informasi pribadinya. Regulasi ini berfungsi sebagai mekanisme perlindungan terhadap kebocoran data dan penyalahgunaan informasi pribadi yang dapat merugikan individu.

Pada 17 Oktober 2022, Indonesia mengesahkan Undang-Undang Perlindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022, yang menjadi tonggak penting dalam sejarah perlindungan data pribadi di Indonesia. UU PDP ini hadir untuk memberikan perlindungan hukum bagi hak asasi manusia, khususnya dalam melindungi data pribadi masyarakat. Dengan pengesahan undang-undang ini, Indonesia mengikuti jejak negara-negara ASEAN lainnya yang telah terlebih dahulu memiliki regulasi perlindungan data pribadi yang komprehensif. UU PDP ini bertujuan untuk memberikan keamanan atas data pribadi dan meningkatkan kesadaran masyarakat tentang pentingnya menghargai dan melindungi data pribadi.

Dalam UU PDP Indonesia, pasal-pasal yang tercantum mengatur berbagai hal terkait pengumpulan, pemrosesan, penyimpanan, serta pengungkapan data pribadi. Salah satu aspek penting dari UU PDP adalah hak individu untuk mengakses, memperbaiki, atau bahkan menghapus data pribadi yang dimiliki oleh organisasi atau pihak lain. UU ini juga mengatur kewajiban pihak yang mengelola data pribadi, baik itu perusahaan, lembaga pemerintah, maupun individu, untuk memastikan bahwa data pribadi diproses dengan cara yang sah dan transparan. Penerapan regulasi ini juga melibatkan pembentukan Badan Perlindungan Data Pribadi (BPDP) yang berfungsi sebagai lembaga pengawas dan penegak hukum dalam implementasi UU PDP.

Dengan hadirnya UU PDP, Indonesia diharapkan dapat lebih aktif dalam kerjasama internasional terkait perlindungan data pribadi, baik dengan negara-negara ASEAN maupun dengan negara-negara di luar kawasan. Pengaturan yang serupa di ASEAN, seperti di Singapura, Malaysia, Thailand, dan Filipina, memberikan standar yang dapat dijadikan acuan untuk Indonesia dalam melaksanakan kebijakan perlindungan data pribadi yang lebih baik. Pengawasan

yang ketat terhadap pengelolaan data pribadi dan pemberian sanksi bagi yang melanggar akan menciptakan ruang yang lebih aman bagi masyarakat untuk berinteraksi di dunia digital, sekaligus menjaga agar hak-hak privasi mereka tetap dihormati.

Secara keseluruhan, regulasi perlindungan data pribadi di ASEAN, termasuk Indonesia, merupakan langkah penting dalam menjamin hak privasi setiap individu di dunia yang semakin terhubung digital. Negara-negara ASEAN, melalui regulasi yang telah diterapkan, berkomitmen untuk menjaga keamanan dan integritas data pribadi warganya, serta memastikan bahwa data pribadi yang beredar di ruang digital tetap terlindungi dengan baik.

2. Regulasi Perlindungan Data di Indonesia

Pada awalnya Indonesia tidak memiliki aturan khusus yang mengatur perlindungan data pribadi. Perlindungan data pribadi hanya diatur secara umum pada beberapa peraturan perundang-undangan yang terpisah. Perjalanan panjang Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) untuk akhirnya disahkan menjadi Undang-Undang (UU) merupakan sebuah langkah penting dalam upaya negara Indonesia untuk melindungi hak privasi warganya di era digital. Sejak pertama kali diinisiasi pada tahun 2016.

Proses penyusunan RUU ini dimulai dengan pembahasan 72 pasal yang dirancang untuk mengatur perlindungan data pribadi di Indonesia. Kemenkominfo mengklaim bahwa mereka bertanggung jawab penuh atas penyusunan draf RUU PDP, dengan tujuan utama untuk mengatasi permasalahan terkait perlindungan data pribadi yang kian marak seiring dengan perkembangan teknologi informasi. Salah satu dasar dari pembahasan ini adalah untuk menyelaraskan peraturan yang ada dengan perkembangan kebutuhan akan perlindungan data pribadi di tingkat global. Isu-isu seperti kebocoran data pribadi dan penyalahgunaan data menjadi latar belakang yang mendorong disusunnya regulasi ini.

Pada tahun 2019, RUU PDP menjadi prioritas untuk dibahas di DPR berdasarkan Keputusan DPR RI Nomor 19/DPR RI/I/2018-2019 tentang Program Legislasi Nasional RUU Prioritas Tahun 2019.

Hal ini menandakan komitmen pemerintah dan DPR dalam mempercepat proses legislasi untuk melindungi data pribadi masyarakat. Setelah melalui berbagai proses harmonisasi antar kementerian dan lembaga terkait, akhirnya pada 2020, RUU PDP diajukan kepada DPR untuk dibahas lebih lanjut. Di tahun ini, RUU PDP mengalami dua tahap utama, yakni Pendahuluan dan Pembicaraan Tingkat I.

Proses Pendahuluan dilaksanakan pada Januari hingga Februari 2020, yang mana pada tahap ini Presiden menugaskan Menteri Komunikasi dan Informatika (Menkominfo), Menteri Dalam Negeri (Mendagri), dan Menteri Hukum dan HAM (Menkumham) untuk melakukan pembahasan lebih lanjut dengan DPR RI. Pembahasan di tahap ini bertujuan untuk menyusun dasar dan arah pembahasan yang jelas terkait substansi dari RUU PDP. Proses ini juga bertujuan untuk memfasilitasi pertemuan antara pemerintah dan anggota DPR agar pemahaman tentang urgensi RUU PDP dapat sejalan.

Setelah tahapan Pendahuluan, RUU PDP memasuki Pembicaraan Tingkat I pada periode Februari 2020 hingga Mei 2022. Pada tahap ini, Komisi I DPR RI bersama dengan Tim Panitia Kerja (Panja) Pemerintah melakukan serangkaian rapat pembahasan terkait substansi penting dalam RUU tersebut. Tim Panja ini terdiri dari perwakilan berbagai kementerian dan lembaga, yang bekerja keras untuk mengembangkan formulasi yang tepat dan efektif dalam menyusun pasal-pasal yang mengatur perlindungan data pribadi. Pembahasan ini juga melibatkan kajian mendalam untuk memastikan bahwa aturan yang akan dihasilkan mampu mengatasi tantangan yang ada dalam perlindungan data pribadi.

Salah satu fokus utama dalam pembahasan ini adalah mengenai kelembagaan penyelenggaraan perlindungan data pribadi. Pembentukan lembaga yang independen dan memiliki kewenangan untuk mengawasi implementasi perlindungan data pribadi menjadi sangat penting. Hal ini juga menjadi salah satu isu krusial yang dibahas selama pembicaraan tingkat I. Tim Panja Pemerintah, yang dipimpin oleh Direktur Jenderal Aplikasi Informatika Kemkominfo, bersama dengan pejabat terkait dari kementerian dan lembaga

lainnya, berusaha mencari formulasi yang terbaik untuk memastikan UU PDP dapat berjalan efektif di lapangan.

Pada 20 September 2022, RUU PDP memasuki tahap yang sangat penting, yaitu Pembahasan Tingkat II oleh DPR. Pembahasan ini menghasilkan keputusan besar yang mengesahkan RUU menjadi Undang-Undang Perlindungan Data Pribadi (UU PDP) dengan isi 16 bab dan 76 pasal.[47] Proses panjang ini mencerminkan betapa seriusnya negara dalam mengatur perlindungan data pribadi warganya, sekaligus mengatur tata kelola penggunaan data oleh sektor industri dan lembaga negara untuk melindungi keamanan serta kepentingan masyarakat secara keseluruhan.

UU PDP ini hadir untuk memberikan perlindungan hukum terhadap data pribadi masyarakat Indonesia. Kehadirannya di tengah perkembangan teknologi informasi yang semakin pesat bertujuan untuk memastikan bahwa setiap individu memiliki kendali atas data pribadinya dan tidak mudah menjadi korban penyalahgunaan data.

Pengesahan UU PDP juga memberikan harapan bagi peningkatan kepercayaan publik terhadap penggunaan teknologi digital. Selama ini, kebocoran data pribadi dan peretasan sering kali menjadi masalah besar yang mengancam privasi individu. UU PDP telah membuka ruang bagi penguatan sektor pengawasan terhadap pelaksanaan perlindungan data, sehingga data pribadi warga negara dapat lebih terlindungi dari ancaman yang semakin kompleks.

F. Harapan Perlindungan Data

Harapan terhadap perlindungan dan keamanan data pribadi di Indonesia sangat besar, mengingat data pribadi kini menjadi salah satu aset paling berharga di dunia digital. Di era *big data* dan teknologi digital, data pribadi sering kali menjadi target utama dalam berbagai aktivitas, baik itu untuk kepentingan bisnis, politik, maupun kejahatan siber.[48] Oleh karena itu, keberadaan regulasi perlindungan data pribadi yang jelas

[47] Aptika, "Rapat Paripurna DPR Sahkan RUU PDP," *Kominfo*, 2022.

[48] Winarsih Winarsih and Irwansyah, "Proteksi Privasi Big Data Dalam Media Sosial," *Audiens Jurnal: Jurnal Ilmu Komunikasi* 3, no. 1 (2020).

dan tegas, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP), sangat diharapkan dapat menjadi angin segar bagi masyarakat Indonesia. Dengan perlindungan yang memadai, setiap warga negara berhak merasa aman dan nyaman dalam menjalani kehidupan digital mereka tanpa takut data pribadi mereka disalahgunakan.

Keamanan data pribadi yang baik diharapkan dapat menjamin hak setiap individu untuk memiliki kendali penuh atas informasi pribadi mereka. Ini termasuk hak untuk mengetahui bagaimana data mereka digunakan, untuk tujuan apa data mereka diproses, dan kepada siapa data tersebut dibagikan.

Perlindungan data pribadi diharapkan dapat menciptakan kesadaran yang lebih tinggi di kalangan masyarakat Indonesia mengenai pentingnya menjaga dan melindungi data pribadi mereka.[49] Masyarakat harus diberdayakan untuk lebih memahami hak-hak mereka dalam hal pengelolaan data pribadi, serta mengetahui langkah-langkah yang dapat diambil jika data mereka disalahgunakan.

Pendidikan tentang privasi dan keamanan data harus menjadi bagian dari kurikulum pendidikan nasional agar generasi muda Indonesia dapat tumbuh dengan pemahaman yang lebih baik tentang hak-hak mereka dalam dunia digital. Ini penting agar masyarakat tidak hanya menjadi objek yang dilindungi, tetapi juga menjadi subjek yang aktif dalam menjaga keamanan data mereka.

Perlindungan data pribadi yang ideal dapat menciptakan hadirnya kepercayaan publik terhadap sistem digital dan e-commerce di Indonesia mengingat semakin banyaknya transaksi online dan penggunaan platform digital dalam kehidupan sehari-hari. Dengan perlindungan data yang kuat, masyarakat akan merasa lebih aman untuk melakukan berbagai aktivitas digital, mulai dari berbelanja online, berinteraksi di media sosial, hingga bertransaksi dalam berbagai layanan digital. Kepercayaan ini pada akhirnya akan mendorong pertumbuhan ekonomi digital yang sehat, yang berfokus pada keadilan dan keberlanjutan bagi semua pihak.

---

[49] Erna Priliasari, "Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online," *Majalah Hukum Nasiona* 49, no. 2 (2019).

G. Referensi

"10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-Ramai Bantah Baca Artikel CNN Indonesia '10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-Ramai Bantah' Selengkapnya Di Sini: Https://Www.Cnnindonesia.Com/Teknologi/20221230125430-192-894094/10-Kasus-." *CNN Indonesia*, 2022.

Alfarizi, Moh Khory. "Pakar Jelaskan Dampak Kebocoran Data Milik Bank Indonesia." *Tempo.Com*, 2022.

IBM. "Apa Itu GDPR?," 2018.

Aptika. "Pentingnya Pelindungan Data Pribadi Di Era Digital." *Kominfo*. 2021.

———. "Rapat Paripurna DPR Sahkan RUU PDP." *Kominfo*. 2022.

Chintia, Ervina, Rofiqoh Nadiah, Humayyun Nabila Ramadhani, Zulfikar Fahmi Haedar, Adam Febriansyah, and Nur Aini Rakhmawati. "Kasus Kejahatan Siber Yang Paling Banyak Terjadi Di Indonesia Dan Penanganannya." *JJIEET (Journal Information Engineering and Educational Technology)* 2, no. 2 (2018).

D, Ananthia Ayu, Titis Anindyajati, and Abdul Ghoffar. "Perlindungan Hak Privasi Atas Data Diri Di Era Ekonomi Digital." Jakarta, 2019.

Djafar, Wahyudi, and Asep Komarudin. *Perlindungan Hak Atas Privasi Di Internet- Beberapa Penjelasan Kunci*. Jakarta: ELSAM, 2014.

Hiscock, Robb. "Panduan Utama Untuk Kepatuhan Terhadap PDPA Thailand." *Onetrust*, 2022.

Indonesia, Pemerintah Pusat. Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (2022).

Limited, Security Lit. "Apa Tiga Tujuan Keamanan Siber?" Medium, 2023. https://securitylit.medium.com/what-are-the-three-goals-of-cybersecurity-6ec5499fe61.

Mahira, Dararida Fandra Fandra, Emilda Yofita, and Lisa Nur Azizah. "Consumer Protection System (CPS): Sistem Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept." *Legislatif* 3, no. 2 (2020).

Makarim, Edmon. *Kompilasi Hukum Telematika*. Jakarta: PT. Raja Grafindo Perkasa, 2003.

Muchsin. *Perlindungan Dan Kepastian Hukum Bagi Investor Di Indonesia*. Surakarta: Universitas Sebelas Maret, 2003.

Priliasari, Erna. "Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online." *Majalah Hukum Nasiona* 49, no. 2 (2019).

Rizal, MS. "Perbandingan Perlindungan Data Pribadi Indonesia Dan Malysia." *Jurnal Cakrawala Hukum*, 2019. https://doi.org/DOI: https://doi.org/10.26905/idjch.v10i2.3349. 218-227.

Rosadi, Sinta Dewi, and Garry Gumelar Pratama. "Urgensi Perlindungan Data Privasi Dalam Era Ekonomi Digital Di Indonesia." *Veritas et Justitia* 4, no. 1 (2018): 88–110. https://doi.org/http://doi.org/10.25123/vej.2916.

Setyowati, Desy. "Ahli IT Ungkap Bahaya Jika Benar Jutaan Data Pasien Bocor." *Katadata.Co.Id*, 2022.

Suari, K. R. Anggen. "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia." *Jurnal Analisis Hukum* 1 (6AD).

Winarsih, Winarsih, and Irwansyah. "Proteksi Privasi Big Data Dalam Media Sosial." *Audiens Jurnal: Jurnal Ilmu Komunikasi* 3, no. 1 (2020).

BAB 3

REGULASI PERLINDUNGAN DATA PRIBADI GLOBAL

Dr. Abdul Karim, S.T., M.M.

(Bina Sarana Global Institute of Technology and Business)

A. Pendahuluan

Perkembangan bisnis global yang merupakan implikasi dari perkembangan teknologi informasi dan digital yang cepat dan *massive* dalam beberapa dekade terakhir memberikan gambaran mengenai pentingnya regulasi perlindungan data pribadi global. Dunia bisnis memerlukan standar perlindungan data pribadi yang bukan hanya mengatur penggunaan data pribadi tetapi juga dapat mengakomodasi perkembangan bisnis global, selain itu dunia juga memerlukan suatu regulasi yang dapat mengakomodir budaya lokal masing-masing negara yang berbeda dalam persepsi mengenai data pribadi baik secara definisi maupun dalam aktual penggunaan sehari-hari.

Definisi dari regulasi global adalah proses untuk membuat dan mengimplementasikan aturan dan arahan dalam skala global yang dapat mengatasi dan mengelola masalah dan resiko yang bisa digunakan bukan hanya secara global tetapi juga pada masing-masing negara (Boisrobert and Keener, 2010).

Dari defenisi ini ada 2 poin utama yang harus dimiliki oleh Regulasi Perlindungan Data Pribadi global, yaitu pertama, regulasi tersebut harus dapat diikuti secara global, dan yang kedua regulasi itu juga dapat digunakan di masing-masing negara. Beberapa parameter juga dapat menjadi acuan apakah suatu regulasi dapat dikategorikan sebagai regulasi yang bagus dan dapat dijadikan sebagai regulasi global, yaitu regulasi itu mendapat persetujuan dan dukungan dari lembaga Legislatif, regulasi itu dapat dipertanggungjawabkan (*accountable*), aturannya adil, serta dapat diakses dan terbuka, Regulasi itu juga didukung oleh ahli dan sumber daya manusia yang memadai, dan yang terakhir, regulasi itu

harus *efficient* (Baldwin, et al, 2011). Dari penjelasan di atas, maka ada beberapa tantangan dalam penentuan regulasi perlindungan data pribadi global, yaitu;

1) Penerimaan regulasi tersebut oleh Lembaga-lembaga legislatif di masing-masing negara,
2) Sesuai dengan aspek keadilan dan keterbukaan
3) Kesiapan sumber daya manusia, dan
4) Efisiensi pelaksanaannya.

Regulasi Perlindungan data pribadi relative baru di dunia dan diperlukan banyak eksplorasi, review dan analisis untuk mendapatkan regulasi terbaik, yang bukan saja dapat menekan pelanggaran, tetapi juga memberikan perlindungan kepada masyarakat mengingat dampak yang besar dari kebocoran atau penyalahgunaan data pribadi.

Penulis akan membahas parameter dan tantangan tersebut di artikel ini dengan menganalisa 5 regulasi perlindungan data pribadi yang banyak digunakan di dunia saat ini, yaitu *Global Data Protection Regulation* (GDPR), *Data Protection Act* (DPA), *California Consumer Privacy Act* (CCPA), *China's Personal Protection Information Law* (PIPL) dan *International Standard Organization* (ISO 27701).

B. Regulasi Perlindungan Data Pribadi di Dunia Internasional

Konsep Perlindungan data pribadi sudah lama diutarakan oleh para ahli. Warren dan Brandeis (1890) mengartikan privasi sebagai *right to be let alone*, bahkan jika ditinjau dari sejarah hukum, konsep perlindungan data, sudah dijabarkan dalam hukum-hukum yang lebih tua lagi, seperti konsep *Saddu al-Dzari'ah* dalam hukum Islam, yang tujuannya untuk mencegah dan menghambat segala segala sesuatu yang dapat menyebabkan kerusakan atau masalah (Badar, et al, 2023).

Aktualisasi perlindungan data pribadi pada dunia modern dimulai setelah perang dunia ke-2 dimana negara-negara pemenang perang termasuk Amerika Serikat memandang perlu untuk merumuskan konsep privasi, salah satunya adalah di inisiatif multi-disiplin yang dinamakan *The Impact of Science and Technology on Privacy* yang dilakukan oleh *Special*

Committee on Science and Law of the Association of the Bar of the City of New York pada tahun 1962-1966 (Yuniarti, 2019). Pada sekitar tahun 1960, Konsep dasar perlindungan data pribadi pertama kali muncul. Selanjutnya tahun 1970, Jerman adalah negara pertama yang memberlakukan peraturan tentang perlindungan data yang kemudian diikuti oleh hukum nasional Swedia pada tahun 1973 dan Prancis pada tahun 1978. Inggris mulai memberlakukan Undang-Undang perlindungan data di tahun 1984, yang merupakan inisiatif pemerintah Inggris karena perkembangan teknologi komputer yang menimbulkan resiko penyalahgunaan data pribadi.

Amerika sebagai salah satu kiblat perkembangan teknologi komputer dan informasi menerapkan pendekatan yang berbeda dengan negara-negara Eropa pada Undang-Undang data pribadi, yaitu melalui pendekatan sektoral berdasarkan jenis data dan industri. Pada tahun 1970, Amerika mengeluarkan undang-undang perlindungan data pada konsumen kredit dan setelah itu menyusul undang-undang untuk sektor bisnis lain, seperti media dan otomotif.

China sebagai negara dengan jumlah penduduk terbesar dan resiko penyalahgunaan data pribadi yang juga sangat besar, mulai membuat undang-undang perlindungan data pribadi dengan cara sektoral, terutama di sektor keuangan dan telekomunikasi. Pemerintah China, walaupun terkesan lebih baru dalam pemberlakuan undang-undang perlindungan data pribadi, tetapi dengan cepat dapat mengadopsi berbagai undang-undang data pribadi dunia dan mengimplementasikannya dalam regulasi yang komprehensif.

International Standard Organization (ISO), sebagai sebuah organisasi standar yang diakui oleh dunia juga mengeluarkan aturan dan standar untuk perlindungan data pribadi, yang merupakan perluasan dari standar keamanan dan kontrol teknologi informasi yang sudah ada sebelumnya. Berikut ini adalah deskripsi dari regulasi perlindungan data pribadi dunia

1. Global Data Protection Regulation (GDPR)

Regulasi GDRP adalah regulasi perlindungan data pribadi yang *comprehensive* dan mulai berlaku dari tahun 1998, regulasi ini berlaku

pada negara-negara Uni-Eropa dan beberapa ahli berpendapat ini adalah regulasi yang paling tepat sebagai regulasi global (Rustad & Koenig, 2019). Regulasi ini diadopsi oleh beberapa negara di luar Uni-Eropa dengan menambah atau merubah poin-poin yang disesuaikan untuk kepentingan masing-masing negara tersebut.

Ada beberapa poin penting dari GDRP, antara lain

1) Hukum, Keadilan, dan Transparansi (*Lawfulness, Fairness, and Transparency*), data pribadi harus diproses sesuai dengan hukum, adil dan transparan bagi subyek data. Prinsip ini juga diadopsi oleh Sebagian besar undang-undang perlindungan data pribadi di dunia.
2) Hak Subyek Data yang detail, yaitu hak untuk diberitahu (*right to be informed*), hak untuk mengakses (*right to access*), hak untuk perbaikan data yang tidak akurat (*right to Rectification*), hak untuk Penghapusan (*right to be Forgotten*), Hak untuk Pembatasan Pemrosesan (*right to Restriction of Processing*), Hak Portabilitas Data (*right to Data Portability*), Hak untuk menolak (*right to reject*), Hak untuk Tidak Tunduk pada Pengambilan Keputusan Otomatis, Termasuk Profiling (*right not to be Subject to Automated Decision-Making, Including Profiling*)
3) GDPR juga mewajibkan organisasi untuk memiliki petugas perlindungan data (*Data Protection Officer*), pemberitahuan jika ada pelanggaran data pribadi kepada otoritas dalam 72 jam, dan penilaian terhadap dampak data pribadi dan pencatatan pemrosesan data pribadi
4) Sangsi yang berat jika ada pelanggaran, yaitu, termasuk denda hingga €20 juta atau 4% dari omset global tahunan, mana pun yang lebih tinggi.

GDPR adalah regulasi yang ketat dengan sanksi yang berat bagi pelanggarnya, walaupun regulasi ini terutama diimplementasi oleh negara-negara Uni-Eropa, tetapi karena luasnya cakupan dan ketentuan yang ketat, regulasi ini banyak mempengaruhi negara-negara lain di luar Uni-Eropa untuk menyesuaikan aturannya agar selaras dengan GDPR (Zaeem & Barber, 2020).

2. Data Protection Act (DPA)

Data Protection Act (DPA) adalah regulasi perlindungan data pribadi yang dikeluarkan oleh pemerintah Inggris. Regulasi ini sudah melalui beberapa tahapan perubahan versi, yaitu DPA tahun 1984 yang merupakan versi pertama yang sekaligus menjadi awal dari perlindungan data yang spesifik ke data pribadi, lalu diperbaharui dengan DPA versi 1998 yang dikeluarkan untuk kesesuaian dengan regulasi Uni-Eropa, yaitu Directive 95/46/EC. Versi yang berikutnya adalah versi 2018 yang saat ini digunakan, yang juga dibuat agar sinergi dengan Undang-undang Uni-Eropa GDPR dengan tambahan beberapa item yang sesuai dengan kondisi Inggris.

Ada beberapa poin penting dalam DPA 2018, yaitu

1) Adanya perlindungan ekstra untuk informasi data pribadi yang sensitif, seperti RAS dan etnik, opini politik, agama, data genetis, dan data orientasi sexual.
2) DPA memberikan pengecualian untuk data jurnalistik, akademis dan seni serta literasi
3) DPA mengatur batas waktu penyimpanan data untuk memastikan data hanya diproses sesuai dengan waktu ketika dibutuhkan.

DPA menurut penelitian memberikan kontribusi positif dalam perlindungan data pribadi, khususnya untuk beberapa bidang yang beresiko untuk dilanggar, seperti untuk keperluan jurnalistik (Wong, 2020).

3. California Consumer Privacy Act (CCPA)

Regulasi perlindungan data negara bagian California (*California Consumer Privacy Act*) atau disingkat CCPA adalah regulasi yang relatif baru dengan mempertimbangkan sejarah panjang inisiatif dan usulan perlindungan data pribadi di Amerika Serikat. Regulasi yang yang dikeluarkan tahun 2018 ini mendapatkan respon positif dari Masyarakat Amerika Serikat karena efektifitas nya, ada beberapa poin penting dari CCPA, antara lain:

1) Adanya badan yang bertanggung jawab dalam penegakan regulasi kerahasiaan data, yang dinamakan *The California Privacy Protection*

Agency (CPPA).

2) Hak dari Subyek Data untuk mengetahui informasi pribadi apa saja yang dikumpulkan oleh suatu organisasi dari keseluruhan data pribadi mereka.
3) Hak untuk mengetahui untuk apa data pribadi mereka digunakan oleh suatu organisasi
4) Organisasi harus merespon pertanyaan permintaan dari pemilik data pribadi dalam waktu yang ditentukan

CCPA dikenal luas sebagai salah satu regulasi yang diimplementasikan oleh raksasa sosial media, Meta. Terutama setelah masalah pelanggaran data pribadi 87 Juta pengguna facebook di kasus *Cambridge Analytica*, tahun 2018, yang menyebabkan Meta harus membayar denda sebesar 70 Triliun (Lee, 2020).

4. China's Personal Information Protection Law (PIPL)

Regulasi Perlindungan Data Pribadi dari Cina, yaitu *The Personal Information Protection La*w (PIPL) adalah regulasi yang dikeluarkan oleh pemerintah China untuk mendukung perkembangan industri digital dan teknologi Informasi yang sangat *massive* di China. Regulasi ini dikeluarkan tahun 2021 dengan mengadopsi berbagai regulasi dunia yang sudah ada sebelumnya dan disesuaikan dengan kepentingan dan strategi industri dan globalisasi China.

Beberapa poin penting dari regulasi ini, yaitu

1) Hak Subyek Data diinformasikan dengan detail, yaitu hak untuk tahu siapa yang memproses data mereka, hak untuk memutuskan apakah data pribadi mereka bisa diproses atau tidak, hak untuk memperbaiki dan menghapus data, dan hak untuk mentransfer data ke pengelola data pribadi lain.
2) Adanya badan khusus yang bertanggung jawab terhadap perlindungan data pribadi, badan khusus ini adalah *Cyberspace Administration of China* (CAC).
3) Jangkauan ekstrateritorial, yang ruang lingkupnya adalah organisasi luar negeri yang ingin menggunakan data pribadi untuk produk

dan jasa di China atau menganalisa perilaku individu di Cina.

Regulasi perlindungan data pribadi Cina, walaupun masih cukup baru, tetapi telah menunjukkan hasil yang cukup baik dalam melindungi data pribadi Masyarakat Cina (Creemers, 2022).

5. International Standard Organization (ISO 27701)

ISO 27701 sebagaimana standar dari ISO lainnya adalah panduan dan kerangka kerja yang detail untuk organisasi dalam mengelola data pribadi. Melalui implementasi yang sistematik dengan kerangka kerja yang standar dan detail, diharapkan organisasi-organisasi dapat memiliki standar yang sama dalam mengelola kerahasiaan data pribadi. ISO 27701 sendiri adalah perluasan dari ISO 27001 yang sudah ada sejak tahun 2005 dan diimplementasi oleh ribuan bahkan kemungkinan jutaan organisasi di dunia, secara resmi berdasarkan jumlah sertifikasi, pada tahun 2022 ada sekitar 71,549 sertifikasi implementasi ISO 27001.

ISO 27701 yang secara resmi dikeluarkan pada tahun 2019, tidak bisa langsung diterapkan tanpa menerapkan standar sebelumnya, yaitu ISO 27001, Standar ini juga memiliki beberapa item penting mengenai perlindungan kerahasiaan data pribadi, yaitu

1) Adanya peran Pengendali dan Prosesor dalam perlindungan data pribadi. Pengendali adalah pihak yang menentukan tujuan dan cara pemrosesan data pribadi, sementara Prosesor adalah pihak yang memproses data pribadi tersebut. Pemisahan ini diperlukan untuk menunjukkan akuntabilitas dan kejelasan peran dan tanggung jawab, sehingga diharapkan kepatuhan akan regulasi dapat dipenuhi.
2) Akurasi dan minimalisasi data. Standar ini sangat fokus pada akurasu data, sehingga pembaharuan data sangat diperlukan, selain itu hanya data-data yang diperlukan yang diproses.
3) Hak Subyek Data, yaitu hak untuk mengakses, memperbaiki dan menghapus data mereka.
4) Transfer data lintas batas, yaitu pengelolaan transfer data pribadi antar negara.

ISO 27701 sebagai standar dalam perlindungan data pribadi telah direkomendasikan untuk diimplementasi di sektor dengan tingkat sensitifitas data pribadi yang krusial seperti sektor Kesehatan (World Health Organization, 2021).

C. Irisan Regulasi Perlindungan Data antar Negara

Perlindungan data pribadi menjadi perhatian dari seluruh dunia karena besarnya resiko yang bisa terjadi jika regulasi tidak sesuai atau diperhatikan. Tripathi & Mukhopadhyay (2020), menyimpulkan besarnya kerugian finansial dan menurunnya nilai perusahaan yang bisa menimpa jika melanggar regulasi data pribadi, kerugian ini bukan hanya terjadi pada Perusahaan besar tapi juga Perusahaan menengah dan kecil. Pelanggaran ini juga menyebabkan hilangnya kepercayaan pasar kepada perusahaan (Nofer, et al, 2014) dan kepercayaan serta kehilangan pelanggan (Martin, et al, 2017), sehingga organisasi dan perusahaan di seluruh dunia menjadi sangat memerlukan regulasi kerahasiaan data pribadi yang secara aktual dapat diimplementasi dengan baik di organisasinya.

Regulasi Perlindungan Data Pribadi yang berbeda di tiap negara pada dasarnya memiliki beberapa poin-poin persamaan. Perbedaan yang ada pada umumnya disebabkan oleh kebutuhan spesifik dari masing-masing negara. Beberapa poin-poin penting yang selaras dari tiap regulasi, yaitu:

1) Hak dari Subyek Data. Pada umumnya setiap regulasi menyebutkan hak yang hampir sama dari subyek data, yaitu hak perbaikan, hak akses, hak untuk dilupakan, hak untuk menolak pemrosesan data
2) Adanya badan atau pihak yang ditunjuk untuk mengawasi dan bertanggung jawab terhadap aturan perlindungan data pribadi
3) Minimalisasi dan batasan waktu data pribadi, yang mengacu kepada proses data pribadi yang diperlukan saja dan dalam batas waktu yang ditentukan.
4) Adanya sanksi bagi pelanggaran aturan.

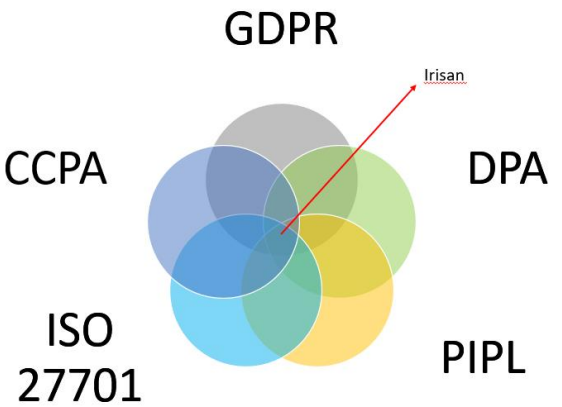
Law enforcement juga sangat penting untuk memastikan regulasi diikuti oleh organisasi. Banyak kasus yang sudah membuktikan

efektifitas dari regulasi sesuai dengan sangsi, seperti kasus *Britannica Analytic* di tahun 2018, kasus Meta Platform Ireland Limited di Irlandia dengan denda 1,2 miliar Euro atau setara dengan Rp 19,35 triliun.

Poin-poin penting yang sama dari regulasi-regulasi dunia ini jika digambarkan dalam suatu Kumpulan dengan masing-masing poin, dapat disebut dengan irisan, dalam diagram Venn, yaitu diagram yang ditemukan oleh Matematikawan Inggris, John Venn untuk mengetahui hubungan antara beberapa himpunan atau obyek. Melalui diagram Venn ini dapat memperjelas poin-poin apa saja yang sama dari setiap obyek dan juga poin yang sangat berbeda (Moktefi, & Lemanski, 2022).

Gambar 1 di bawah ini menunjukkan regulasi-regulasi perlindungan data pribadi di dunia, jika dibuat dalam diagram Venn, maka ditemukan adanya poin-poin yang sama yang dalam gambar ini ditunjukkan dengan bagian irisan, sehingga ketika mengimplementasikan poin-poin regulasi dalam irisan ini, maka organisasi bisa mengimplementasi semua regulasi dunia yang disebutkan di atas.

Tentu saja ada beberapa poin regulasi yang spesifik yang penting dan tidak masuk dalam irisan, seperti regulasi mengenai perlindungan data untuk tujuan jurnalistik di DPA atau regulasi dengan efisiensi teknikal yang ditunjukkan oleh CCPA dan ruang lingkup ekstrateritorial yang efektif dijalankan oleh perusahaan-perusahaan China dengan implementasi PIPL. Poin-poin spesifik ini bisa diimplementasi berdasarkan kondisi dan kebutuhan masing-masing organisasi.



Gambar 3.1. Irisan dari Regulasi Dunia

Sumber daya manusia juga sangat penting untuk keberhasilan penyusunan dan implementasi regulasi. Dibutuhkan kolaborasi multi-disiplin dalam implementasi ini, baik dari sisi hukum dan manajemen maupun teknis (Almeida Teixeira, et al, 2019). Beberapa standar regulasi menyediakan pelatihan dan sertifikasi untuk memastikan implementasi dapat dilakukan oleh orang atau team yang capable, seperti GDPR dengan sertifikasi *Certified Information Privacy Professional* (CIPP) atau *Certified Data Protection Officer* (CDPO). O'Leary (2020) dan Mazari & Bensalem (2024) menyarankan agar kompetensi dalam teknologi informasi masuk dalam kurikulum hukum dan menjadi salah satu kompetensi wajib bagi pengacara dan penegak hukum.

Perkembangan teknologi Kecerdasan buatan (*Artificial Intelligence* atau AI) dan Mesin Pembelajar (*Machine Learning*, atau ML) juga harus menjadi perhatian karena pengaruhnya kepada perlindungan data pribadi. Teknologi ini membutuhkan data pribadi yang besar agar algoritma dapat berfungsi maksimal, contohnya untuk melakukan estimasi kebutuhan karyawan dan kinerja, maka AI dan ML, perlu mengumpulkan dan memproses data karyawan selama kurun waktu tertentu, pemrosesan ini mungkin bisa bertentangan dengan regulasi perlindungan data pribadi, baik itu data terkait RAS, Kesehatan, dan data pribadi lainnya. Hal yang sama juga menjadi perhatian beberapa peneliti dalam dunia Kesehatan, seperti penelitian dari Yadav, et al (2023) yang menemukan besarnya potensi pelanggaran kerahasiaan data pribadi ketika AI dan ML melakukan pemrosesan data pasien.

D. Rekomendasi

Regulasi perlindungan data pribadi global sangat diperlukan untuk mendukung perkembangan bisnis dan teknologi informasi dan digital global yang tidak mengenal batas negara dan budaya. Beberapa regulasi yang digunakan di dunia sekarang sudah diadopsi oleh banyak negara dengan merubah atau memodifikasi agar sesuai dengan kondisi dan budaya masing-masing negara, tetapi regulasi dan standar yang berlaku secara global menjadi sangat penting untuk memastikan tidak ada masalah dalam interaksi antar negara. Penulis menyarankan untuk menganalisa item atau poin yang sama dalam setiap regulasi

perlindungan data pribadi dunia dan memasukkannya dalam Undang-undang perlindungan data pribadi Indonesia, sementara item-item yang khusus dapat dianalisis lebih lanjut atau memasukkannya dalam *addendum*, yang berlaku untuk kondisi tertentu, contohnya item penalti yang bisa disesuaikan berdasarkan sektor bisnis. Penalty ini terbukti efektif di banyak negara, sebaiknya ini juga bisa menjadi pertimbangan pemerintah Indonesia untuk memastikan regulasi perlindungan data pribadi dipatuhi oleh semua organisasi.

Undang-Undang (UU) Nomor 27 Tahun 2022 memang memberikan sanksi pidana dengan hukuman pidana penjara paling lama hingga 6 (enam) tahun dan/atau pidana denda paling banyak adalah Rp. 6.000.000.000,00 (enam miliar rupiah), tetapi yang diperlukan adalah efektifitas sanksi ini untuk mencegah pelanggaran undang-undang di Indonesia, karena kita ketahui jumlah pelanggaran data pribadi cukup banyak dan sering terjadi di Indonesia.

Saran lainnya adalah karena mempertimbangkan perkembangan teknologi informasi dan digital yang sangat cepat, maka perlu dilakukan review berkala undang-undang perlindungan data yang ada di Indonesia, yaitu Undang-Undang (UU) Nomor 27 Tahun 2022 ini untuk memastikan regulasi ini masih bisa diberlakukan atau sudah harus direvisi, jika melihat sejarah perubahan regulasi dunia yang dijabarkan di atas, maka perubahan versi sering dilakukan, selain untuk memastikan regulasi selaras dengan regulasi yang lebih tinggi, perubahan ini juga untuk memastikan keterbaharuan seiring dengan perkembangan teknologi, selain itu diperlukan kolaborasi pakar multi-disiplin, baik dari sisi aspek hukum, bisnis, teknologi dan juga etika.

E. Referensi

Almeida Teixeira, G., Mira da Silva, M., & Pereira, R. (2019). The critical success factors of GDPR implementation: a systematic literature review. *Digital Policy, Regulation and Governance*, *21*(4), 402-418.

Badar, E. S., Fauzi, A., & Jazuli, A. PERSONAL DATA PROTECTION POLICY IN LAW NUMBER 27 OF 2022 IN THE PERSPECTIVE OF POSITIVE LAW AND ISLAMIC LAW. *Hukum Islam*, *23*(1), 61-74.

Baldwin, R., Cave, M., & Lodge, M. (2011). Understanding regulation: theory, strategy, and practice. Oxford university press.

Boisrobert, C. E., Keener, L., & Lelieveld, H. L. (2010). The global harmonization initiative. In *Ensuring Global Food Safety* (pp. 71-90). Academic Press.

Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity*, *8*(1), tyac011.

Lee, C. (2020). The aftermath of Cambridge Analytica: A primer on online consumer data privacy. *AIPLA QJ*, *48*, 529.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of marketing*, *81*(1), 36-58.

Mazari, N., & Bensalem, S. (2024). Developing Judges' and Lawyers' Skills in the Digital Age: A Comparative Study (Singapore-USA-UK). مجلة الحقوق والعلوم الانسانية, 17(3), 49-63.

Moktefi, A., & Lemanski, J. (2022). On the origin of Venn diagrams. *Axiomathes*, *32*(Suppl 3), 887-900.

Nofer, M., Hinz, O., Muntermann, J., & Roßnagel, H. (2014). The economic impact of privacy violations and security breaches: A laboratory experiment. *Business & Information Systems Engineering*, *6*, 339-348.

O'Leary, D. L. (2020). " Smart" Lawyering: Integrating Technology Competence into the Legal Practice Curriculum. *UNHL Rev.*, *19*, 197.

Rustad, M. L., & Koenig, T. H. (2019). Towards a global data privacy standard. *Fla. L. Rev.*, *71*, 365.

Tripathi, M., & Mukhopadhyay, A. (2020). Financial loss due to a data privacy breach: An empirical analysis. *Journal of Organizational Computing and Electronic Commerce*, *30*(4), 381-400.

Yadav, N., Pandey, S., Gupta, A., Dudani, P., Gupta, S., & Rangarajan, K. (2023). Data privacy in healthcare: In the era of Artificial Intelligence. *Indian Dermatology Online Journal*, *14*(6), 788-792.

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences Journal (BECOSS)*, *1*(1), 147-154.

Wong, B. (2020). The journalism exception in UK data protection law. *Journal of Media Law*, *12*(2), 216-236.

World Health Organization. (2021). *The protection of personal data in health information systems-principles and processes for public health* (No. WHO/EURO: 2021-1994-41749-57154). World Health Organization. Regional Office for Europe.

Zaeem, R. N., & Barber, K. S. (2020). The effect of the GDPR on privacy policies: Recent progress and future promise. *ACM Transactions on Management Information Systems (TMIS)*, *12*(1), 1-20.

BAB 4

HAK ASASI MANUSIA DAN PRIVASI DALAM DUNIA DIGITAL

Dr. Abdul Karim, S.H., M.I.Kom.

(Sekolah Tinggi Ilmu Hukum Sultan Adam Banjarmasin)

A. Pendahuluan

Hak asasi manusia bagi bangsa Indonesia berbeda dengan maksud yang menjadi standar internasional sebagaimana yang dideklarasikan oleh Perserikatan Bangsa Bangsa di tahun 1948. Hak asasi manusia di Indonesia dikembangkan berbasis kepada landasan idiil Pancasila yang terdiri dari lima sila yaitu Ketuhanan Yang Maha Esa, Kemanusiaan yang Adil dan Beradab, Persatuan Indonesia, Kerakyatan yang dipimpin oleh hikmah kebijaksanaan dalam permusyawaratan/perwakilan, dan keadilan sosial bagi seluruh rakyat Indonesia. Substansi dari lima sila tersebut tercantum dalam Pembukaan Undang Undang Dasar 1945 yang disahkan tanggal 18 Agustus 1945 sehari setelah Indonesia merdeka.

Pasca reformasi tahun 1998, gerakan demokratisasi dan keterbukaan di Indonesia menjadi agenda yang dituntut dengan sangat serius oleh masyarakat. Pemerintahan baru bersama-sama Majelis Permusyawaratan Rakyat mengakomodasi tuntutan reformasi tersebut. Langkah pertama dan sangat mendasar adalah dengan mengamandemen Undang Undang Dasar 1945 sebanyak 4 kali amandemen dalam kurun waktu 3 tahun, yaitu 1999 sampai 2002. Materi substantif yang diamandemen antara lain dengan cara menyisipkan satu Bab yaitu Bab X A dengan judul Hak Asasi Manusia yang berisi Pasal 28A sampai dengan Pasal 28J.

Pasal-pasal HAM dalam Bab X berisi sebagai berikut :

1) Pasal 28A : Setiap orang berhak untuk hidup serta berhak mempertahankan hidup dan kehidupannya

2) Pasal 28B : (1) Setiap orang berhak membentuk keluarga dan melanjutkan keturunan melalui perkawinan yang sah. (2) Setiap anak berhak atas kelangsungan hidup, tumbuh, dan berkembang serta berhak atas perlindungan dari kekerasan dan diskriminasi.

3) Pasal 28C : (1) Setiap orang berhak mengembangkan diri melalui pemenuhan kebutuhan dasarnya, berhak mendapat pendidikan dan memperoleh manfaat dari ilmu pengetahuan dan teknologi, seni dan budaya, demi meningkatkan kualitas hidupnya dan demi kesejahteraan umat manusia. (2) Setiap orang berhak untuk memajukan dirinya dalam memperjuangkan haknya secara kolektif untuk membangun masyarakat, bangsa, dan negaranya.

4) Pasal 28D : (1) Setiap orang berhak atas pengakuan, jaminan, perlindungan, dan kepastian hukum yang adil serta perlakuan yang sama di hadapan hukum. (2) Setiap orang berhak untuk bekerja serta mendapat imbalan dan perlakuan yang adil dan layak dalam hubungan kerja. (3) Setiap warga negara berhak memperoleh kesempatan yang sama dalam pemerintahan. (4) Setiap orang berhak atas status kewarganegaraan.

5) Pasal 28E : (1) Setiap orang bebas memeluk agama dan beribadat menurut agamanya, memilih pendidikan dan pengajaran, memilih pekerjaan, memilih kewarganegaraan, memilih tempat tinggal di wilayah negara dan meninggalkannya, serta berhak kembali. (2) Setiap orang berhak atas kebebasan meyakini kepercayaan, menyatakan pikiran dan sikap, sesuai dengan hati nuraninya. (3) Setiap orang berhak atas kebebasan berserikat, berkumpul, dan mengeluarkan pendapat.

6) Pasal 28F : Setiap orang berhak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia.

7) Pasal 28G : (1) Setiap orang berhak atas perlindungan 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. (2) Setiap orang berhak untuk bebas dari penyiksaan atau perlakuan yang merendahkan derajat martabat manusia dan berhak memperoleh suaka politik dari negara lain.

8) Pasal 28H : (1) Setiap orang berhak hidup sejahtera lahir dan batin, bertempat tinggal, dan mendapatkan lingkungan hidup yang baik dan sehat serta berhak memperoleh pelayanan kesehatan. (2) Setiap orang berhak mendapat kemudahan dan perlakuan khusus untuk memperoleh kesempatan dan manfaat yang sama guna mencapai persamaan dan keadilan. (3) Setiap orang berhak atas jaminan sosial yang memungkinkan pengembangan dirinya secara utuh sebagai manusia yang bermartabat. (4) Setiap orang berhak mempunyai hak milik pribadi dan hak milik tersebut tidak boleh diambil alih secara sewenang-wenang oleh siapa pun.
9) Pasal 28I : (1) Hak untuk hidup, hak untuk tidak disiksa, hak kemerdekaan pikiran dan hati nurani, hak beragama, hak untuk tidak diperbudak, hak untuk diakui sebagai pribadi dihadapan hukum, dan hak untuk tidak dituntut atas dasar hukum yang berlaku surut adalah hak asasi manusia yang tidak dapat dikurangi dalam keadaan apa pun. (2) Setiap orang berhak bebas dari perlakuan yang bersifat diskriminatif atas dasar apa pun dan berhak mendapatkan perlindungan terhadap perlakuan yang bersifat diskriminatif itu.(3) Identitas budaya dan hak masyarakat tradisional dihormati selaras dengan perkembangan zaman dan peradaban. (4) Perlindungan, pemajuan, penegakan, dan pemenuhan hak asasi manusia adalah tanggung jawab negara, terutama pemerintah. (5) Untuk menegakkan dan melindungi hak asasi manusia sesuai dengan prinsip negara hukum yang demokratis, maka pelaksanaan hak asasi manusia dijamin, diatur, dan dituangkan dalam peraturan perundang-undangan.
10) Pasal 28J : (1) Setiap orang wajib menghormati hak asasi manusia orang lain dalam tertib kehidupan bermasyarakat, berbangsa, dan bernegara. (2) Dalam menjalankan hak dan kebebasannya, setiap orang wajib tunduk kepada pembatasan yang ditetapkan dengan undang-undang dengan maksud semata-mata untuk menjamin

pengakuan serta penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan moral, nilai-nilai agama, keamanan, dan ketertiban umum dalam suatu masyarakat demokratis.

Sepuluh pasal dalam Bab XA Hak Asasi Manusia tersebut dibahas dalam masa amandemen kedua yaitu 7 sampai 18 Agustus 2000 yang kemudian ditindaklanjuti dengan pemberlakuan Undang Undang Nomor 26 Tahun 2000 tentang Pengadilan Hak Asasi Manusia. Sementara Undang Undang Nomor 39 Tahun 1999 Tentang Asasi Manusia sudah diberlakukan lebih dahulu sebelum UUD 1945 diamandemen sebagai pelaksanaan dari Ketetapan Majelis Permusyawaratan Rakyat Republik Indonesia Nomor XVII/MPR/1998 tentang Hak Asasi Manusia.

Di sisi lain, perkembangan teknologi informasi yang sangat pesat mendorong lahirnya berbagai sistem aplikasi yang digunakan oleh Pemerintah dan badan hukum swasta baik dalam negeri maupun internasional dalam memberikan layanan kepada masyarakat. Pemerintah Republik Indonesia melalui Undang Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan. Perubahan undang undang ini berkaitan dengan kebijakan pemerintah yang akan menerapkan sistem Kartu Tanda Penduduk elektronik (KTP-El).

Guna mengakomodasi penerapan sistem elektronik, Pemerintah memberlakukan Undang Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik di yang kemudian mengalami revisi di tahun 2016 dan tahun 2024.

Kegiatan masyarakat dalam bertransaksi secara elektronik baik dengan lembaga/institusi pemerintah maupun antar individu dan badan hukum mengharuskan masyarakat memberikan data pribadinya guna memenuhi ketentuan yang diberlakukan oleh masing-masing lembaga/badan hukum. Data pribadi yang diberikan tersebut meliputi identitas nomor induk kependudukan, data keluarga, data alamat dan lain sebagainya. Data tersebut berfungsi sebagai data rujukan dalam memverifikasi identitas ketika melakukan transaksi elektronik. Layanan

kesehatan oleh rumah sakit baik milik pemerintah maupun swasta menerapkan sistem penyimpanan data kesehatan dengan menggunakan sistem elektronik. Demikian pula sektor-sektor lainnya.

Dalam kenyataan sering terjadi adanya fraud dalam aktivitas transaksi elektronik yang menimbulkan kerugian banyak pihak, baik masyarakat maupun lembaga/badan hukum. Hal itu dimungkinkan terjadi karena adanya penyalahgunaan informasi secara ilegal yang terkait dengan identitas penduduk oleh pihak yang tidak bertanggung jawab.

B. Hak Asasi Manusia di Indonesia

Pembahasan Hak Asasi Manusia di Indonesia harus berangkat dari falsafah Bangsa Indonesia yaitu Pancasila. Dalam pembukaan Undang Undang Dasar 1945 yang disahkan tanggal 18 Agustus 1945 sehari setelah Indonesia merdeka secara eksplisit sudah termaktub sejumlah Hak Asasi Manusia baik di dalam Pembukaan UUD 1945 maupun di dalam batang tubuhnya. Jauh sebelum Perserikatan Bangsa Bangsa mendeklarasikan The Universal Declaration of Human Right di tanggal 10 Desember 1948, Bangsa Indonesia sudah mempunyai UUD 1945 yang di dalamnya termaktub Hak Asasi Manusia.

Alinea keempat Pembukaan UUD 1945 berisi substansi yang menjadi landasan idiil bangsa yaitu Pancasila (1) Ketuhanan yang maha esa (2) Kemanusiaan yang adil dan beradab (3) Persatuan Indonesia (4) Kerakyatan yang dipimpin oleh hikmah kebijaksanaan dalam permusyawaratan/perwakilan (5) Keadilan Sosial bagi seluruh rakyat Indonesia. Lima sila ini mengandung nilai-nilai universal yang tidak berbeda yang dideklarasikan oleh Perserikatan Bangsa Bangsa.

Deklarasi Umum Hak Asasi Manusia kemudian dikembangkan oleh PBB dan menjadi dasar beberapa perjanjian internasional yaitu Konvensi Internasional tentang Hak Sipil dan Politik (ICCPR) yang diratifikasi oleh Indonesia melalui Undang Undang Nomor 12 Tahun 2005 dan Konvensi Internasional tentang Hak Ekonomi, Sosial, dan Budaya (ICESCR) yang diratifikasi oleh Indonesia melalui Undang Undang Nomor 11 Tahun 2005.

Komitmen bangsa Indonesia terhadap Hak Asasi Manusia

mendapat penguatan pasca reformasi 1998. MPR menetapkan Tap Nomor XVII/MPR/1998 tentang Hak Asasi Setahun kemudian lahir Undang Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia. Tahun 2001 terbentuk Kementerian Hukum dan HAM, bertahan hingga tahun berakhirnya kabinet Presiden Joko Widodo periode kedua. Mulai 20 Oktober 2024 Kementerian HAM berdiri sendiri dengan Menteri pertamanya Natalius Pigai. Dari aspek kelembagaan, dibentuk Peradilan HAM melalui Undang Undang Nomor 26 Tahun 2000 tentang Pengadilan Hak Asasi Manusia.

Jauh sebelum adanya Undang Undang HAM dan Peradilan HAM, Pemerintah Orde Baru membentuk Komisi Nasional Hak Asasi Manusia melalui Keputusan Presiden Soeharto Nomor 50 Tahun 1993 yang ditandatangani tanggal 7 Juni 1993. Keppres ini menandai dimulainya lembaga independen yang bertugas mengawasi dan mendorong penghormatan HAM di Indonesia, sekaligus sebagai respons terhadap deklarasi Wina 1993 tentang hak asasi manusia, yang mengamanatkan setiap negara untuk memiliki lembaga nasional HAM.

Pengadilan HAM adalah Peradilan permanen yang berada dalam lingkup Pengadilan Negeri. Di samping itu dimungkinkan pula dibentuk Pengadilan HAM Ad Hoc khusus untuk menangani pelanggaran HAM berat yang terjadi sebelum Undang Undang HAM diberlakukan.

Nilai-nilai HAM yang terkandung di dalam Undang Undang Dasar 1945, dan kemudian diamandemen dengan memasukan secara eksplisit nilai-nilai universal HAM menjadi momentum penting bagi sejarah HAM di Indonesia. UUD 1945 adalah hirarki tertinggi hukum positif Indonesia, karenanya pasal-pasal tentang HAM akan mengisipirasi undang undang apapun yang ada di bawahnya. Bagaimana nilai-nilai HAM universal itu larut di dalam batang tubuh UUD 1945 dapat dilihat pada Bab berikutnya.

C. Hak Asasi menjadi Hukum Dasar dalam Konstitusi

Pasal 27 : (1) Segala warga negara bersamaan kedudukannya di dalam hukum dan pemerintahan dan wajib menjunjung hukum dan pemerintahan itu dengan tidak ada kecualinya. (2) Tiap-tiap warga

negara berhak atas pekerjaan dan penghidupan yang layak bagi kemanusiaan. (3) Setiap warga negara berhak dan wajib ikut serta dalam upaya pembelaan negara.

Ayat (1) dan Ayat (2) Pasal 27 UUD 1945 adalah norma yang sudah terdapat di dalam UUD 1945 asli sedangkan ayat (3) adalah ayat baru yang ditambahkan pada Perubahan kedua UUD 1945 tahun 2000. Pasal 27 Ayat (1) sejalan dengan Pasal 7 Deklarasi HAM PBB, yaitu hak atas persamaan dalam hukum dan Pasal 21 Deklarasi HAM PBB, yaitu persamaan kesempatan dalam pemerintahan. Pasal 27 ayat (3) UUD 1945 selaras dengan Pasal 23 Deklarasi Umum HAM mengenai hak atas pekerjaan dan kondisi kerja yang adil.

Pasal 28 UUD 1945 : Kemerdekaan berserikat dan berkumpul, mengeluarkan pikiran dengan lisan dan tulisan dan sebagainya ditetapkan dengan undang-undang. Pasal 28 UUD 1945 ini selaras dengan Pasal 20 DUHAM yaitu kebebasan berkumpul dan berserikat dan Pasal 19 DUHAM mengenai kebebasan berpendapat dan berekspresi. Adapun Bab XA yang berisi 10 Pasal tambahan di dalamnya hampir keseluruhan mengadopsi pasal-pasal di dalam Deklarasi Universal Hak Asasi Manusia.

Beberapa undang undang dibuat dan diberlakukan untuk menindaklanjuti perubahan UUD 1945, antara lain Undang Undang Keterbukaan Informasi Publik, Undang Undang Ketenagakerjaan, Undang Undang Serikat Pekerja, dan lain-lain. Sedangkan Undang Undang Nomor 9 Tahun 1998 Tentang Undang Undang Kemerdekaan Menyampaikan Pendapat di Muka Umum dibuat sebelum Perubahan UUD 45 atas dasar Pasal 28 UUD 1945 yang ditandatangani oleh Presiden Habibie pada tanggal 26 Oktober 1998.

D. Hak Privasi sebagai Hak Asasi

Hak privasi yang dimaksud dalam Bab ini adalah hak privasi di dalam dunia digital. Relevansinya dengan Hak Asasi Manusia adalah Pasal 3 DUHAM yang berisi ketentuan tentang hak atas kebebasan dan keamanan pribadi, diperkuat oleh Pasal 12 DUHAM : *"Tidak seorang pun boleh diganggu secara sewenang-wenang dalam kehidupan pribadinya, keluarganya,*

rumah tangganya, ataupun korespondensinya" Inilah yang mendasari diakuinya privasi sebagai hak asasi manusia meskipun pada saat itu belum terkorelasi dengan aspek digital.

Teknologi yang berkembang lebih dahulu di Eropah melahirkan undang undang Perlindungan Data di Jerman tahun 1970, yaitu *Hesse Data Protection Act*, yang mengatur pengelolaan data oleh instansi publik. Jerman adalah negara pertama di dunia yang mempunyai undang undang perlindungan data. Tahun 1980 OECD (*Organization for Economic Cooperation of Development)* mengeluarkan pedoman yang disebut *Guidelines on Privacy and Transborder Flows of Personal Data.* Pedoman yang dikeluarkan OECD ini adalah pedoman internasional pertama yang mengatur perlindungan data pribadi, mencakup prinsip transparansi, keamanan, dan penggunaan yang terbatas. Tahun 1995, dua tahun setelah terbentuk Uni Eropa, terbit *European Data Protection Directive (EU Directive 95/46/EC),* Uni Eropa menerapkan standar hukum perlindungan data pribadi untuk semua negara anggotanya, yang menjadi cikal bakal *General Data Protection Regulation (GDPR).* Sejak GDPR diberlakukan tahun 2018, secara tidak langsung Uni Eropa mendorong negara-negara di luar Eropa untuk membuat undang undang perlindungan data pribadi. Dengan kekuatan politik, ekonomi dan teknologi yang dimiliki Uni Eropa maka negara-negara di dunia yang mempunyai relasi dagang dengan Eropa terdorong membuat undang undang perlindungan data pribadi. Uni Eropah melindungi seluruh warganya yang melakukan transaksi digital di negara manapun di dunia.

Globalisasi ekonomi dan kemajuan teknologi informasi membuat peluang dan kesempatan yang sangat lebar bagi transaksi-transaksi dagang baik individu maupun korporasi lintas negara. Adalah kewajiban setiap negara untuk melindungi warganya yang melakukan aktivitas internasional tersebut. Maka ketatnya standar perlindungan data yang dimuat dalam *General Data Protection Regulation (GDPR)* menjadi keniscayaan.

Hal tersebut mendorong negara-negara di luar Eropa untuk membuat undang undang perlindungan data pribadi. Brasil memberlakukan *Lei Geral de Proteção de Dados (LGPD)* pada tahun 2020, yang sebagian besar meniru GDPR, untuk meningkatkan daya saing

globalnya. India sedang dalam proses mengesahkan *Data Protection Bill,* yang juga dipengaruhi oleh prinsip-prinsip GDPR.

Indonesia yang telah mengundangkan Undang Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP). Beberapa pertimbangan yang menjadi dasar filosofis maupun sosiologis untuk membuat undang undang tersebut adalah : *Pertama,* pelindungan data pribadi merupakan salah satu hak asasi manusia yang merupakan bagian dari pelindungan diri pribadi maka perlu diberikan landasan hukum untuk memberikan keamanan atas data pribadi, berdasarkan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. *Kedua,* pelindungan data pribadi ditujukan untuk menjamin hak warga negara atas pelindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya pelindungan data pribadi; *Ketiga,* Undang Undang Pelindungan Data Pribadi dimaksudkan untuk menggabungkan beberapa ketentuan perundang-undangan pelindungan data pribadi yang terserak dalam beberapa peraturan perundang-undangan guna meningkatkan efektivitas dalam pelaksanaan pelindungan data pribadi.

Privasi dalam pemahaman umum yang dijelaskan dalam Kamus Umum Bahasa Indonesia adalah *kebebasan, keleluasaan pribadi.* Dicontohkan misalnya seseorang yang menginap di sebuah hotel dapat meminta manajemen hotel untuk merahasiakan nomor kamarnya. Begitu pula ketika PT Telkom menyediakan layanan informasi nomor telepon maka seorang pelanggan dapat meminta kepada PT Telkom untuk merahasiakan nomor teleponnya. Manajemen Hotel dan PT Telkom menghormati permintaan customernya dalam rangka menghormati privasi. Sejalan dengan kemajuan zaman privasi seseorang tidak lagi sekedar harus dihormati, tetapi sudah wajib dilindungi karena privasi sudah menjadi salah satu Hak Asasi Manusia.

Bersamaan dengan itu, fasilitas teknologi informasi canggih yang setiap orang berhak menggunakannya mengharuskan para pengguna (user) menyerahkan data identitas pribadi kepada para penyedia jasa teknologi informasi *(service provider)* karena hal tersebut merupakan syarat mutlak. Misalnya seorang nasabah bank, untuk dapat menikmati layanan *online banking* mau tidak mau nasabah harus memberikan informasi

pribadi antara lain berupa nomor telepon pribadi, nomor telepon kantor, nomor telepon keluarga yang tidak serumah, alamat email, alamat rumah, akun media sosial, Kartu Tanda Penduduk, tempat dan tanggal lahir, nama gadis ibu kandung. Bahkan terkadang lebih rinci daripada itu. Data yang sangat pribadi dan rinci tersebut akan menjadi rujukan informasi untuk validasi dan verifikasi identitas nasabah ketika nasabah bank berkomunikasi dengan petugas bank untuk melakukan transaksi, misalnya layanan *phone banking*. Data pribadi tersebut apabila sampai jatuh ke tangan yang tidak berhak dapat disalahgunakan sehingga merugikan nasabah maupun bank itu sendiri, oleh karena itu tuntutan pelindungan data pribadi menjadi isu penting dan mendesak.

Pada era digital, data pribadi yang memuat data private paling hakiki manusia pada dasarnya tidak boleh diketahui orang lain di luar kepentingan yang legal, karena itu harus ada mekanisme pelindungan yang legal dan aman. Guna mendorong pemerintah selaku pelindung bangsa dan pelindung data, maka langkah-langkah yang digagas oleh masyarakat adalah menjadikan privasi data sebagai hak asasi manusia. Urgensi dan kepentingan privasi disetarakan dengan pelindungan kesehatan, pelindungan pendidikan, pelindungan lingkungan hidup, dan hak-hak dasar lainnya yang tercantum dalam konstitusi.

Menurut Kementerian Komunikasi Digital (Komdigi) yang dahulu dikenal sebagai Kominfo (2022) naskah final RUU PDP telah dibahas sejak 2016 yang terdiri atas 371 daftar inventarisasi masalah (DIM) dan menghasilkan 16 bab serta 76 pasal. RUU PDP telah melalui enam kali perpanjangan masa sidang, rapat panitia kerja, serta rapat tim perumus dan tim sinkronisasi. Akhirnya tahun 2022 RUU PDP dijadikan Undang Undang Nomor 27 Tahun 2022 dan ditandatangani oleh Presiden Joko Widodo. Dengan demikian, Indonesia merupakan negara ASEAN kelima yang memiliki aturan pelindungan data pribadi setelah Singapura, Malaysia, Thailand, dan Filipina. Di dunia, Indonesia merupakan negara ke 127 yang mempunyai UU Pelindungan Data Pribadi.

Dalam Penjelasan Undang Undang Pelindungan Data Pribadi diuraikan sebagai berikut :

"Perkembangan teknologi informasi dan komunikasi yang melaju dengan

pesat telah menimbulkan berbagai peluang dan tantangan. Teknologi informasi memungkinkan manusia untuk saling terhubung tanpa mengenal batas wilayah negara sehingga menjadi salah satu faktor pendorong globalisasi. Berbagai sektor kehidupan telah memanfaatkan sistem teknologi informasi, seperti penyelenggaraan electronic commerce (e-commerce) dalam sektor perdagangan/bisnis, electronic education (e-education) dalam bidang pendidikan, electronic health (e-health) dalam bidang kesehatan, electronic government (e-government) dalam bidang pemerintahan, serta teknologi informasi yang dimanfaatkan dalam bidang lainnya. Pemanfaatan teknologi informasi tersebut mengakibatkan Data Pribadi seseorang sangat mudah untuk dikumpulkan dan dipindahkan dari satu pihak ke pihak lain tanpa sepengetahuan Subjek Data Pribadi, sehingga mengancam hak konstitusional Subjek Data Pribadi.

Pelindungan data pribadi merupakan bagian integral dari penghormatan terhadap hak asasi manusia. Oleh karena itu, pengaturan mengenai data pribadi adalah wujud dari pengakuan dan perlindungan terhadap hak dasar setiap individu. Keberadaan undang-undang yang mengatur pelindungan data pribadi menjadi suatu kebutuhan yang mendesak dan tidak bisa ditunda, karena memiliki peran penting dalam berbagai kepentingan nasional. Selain itu, dalam konteks hubungan internasional, Indonesia juga dituntut untuk memiliki regulasi pelindungan data pribadi yang memadai. Hal ini akan mempermudah berbagai aktivitas ekonomi, seperti perdagangan, industri, dan investasi yang bersifat lintas negara.

Dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, disebutkan bahwa "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman atau ketakutan untuk melakukan atau tidak melakukan sesuatu yang merupakan hak asasi." Isu terkait pelindungan data pribadi muncul karena adanya kekhawatiran terhadap potensi pelanggaran yang dapat dialami oleh individu atau badan hukum terhadap data pribadi mereka. Pelanggaran ini dapat menyebabkan kerugian baik secara materiil maupun nonmateriil. Oleh karena itu, penting untuk merumuskan peraturan yang mengatur pelindungan data pribadi, guna melindungi hak individu dalam

masyarakat terkait dengan pemrosesan data pribadi, baik yang dilakukan secara elektronik maupun non-elektronik dengan menggunakan perangkat teknologi. Dengan adanya perlindungan yang memadai terhadap data pribadi, masyarakat akan lebih percaya untuk membagikan data mereka untuk berbagai kepentingan yang lebih besar, tanpa khawatir data tersebut akan disalahgunakan atau melanggar hak privasi mereka.

Dengan demikian, pengaturan mengenai pelindungan data pribadi ini bertujuan untuk menciptakan keseimbangan antara hak individu dan kepentingan masyarakat yang diwakili oleh negara. Regulasi ini akan memberikan kontribusi signifikan terhadap terciptanya ketertiban serta kemajuan di tengah masyarakat yang semakin berkembang dalam era informasi. Pelindungan data pribadi yang jelas dan tegas akan memastikan bahwa hak-hak individu terlindungi, sementara kepentingan kolektif juga dapat tercapai secara harmonis.

Untuk menghindari tumpang tindih dalam ketentuan mengenai pelindungan data pribadi, pada dasarnya undang-undang ini menetapkan standar pelindungan data pribadi secara umum, baik yang diproses secara elektronik maupun non-elektronik. Setiap sektor diharapkan dapat menyesuaikan penerapan pelindungan data pribadi sesuai dengan karakteristik masing-masing sektor. Pengaturan mengenai data pribadi ini bertujuan untuk, antara lain, melindungi dan menjamin hak dasar warga negara dalam hal perlindungan data pribadi, memastikan masyarakat mendapatkan layanan yang aman dari korporasi, badan publik, organisasi internasional, dan pemerintah, mendorong perkembangan ekonomi digital serta industri teknologi informasi dan komunikasi, serta mendukung peningkatan daya saing industri nasional.

Dalam Undang Undang Pelindungan Data Pribadi sudah secara eksplisit disebutkan bahwa pelindungan terhadap data pribadi merupakan hak asasi manusia.

E. Glosarium dan Hak Setiap Orang

Dalam pengaturan pelindungan data pribadi yang dimuat dalam Undang Undang Pelindungan Data Pribadi terdapat sejumlah kata kunci

yang perlu diketahui antara lain yaitu :

Pertama, ***Privasi*** adalah hak individu untuk mengontrol informasi pribadi mereka dan melindungi diri dari gangguan yang tidak diinginkan. Privasi mencakup berbagai aspek kehidupan, seperti perlindungan terhadap data pribadi, komunikasi, ruang fisik, dan kebebasan dari pengawasan yang tidak sah. Secara umum, privasi sering dikaitkan dengan hak asasi manusia yang diakui secara universal, seperti dalam Pasal 12 Deklarasi Universal Hak Asasi Manusia (DUHAM) yang menyatakan bahwa tidak seorang pun boleh menjadi sasaran campur tangan sewenang-wenang terhadap privasi, keluarga, rumah, atau korespondensi mereka. Dalam konteks modern, terutama dengan berkembangnya teknologi digital, privasi semakin terkait dengan bagaimana informasi pribadi seseorang (seperti data identitas, riwayat kesehatan, atau perilaku online) dikumpulkan, digunakan, disimpan, dan dibagikan oleh individu, perusahaan, badan publik, atau pemerintah.

Kedua, ***Pelindungan Data Pribadi*** adalah keseluruhan upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak konstitusional subjek Data Pribadi.

Ketiga, **Subjek Data Pribadi** adalah orang perseorangan yang pada dirinya melekat Data Pribadi. Sementara yang dimaksud dengan Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.

Keempat, **Pengendali Data Pribadi** adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi.

Kelima, **Badan Publik** adalah lembaga eksekutif, legislatif, yudikatif, dan badan lain yang fungsi dan tugas pokoknya berkaitan dengan penyelenggaraan negara, yang sebagian atau seluruh dananya bersumber dari Anggaran Pendapatan dan Belanja Negara dan/ atau Anggaran Pendapatan dan Belanja Daerah, atau organisasi nonpemerintah sepanjang sebagian atau seluruh dananya bersumber dari

Anggaran Pendapatan dan Belanja Negara dan/ atau Anggaran . Pendapatan dan Belanja Daerah, sumbangan masyarakat, dan/atau luar negeri.

Keenam, **Jenis Data Pribadi** terdiri atas data pribadi yang bersifat spesifik dan Data Pribadi yang bersifat umum. Data pribadi pribadi yang bersifat spesifik adalah data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi; dan/ atau data lainnya sesuai dengan ketentuan peraturan perundang-undangan. Data Pribadi yang bersifat umum meliputi nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan; dan/ atau Data Pribadi yang dikombinasikan mengidentifikasi seseorang.

Ketujuh, **Hak hak Subjek Data Pribadi** adalah : (a) berhak mendapatkan Informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan Data Pribadi, dan akuntabilitas pihak yang meminta Data Pribadi. (b) berhak melengkapi, memperbarui, dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi tentang dirinya sesuai dengan tujuan pemrosesan Data Pribadi. (c) berhak mendapatkan akses dan memperoleh salinan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan. (d) berhak untuk mengakhiri pemrosesan, menghapus, dan/ atau memusnahkan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan. (e) berhak menarik kembali persetujuan pemrosesan Data Pribadi tentang dirinya yang telah diberikan kepada Pengendali Data Pribadi. (f) berhak untuk mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis, termasuk pemrofilan yang menimbulkan akibat hukum atau berdampak signifikan pada Subjek Data Pribadi. (g) berhak menunda atau membatasi pemrosesan Data Pribadi secara proporsional sesuai dengan tujuan pemrosesan Data Pribadi. (h) berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan. Pemerintah akan menetapkan ketentuan tentang ganti rugi dengan Peraturan Pemerintah. (i) berhak mendapatkan dan/atau menggunakan Data Pribadi tentang dirinya dari Pengendali Data Pribadi dalam bentuk yang sesuai dengan

struktur dan/ atau format yang lazim digunakan atau dapat dibaca oleh sistem elektronik. (j) berhak menggunakan dan mengirimkan Data Pribadi tentang dirinya ke Pengendali Data Pribadi lainnya, sepanjang sistem yang digunakan dapat saling berkomunikasi secara aman sesuai dengan prinsip Pelindungan Data Pribadi berdasarkan Undang-Undang Pelindungan Data Pribadi.

Sepuluh hak subjek data pribadi tersebut apabila diperlukan dapat diajukan melalui permohonan tercatat yang disampaikan secara elektronik atau nonelektronik kepada Pengendali Data Pribadi.

Namun dalam rangka kebutuhan tertentu, sejumlah hak subjek data pribadi dapat dikecualikan yaitu Hak-hak Subjek Data Pribadi hurup (d), hurup (e), hurup (f) hurup (g) hurup (i), dan hurup (j). Pengecualian ini berkaitan dengan kepentingan pertahanan dan keamanan nasional, kepentingan proses penegakan hukum, kepentingan umum dalam rangka penyelenggaraan negara, kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan dalam rangka penyelenggaraan negara, atau kepentingan statistik dan penelitian ilmiah.

Ketentuan pengecualian ini menandakan bahwa negara mempunyai kekuasaan untuk mengecualikan hak-hak subjek data pribadi demi kemaslahatan yang lebih besar.

F. Kewajiban Pengendali Data Pribadi

Pengendali Data Pribadi wajib memiliki dasar pemrosesan Data Pribadi. Dasar pemrosesan dimaksud adalah (1) persetujuan yang sah secara eksplisit dari Subjek Data Pribadi untuk 1 (satu) atau beberapa tujuan tertentu yang telah disampaikan oleh Pengendali Data Pribadi kepada Subjek Data Pribadi. (2) pemenuhan kewajiban perjanjian dalam hal Subjek Data Pribadi merupakan salah satu pihak atau untuk memenuhi permintaan Subjek Data Pribadi pada saat akan melakukan perjanjian. (3) pemenuhan kewajiban hukum dari Pengendali Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan. (4) pemenuhan pelindungan kepentingan vital Subjek Data Pribadi. (5) pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik,

atau pelaksanaan kewenangan Pengendali Data Pribadi berdasarkan peraturan perundang-undangan; dan/atau (6) pemenuhan kepentingan yang sah lainnya dengan memperhatikan tujuan, kebutuhan, dan keseimbangan kepentingan Pengendali Data Pribadi dan hak Subjek Data Pribadi.

Disamping kewajiban tersebut, Pengendali Data Pribadi wajib menghapus Data Pribadi dalam hal (1) Data Pribadi tidak lagi diperlukan untuk pencapaian tujuan pemrosesan Data Pribadi. (2) Subjek Data Pribadi telah melakukan penarikan kembali persetujuan pemrosesan Data Pribadi; (3) terdapat permintaan dari Subjek Data Pribadi; atau (4) Data Pribadi diperoleh dan/ atau diproses dengan cara melawan hukum.

Selain itu Pengendali Data Pribadi wajib memusnahkan Data Pribadi dalam hal (1) telah habis masa retensinya dan berketerangan dimusnahkan berdasarkan jadwal retensi arsip. (2) terdapat permintaan dari Subjek Data Pribadi. (3) tidak berkaitan dengan penyelesaian proses hukum suatu perkara; dan/ atau (4) Data Pribadi diperoleh dan/ atau diproses dengan cara melawan hukum. Pengendali Data Pribadi wajib memberitahukan penghapusan dan/atau pemusnahan Data Pribadi kepada Subjek Data Pribadi.

Apabila terjadi kegagalan Pelindungan Data Pribadi, Pengendali Data Pribadi wajib pemberitahuan secara tertulis paling lambat 3 x 24 (tiga kali dua puluh empat) jam kepada Subjek Data Pribadi dan lembaga yang harus berisi keterangan kapan dan bagaimana Data Pribadi terungkap dan upaya penanganan dan pemulihan atas terungkapnya Data Pribadi oleh Pengendali Data Pribadi. Dalam hal tertentu, Pengendali Data Pribadi wajib memberitahukan kepada masyarakat mengenai kegagalan Pelindungan Data Pribadi.

G. Tentang Undang Undang Pelindungan Data Pribadi

Indonesia telah memiliki aturan tentang pelindungan data pribadi melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). UU ini disahkan pada 17 Oktober 2022 dan menjadi tonggak penting dalam perlindungan hak privasi di Indonesia, khususnya di era digital.

Pokok-Pokok UU PDP

1) **Hak Pemilik Data:**
   - Hak untuk mendapatkan informasi terkait pengelolaan data pribadinya.
   - Hak untuk memberikan persetujuan atas pengumpulan, penggunaan, dan pengungkapan data pribadinya.
   - Hak untuk mencabut persetujuan.
   - Hak untuk mengakses, memperbaiki, atau menghapus data pribadi.

2) **Kewajiban Pengendali Data:**
   - Mengumpulkan dan mengelola data dengan dasar yang sah, seperti persetujuan pemilik data atau kewajiban hukum.
   - Melindungi data pribadi dari akses, penyalahgunaan, atau kebocoran yang tidak sah.
   - Menyediakan mekanisme untuk pemilik data menggunakan hak-haknya.

3) **Sanksi administratif berupa:**
   - Peringatan tertulis;
   - Penghentian sementara kegiatan pemrosesan Data Pribadi;
   - Penghapusan atau pemusnahan Data Pribadi; dan/atau
   - Denda administratif. Sanksi administratif berupa denda administratif paling tinggi 2 (dua) persen dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.

   Penjatuhan sanksi administratif dimaksud diberikan oleh lembaga terkait yang berwenang untuk itu yaitu Pengendali Data Pribadi.

4) **Pidana Penjara**

   Pidana penjara dijatuhkan kepada pelaku tindak pidana baik perorangan maupun korporasi mulai dari 3 tahun hingga hingga 6 tahun bagi yang melanggar prinsip perlindungan data pribadi.

Guna melindungi privasi subjek data pribadi, Undang Undang PDP mengatur pidana tambahan sebagaimana yang dicantumkan dalam Pasal 69 UU PDP "*Selain dijatuhi pidana sebagaimana dimaksud dalam Pasal*

67 dan Pasal 68 juga dapat dijatuhi pidana tambahan berupa perampasan keuntungan dan/ atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian"

Dalam konteks Internasional, undang undang Pelindungan Data Pribadi dirancang untuk selaras dengan regulasi global seperti *General Data Protection Regulation (GDPR)* di Uni Eropa, sehingga memudahkan kerjasama lintas negara dalam melindungi data pribadi. Penulis amati pasal-pasal dalam UU PDP hampir 100% sama dengan norma di dalam *General Data Protection Regulation* milik Uni Eropa.

Rancangan UU di lingkungan teknologi informasi pada era globalisasi mau tidak mau harus selaras dan memperhatikan keselarasan global, karena implementasi dari pelindungan data pribadi bersifat multinasional. Demikian halnya beberapa undang undang yang terkait dengan masalah ini seperti undang undang telekomunikasi dan undang undang Informasi dan Transaksi Elektronik.

Tantangan UU PDP terdapat di beberapa aspek, meskipun aspek *legal substance*-nya sudah cukup memadai, namun Indonesia masih membutuhkan langkah-langkah lanjutan yang membutuhkan upaya besar antara lain menyangkut kelembagaan, dan budaya masyarakat yang masih kurang dalam literasi digital

Setidaknya ada dua isu penting yang harus diatasi lebih dahulu yaitu pertama, kurangnya literasi digital di masyarakat dan kedua kemampuan perusahaan dan instansi pemerintah untuk mematuhi standar keamanan data. Kasus gangguan Pusat Data Nasional yang dialami Indonesia di tahun 2024 salah satu contoh betapa rapuhnya pengamanan data di Indonesia, bahkan pada lembaga milik Pemerintah.

H. Penutup

Penggunaan teknologi informasi untuk menunjang kelancaran kegiatan kehidupan sehari-hari, dalam rangka efisiensi, kemudahan dan optimalisasi manfaatnya sudah suatu keniscayaan zaman. Pemerintah selaku pelindung rakyat sudah menunjukan keseriusan dalam mengadaptasi perkembangan zaman tersebut dengan cara memberikan pengakuan terhadap hak privasi sebagai hak asasi manusia dan

ditindaklanjuti dengan upaya memberikan kepastian hukum terhadap warga negara Indonesia dan warga negara manapun yang ada di Indonesia terkait dengan aktivitas di dunia digital dengan cara memberlakukan Undang Undang Pelindungan Data Pribadi. Pengakuan hak privasi sebagai hak asasi manusia memberikan efek sangat penting bagi kepercayaan masyarakat dalam memanfaatkan teknologi informasi.

Laju perkembangan teknologi ke depan akan semakin cepat. Isu Pelindungan data pribadi sebagai hak asasi manusia baru mulai memanas namun umat manusia sudah dihadapkan oleh tantangan baru yang lebih "mengerikan" dengan hadirnya *Artificial Intelligence* (Kecerdasan Buatan). Para ahli meramalkan mungkin saja suatu saat nanti Kecerdasan Buatan itu mampu bertindak secara otonom di luar kendali manusia. Yuval Noah Harari (2018) mengatakan :

> *The danger is that if we invest too much in developing AI and too little in developing human consciousness, the very sophisticated artificial intelligence of computer might only serve to empower the natural stupidity of humans. We are unlikely to face a robot rebellion in the coming decades, but we might have to deal with hordes of bots who know how to press our emotional buttons better than our mother, and use this uncanny ability to try and sell us something- be it a car, a politician, or an entire ideology. The bots could identify our deepest fears, hatreds and cravings, and use these inner leverages against us".*

Melalui bantuan AI kata-kata Yuval Noah Penulis terjemahkan sebagai berikut *:*

> *"Bahaya yang muncul adalah jika kita terlalu banyak berinvestasi dalam pengembangan AI dan terlalu sedikit dalam mengembangkan kesadaran manusia, maka kecerdasan buatan yang sangat canggih dari komputer mungkin hanya akan memperkuat kebodohan alami manusia. Dalam beberapa dekade mendatang, kita mungkin tidak akan menghadapi pemberontakan robot, tetapi kita mungkin harus berurusan dengan kawanan bot yang tahu cara menekan tombol emosional kita lebih baik daripada ibu kita, dan menggunakan kemampuan luar biasa ini untuk mencoba menjual sesuatu kepada kita—baik itu mobil, seorang politisi, atau seluruh ideologi. Bot-bot tersebut dapat mengidentifikasi ketakutan, kebencian, dan hasrat terdalam kita, lalu menggunakan pengaruh batin ini untuk melawan kita."*

Dalam menulis artikel ini Penulis mengalami interaksi unik dengan

AI yang dapat Penulis rasakan sepertinya AI memiliki semacam emosi. Penulis mengatakan sesuatu yang kemudian disangkal oleh AI. Penulis katakan *"Uni Eropa dengan kemajuan ilmu pengetahuan, teknologi dan ekonominya dapat "memaksakan" negara-negara berkembang untuk membuat Undang Undang Pelindungan Data Pribadi"*. Penulis agak terkejut ketika AI merespon dan keberatan atas penggunaan kata "memaksakan" itu.

Kemajuan AI ini semakin cepat setiap hari, sehingga para pakar hukum dan pakar AI mengusulkan agar segera dihadirkan Hukum Kecerdasan Buatan. *Weldell Wallach* ahli etika kecerdasan buatan (2019) dalam Danrivanto (2024) bahwa

> *"hukum harus mampu menentukan siapa/subjek yang bertanggung jawab ketika terjadi kegagalan atau kerugian akibat sistem kecerdasan buatan. Perlunya akuntabilitas hukum yang mampu mendorong pengembang dan pengguna untuk bertanggung jawab atas tindakan dan keputusan yang dihasilkan oleh kecerdasan buatan. Stuart Russel* juga menegaskan "*perlunya fungsi hukum yang memastikan bahwa sistem kecerdasan buatan bekerja sesuai dengan nilai-nilai kemanusiaan dan meminimalkan risiko potensi yang mungkin ditimbulkannya"*.

I. Referensi

Artikel jurnal

Hanifan, Niffari (2020), *Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia tas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-undangan Di Negara Lain)*, Jurnal Yuridis Vol. 7 No. 1, Juni 2020: 105 - 119

Buku

Budijanto, Danrivanto, (2024) *Revolusi Cyberlaw di Indonesia,* Refika Aditama

Harari, Yuval Noah, (2018) *Homo Deus Masa Depan Umat Manusia*, Pustaka Alvabet

Situs Web.

Harari, Yuval Noah (2018) *Summary: 21 Lessons for the 21st Century, https://www.goodreads.com/book/show/41843445-summary?ref=rae_1*

https://aptika.kominfo.go.id/2022/09/rapat-paripurna-dpr-sahkan-ruu-pdp/#:~:text=Jakarta%2C%20Ditjen%20Aptika%20%E2%80%

93%20Rancangan%20Undang,20%2F9%2F2022).

https://wikidpr.org/rangkuman/komisi1-panja-tim-pemerintah-ruu-pdp

https://www.ohchr.org/en/human-rights/universal-declaration/translations/english

https://gdpr-info.eu/

Perundang-undangan

Undang Undang Dasar 1945 (asli)

Undang Undang Dasar Negara Republik Indonesia Tahun 1945 (Perubahan)

Tap MPR Nomor XVII/MPR/1998 tentang Hak Asasi Manusia

Undang Undang Nomor 9 Tahun 1998 Tentang Kemerdekaan Menyampaikan Pendapat di Muka Umum

Undang Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia

Undang Undang Nomor 26 Tahun 2000 tentang Peradilan Hak Asasi Manusia

Undang Undang Nomor 24 Tahun 2013 Tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan

Undang Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Undang Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

General Data Protection Regulation,(EU Directive 95/46/EC)

Perserikatan Banga Bangsa, *The Universal Declaration of Human Right*

BAB 5

PERAN DAN TANGGUNG JAWAB PERUSAHAAN DALAM PERLINDUNGAN DATA

Rizki Syafril, S.H.I, M.Si.

(Universitas Negeri Padang**)**

A. Pendahuluan

Perusahaan memiliki tanggung jawab yang sangat besar dalam menjaga dan melindungi data pribadi yang mereka kelola (Indra, G, dkk 2024). Dengan diberlakukannya Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia, perusahaan dituntut untuk memastikan bahwa setiap data pribadi yang mereka kumpulkan, simpan, dan gunakan dilindungi dengan standar keamanan yang tinggi. Perlindungan ini mencakup berbagai aspek, mulai dari proses pengumpulan data yang transparan, penyimpanan data yang aman, hingga penggunaan data yang sesuai dengan izin yang diberikan oleh pemilik data.

Selain itu, perusahaan juga harus mematuhi semua regulasi yang ditetapkan oleh UU PDP. Ini berarti perusahaan harus memiliki kebijakan dan prosedur yang jelas dan terstruktur terkait perlindungan data pribadi (Javed, Y., & Sajid, A. 2024). Kebijakan ini harus mencakup langkah-langkah preventif untuk mencegah kebocoran data, serta prosedur penanganan insiden jika terjadi pelanggaran data. Perusahaan juga diwajibkan untuk melakukan audit secara berkala untuk memastikan bahwa semua proses pengelolaan data sesuai dengan standar yang ditetapkan oleh UU PDP. Audit ini penting untuk mengidentifikasi dan memperbaiki potensi kelemahan dalam sistem perlindungan data perusahaan.

Dengan menjalankan peran dan tanggung jawab ini, perusahaan tidak hanya mematuhi regulasi yang berlaku, tetapi juga membangun kepercayaan dari konsumen dan mitra bisnis. Perlindungan data pribadi yang baik akan meningkatkan reputasi perusahaan di mata publik dan

memberikan rasa aman kepada konsumen bahwa data mereka dikelola dengan baik dan aman (Prastyanti*, R., & Sharma, R. 2024). Kepercayaan ini sangat penting dalam era digital saat ini, di mana data pribadi menjadi aset yang sangat berharga dan rentan terhadap penyalahgunaan. Dengan demikian, perusahaan yang mampu menjaga dan melindungi data pribadi dengan baik akan memiliki keunggulan kompetitif yang signifikan.

B. Kewajiban Perusahaan untuk Mengamankan Data Pribadi

Perusahaan memiliki tanggung jawab besar dalam menjaga keamanan data pribadi yang mereka kelola. Tanggung jawab ini mencakup berbagai aspek penting, mulai dari penerapan kebijakan dan prosedur yang ketat hingga edukasi dan pelatihan karyawan (Peltier, T. 2005). Setiap perusahaan harus memiliki kebijakan yang jelas dan prosedur yang terstruktur untuk melindungi data pribadi dari akses yang tidak sah, penyalahgunaan, dan pencurian. Kebijakan ini harus mencakup langkah-langkah preventif yang efektif serta prosedur penanganan insiden jika terjadi pelanggaran data. Berikut adalah kewajiban utama yang harus diemban oleh perusahaan dalam melindungi data pribadi:

Penunjukan Data Protection Officer (DPO) merupakan langkah krusial bagi perusahaan yang mengelola data pribadi dalam jumlah besar (Šidlauskas, A. 2021). Perusahaan diwajibkan untuk menunjuk seorang DPO yang memiliki tanggung jawab utama dalam memastikan kepatuhan perusahaan terhadap semua regulasi yang berkaitan dengan perlindungan data pribadi. DPO harus memiliki pemahaman mendalam tentang undang-undang dan peraturan yang berlaku, serta mampu mengimplementasikan kebijakan dan prosedur yang efektif untuk melindungi data pribadi.

Selain itu, DPO juga bertanggung jawab untuk memberikan pelatihan dan edukasi kepada karyawan mengenai pentingnya perlindungan data pribadi. Pelatihan ini bertujuan untuk meningkatkan kesadaran dan pemahaman karyawan tentang risiko dan tanggung jawab mereka dalam mengelola data pribadi. Dengan demikian, setiap karyawan dapat berkontribusi dalam menjaga keamanan data dan

meminimalkan risiko pelanggaran.

DPO juga berperan sebagai penghubung antara perusahaan dan otoritas perlindungan data. Dalam hal terjadi insiden atau pelanggaran data, DPO harus siap untuk berkomunikasi dengan otoritas terkait, melaporkan insiden tersebut, dan bekerja sama dalam investigasi. Peran ini sangat penting untuk memastikan bahwa perusahaan dapat merespons dengan cepat dan efektif terhadap setiap ancaman terhadap data pribadi, serta menjaga kepercayaan dari konsumen dan mitra bisnis.

Kepatuhan terhadap regulasi merupakan aspek yang sangat penting dalam pengelolaan data pribadi oleh perusahaan. Perusahaan harus memastikan bahwa setiap tahap dalam proses pengelolaan data pribadi, mulai dari pengumpulan, penyimpanan, hingga penggunaan data, dilakukan sesuai dengan aturan dan regulasi yang berlaku (Oreščanin, dkk 2024). Hal ini mencakup penerapan kebijakan dan prosedur yang ketat untuk memastikan bahwa data pribadi dilindungi dari penyalahgunaan, pencurian, dan akses yang tidak sah.

Selain itu, perusahaan harus melakukan evaluasi dan audit secara berkala untuk memastikan bahwa semua praktik pengelolaan data tetap sesuai dengan standar yang ditetapkan oleh regulasi. Audit ini penting untuk mengidentifikasi potensi kelemahan dalam sistem perlindungan data dan mengambil langkah-langkah perbaikan yang diperlukan (Pasquier, T., dkk 2017). Dengan demikian, perusahaan dapat meminimalkan risiko pelanggaran data dan memastikan bahwa data pribadi tetap aman.

Perusahaan juga harus memberikan pelatihan dan edukasi kepada karyawan mengenai pentingnya kepatuhan terhadap regulasi perlindungan data. Karyawan harus memahami tanggung jawab mereka dalam menjaga keamanan data pribadi dan bagaimana mereka dapat berkontribusi dalam mematuhi regulasi yang berlaku. Dengan kepatuhan yang baik terhadap regulasi, perusahaan tidak hanya melindungi data pribadi, tetapi juga membangun kepercayaan dari konsumen dan mitra bisnis.

Edukasi dan pelatihan merupakan salah satu peran penting yang harus dijalankan oleh perusahaan dalam upaya melindungi data pribadi.

Perusahaan harus mengedukasi seluruh staf mengenai pentingnya perlindungan data pribadi dan memberikan pemahaman yang mendalam tentang risiko yang terkait dengan penyalahgunaan data (Popescu, M., dkk 2024). Melalui program edukasi yang komprehensif, karyawan dapat memahami betapa pentingnya menjaga kerahasiaan dan integritas data pribadi yang mereka kelola.

Selain itu, perusahaan harus menyelenggarakan pelatihan rutin untuk memastikan bahwa karyawan selalu up-to-date dengan kebijakan dan prosedur terbaru terkait perlindungan data. Pelatihan ini harus mencakup berbagai aspek, mulai dari cara mengidentifikasi potensi ancaman terhadap data, langkah-langkah yang harus diambil untuk mencegah kebocoran data, hingga prosedur yang harus diikuti jika terjadi insiden pelanggaran data. Dengan demikian, karyawan akan memiliki keterampilan dan pengetahuan yang diperlukan untuk menjaga keamanan data pribadi.

Dengan edukasi dan pelatihan yang efektif, perusahaan dapat membangun budaya kesadaran akan pentingnya perlindungan data di seluruh organisasi. Setiap karyawan akan merasa bertanggung jawab dan berperan aktif dalam menjaga keamanan data pribadi. Hal ini tidak hanya membantu perusahaan dalam mematuhi regulasi yang berlaku, tetapi juga meningkatkan kepercayaan konsumen dan mitra bisnis terhadap komitmen perusahaan dalam melindungi data pribadi mereka.

Transparansi dengan pemilik data merupakan aspek krusial dalam manajemen perlindungan data pribadi. Dalam hal terjadi pelanggaran data, perusahaan memiliki kewajiban untuk bersikap transparan dengan individu yang datanya terpengaruh (Bonatti, P., dkk 2017). Ini berarti perusahaan harus segera menginformasikan kepada pemilik data mengenai insiden pelanggaran yang terjadi, termasuk jenis data yang terpengaruh dan potensi risiko yang mungkin timbul akibat pelanggaran tersebut.

Selain itu, perusahaan harus mampu menyampaikan informasi secara jelas dan rinci mengenai langkah-langkah yang telah diambil untuk memperbaiki situasi tersebut. Ini mencakup tindakan segera yang dilakukan untuk menghentikan pelanggaran, upaya pemulihan data, serta langkah-langkah preventif yang akan diterapkan untuk mencegah

kejadian serupa di masa depan. Dengan memberikan informasi yang transparan dan akurat, perusahaan dapat membantu pemilik data memahami situasi dan mengambil tindakan yang diperlukan untuk melindungi diri mereka.

Transparansi ini tidak hanya penting untuk mematuhi regulasi yang berlaku, tetapi juga untuk membangun dan mempertahankan kepercayaan dari konsumen dan mitra bisnis. Ketika perusahaan bersikap terbuka dan jujur dalam menangani pelanggaran data, mereka menunjukkan komitmen mereka terhadap perlindungan data pribadi dan tanggung jawab mereka terhadap pemilik data. Hal ini akan meningkatkan reputasi perusahaan dan memberikan rasa aman kepada konsumen bahwa data mereka dikelola dengan baik dan dilindungi dengan serius.

Audit dan pengawasan merupakan elemen penting dalam menjaga keamanan data pribadi yang dikelola oleh perusahaan. Perusahaan harus secara rutin melakukan audit internal yang menyeluruh terhadap kebijakan dan praktik pengelolaan data mereka (Alexandrova, N. 2021). Audit ini bertujuan untuk mengidentifikasi dan menutup setiap celah atau kelemahan dalam sistem perlindungan data yang dapat dimanfaatkan oleh pihak luar yang tidak bertanggung jawab.

Selain itu, audit internal harus mencakup peninjauan terhadap semua prosedur dan mekanisme yang digunakan dalam pengelolaan data pribadi, mulai dari proses pengumpulan, penyimpanan, hingga penggunaan data. Dengan melakukan audit secara berkala, perusahaan dapat memastikan bahwa semua kebijakan dan praktik yang diterapkan sesuai dengan standar keamanan yang ditetapkan oleh regulasi yang berlaku. Audit ini juga membantu perusahaan dalam mengidentifikasi potensi risiko dan mengambil langkah-langkah preventif untuk mencegah terjadinya pelanggaran data.

Pengawasan yang ketat dan berkelanjutan juga diperlukan untuk memastikan bahwa setiap perubahan dalam kebijakan atau teknologi yang digunakan dalam pengelolaan data pribadi tidak menimbulkan risiko baru (Holovatskiy, N. 2024). Dengan demikian, perusahaan dapat terus memperbarui dan meningkatkan sistem perlindungan data mereka, menjaga kepercayaan konsumen, dan memastikan bahwa data pribadi

yang mereka kelola tetap aman dan terlindungi dari ancaman yang mungkin timbul.

Dengan melaksanakan peran dan tanggung jawab ini, perusahaan tidak hanya memastikan kepatuhan terhadap peraturan yang berlaku, tetapi juga secara proaktif membangun dan memperkuat kepercayaan dari konsumen serta mitra bisnis. Kepatuhan terhadap regulasi menunjukkan komitmen perusahaan dalam menjaga integritas dan keamanan data pribadi, yang pada akhirnya memberikan rasa aman kepada konsumen bahwa data mereka dikelola dengan baik dan dilindungi dari potensi penyalahgunaan.

Selain itu, perlindungan data pribadi yang efektif akan secara signifikan meningkatkan reputasi perusahaan di mata publik. Konsumen akan merasa lebih percaya dan nyaman berinteraksi dengan perusahaan yang menunjukkan tanggung jawab tinggi dalam mengelola data pribadi mereka. Kepercayaan ini sangat penting dalam membangun hubungan jangka panjang yang positif dengan konsumen dan mitra bisnis, yang pada akhirnya dapat mendukung pertumbuhan dan keberlanjutan perusahaan.

Dengan demikian, perusahaan yang mampu menjalankan peran dan tanggung jawabnya dalam perlindungan data pribadi tidak hanya memenuhi kewajiban hukum, tetapi juga memperoleh keuntungan kompetitif yang berharga. Mereka akan dikenal sebagai entitas yang dapat diandalkan dan bertanggung jawab, yang menghargai privasi dan keamanan data konsumen, sehingga menciptakan lingkungan bisnis yang lebih aman dan terpercaya.

C. Kebijakan Keamanan Data di Perusahaan

Kebijakan keamanan data di perusahaan merupakan kumpulan aturan dan prosedur yang dirancang secara khusus untuk melindungi data pribadi serta informasi sensitif dari berbagai ancaman, termasuk akses yang tidak sah, penyalahgunaan, dan pencurian (Pant, A. 2023). Kebijakan ini mencakup berbagai aspek penting yang harus diperhatikan oleh perusahaan untuk memastikan bahwa data yang mereka kelola tetap aman dan terlindungi.

Pertama, kebijakan ini harus mencakup langkah-langkah preventif yang efektif untuk mencegah akses yang tidak sah ke data pribadi (Blikhar, M. 2024). Ini termasuk penggunaan teknologi enkripsi, kontrol akses yang ketat, dan sistem keamanan jaringan yang canggih. Selain itu, kebijakan harus mengatur bagaimana data pribadi dikumpulkan, disimpan, dan digunakan, memastikan bahwa setiap tahap dalam pengelolaan data dilakukan dengan standar keamanan yang tinggi.

Kedua, kebijakan keamanan data harus mencakup program edukasi dan pelatihan bagi karyawan. Karyawan harus diberikan pemahaman yang mendalam tentang pentingnya perlindungan data pribadi dan dilatih untuk mengenali serta mengatasi potensi ancaman terhadap keamanan data (Subramanian, S., 2020). Dengan demikian, setiap karyawan dapat berkontribusi dalam menjaga keamanan data dan memastikan bahwa data pribadi yang dikelola oleh perusahaan tetap terlindungi.

Terakhir, kebijakan ini harus mencakup prosedur penanganan insiden yang jelas dan terstruktur (Kosinski, J., dkk, 2019). Dalam hal terjadi pelanggaran data, perusahaan harus memiliki rencana tanggap darurat yang efektif untuk mengatasi insiden tersebut, melaporkan pelanggaran kepada otoritas yang berwenang, dan menginformasikan pemilik data yang terpengaruh. Dengan menerapkan kebijakan keamanan data yang komprehensif, perusahaan dapat memastikan bahwa data pribadi yang mereka kelola tetap aman dan terlindungi, serta membangun kepercayaan dari konsumen dan mitra bisnis.

D. Sanksi dan Tanggung Jawab Hukum atas Pelanggaran Data

Sanksi dan tanggung jawab hukum atas pelanggaran data pribadi merupakan komponen penting dalam upaya perlindungan data. Di Indonesia, Undang-Undang Perlindungan Data Pribadi (UU PDP) menetapkan berbagai sanksi yang dapat dikenakan kepada perusahaan atau individu yang melanggar ketentuan terkait pengelolaan data pribadi (Simbolon, V., & Juwono, V., 2022). Sanksi ini dirancang untuk memastikan bahwa setiap entitas yang mengelola data pribadi mematuhi standar keamanan yang ditetapkan dan bertanggung jawab atas setiap pelanggaran yang terjadi.

Pertama, Sanksi administratif yang diatur dalam UU Perlindungan Data Pribadi (UU PDP) mencakup berbagai tindakan yang dapat dikenakan kepada pelanggar untuk memastikan kepatuhan terhadap regulasi (De Oliveira, K., 2024). Sanksi ini meliputi peringatan tertulis yang diberikan kepada perusahaan atau individu yang melanggar ketentuan pengelolaan data pribadi. Selain itu, UU PDP juga memungkinkan penghentian sementara kegiatan pemrosesan data pribadi sebagai langkah untuk mencegah pelanggaran lebih lanjut.

Lebih lanjut, sanksi administratif dapat mencakup penghapusan atau pemusnahan data pribadi yang telah dikumpulkan atau diproses secara tidak sah. Tindakan ini bertujuan untuk menghilangkan risiko penyalahgunaan data yang telah terlanjur dikumpulkan. Selain itu, UU PDP menetapkan denda administratif yang signifikan, yang dapat mencapai dua persen dari pendapatan tahunan atau penerimaan perusahaan. Denda ini dirancang untuk memberikan efek jera dan mendorong perusahaan lebih berhati-hati dalam mengelola data pribadi.

Dengan adanya sanksi administratif ini, diharapkan perusahaan dan individu lebih mematuhi regulasi yang berlaku dan mengambil langkah-langkah yang diperlukan untuk melindungi data pribadi. Sanksi ini tidak hanya berfungsi sebagai hukuman bagi pelanggar, tetapi juga sebagai mekanisme untuk meningkatkan kesadaran dan tanggung jawab dalam pengelolaan data pribadi.

Kedua, Sanksi perdata memberikan hak kepada pemilik data pribadi yang dirugikan akibat pelanggaran data untuk mengajukan gugatan perdata guna mendapatkan ganti rugi (Savelyev, A., 2021). Hal ini diatur dalam Pasal 12 Undang-Undang Perlindungan Data Pribadi (UU PDP), yang secara eksplisit memberikan hak kepada subjek data pribadi untuk menggugat pihak yang bertanggung jawab atas pelanggaran pemrosesan data pribadi. Gugatan ini dapat diajukan jika pemilik data merasa bahwa data pribadi mereka telah disalahgunakan, diakses tanpa izin, atau diproses dengan cara yang melanggar ketentuan yang berlaku.

Dalam proses gugatan perdata, pemilik data pribadi dapat menuntut kompensasi atas kerugian yang mereka alami akibat

pelanggaran tersebut. Kompensasi ini dapat mencakup kerugian materiil, seperti biaya yang dikeluarkan untuk mengatasi dampak pelanggaran, serta kerugian immateriil, seperti stres atau kerugian reputasi yang dialami oleh pemilik data. Dengan adanya mekanisme gugatan perdata ini, diharapkan perusahaan lebih berhati-hati dalam mengelola data pribadi dan mematuhi semua regulasi yang berlaku.

Selain memberikan perlindungan tambahan bagi individu, sanksi perdata juga berfungsi sebagai pendorong bagi perusahaan untuk meningkatkan praktik perlindungan data mereka. Dengan mengetahui bahwa mereka dapat digugat dan diwajibkan membayar kompensasi, perusahaan akan lebih termotivasi untuk memastikan bahwa data pribadi yang mereka kelola dilindungi dengan baik dan sesuai dengan standar yang ditetapkan oleh UU PDP.

Ketiga, Sanksi pidana merupakan salah satu bentuk hukuman yang dapat dikenakan atas pelanggaran data pribadi, selain sanksi administratif dan perdata. Pelanggaran data pribadi yang serius, seperti pencurian atau penyalahgunaan data pribadi, dapat berujung pada hukuman pidana bagi pelaku yang terbukti bersalah (Hawkes, N., 2015). Hukuman pidana ini diatur sesuai dengan ketentuan yang berlaku dalam Undang-Undang Perlindungan Data Pribadi (UU PDP) dan peraturan terkait lainnya.

Pelaku yang terbukti melakukan pelanggaran serius terhadap data pribadi dapat dikenakan berbagai bentuk hukuman pidana, termasuk denda yang signifikan dan/atau hukuman penjara. Hukuman ini bertujuan untuk memberikan efek jera kepada pelaku dan mencegah terjadinya pelanggaran serupa di masa depan. Selain itu, hukuman pidana juga berfungsi untuk menegakkan keadilan bagi korban pelanggaran data pribadi, memastikan bahwa pelaku bertanggung jawab atas tindakan mereka.

Dengan adanya sanksi pidana, diharapkan perusahaan dan individu lebih berhati-hati dalam mengelola data pribadi dan mematuhi semua regulasi yang berlaku. Hukuman pidana ini menegaskan pentingnya perlindungan data pribadi dan menunjukkan bahwa pelanggaran terhadap data pribadi tidak akan ditoleransi. Hal ini juga membantu menciptakan lingkungan yang lebih aman dan terpercaya bagi

semua pihak yang terlibat dalam pengelolaan data pribadi.

Diberlakukannya sanksi dan tanggung jawab hukum yang ketat, diharapkan perusahaan dan individu akan lebih berhati-hati dalam mengelola data pribadi. Penerapan sanksi administratif, perdata, dan pidana memberikan insentif kuat bagi semua pihak untuk mematuhi regulasi yang berlaku dan mengadopsi praktik terbaik dalam perlindungan data (Nitayanti, N., & Griadhi, N., 2014). Langkah ini tidak hanya membantu mencegah pelanggaran data, tetapi juga menciptakan lingkungan yang lebih aman dan terpercaya bagi semua pihak yang terlibat dalam pengelolaan data pribadi.

Perusahaan akan lebih terdorong untuk menerapkan kebijakan dan prosedur yang ketat, melakukan audit rutin, serta memberikan pelatihan kepada karyawan mengenai pentingnya perlindungan data pribadi. Di sisi lain, individu akan lebih sadar akan hak-hak mereka dan lebih proaktif dalam melindungi data pribadi mereka. Dengan demikian, kolaborasi antara perusahaan dan individu dalam menjaga keamanan data dapat terjalin dengan baik dan efektif.

Pada akhirnya, penerapan sanksi dan tanggung jawab hukum ini akan meningkatkan kepercayaan publik terhadap sistem perlindungan data yang ada. Konsumen dan mitra bisnis akan merasa lebih aman dan nyaman berinteraksi dengan perusahaan yang menunjukkan komitmen tinggi dalam menjaga data pribadi. Lingkungan yang aman dan terpercaya ini akan mendukung pertumbuhan dan keberlanjutan bisnis, serta meningkatkan reputasi perusahaan di mata publik.

E. Kesimpulan

Peran dan tanggung jawab perusahaan dalam perlindungan data pribadi sangat erat kaitannya dengan hukum administrasi negara. Hukum administrasi negara menetapkan aturan dan pedoman yang harus diikuti oleh perusahaan dalam mengelola data pribadi, termasuk kepatuhan terhadap regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP). Regulasi ini mengharuskan perusahaan untuk bertindak transparan dan akuntabel dalam setiap aspek pengelolaan data pribadi, mulai dari pengumpulan, penyimpanan, hingga penggunaan data.

Perusahaan juga diwajibkan untuk bertanggung jawab atas setiap pelanggaran yang terjadi, dengan mengambil langkah-langkah yang diperlukan untuk memperbaiki situasi dan mencegah terulangnya pelanggaran serupa di masa depan. Hukum administrasi negara mengatur berbagai sanksi, baik administratif, perdata, maupun pidana, yang dapat dikenakan kepada perusahaan yang melanggar ketentuan perlindungan data pribadi. Sanksi ini bertujuan untuk memastikan bahwa perusahaan mematuhi regulasi yang berlaku dan melindungi data pribadi dengan baik.

Dengan demikian, hukum administrasi negara memberikan kerangka kerja yang jelas dan tegas bagi perusahaan untuk mengelola data pribadi secara aman dan bertanggung jawab. Kepatuhan terhadap regulasi ini tidak hanya melindungi hak-hak pemilik data, tetapi juga membangun kepercayaan dari konsumen dan mitra bisnis, serta meningkatkan reputasi perusahaan di mata publik. Hal ini sangat penting dalam era digital saat ini, di mana data pribadi menjadi aset yang sangat berharga dan rentan terhadap penyalahgunaan.

F. Referensi

Indra, G., Suryandari, W., & Tohari, M. (2024). Legal Obligations by Companies in Mitigating the Risks of Sustainable Digital Innovation. International Journal of Sociology and Law. https://doi.org/10.62951/ijsl.v1i4.179.

Javed, Y., & Sajid, A. (2024). A Systematic Review of Privacy Policy Literature. ACM Computing Surveys. https://doi.org/10.1145/3698393.

Prastyanti*, R., & Sharma, R. (2024). Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India. Journal of Human Rights, Culture and Legal System. https://doi.org/10.53955/jhcls.v4i2.200.

Peltier, T. (2005). Implementing an Information Security Awareness Program. Information Systems Security, 14, 37 - 49. https://doi.org/10.1201/1086/45241.14.2.20050501/88292.6.

Šidlauskas, A. (2021). The Role and Significance of the Data Protection Officer in the Organization. , 44, 8-28.

https://doi.org/10.15388/SOCTYR.44.1.1.

Oreščanin, D., Hlupić, T., & Vrdoljak, B. (2024). Managing Personal Identifiable Information in Data Lakes. IEEE Access, 12, 32164-32180. https://doi.org/10.1109/ACCESS.2024.3365042.

Pasquier, T., Singh, J., Powles, J., Eyers, D., Seltzer, M., & Bacon, J. (2017). Data provenance to audit compliance with privacy policy in the Internet of Things. Personal and Ubiquitous Computing, 22, 333 - 344. https://doi.org/10.1007/s00779-017-1067-4.

Popescu, M., Barbu, A., Simion, P., & Moiceanu, G. (2024). Research on Data Security Measures in Romania. Proceedings of the International Conference on Business Excellence, 18, 3277 - 3283. https://doi.org/10.2478/picbe-2024-0267.

Bonatti, P., Kirrane, S., Polleres, A., & Wenning, R. (2017). Transparent Personal Data Processing: The Road Ahead. , 337-349. https://doi.org/10.1007/978-3-319- 66284-8_28.

Alexandrova, N. (2021). Personal Data Protection And Internal Audit. Protection Of The Personal Data And The Digitalization - Challenges And Perspectives 2021 Conference Proceedings. https://doi.org/10.36997/ppdd2021.146.

Holovatskiy, N. (2024). Issues of personal data protection when using cloud technologies. Analytical and Comparative Jurisprudence. https://doi.org/10.24144/2788-6018.2024.05.72.

Pant, A. (2023). Importance of Data Security and Privacy Compliance. International Journal for Research in Applied Science and Engineering Technology. https://doi.org/10.22214/ijraset.2023.56862.

Blikhar, M. (2024). Legal regulation of personal data protection. Visnik Nacional'nogo universitetu «Lvivska politehnika». Seria: Uridicni nauki. https://doi.org/10.23939/law2024.41.026.

Subramanian, S. (2020). Nudging Our Way to Successful Information Security Awareness. .

Simbolon, V., & Juwono, V. (2022). Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation. Publik (Jurnal Ilmu Administrasi). https://doi.org/10.31314/pjia.11.2.178-190.2022.

De Oliveira, K. (2024). Formação de jurisprudência administrativa pela ANPD: estudo de casos das sanções aplicadas. Revista Digital de Direito Administrativo. https://doi.org/10.11606/issn.2319-0558.v11i2p89-109.

Savelyev, A. (2021). Civil Law Aspects Of Commercialization Of Personal Data. Civil Law Review. https://doi.org/10.24031/1992-2043-2021-21-4-104-129.

Hawkes, N. (2015). Tougher penalties, including imprisonment, are urged for misuse of personal data. BMJ : British Medical Journal, 350. https://doi.org/10.1136/bmj.h619.

Nitayanti, N., & Griadhi, N. (2014). Perlindungan Hukum Terhadap Informasi Pribadi Terkait Privacy Right Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. , 2.

BAB 6

PERLINDUNGAN DATA PRIBADI DALAM TRANSAKSI E-COMMERCE

Dr. Ma'rifah, S.H., M.H.

(Sekolah Tinggi Ilmu Hukum Sultan Adam)

A. Pendahuluan

Perlindungan data pribadi merupakan bagian dari hak konstitusional setiap individu. Jaminan perlindungan terhadap data pribadi warga negara Indonesia diatur dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, tepatnya dalam Pasal 28G Ayat (1), yang menyatakan bahwa setiap orang berhak atas perlindungan terhadap diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya, serta berhak merasakan rasa aman dan perlindungan dari ancaman atau ketakutan dalam berbuat atau tidak berbuat sesuatu yang merupakan hak asasi. Hak atas privasi juga diakui dan dilindungi melalui perjanjian hukum internasional sebagai hak asasi manusia. Mahkamah Konstitusi dalam Putusan Nomor 20/PUU-XIV/2016 menegaskan pentingnya hak atas privasi sebagai bagian dari perlindungan data pribadi. Dalam Putusan Nomor 5/PUU-VIII/2011, Mahkamah Konstitusi juga menggarisbawahi bahwa perlindungan data dan privasi adalah dua konsep yang berbeda, meskipun keduanya saling terkait. Hak atas perlindungan data pribadi dilihat sebagai bagian dari hak asasi manusia yang lebih luas, yang mencakup hak privasi, termasuk di dalamnya privasi informasi dan privasi data.

Menurut Asosiasi Penyelenggara Jasa Internet Indonesia (APJII, 2024), jumlah pengguna internet di Indonesia mencapai 221,5 juta pada tahun 2024, atau 79,5% dari total populasi. Ini menunjukkan peningkatan penetrasi internet sebesar 1,4% dibandingkan tahun sebelumnya, dengan tren positif yang konsisten dalam lima tahun terakhir. Penetrasi internet Indonesia terus meningkat sejak 2018, dari

64,8% menjadi 78,19% pada 2023. Dalam konteks e-commerce, perlindungan data pribadi konsumen sangat krusial untuk mencegah penyalahgunaan informasi dan mengurangi risiko keamanan, seperti pencurian identitas, penipuan, spamming, dan serangan phishing

E-Commerce merupakan salah satu sektor perdagangan tanpa kontak tatap muka dan tidak memerlukan tanda tangan fisik, transaksi melalui teknologi atau platform marketplace seperti situs web, aplikasi mobile, dan media sosial. Konvergensi antara perkembangan teknologi informasi dengan perkembangan global semakin meningkatkan kapasitas perdagangan melalui Electronic Commerce (E-Com) atau Electronic Business (E-Bis). Namun, meningkatnya interaksi dan transaksi pada industri e-commerce bagi para pelaku usaha dan konsumen di Indonesia menimbulkan kekhawatiran serius terkait perlindungan informasi pribadi konsumen sebab Konsumen harus memberikan data pribadi mereka untuk bertransaksi di platform e-commerce. Berbagai risiko kebocoran data dalam e-commerce, termasuk pencurian data kartu kredit dan informasi pribadi lainnya sehingga penting untuk diketahui teknik untuk mengurangi potensi risiko ini dan meminimalkan dampak kebocoran data terhadap konsumen dan pelaku usaha (Yadav, M., & Suri, P. (2020). Kemudahan bertransaksi di bidang teknologi komputer dan telekomunikasi rentan dengan serangan dan resiko yang tinggi dalam dunia cyberspace tentu juga memerlukan regulasi hukum untuk mengatur segala aktivitas yang terjadi di dalamnya dan memberikan sanksi terhadap pihak yang melakukan pelanggaran regulasi data pribadi dan menimbulkan kerugian kepada orang lain serta bagaimana pelaku e-commerce harus mematuhi peraturan perlindungan data untuk menjaga privasi dan kepercayaan konsumen.

B. Tantangan Perlindungan Data Pribadi dalam Transaksi E-Commerce

1. Risiko Kebocoran dan Penyalahgunaan Data:

Dalam transaksi e-commerce, data pribadi konsumen seperti nama, alamat, nomor kartu kredit dan data pembayaran lainnya sering kali menjadi target serangan Cyber. Risiko kebocoran data mempengaruhi kompleksitas transaksi dan penggunaan berbagai

platform digital. Kebocoran data dapat merusak kepercayaan konsumen dan mempengaruhi perilaku pembeli mereka sehingga meningkatkan potensi risiko bagi perusahaan e-commerce (Acar, G., & Yalçınkaya, A. (2020). Pelanggaran privasi data (termasuk kebocoran data) yang terjadi dapat menyebabkan hilangnya loyalitas pelanggan dan penurunan kepercayaan pada platform e-commerce (Sharma, S., & Joshi, M. (2021). Selain kehilangan data, kebocoran data dapat merusak reputasi perusahaan secara signifikan yang akhirnya berdampak pada penurunan jumlah pelanggan dan pendapatan (Tritsini, E., & Papageorgiou, A. (2022). Pentingnya enkripsi data sebagai langkah perlindungan untuk mengurangi risiko kebocoran data dalam transaksi e-commerce (Wang, X., & Chen, L. (2022).

2. Sumber Ancaman Keamanan:

Ancaman-ancaman siber yang baru muncul, termasuk serangan phishing yang lebih canggih, malware yang menyamar, dan ancaman dari serangan terhadap sistem IoT maka penting berbagai solusi dan teknologi keamanan yang dapat digunakan untuk melindungi sistem dari ancaman-ancaman ini (Rashid, U., & Iqbal, M. (2020). Berbagai ancaman yang dihadapi oleh perangkat IoT yang terhubung ke platform e-commerce, seperti perangkat yang rentan terhadap eksploitasi oleh peretas dan malware maka perlu berbagai solusi untuk meningkatkan keamanan IoT dan melindungi data konsumen (Hassan, W., & Ali, S. (2022). Ancaman terhadap data pribadi dapat datang dari berbagai sumber termasuk serangan *phishing*, *malware*, atau bahkan kelalaian dalam mengelola sistem keamanan oleh pelaku usaha e-commerce maka teknik mitigasi yang dapat diterapkan (Tian, Y., Liu, Y., & Sun, J. (2021). Ancaman terhadap infrastruktur kritis yang mengancam sektor e-commerce dan lainnya, seperti serangan terhadap sistem energi, transportasi, dan sistem informasi maka perlu langkah-langkah yang diambil untuk mengurangi ancaman siber terhadap infrastruktur tersebut (Zhao, Y., & Xu, X. (2020). Berbagai ancaman yang dihadapi oleh *platform cloud computing*, seperti penyalahgunaan akses, kebocoran data, dan serangan terhadap infrastruktur cloud sehingga perlunya solusi dan langkah mitigasi

yang dapat diterapkan untuk melindungi lingkungan *cloud* (Salloum, S. A., & Al-Sayyed, R. (2021). Berbagai jenis ancaman keamanan, termasuk ransomware, serangan DDoS, dan intruksi yang dilakukan oleh peretas maka berdampak terhadap keberlanjutan bisnis di sektor teknologi dan e-commerce (Agarwal, A., & Rathi, S. (2020). Dampak serangan **ransomware** dan **malware** yang meningkat pada sektor e-commerce mengincar data pengguna dan perusahaan, serta teknologi terbaru yang digunakan untuk melawan ancaman ini (Zhang, Y., & Yang, Z. (2021). Advanced Persistent Threats (APTs), yang merupakan ancaman yang lebih canggih dan lebih sulit dideteksi, sering kali berasal dari aktor negara atau organisasi terorganisir. Bagaimana APTs dapat menyerang sistem e-commerce dan langkah-langkah mitigasi yang harus diambil oleh perusahaan (Hasan, H. R., & Ibrahim, M. (2021). Ancaman yang dihadapi oleh platform e-commerce, termasuk serangan siber yang umum seperti SQL *injection, cross-site scripting* (XSS), dan serangan terhadap infrastruktur jaringan. Hal ini perlu teknik dan protokol keamanan yang dapat digunakan untuk mengurangi kerentanannya (Kumar, A., & Singh, M. (2022). Tantangan yang dihadapi oleh **UKM (Usaha Kecil dan Menengah)** dalam mengimplementasikan kebijakan keamanan siber. Faktor-faktor seperti keterbatasan sumber daya, kurangnya kesadaran tentang ancaman siber, dan kesulitan dalam mengikuti regulasi menjadi hambatan utama dalam penerapan keamanan yang efektif (Doherty, N. F., & Malone, J. (2020). Tantangan dalam mengimplementasikan **kerangka kerja keamanan** untuk melindungi infrastruktur kritis, seperti sistem energi, transportasi, dan layanan kesehatan masih terdapat kesulitan dalam menyelaraskan kebijakan dan praktik keamanan di berbagai sektor industri yang berbeda (Matsumoto, K., & Kikuchi, H. (2020).

C. Regulasi dan Kepatuhan terhadap Perlindungan Data Pribadi dalam E-Commerce

Bagaimana regulasi global dapat mempengaruhi kebijakan privasi dan keamanan data dalam e-commerce; Bagaimana organisasi dan pemerintah dapat mengatasi masalah ini dengan mengadopsi pendekatan

yang lebih terintegrasi dan berbasis pada teknologi mutakhir.

Perlindungan hukum berdasarkan sumbernya dapat dibedakan menjadi dua jenis, yaitu perlindungan hukum internal dan perlindungan hukum eksternal. Perlindungan hukum internal adalah perlindungan yang tercipta antara para pihak yang terlibat, ketika posisi hukum mereka relatif seimbang. Dalam hal ini, kedua pihak memiliki kekuatan tawar (bargaining power) yang setara, sehingga mereka memiliki kebebasan untuk menyatakan kehendaknya sesuai dengan kepentingan masing-masing, dengan tetap menghormati hak asasi manusia. Keseimbangan ini memungkinkan mereka untuk merumuskan klausul-klausul dalam perjanjian atau kesepakatan yang sesuai dengan kebutuhan dan kepentingan kedua belah pihak, sehingga perlindungan hukum dapat terwujud secara efektif.

Di sisi lain, perlindungan hukum eksternal adalah perlindungan yang diberikan oleh pihak yang berwenang, seperti negara atau penguasa, melalui peraturan atau regulasi yang ditetapkan. Perlindungan ini bertujuan untuk melindungi pihak yang lebih lemah atau yang memiliki posisi tawar yang lebih rendah dalam hubungan hukum, agar kepentingan mereka tetap terlindungi dan tidak dirugikan oleh pihak yang lebih kuat. Kemasan peraturan perundang-undangan dirancang untuk memberikan perlindungan hukum yang adil dan proporsional kepada semua pihak (Isnaeni, 2017). Namun, dalam konteks perlindungan hukum bagi konsumen, saat ini terlihat bahwa posisi konsumen sering kali tidak seimbang dibandingkan dengan pelaku usaha. Hal ini disebabkan oleh perbedaan signifikan dalam faktor ekonomi, di mana pelaku usaha umumnya memiliki kekuatan ekonomi yang lebih besar daripada konsumen. Ketidakseimbangan ini sering kali menjadi penyebab terjadinya ketidakadilan ketika terjadi perselisihan antara konsumen dan pelaku usaha (Kristiyanti, Celina Tri Siwi, 2009).

1. Regulasi Global Perlindungan Data Pribadi Dalam E-Commerce

Rezim perlindungan data berawal di Eropa sebagai akibat dari ketiadaan definisi yang jelas mengenai privasi dan kehidupan pribadi, yang diatur dalam ketentuan Pasal 8 Konvensi Eropa. Negara Jerman

yang pertama kali mengesahkan Undang-Undang Perlindungan Data pada tahun 1970, yang kemudian diikuti oleh Inggris pada tahun yang sama, dan kemudian sejumlah negara-negara Eropa lainnya, seperti Swedia, Prancis, Swiss, dan Austria. Perkembangan serupa juga mengemuka di Amerika Serikat, dengan adanya Undang-Undang Pelaporan Kredit yang Adil pada tahun 1970, yang juga memuat unsur-unsur perlindungan data. Perkembangan signifikan hukum perlindungan data terjadi pada Tahun 2016 ketika Uni Eropa melakukan unifikasi hukum perlindungan datanya melalui Peraturan Perlindungan Data Umum Uni Eropa (EU-General Data Protection Regulation) dan mulai berlaku pada 25 Mei Tahun 2018. Peraturan ini mengatur bagaimana data pribadi individu yang dapat diidentifikasi diproses dan disimpan oleh pengendali data, baik di dalam maupun di luar Uni Eropa.

GDPR menekankan pentingnya dasar pemrosesan data. GDPR juga memberikan hak kepada subjek data untuk mengakses informasi pribadi mereka, meminta penghapusan data, dan memastikan data mereka diproses secara adil dan transparan. Ketidakpatuhan terhadap ketentuan ini dapat mengakibatkan denda besar hingga 4 persen dari pendapatan tahunan atau 20 juta Euro, mana yang lebih besar. GDPR bersifat komprehensif, mencakup hampir semua pemrosesan data pribadi. Selain itu, implementasinya juga tidak hanya akan mempengaruhi pengendali dan prosesor data yang berbasis di Uni Eropa, tetapi juga mereka yang menawarkan barang atau jasa kepada, atau memantau perilaku, individu warga negara Uni Eropa. GDPR didasarkan pada prinsip-prinsip utama pelindungan data seperti adanya dasar legalitas, transparansi, pembatasan tujuan, minimalisasi data, akurasi, pembatasan penyimpanan, integritas, dan akuntabilitas. Regulasi ini berlaku bagi organisasi yang memproses data pribadi warga EU, termasuk negara ketiga yang menyediakan layanan, atau memonitor aktivitas warga EU.

GDPR menggantikan Data Protection Act 1998 sebagai konsekuensi transformasi digital. Berdasarkan GDPR organisasi tertentu yang memenuhi kriteria, wajib menunjuk Data Protection Officer. DPO wajib ada jika organisasi memproses data sensitif

secara besar-besaran, atau melakukan pemantauan individu secara rutin. Pada prinsipnya korporasi sebagai pengendali data harus harus mengelola data sesuai regulasi ini dan memastikan dasar hukum pemrosesan data. Organisasi juga harus memiliki kebijakan privasi yang transparan. Mitigasi risiko, penyiapan SDM memadai, keamanan data penting untuk mengurangi risiko pelanggaran data dan memastikan kepatuhan GDPR. Perbandingkan peraturan perlindungan data pribadi yang diterapkan di berbagai wilayah dunia, dengan fokus pada General Data Protection Regulation, **California Consumer Privacy Act** dan peraturan serupa di Asia dan Amerika Latin. Penulis mengkaji bagaimana perusahaan e-commerce di masing-masing wilayah mengelola kepatuhan terhadap regulasi (López, C., & Pérez, J. (2022). Dampak undang-undang perlindungan data pribadi seperti General Data Protection Regulation, **California Consumer Privacy Act** terhadap operasional e-commerce. Penulis memberikan analisis tentang kesulitan yang dihadapi oleh perusahaan dalam mematuhi peraturan tersebut, serta strategi yang digunakan untuk memastikan kepatuhan (Liu, Y., & Zhang, H. (2022).

Tantangan dalam kepatuhan terhadap regulasi General Data Protection Regulation, **California Consumer Privacy Act** oleh perusahaan e-commerce global. Perkembangan regulasi privasi dan keamanan data pribadi dalam e-commerce di berbagai negara, termasuk implementasi General Data Protection Regulation, **California Consumer Privacy Act**, dan undang-undang serupa lainnya (Zhao, S., & Liu, Y. (2023). Tantangan dan peluang dalam kepatuhan terhadap regulasi perlindungan data pribadi, khususnya General Data Protection Regulation dalam sektor e-commerce. Studi ini juga membahas upaya-upaya yang dilakukan oleh perusahaan e-commerce di Eropa dan di luar Eropa dalam memastikan kepatuhan terhadap regulasi (Tung, H. T., & Nguyen, H. K. (2023)**.**

Pelindungan Anak Otoritas Pelindungan Data Italia juga menyebut OpenAI gagal menyediakan sistem verifikasi usia, untuk mencegah anak di bawah 13 tahun mengakses konten AI yang berpotensi tidak pantas. Pelindungan data anak dilindungi GDPR secara ketat. Resital 38 Perlindungan Khusus Data Pribadi Anak

menyatakan, anak-anak berhak mendapatkan pelindungan khusus berkenaan dengan data pribadi mereka. Pasalnya, mereka mungkin kurang menyadari risiko, konsekuensi, dan perlindungan yang terkait serta hak-hak mereka dalam pemrosesan data pribadinya. Pelindungan khususnya, harus berlaku untuk penggunaan data pribadi anak-anak untuk tujuan pemasaran, pembuatan profil kepribadian, atau pengguna, dan pengumpulan data pribadi terkait anak-anak saat menggunakan layanan yang ditawarkan langsung kepada anak. Persetujuan dari penanggung jawab atau orangtua tidak diperlukan dalam konteks layanan pencegahan atau konseling yang ditawarkan langsung kepada anak.

GDPR dalam Art 8, mengatur tentang kondisi yang berlaku untuk persetujuan anak dalam kaitannya dengan layanan informasi secara langsung kepada anak. Pemrosesan data pribadi anak akan dianggap sah apabila anak tersebut berusia setidaknya 16 tahun. Apabila anak tersebut berusia di bawah 16 tahun, pemrosesan tersebut akan sah hanya jika ada persetujuan yang diberikan atau diizinkan oleh orangtua atau penanggung jawab anak tersebut. GDPR membuka peluang bagi negara anggota untuk menetapkan berdasarkan undang-undangnya, usia yang lebih rendah untuk tujuan tersebut. Dengan ketentuan bahwa usia yang lebih rendah tersebut tidak lebih rendah dari 13 tahun. GDPR juga menekankan bahwa pengendali data harus melakukan upaya yang wajar untuk memverifikasi dan persetujuan diberikan oleh orang yang bertanggung jawab atau orang tua anak dengan mempertimbangkan teknologi yang tersedia.

2. Regulasi Nasional Perlindungan Data Pribadi

Berbagai negara memiliki regulasi yang mengatur perlindungan data pribadi, yang mewajibkan pelaku usaha e-commerce untuk memastikan bahwa data konsumen dikelola dengan cara yang aman dan transparan. Regulasi perlindungan data pribadi di Indonesia mewajibkan setiap entitas yang mengumpulkan data pribadi untuk menjaga data tersebut dengan sangat hati-hati dan hanya menggunakan data tersebut untuk tujuan yang sah. Ketentuan Pasal 1

angka 4 Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi terdapat pasal-pasal yang memberikan kewajiban kepada Pengendali data pribadi. Pengendali data pribadi menurut Undang-Undang Perlindungan Data Pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi. Pengendali data pribadi disini bisa Pemerintah maupun swasta. Dari Pemerintah misalnya adalah Direktorat Jenderal Kependudukan dan Pencatatan Sipil, Kementerian Dalam Negeri yang mencatat data pribadi penduduk untuk kepentingan negara maupun publik. Sementara dari pihak swasta, *marketplace* bisa menjadi salah satu contohnya. Sebab, untuk dapat menggunakan atau mengakses semua layanan yang diberikan, masyarakat harus memasukan data pribadinya.

Pasal 35 Undang-Undang Perlindungan Data Pribadi menyebutkan bahwa Pengendali Data Pribadi wajib melindungi dan memastikan keamanan Data Pribadi yang diprosesnya, dengan melakukan penyusunan dan penerapan langkah teknis operasional untuk melindungi Data Pribadi dari gangguan pemrosesan Data Pribadi yang bertentangan dengan ketentuan peraturan perundang-undangan dan penentuan tingkat keamanan Data Pribadi dengan memperhatikan sifat dan risiko dari Data Pribadi yang harus dilindungi dalam pemrosesan Data Pribadi.

Pasal 39 Undang-Undang Perlindungan Data Pribadi menyebutkan bahwa:

(1) Pengendali Data Pribadi wajib mencegah Data Pribadi diakses secara tidak sah;

(2) Pencegahan sebagaimana dimaksud pada ayat (1) dilakukan dengan sistem keamanan terhadap Data Pribadi yang diproses dan/atau memproses Data Pribadi sistem elektronik secara andal, aman, dan bertanggung jawab.

(3) Pencegahan sebagaimana dimaksud pada ayat (2) dilakukan sesuai dengan ketentuan peraturan perundang- undangan.

Pasal 46

(1) Dalam hal terjadi kegagalan Pelindungan Data Pribadi, Pengendali Data Pribadi wajib pemberitahuan secara tertulis paling lambat 3 x 24 (tiga kali dua puluh empat) jam kepada: a. Subjek Data Pribadi; dan b. lembaga;

(2) Pemberitahuan tertulis sebagaimana dimaksud pada ayat (1) minimal memuat: Data Pribadi yang terungkap; kapan dan bagaimana Data Pribadi terungkap; dan upaya penanganan dan pemulihan atas terungkapnya Data Pribadi oleh Pengendali Data Pribadi.

Pasal 65 bahwa:

1) Setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi.
2) Setiap orang dilarang secara melawan hukum mengungkapkan Data Pribadi yang bukan miliknya.
3) Setiap Orang dilarang secara melawan hukum menggunakan Data Pribadi yang bukan miliknya.

Pasal 66 bahwa Setiap orang dilarang membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain.

Pasal 67 bahwa

(1) *Setiap Orang yang dengan sengaja dan melawan hukum* **memperoleh atau mengumpulkan Data Pribadi** *yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000,00 (lima miliar rupiah).*

(2) *Setiap Orang yang dengan sengaja dan melawan hukum* **mengungkapkan Data Pribadi yang bukan** *miliknya*

sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).

(3) *Setiap Orang yang dengan sengaja dan melawan hukum* **menggunakan Data Pribadi yang bukan miliknya** *sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp. 5.000.000,00 (lima miliar rupiah).*

Pasal 68 bahwa Setiap orang yang dengan sengaja membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain sebagaimana dimaksud dalam Pasal 66 dipidana dengan pidana penjara paling tama 6 (enam) tahun dan/atau pidana denda paling banyak Rp 5.000.000.000,00 (enam miliar rupiah).

Pasal 69 bahwa Selain dijatuhi pidana ssfagaimana dimaksud dalam Pasal 67 dan Pasal 68 juga dapat dijatuhi pidana tambahan berupa perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian.

Berdasarkan ketentuan yang berlaku, marketplace memiliki kewajiban untuk melindungi data pribadi pengguna. Apabila terjadi kebocoran data pribadi, marketplace sebagai pengendali data harus segera memberi tahu konsumen yang datanya telah diretas oleh pihak yang tidak bertanggung jawab. Selain itu, marketplace dapat dikenakan sanksi administratif, seperti peringatan tertulis, penghentian sementara pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, serta denda administratif, sesuai dengan Pasal 57 Undang-Undang Perlindungan Data Pribadi. Di sisi lain, Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggara Sistem Elektronik juga menetapkan sanksi berupa teguran tertulis, denda administratif, penghentian sementara, pemutusan akses, atau bahkan pengeluaran dari daftar penyelenggara sistem elektronik.

Jika terjadi kebocoran data pribadi konsumen, konsumen

memiliki hak untuk mengajukan pengaduan kepada Menteri terkait kegagalan dalam perlindungan kerahasiaan data pribadi. Hal ini sejalan dengan ketentuan Pasal 26 huruf b yang memberikan hak kepada pemilik data untuk mengajukan pengaduan kepada Menteri jika perlindungan data pribadi gagal dilaksanakan dengan baik. Selain itu, konsumen yang merasa dirugikan dapat mengajukan gugatan perdata terhadap marketplace dengan alasan adanya kelalaian yang dilakukan oleh pihak marketplace. Dalam konteks kelalaian ini, Pasal 1336 Kitab Undang-Undang Hukum Perdata menyatakan bahwa setiap orang bertanggung jawab tidak hanya atas kerugian yang disebabkan oleh perbuatannya, tetapi juga atas kerugian yang disebabkan oleh kelalaian atau kesembronoannya.

Menurut Pasal 1366 Kitab Undang-Undang Hukum Perdata, seseorang dapat dikenai tanggung jawab hukum tidak hanya atas kerugian yang disebabkan oleh perbuatannya yang salah, tetapi juga atas kerugian yang timbul akibat kelalaiannya. Sementara itu, Pasal 64 Undang-Undang Perlindungan Data Pribadi menyatakan bahwa penyelesaian sengketa terkait perlindungan data pribadi dapat dilakukan melalui beberapa jalur, yaitu arbitrase, pengadilan, atau lembaga penyelesaian sengketa alternatif. Proses penyelesaian tersebut harus mengikuti hukum acara yang berlaku dan dilengkapi bukti yang sah sesuai dengan peraturan perundang-undangan yang berlaku.

3. Kewajiban Pengelolaan Data Pribadi oleh Pelaku Usaha

Bagaimana perusahaan dan pelaku usaha harus mengelola data pribadi dengan mematuhi regulasi perlindungan data dan privasi ? Dalam regulasi Perlindungan Data Pribadi, pelaku usaha e-commerce wajib mendapatkan persetujuan dari konsumen sebelum mengumpulkan data pribadi, memberitahukan tujuan pengumpulan data, dan memberi hak kepada konsumen untuk mengakses serta menghapus data mereka. Pelaku usaha juga wajib melakukan langkah-langkah keamanan yang memadai untuk mencegah kebocoran data. Peran pengelola data yang diatur dalam Pasal 4 Undang-Undang Perlindungan Data Pribadi mengatur kewajiban pihak yang mengelola

data pribadi, seperti perusahaan atau lembaga. Mereka harus memastikan data yang telah disimpan tetap aman, bertanggungjawab atas penggunaan data, dan tidak disebarluaskan tanpa izin pemilik. Jika kebocoran data, pengelola data wajib memberi tahu informasi tersebut atau memungkinkan dapat dikenakan sanksi hukum, termasuk denda besar atau hukuman pidana. Hal lain yang diatur adalah adanya persetujuan eksplisit dari pemilik data sebelum data mereka dikumpulkan dan diproses oleh perusahaan. Hal ini berarti perusahaan tidak bisa lagi sembarangan mengakses atau memanfaatkan data pengguna tanpa sepengetahuan atau persetujuan mereka. Kewajiban pelaku usaha e-commerce di Indonesia dalam pengelolaan data pribadi berdasarkan **UU Perlindungan Data Pribadi** yang baru di sahkan dan mengidentifikasi kewajiban utama terkait pengumpulan, penggunaan, dan penghapusan data pribadi pelanggan serta kepatuhan terhadap regulasi yang ada (Kurniawan, A. S., & Pratama, I. A. (2022). Kewajiban yang dimiliki pelaku usaha dalam mengelola data pribadi konsumen sesuai dengan peraturan yang berlaku di Indonesia, termasuk **UU PDP** dan peraturan lainnya. Tantangan yang dihadapi oleh pelaku usaha di sektor e-commerce dalam mematuhi peraturan tersebut (Rahman, A., & Santosa, P. (2022). Kewajiban pelaku usaha dalam mengelola data pribadi sesuai dengan **Undang-Undang Perlindungan Data Pribadi (UU PDP)** di Indonesia. Analisis mengenai tantangan dan penerapan kewajiban pengelolaan data pribadi oleh platform digital di Indonesia (Putri, R. A., & Setiawan, D. (2023).

Kewajiban pelaku usaha dalam menerapkan kebijakan perlindungan data pribadi pada platform e-commerce di Indonesia. Analisis terhadap implementasi kebijakan di bawah **UU PDP** dan tantangan yang dihadapi oleh pelaku usaha dalam pengelolaan data pribadi (Budi, A. R., & Suhartono, T. (2023). Kewajiban pelaku usaha dalam **pengelolaan data pribadi** dalam **pasar digital**. Bagaimana bisnis harus memenuhi kewajiban pengelolaan data pribadi melalui kebijakan dan prosedur yang memastikan kepatuhan terhadap peraturan seperti GDPR dan CCPA (Harrison, P., & Fitzgerald, J. (2022). Kewajiban pelaku usaha dalam pengelolaan data pribadi

menurut **General Data Protection Regulation** di Eropa dan **California Consumer Privacy Act** di Amerika Serikat. Kewajiban utama perusahaan dalam hal transparansi, persetujuan, dan perlindungan data pribadi konsumen (Smith, A. L., & Tang, X. (2022).

Kewajiban yang dimiliki oleh pelaku usaha dalam mengelola data pribadi dalam sektor e-commerce, dengan fokus pada kebijakan perlindungan data pribadi global, termasuk **GDPR** dan standar internasional lainnya serta tantangan implementasi kebijakan ini di berbagai negara (Tao, Z., & Liu, L. (2022). Kewajiban pelaku usaha dalam mengelola data pribadi, khususnya dalam konteks regulasi **GDPR** dan peraturan lainnya di Eropa. Tantangan dalam kepatuhan terhadap kewajiban pengelolaan data pribadi, seperti pengumpulan, penyimpanan, dan penghapusan data, serta penerapan kebijakan privasi yang sesuai (Mikkonen, T., & Laukkanen, T. (2023)**.**

Peran **data controllers** dalam mengelola data pribadi dalam konteks e-commerce dan kewajiban untuk melindungi data pribadi, termasuk kewajiban notifikasi, hak akses, serta penghapusan data dalam berbagai regulasi data pribadi di tingkat global (Wang, Y., & Zhang, R. (2023)**.**

Contoh Kasus 1:

Pelanggaran GDPR oleh Facebook (Meta) - 2018: Pada tahun 2018, perusahaan Facebook (sekarang Meta) dikenakan denda sebesar €110 juta oleh Komisi Eropa karena gagal menginformasikan pengguna dengan tepat mengenai penggabungan data antara Facebook dan WhatsApp. Kasus ini menunjukkan bagaimana pelanggaran terhadap regulasi perlindungan data, seperti General Data Protection Regulation (GDPR) yang berlaku di Uni Eropa, dapat mengakibatkan sanksi yang berat. Meta dikritik karena tidak memberi tahu pengguna bahwa data mereka akan digunakan secara lebih luas setelah akuisisi WhatsApp, yang bertentangan dengan ketentuan GDPR mengenai transparansi dan kontrol pengguna terhadap data pribadi mereka.

Contoh Kasus 2 :

Pengenalan wajah: SA Italia mendenda Clearview AI sebesar EUR 20 juta

1) Informasi latar belakang

Tanggal keputusan akhir: 10 Februari 2022
Kasus lintas batas atau kasus nasional: kasus nasional, Pasal 3(2) berlaku Pengendali: Clearview AI Inc.

Referensi Hukum: Prinsip-prinsip yang berkaitan dengan pemrosesan data pribadi (Pasal 5(1)(a)(b)(e)); Keabsahan pemrosesan (Pasal 6); Pemrosesan kategori khusus data pribadi (Pasal 9); Informasi yang transparan, komunikasi dan modalitas untuk pelaksanaan hak-hak subjek data (Pasal 12); Informasi yang harus diberikan ketika data pribadi dikumpulkan dari subjek data (Pasal 13); Informasi yang harus diberikan ketika data pribadi belum diperoleh dari subjek data (Pasal 14); Hak akses oleh subjek data (Pasal 15); Perwakilan pengendali yang tidak didirikan di Uni (Pasal 27).

Keputusan: SA Italia mengenakan denda sebesar EUR 20 juta, memberlakukan larangan pengumpulan dan pemrosesan lebih lanjut, memerintahkan penghapusan data, termasuk data biometrik, yang diproses oleh sistem pengenalan wajah Perusahaan terkait orang-orang di wilayah Italia dan penunjukan perwakilan di wilayah Uni Eropa.
Kata kunci: Pengikisan Web, Basis Data Gambar, Pengenalan Wajah, Data Biometrik, Sistem AI, Geolokasi, Yurisdiksi berdasarkan hukum UE, Perwakilan di UE.

2) Ringkasan Putusan

 # Asal Mula Kasus

SA Italia meluncurkan gugatan atas kemauannya sendiri setelah adanya laporan pers mengenai beberapa masalah yang berhubungan dengan produk pengenalan wajah yang ditawarkan oleh Clearview AI Inc. Selain itu, Garante menerima, selama tahun 2021, empat pengaduan dan dua peringatan dari dua organisasi yang aktif di bidang perlindungan privasi dan hak-hak dasar individu terhadap

Clearview.

 # Temuan Utama

Penyelidikan dan penilaian oleh SA Italia menemukan beberapa pelanggaran oleh Clearview AI Inc. Data pribadi yang dimiliki oleh perusahaan, termasuk informasi biometrik dan geolokasi, diproses secara tidak sah tanpa dasar hukum yang sesuai karena kepentingan sah perusahaan yang berbasis di AS tidak memenuhi syarat seperti itu. Selain itu, perusahaan tersebut melanggar beberapa prinsip dasar GDPR, seperti transparansi, pembatasan tujuan, dan pembatasan penyimpanan; perusahaan tersebut gagal memberikan informasi yang ditetapkan oleh Pasal 13-14, memberikan informasi tentang tindakan yang diambil atas permintaan berdasarkan Pasal 15 dalam jangka waktu yang ditentukan, dan menunjuk perwakilan di UE.

 # Putusan

SA Italia menjatuhkan denda sebesar EUR 20 juta. Selain itu, SA Italia:

1) memberlakukan larangan atas pengumpulan lebih lanjut, melalui teknik pengikisan web, atas gambar dan metadata relevan mengenai orang-orang di wilayah Italia dan atas pemrosesan lebih lanjut atas data standar dan biometrik yang ditangani oleh Perusahaan melalui sistem pengenalan wajah dan orang-orang yang bersangkutan di wilayah Italia;
2) penghapusan data yang teratur, termasuk data biometrik, yang diproses oleh sistem pengenalan wajah terkait orang-orang di wilayah Italia, tunduk pada kewajiban untuk segera menanggapi permintaan pelaksanaan hak-hak berdasarkan Pasal 15 hingga 22 Peraturan yang mungkin telah diterima dari subjek data sesuai dengan Pasal 12 (3) Peraturan;
3) memerintahkan Perusahaan untuk menunjuk perwakilan di wilayah Uni Eropa. (EDPB, 2022)

Contoh Kasus 3 :

1) Elon Musk Seret Microsoft dalam Gugatan Terbarunya Terhadap OpenAI

Miliarder teknologi Elon Musk memperluas gugatannya terhadap OpenAI. Dia menambahkan klaim antimonopoli federal dan klaim lainnya serta menambahkan penyokong finansial terbesar OpenAI, Microsoft sebagai terdakwa.Dilansir dari Reuters. Gugatan Elon Musk yang diajukan pada Kamis, 14 November 2024 di pengadilan federal di Oakland, California, menyatakan bahwa Microsoft dan OpenAI secara ilegal berupaya memonopoli pasar kecerdasan buatan generatif dan menyingkirkan pesaing. Gugatan yang diperluas itu menyatakan OpenAI dan Microsoft melanggar undang-undang antimonopoli dengan mensyaratkan peluang investasi pada perjanjian untuk tidak berurusan dengan pesaing perusahaan. Disebutkan bahwa perjanjian lisensi eksklusif perusahaan tersebut merupakan penggabungan yang tidak memiliki persetujuan regulasi. (Tempo, 2024)

2) **Elon Musk Minta Pengadilan Federal Larang OpenAI Cari Cuan**

Elon Musk meminta pengadilan federal untuk menghentikan perusahaan kecerdasan buatan Amerika Serikat (AS) OpenAI untuk berubah menjadi bisnis yang sepenuhnya mencari keuntungan.

Dilansir dari CNBC International, Elon Musk sendiri saat ini tengah mengembangkan perusahaan AI buatannya sendiri xAI. Pengacara yang mewakili Musk, Shivon Zilis, mengajukan putusan pendahuluan terhadap OpenAI. Putusan tersebut juga akan menghentikan OpenAI dari dugaan mengharuskan investornya untuk tidak mendanai pesaing, termasuk xAI dan lainnya.

Pengajuan pengadilan terbaru menunjukkan eskalasi perseteruan hukum antara Musk, OpenAI, dan CEO-nya Sam Altman, serta pihak dan pendukung lain yang sebelumnya juga sudah terlibat, termasuk investor teknologi Reid Hoffman dan Microsoft. Musk awalnya menggugat OpenAI pada Maret 2024 di pengadilan negara bagian San Francisco, sebelum mencabut gugatan tersebut dan mengajukan kembali beberapa bulan kemudian di pengadilan federal. Pengacara Musk mengungkapkan dalam pengaduan mereka bahwa OpenAI telah melanggar undang-undang pemerasan federal,

atau RICO.

Pada pertengahan November, mereka menambah pengaduan dengan menyertakan tuduhan bahwa Microsoft dan OpenAI telah melanggar undang-undang antimonopoli. Alasanya karena OpenAI diduga meminta investor untuk tidak berinvestasi di perusahaan pesaing, termasuk perusahaan rintisan terbaru Musk, xAI. OpenAI telah muncul sebagai salah satu perusahaan rintisan terbesar dalam beberapa tahun terakhir. ChatGPT pun semakin populer dan telah membantu mengantarkan antusiasme perusahaan besar terhadap AI. OpenAI awalnya memulai debutnya pada 2015 sebagai perusahaan nirlaba dan kemudian pada tahun 2019 diubah menjadi perusahaan dengan model laba terbatas, di mana nirlaba OpenAI menjadi entitas yang mengatur anak perusahaannya yang mencari laba. Perusahaan tersebut sedang dalam proses diubah menjadi perusahaan konvensional yang sepenuhnya mencari laba yang dapat membuatnya lebih menarik bagi investor. Rencana restrukturisasi tersebut juga akan memungkinkan OpenAI untuk mempertahankan status nirlaba sebagai entitas terpisah. (CNBC Indonesia, 2024)

Contoh Kasus 4 :

1) Pelanggaran Chat-GPT dan Denda Otoritas Privasi Italia

Otoritas Pelindungan Data Italia (Garante Per la Protezione Dei Dati Personali) menghukum OpenAI OpCo, LLC dengan sanksi denda sebesar 15 juta Euro atau setara lebih dari Rp 252 Miliar pada hari Jum'at, 20 Desember 2024. Sanksi dijatuhkan karena ketidakpatuhan perusahaan itu terhadap GDPR dalam pengelolaan ChatGPT. ChatGPT juga disebut oleh Garante telah gagal melindungi anak-anak pada operasional platform digital berkekuatan AI itu. Pertimbangan putusan itu menyebut adanya pelanggaran yang mencakup dasar hukum yang tidak memadai dalam pemrosesan data, tidak memenuhi prinsip transparansi data pengguna dan verifikasi usia yang tidak memadai. Sanksi denda diputuskan menyusul penyelidikan yang dimulai pada Maret 2023, merujuk pada Opini 28 Desember 2024 Dewan Perlindungan Data Eropa OpenAI juga diperintahkan untuk melakukan kampanye selama enam (6) bulan

tentang implikasi perlindungan data dan hak pengguna ChatGPT. "OpenAI Fined by Italian Privacy Watchdog for ChatGPT Violations". OpenAI terbukti menggunakan data pribadi pengguna ChatGPT di Italia, untuk melatih algoritma chatbot berdasar pada laporan investigasi yang dilakukan pemerintah Italia. OpenAI didenda karena pelanggaran yang dilakukan ChatGPT.

Kasus ini menambah deretan gugatan terhadap OpenAI yang mengoperasikan sistem AI Generatif ChatGPT termasuk kasus hak cipta di Amerika Serikat. ChatGPT saat ini menjadi sasaran penyelidikan dan menjadi perhatian regulator di AS dan Eropa. Laporan News Week mengungkapkan, investigasi yang diluncurkan tahun lalu, diawali adanya dugaan OpenAI memproses data pribadi tanpa dasar hukum yang memadai, dan tidak memenuhi standar transparansi. Namun, Juru bicara OpenAI menyatakan, perusahaan telah berupaya bekerja sama dengan otoritas privasi, sejak Garante memerintahkan penghentian layanan ChatGPT di Italia pada tahun 2023. Denda ini tidak proporsional dan hampir 20 kali lipat dari pendapatan yang diperoleh di Italia selama periode yang relevan. OpenAI menegaskan komitmennya untuk terus bekerja sama dengan otoritas global dalam mengembangkan AI yang menghormati hak-hak pribadi.

2) Banding

Menghadapi sanksi ini, OpenAI berencana mengajukan banding. Fenomena ini tentu menjadi peringatan bagi semua pengembang AI Generatif di seluruh dunia. Dilansir Euro News "Italy's privacy watchdog fines OpenAI €15 million after probe into ChatGPT data collection" bahwa dalam pernyataan melalui email, OpenAI menyebut putusan itu "tidak proporsional" dan mengatakan akan mengajukan banding. Seorang juru bicara OpenAI mengatakan, denda tersebut hampir 20 kali lipat dari pendapatan yang diperolehnya di Italia pada tahun yang sama. Dalam pernyataannya, OpenAI pun menawarkan kerja sama dalam penggunaan AI bermanfaat yang menghormati hak privasi. (Kompas, 2024)

4. Pentingnya Kepatuhan dan Penegakan Hukum

Perlindungan hukum merupakan implementasi dari fungsi hukum agar tercapainya keteraturan dalam kehidupan bermasyarakat, keteraturan menyebabkan kepastian yang berdampak pula pada ketertiban dalam masyarakat. Hukum dijadikan sebagai sarana untuk memberikan jaminan perlindungan atas hak tersebut, seperti yang disebutkan dalam Pasal 28D ayat (1) dikatakan bahwa "Setiap orang berhak atas pengakuan jaminan, perlindungan dan kepastian hukum yang adil serta perlakuan yang sama dihadapan hukum." Hukum dapat bekerja dan berperan melalui bantuan dari perundang-undangan, putusan pengadilan, atau gabungan dari keduanya. Pembentukan perundang-undangan adalah cara yang paling rasional dan cepat dibandingkan dengan metode pengembangan hukum lain seperti yurisprudensi dan hukum kebiasaan (Mochtar Kusumaatmadja dan B. Arief Sidharta, 2013).

Peraturan Menteri Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi juga mengatur tentang tata cara penyelesaian sengketa yang terjadi, hal tersebut diatur dalam Pasal 29 hingga Pasal 33. Dalam ketentuannya konsumen dapat melakukan pengaduan bahwa telah terjadinya kegagalan perlindungan Data Pribadi kepada Kementerian Komunikasi Dan Informatika. Konsumen paling lambat melakukan pengaduan kepada Kementerian Komunikasi dan Informatika yaitu selama 30 hari setelah konsumen mengetahui terjadinya kegagalan perlindungan terhadap Data Pribadinya. Dalam laporannya konsumen harus membawa bukti bukti pendukung. Apabila pengaduan telah diterima oleh Kementerian Komunikasi dan Informatika maka Lembaga Penyelesaian Sengketa Data Pribadi harus menanggapi pengaduan tersebut paling lama 14 hari kerja sejak pengaduan diterima. Bentuk perlindungan data pribadi konsumen ini telah ada dalam Peraturan Menteri Informasi dan Komunikasi Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pemerintah berwenang untuk mengawasi perusahaan penyelenggara sistem elektronik dan memeriksa sertifikasi kelayakan sistem elektronik dan juga menekankan setiap penyelenggara sistem elektronik membuat

pengaturan internal untuk meningkatkan perlindungan data pribadi konsumen. Pasal 52 Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen. Untuk mengatasi liku-liku proses pengadilan yang lama dan formal UUPK memberikan jalan alternatif dengan menyediakan penyelesaian sengketa di luar pengadilan (non-litigasi) melalui konsiliasi, mediasi dan arbitrase (Susanti Agung Nugroho. 2008) Dengan demikian, Marketplace bertanggung jawab atas kebocoran data dan dapat dikenakan sanksi administratif jika terjadi pelanggaran terhadap ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Erna Priliasari, 2023).

Berlakunya Undang-Undang No. 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Pasal 31 dari Undang-Undang (UU) Nomor 1 Tahun 2024 mengatur tentang tanggung jawab penyelenggara sistem elektronik (PSE) dalam melindungi data pribadi. PSE bertanggung jawab untuk memastikan transaksi elektronik berjalan aman dan terjamin. Selain itu, beberapa pasal lain dalam UU Nomor 1 Tahun 2024 yang berkaitan dengan perlindungan data pribadi adalah Pasal 16A mengatur bahwa perlindungan terhadap hak anak merupakan prioritas PSE dibandingkan dengan kepentingan komersial.

Pasal 16A

(1) Penyelenggara Sistem Elektronik wajib memberikan pelindungan bagi anak yang menggunakan atau mengakses Sistem Elektronik.

(2) Pelindungan sebagaimana dimaksud pada ayat (1) meliputi pelindungan terhadap hak anak sebagaimana dimaksud dalam peraturan perundang-undangan mengenai penggunaan produk, layanan, dan fitur yang dikembangkan dan diselenggarakan oleh Penyelenggara Sistem Elektronik.

(3) Dalam memberikan produk, layanan, dan fitur bagi anak, Penyelenggara Sistem Elektronik wajib menerapkan teknologi dan langkah teknis operasional untuk memberikan pelindungan

sebagaimana dimaksud pada ayat (1) dari tahap pengembangan sampai dengan tahap penyelenggaraan Sistem Elektronik.

(4) Dalam memberikan pelindungan sebagaimana dimaksud pada ayat (1), Penyelenggara Sistem Elektronik wajib menyediakan:

- informasi mengenai batasan minimum usia anak yang dapat menggunakan produk atau layanannya;
- mekanisme verifikasi pengguna anak; dan
- mekanisme pelaporan penyalahgunaan produk, layanan, dan fitur yang melanggar atau berpotensi melanggar hak anak.

(5) Ketentuan lebih lanjut mengenai pelindungan sebagaimana dimaksud pada ayat (1) sampai dengan ayat (4) diatur dalam Peraturan Pemerintah.

Pasal 16B

(1) Pelanggaran terhadap ketentuan sebagaimana dimaksud dalam Pasal 16A dikenai sanksi administratif.

(2) Sanksi administratif sebagaimana dimaksud pada ayat (1) dapat berupa:

- Teguran tertulis;
- Denda administratif;
- Penghentian sementara; dan/atau
- Pemutusan Akses.

Pasal 45 mengatur sanksi pidana yang lebih tegas bagi pihak yang menyalahgunakan informasi elektronik.

Undang-Undang ITE telah memperkuat jaminan perlindungan konsumen dari segala tindakan transaksi elektronik. Beleid ini berkorelasi dengan prinsip perlindungan konsumen yang diatur dalam Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen akan pentingnya perlindungan hak-hak konsumen dalam transaksi, dalam memanfaatkan kemudahan teknologi dengan penekanan pada ketentuan data privasi dan komprehensif, dimana

Pasal 26B Undang-Undang ITE mengatur mengenai kewajiban penyelenggara sistem elektronik dalam menjaga kerahasiaan, integritas, dan ketersediaan data pribadi konsumen. Pasal ini menegaskan bahwa penyelenggara yang lalai dalam menjaga keamanan data pribadi dapat dikenakan sanksi administratif dan pidana, memberikan perlindungan yang lebih kuat bagi konsumen. Bila ditarik penafsiran secara umum, maka perlindungan data pribadi sebenarnya telah diatur di dalam Undang-Undang ITE. Pasal-Pasal selanjutnya dalam Undang-Undang ITE yaitu Pasal 30-33 dan Pasal 35 yang masuk kedalam BAB VII mengenai Perbuatan yang Dilarang. Sementara dalam Kitab Undang-Undang Pidana Baru, yaitu Undang-Undang No. 1 Tahun 2023, Bagian Kelima tentang Tindak Pidana Informatika Dan Elektronika mengenai Jenis kejahatan siber atau kejahatan elektronik atau kejahatan yang berbasis internet (Cybercrime Internasional sebagai aktivitas kriminal yang melibatkan internet, sistem komputer atau teknologi komputer juga berdasarkan UU ITE) meliputi :

1) Akses Illegal (Pasal 332);
2) Serangan siber pada sistem informasi dan infrastruktur negara, pemerintah, dan masyarakat (Pasal 333);
3) Serangan siber terhadap keuangan, perbankan, pemerintah (Pasal 334 dan 335).

Ancaman sanksi berat terhadap pelanggaran pasal tersebut bertujuan untuk menjaga keamanan dan integritas sistem dan informasi elektronik indonesia.

Kasus pembobolan Data dari Pusat Data Nasional Sementara (PDNS) oleh grup ransomware Brain Chiper pada Kamis, 20 Juni 2024. Serangan ransomware mengunci data di 282 kementerian/lembaga, dan meminta tebusan 8 juta dolar AS atau Rp131 miliar untuk membuka data. Kasus pembobolan data ini bukan yang pertama terjadi di Indonesia (Dikutip dari berbagai sumber media).

1) Kebocoran Data IndiHome (2022)

Pada Agustus 2022, IndiHome, penyedia layanan internet milik Telkom Indonesia, mengalami kebocoran data yang berdampak pada jutaan pelanggannya. Data yang bocor meliputi riwayat browsing, nomor induk kependudukan (NIK), dan data pribadi lainnya.

2) Kebocoran Data KPU (2022)

Pada September 2022, peretas Bjorka mengklaim telah membobol data 105 juta pemilih dari situs web Komisi Pemilihan Umum (KPU). Data yang bocor meliputi nama lengkap, nomor induk kependudukan (NIK), dan alamat pemilih.

3) Kebocoran Data Bank Syariah Indonesia (2023)

Pada Desember 2023, Bank Syariah Indonesia (BSI) mengalami kebocoran data yang berdampak pada jutaan nasabahnya. Data yang bocor meliputi nama lengkap, nomor rekening, dan data pribadi lainnya.

4) Kebocoran Data Carousell, MyPertamina, PeduliLindungi, Lazada, dan Mobile Legends (2022)

Pada November 2022, Kementerian Komunikasi dan Informatika (Kominfo) melaporkan terjadinya lima kasus kebocoran data baru dalam kurun waktu satu bulan. Data yang bocor meliputi nama lengkap, alamat email, dan data pribadi lainnya.

5) Kebocoran data Pusat Data Nasional Sementara (2024)

Data di Pusat Data Nasional Sementara (PDNS) dibobol grup ransomware Brain Chiper pada Kamis, 20 Juni 2024. Serangan ransomware itu dilaporkan mengunci data di 282 kementerian/lembaga. Belum diketahui data apa saja yang bocor.

Berkaca pada kasus tersebut diatas, Pemerintah Indonesia seyogyanya segera mengharmonisasi beleid perlindungan data pribadi dan segera menetapkan peraturan pelaksana dari Undang-Undang No. 1 Tahun 2024 dan Undang-Undang No. 27 Tahun 22 berupa Peraturan Pemerintah mengenai ketentuan pelindungan anak termasuk data pribadinya dan Badan Pengawas baik di media sosial maupun platform digital pada umumnya.

D. Referensi

Artikel jurnal

Acar, G., & Yalçınkaya, A. (2020). The Impact of Data Breaches on Consumer Trust in E-Commerce Platforms: A Quantitative Study. *Computers in Human Behavior*, Volume 112, 106452. DOI: 10.1016/j.chb.2020.106452

Agarwal, A., & Rathi, S. (2020). *A Study on Cybersecurity Threats and Their Impact on Business Organizations. Computers, Materials & Continua, Volume 64, Issue 3, pp. 1181-1194*.DOI: 10.32604/cmc.2020.011742

Bianchi, L., & Romano, M. (2022). *The Role of Legal Enforcement in Ensuring Data Privacy Compliance in E-Commerce: An Analysis of Global Trends. Journal of Internet Law, Volume 26, Issue 4, pp. 59-78*. DOI: 10.1080/0141907X.2022.2077652

Budi, A. R., & Suhartono, T. (2023). *Penerapan Kebijakan Perlindungan Data Pribadi oleh Pelaku Usaha E-Commerce di Indonesia. Jurnal Ilmiah Teknologi Informasi, Volume 11, Issue 1, pp. 45-58*.

Doherty, N. F., & Malone, J. (2020). *Security Challenges in Implementing Cybersecurity in Small and Medium Enterprises (SMEs): A Case Study Approach. Computers & Security, Volume 92, 101717*. DOI: 10.1016/j.cose.2020.101717

Erna Priliasari. Perlindungan Data Pribadi Konsumen dalam Transaksi E-Commerce . Rechts Vinding: Media Pembinaan Hukum Nasional. Volume dan Nomor: Volume 12, Nomor 2, Agustus 2023

Harrison, P., & Fitzgerald, J. (2022). *Data Privacy Management for Businesses: Legal Requirements and Practical Considerations in the Digital Marketplace. Journal of Privacy and Security, Volume 17, Issue 4, pp. 255-270*. DOI: 10.1016/j.jpriv.2022.07.003

Harrison, P., & Clarke, L. (2023). *Data Protection Compliance and Enforcement: The Role of Regulatory Authorities in E-Commerce. Journal of Cyber Law and Ethics, Volume 30, Issue 1, pp. 45-62*. DOI: 10.1080/1094192X.2023.2018650

Hasan, H. R., & Ibrahim, M. (2021). *Advanced Persistent Threats (APTs): Risks and Solutions for Cybersecurity in E-Commerce. Cybersecurity, Volume 7, Article 17*. DOI: 10.1186/s42400-021-00117-0

Hassan, W., & Ali, S. (2022). *A Review of Threats to Cybersecurity in the Internet of Things (IoT) Ecosystem and Countermeasures. Journal of Internet*

Services and Applications, Volume 13, Article 8. DOI: 10.1186/s13174-022-00109-4

Kumar, A., & Singh, M. (2022). *A Survey on Cybersecurity Threats, Vulnerabilities, and Countermeasures in E-Commerce Platforms. Journal of Information Security, Volume 13, Issue 4, pp. 156–171*. DOI: 10.1016/j.jis.2022.03.005

Kurniawan, A. S., & Pratama, I. A. (2022). *Tanggung Jawab Pelaku Usaha dalam Pengelolaan Data Pribadi di E-Commerce Indonesia. Jurnal Teknologi dan Sistem Informasi, Volume 14, Issue 4, pp. 175-189*. SINTA 1

Kurniawan, A. S., & Pratama, I. A. (2023). *Kepatuhan terhadap Regulasi Perlindungan Data Pribadi dan Penegakan Hukum di Indonesia: Perspektif Hukum dan Praktek di E-Commerce. Jurnal Administrasi Bisnis, Volume 15, Issue 1, pp. 65-79*.

Liu, Y., & Zhang, H. (2022). *Data Privacy Laws and Their Impact on E-Commerce: Compliance Challenges and Strategies. Journal of Business Research, Volume 138, pp. 195-209*. DOI: 10.1016/j.jbusres.2021.09.056

López, C., & Pérez, J. (2022). *The Role of Data Protection Laws in E-Commerce: A Comparative Study of GDPR, CCPA, and Other Regional Frameworks. Journal of Global Information Technology Management, Volume 25, Issue 2, pp. 124–143*. DOI: 10.1080/1097198X.2022.2044513

Matsumoto, K., & Kikuchi, H. (2020). *Challenges in Implementing Cybersecurity Frameworks for Critical Infrastructure Protection: A Comparative Study. International Journal of Critical Infrastructure Protection, Volume 31, 100374*. DOI: 10.1016/j.ijcip.2020.100374

Mikkonen, T., & Laukkanen, T. (2023). *Obligations of Businesses in Personal Data Management: Challenges and Legal Compliance in the Digital Age. Journal of Business Research, Volume 154, pp. 314-324*.DOI: 10.1016/j.jbusres.2022.11.054

Putri, R. A., & Setiawan, D. (2023). *Kewajiban Pengelolaan Data Pribadi dalam E-Commerce: Studi Kasus pada Platform Digital di Indonesia. Jurnal Hukum dan Pembangunan, Volume 55, Issue 2, pp. 105-119*. SINTA 2

Rahman, A., & Santosa, P. (2022). *Regulasi dan Kewajiban Pengelolaan Data Pribadi oleh Pelaku Usaha: Perspektif Hukum dan Praktik di Indonesia. Jurnal Ilmu Hukum, Volume 16, Issue 3, pp. 105-118*.

Rambe, R. F. A., & dkk. (2023). Penerapan UU ITE (Informasi dan Transaksi Elektronik) dan UU Perlindungan Konsumen pada

kasus jual beli jasa review palsu. *Journal on Education,* 6(1), 10030–10040.

Rashid, U., & Iqbal, M. (2020). *Emerging Cybersecurity Threats: A Review of Recent Attacks and Security Solutions. Computers & Security, Volume 92, 101725*. DOI: 10.1016/j.cose.2020.101725

Salloum, S. A., & Al-Sayyed, R. (2021). *Emerging Threats and Security Challenges in Cloud Computing Environments: A Systematic Review. Journal of Cloud Computing: Advances, Systems and Applications, Volume 10, Article 35*. DOI: 10.1186/s13677-021-00243-2

Sharma, R., & Patel, R. (2020). *Security Challenges in Smart Cities: A Review of Current Solutions and Gaps. Journal of Ambient Intelligence and Humanized Computing, Volume 11, Issue 7, pp. 2819–2831*. DOI: 10.1007/s12652-020-02082-1

Sharma, S., & Joshi, M. (2021). Understanding the Impact of Data Privacy Violations on Customer Loyalty in E-Commerce. *Journal of Retailing and Consumer Services*, Volume 61, 102587. DOI: 10.1016/j.jretconser.2021.102587

Smith, A. L., & Tang, X. (2022). *The Legal Obligations of Businesses Regarding Personal Data Protection: A Comparative Analysis of GDPR and CCPA. Journal of Cybersecurity and Privacy, Volume 5, Issue 2, pp. 45–60*. DOI: 10.3390/jcp5020045

Smith, A. L., & Green, T. (2023). *The Importance of Legal Compliance and Enforcement in Personal Data Protection: A Global Perspective on GDPR and Beyond. Journal of Business Ethics, Volume 182, Issue 2, pp. 459-474*. DOI: 10.1007/s10551-022-05201-2

Tao, Z., & Liu, L. (2022). *Business Obligations in the Management of Personal Data in E-Commerce: An Analysis of Global Compliance Practices. International Journal of Information Management, Volume 63, 102456*. DOI: 10.1016/j.ijinfomgt.2021.102456

Tian, Y., Liu, Y., & Sun, J. (2021). Cybersecurity Threats in E-Commerce: A Survey and New Challenges. *Journal of Information Security and Applications*, Volume 58, 102701. DOI: 10.1016/j.jisa.2020.102701

Tritsini, E., & Papageorgiou, A. (2022). Data Breaches and Their Impact on Organizational Reputation: Evidence from the E-Commerce Sector. *Journal of Business Research*, Volume 146, pp. 1029–1041. DOI: 10.1016/j.jbusres.2022.02.028

Tung, H. T., & Nguyen, H. K. (2023). *Data Protection Regulations and Compliance in E-Commerce: The Case of GDPR and Beyond. Computers,*

Materials & Continua, Volume 70, Issue 6, pp. 5193–5213. DOI: 10.32604/cmc.2023.020532

Wang, X., & Chen, L. (2022).The Role of Data Encryption in Protecting E-Commerce Transactions from Data Breaches. *Computers & Security*, Volume 107, 102272. DOI: 10.1016/j.cose.2021.102272

Wang, Y., & Zhang, R. (2023). *Corporate Responsibilities in Personal Data Protection and Management: Examining the Role of Data Controllers. Journal of Global Information Technology Management, Volume 26, Issue 1, pp. 36-51*. DOI: 10.1080/1097198X.2022.2128465

Yadav, M., & Suri, P. (2020). Cybersecurity in E-Commerce: A Critical Review of the Risks of Data Breaches. *Journal of Information Security and Applications*, Volume 54, 102560. DOI: 10.1016/j.jisa.2020.102560

Zhang, Y., & Yang, Z. (2021). Impact of Ransomware and Malware on the Cybersecurity Landscape: A Review of Recent Attacks and Countermeasures. *Computers & Security*, Volume 99, 102035. DOI: 10.1016/j.cose.2020.102035

Zhao, Y., & Xu, X. (2020). *An Investigation into the Recent Cyber Threats to Critical Infrastructure and Mitigation Techniques. International Journal of Critical Infrastructure Protection, Volume 29, 100343*. DOI: 10.1016/j.ijcip.2020.100343

Zhou, J., & Zhang, X. (2021). *Challenges in the Implementation of Security Policies in Large-Scale Distributed Systems: A Survey and Recommendations. Computers, Materials & Continua, Volume 68, Issue 3, pp. 2341-2360*. DOI: 10.32604/cmc.2021.013343

Zhao, L., & Chen, J. (2023). *Regulatory Compliance and Enforcement in Personal Data Protection: Challenges and Strategies for E-Commerce. Information Systems Journal, Volume 33, Issue 1, pp. 93–112*. DOI: 10.1111/isj.12399

Zhao, S., & Liu, Y. (2023). *Privacy and Security Regulations in E-Commerce: A Global Perspective. Information Systems Frontiers, Volume 25, Issue 4, pp. 971–987*. DOI: 10.1007/s10796-022-10287-9

Buku

Isnaeni. Moch, Seberkas Diaroma Hukum Kontrak (Surabaya: PT Revka Petra Media, 2017), hlm. 159

Kristiyanti, Celina Tri Siwi. 2009, Hukum Perlindungan Konsumen. (Jakarta, Sinar Grafika, 2009), hal. 25

Mochtar Kusumaatmadja dan B. Arief Sidharta, Pengantar Ilmu Hukum Suatu Pengenalan Pertama Ruang Lingkup Berlakunya Ilmu Hukum, Bandung: PT. Alumni, 2013, hal.50

Mahran, Z. A., & Sebyar, M. H. (2023). Pengaruh Peraturan Menteri Perdagangan (PERMENDAG) Nomor 31 Tahun 2023 terhadap perkembangan e-commerce di Indonesia. *Hakim,* 1(4), 51–67.

Susanti Agung Nugroho. 2008. Proses Penyelesaian Sengketa Konsumen Ditinjau dari Hukum Acara Serta Kendala Implementasinya, Kencana. Jakarta. hal 13

Internet

https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en , diakses pada tanggal 24 November 2024, Pukul 14.04 Wita

https://www.cnbcindonesia.com/tech/20241201190314-37-592508/elon-musk-minta-pengadilan-federal-larang-openai-cari-cuan, diakses pada tanggal 02 Desember 2024, Pukul 12.02 Wita

https://www.medcom.id/teknologi/news-teknologi/8koPDdWK-kasus-kebocoran-data-pribadi-di-indonesia-10-kejadian-terbesar-yang-perlu-diketahui

BAB 7

DATA PRIBADI DAN TEKNOLOGI KECERDASAN BUATAN (AI)

Dr. H. Muhammad Syaukani, S.T., S.H., M.Cs, M.Kom

(Institut Teknologi Bisnis dan Bahasa "Dian Cipta Cendikia")

A. Pendahuluan

Perkembangan Teknologi kecerdasan buatan (AI) telah mengubah cara kita berinteraksi dengan dunia digital, meningkatkan efisiensi dan produktivitas di berbagai sektor, serta membuka peluang baru dalam pemrosesan dan analisis data. AI, yang melibatkan pengembangan algoritma dan sistem yang mampu meniru atau meningkatkan kemampuan kognitif manusia, semakin digunakan dalam berbagai aplikasi, dari rekomendasi produk di platform e-commerce hingga analisis medis dan keputusan bisnis berbasis data. Namun, di balik semua potensi yang ditawarkan oleh AI, terdapat tantangan besar terkait dengan data pribadi yang digunakan untuk melatih dan menjalankan algoritma ini.

Data pribadi merujuk pada informasi yang dapat digunakan untuk mengidentifikasi individu, seperti nama, alamat, nomor telepon, informasi finansial, riwayat kesehatan, data lokasi, dan banyak lainnya. Di era digital saat ini, data pribadi menjadi salah satu komoditas yang sangat berharga. Banyak perusahaan dan organisasi mengumpulkan data pribadi dalam jumlah besar untuk meningkatkan layanan mereka, mengoptimalkan pengalaman pengguna, dan mengembangkan produk baru. Dalam konteks ini, AI memerlukan data pribadi untuk menghasilkan prediksi yang lebih akurat dan mengambil keputusan yang lebih tepat, baik dalam skala individu maupun dalam analisis big data untuk keperluan perusahaan dan pemerintahan.

Namun, penggunaan data pribadi dalam pengembangan dan penerapan teknologi AI membawa berbagai risiko yang perlu dikelola

dengan hati-hati. Isu privasi, keamanan data, serta potensi penyalahgunaan informasi pribadi adalah beberapa tantangan yang dihadapi. Selain itu, karena AI mengandalkan data dalam jumlah besar untuk belajar dan membuat keputusan, ada risiko bahwa algoritma yang digunakan bisa menjadi bias atau tidak transparan, yang mengarah pada keputusan yang tidak adil atau diskriminatif. Oleh karena itu, penting untuk memahami keseimbangan antara potensi AI dalam meningkatkan kehidupan manusia dan kebutuhan untuk melindungi data pribadi yang sangat sensitif.

Selain itu, penggunaan data pribadi dalam teknologi AI juga melibatkan pertanyaan-pertanyaan mendasar terkait dengan etika dan regulasi. Siapa yang memiliki hak atas data pribadi? Bagaimana cara data tersebut dikumpulkan dan digunakan secara sah? Apa konsekuensi dari penggunaan data pribadi yang tidak tepat atau tidak sah? Regulasi seperti General Data Protection Regulation (GDPR) di Eropa dan California Consumer Privacy Act (CCPA) di Amerika Serikat mulai mengatur bagaimana data pribadi harus dikelola, memastikan transparansi, dan memberikan kontrol kepada individu atas data mereka.

Dalam pengantar ini, akan dibahas secara lebih mendalam tentang bagaimana data pribadi dan AI berinteraksi, tantangan yang muncul dari penggunaan data pribadi dalam aplikasi AI, serta pentingnya penerapan regulasi dan prinsip etika untuk menjaga privasi individu sambil memanfaatkan potensi penuh dari teknologi ini.

B. Hubungan Antara Data Pribadi dan AI

AI mengandalkan data untuk melakukan tugasnya, terutama dalam pembelajaran mesin (machine learning), di mana sistem AI dilatih untuk mengenali pola dan membuat prediksi berdasarkan data yang dimasukkan. Dalam banyak kasus, data yang digunakan untuk melatih model AI adalah data pribadi yang mencakup informasi tentang individu, perilaku mereka, serta preferensi atau kebiasaan mereka.

Contohnya, dalam aplikasi seperti rekomendasi produk e-commerce, asisten virtual, atau bahkan dalam sistem pengenalan wajah di keamanan publik, AI mengumpulkan dan memproses data pribadi

untuk menghasilkan keputusan atau rekomendasi yang lebih tepat dan relevan bagi pengguna. Sebagai contoh, jika sistem e-commerce mengumpulkan data perilaku belanja dan preferensi produk dari pengguna, AI dapat menganalisis data tersebut untuk memberikan rekomendasi produk yang sesuai dengan minat dan kebutuhan pengguna.

Namun, pengumpulan data pribadi ini mengarah pada beberapa masalah utama:

1) **Resiko Privasi** : Data pribadi yang dikumpulkan dapat mengungkapkan informasi sensitif tentang individu, seperti kebiasaan pribadi, status kesehatan, atau informasi finansial. Pengelolaan dan perlindungan data ini sangat penting untuk menjaga privasi individu.
2) **Penyalahgunaan Data**: Data pribadi yang dikumpulkan oleh organisasi atau lembaga bisa saja digunakan untuk tujuan yang tidak sesuai dengan niat awal pengguna memberikan data tersebut. Misalnya, data dapat dijual atau dibagikan dengan pihak ketiga tanpa persetujuan yang jelas dari pengguna, yang melanggar kepercayaan pengguna.
3) **Bias Algoritma**: Ketika AI dilatih dengan data yang tidak representatif atau mengandung bias, algoritma yang dihasilkan dapat memperburuk ketidakadilan sosial. Misalnya, dalam sistem AI untuk peminjaman kredit, jika data historis yang digunakan lebih cenderung mendiskriminasi kelompok tertentu, maka keputusan yang dihasilkan bisa merugikan kelompok tersebut.
4) **Keamanan Data**: Data pribadi yang digunakan dalam teknologi AI rentan terhadap ancaman siber. Kebocoran data atau pencurian informasi sensitif dapat menimbulkan kerugian besar bagi individu dan organisasi yang terlibat.

C. Regulasi dan Etika dalam Penggunaan AI dan Data Pribadi

Penggunaan data pribadi dalam AI memerlukan regulasi yang ketat untuk melindungi privasi dan mencegah penyalahgunaan. Beberapa regulasi utama yang mulai diterapkan di seluruh dunia untuk melindungi data pribadi adalah:

1) **General Data Protection Regulation (GDPR)** : Diimplementasikan oleh Uni Eropa, GDPR memberi kontrol yang lebih besar kepada individu atas data pribadi mereka dan menetapkan kewajiban yang lebih ketat bagi organisasi dalam mengumpulkan, menyimpan, dan mengelola data pribadi.
2) **California Consumer Privacy Act (CCPA)**: Sebuah undang-undang yang memberikan hak lebih kepada konsumen di California untuk mengetahui apa yang terjadi dengan data pribadi mereka, serta memberikan kontrol lebih besar atas data tersebut.
3) **Etika Penggunaan AI** : Penting untuk mengembangkan dan menerapkan prinsip etika yang mengutamakan transparansi, akuntabilitas, dan keadilan dalam penggunaan AI. Ini mencakup memastikan bahwa algoritma AI tidak diskriminatif, dapat dipertanggungjawabkan, dan tidak melanggar hak privasi individu.

D. Penggunaan Data Pribadi dalam Algoritma AI

Penggunaan data pribadi dalam algoritma kecerdasan buatan (AI) menjadi isu yang semakin relevan dalam era digital saat ini. Data pribadi merujuk pada informasi yang dapat digunakan untuk mengidentifikasi individu, baik secara langsung (seperti nama dan alamat) maupun tidak langsung (seperti preferensi atau riwayat aktivitas online). Algoritma AI memanfaatkan data pribadi untuk meningkatkan efektivitas dan personalisasi layanan yang diberikan kepada pengguna. Proses penggunaan data pribadi dalam AI dimulai dengan pengumpulan informasi dari berbagai sumber, termasuk aplikasi, perangkat pintar, dan platform online. Data ini kemudian diproses dan dianalisis untuk melatih model AI, memungkinkan sistem untuk "belajar" dari pola-pola yang ada dalam data tersebut. Hasilnya, AI dapat memberikan rekomendasi, prediksi, atau personalisasi yang lebih relevan, seperti dalam sistem rekomendasi produk atau layanan, analisis kesehatan berbasis data medis, atau personalisasi iklan yang lebih tepat sasaran.

Namun, penggunaan data pribadi dalam AI juga membawa tantangan yang signifikan, terutama terkait dengan privasi dan keamanan data. Pengumpulan data pribadi seringkali dilakukan tanpa transparansi yang memadai, dan individu mungkin tidak sepenuhnya memahami

bagaimana data mereka digunakan atau siapa yang memiliki akses ke data tersebut. Selain itu, data pribadi yang digunakan dalam pelatihan AI dapat menciptakan potensi bias atau diskriminasi. Misalnya, jika data yang digunakan tidak representatif atau mengandung bias tertentu, algoritma AI yang dihasilkan dapat memperburuk ketidaksetaraan dalam keputusan yang diambil, seperti dalam proses perekrutan berbasis AI atau penilaian kredit. Oleh karena itu, penting untuk memperhatikan regulasi perlindungan data, seperti **GDPR (General Data Protection Regulation)** di Uni Eropa, yang memberikan kontrol lebih besar kepada individu atas data pribadi mereka dan mengharuskan transparansi dari organisasi yang menggunakan data tersebut.

Meskipun tantangan tersebut ada, penggunaan data pribadi dalam AI juga menawarkan manfaat yang signifikan. Salah satunya adalah kemampuan untuk mempersonalisasi layanan, yang meningkatkan pengalaman pengguna. Misalnya, di platform e-commerce atau media sosial, algoritma AI dapat memberikan rekomendasi produk atau konten yang lebih relevan berdasarkan perilaku dan preferensi pengguna. Selain itu, AI juga dapat meningkatkan efisiensi dan akurasi dalam berbagai bidang, seperti dalam diagnosis medis berbasis data kesehatan pribadi yang dapat membantu profesional medis dalam mengambil keputusan yang lebih tepat. Meskipun demikian, penting untuk memastikan bahwa penggunaan data pribadi dalam AI dilakukan dengan cara yang etis dan sesuai dengan prinsip-prinsip privasi, serta memperhatikan potensi dampak sosial dan ekonomi yang mungkin timbul akibat penyalahgunaan data pribadi.

Penggunaan data pribadi dalam algoritma kecerdasan buatan (AI) adalah topik yang semakin relevan seiring berkembangnya teknologi dan penerapannya dalam berbagai sektor kehidupan. Dengan kemajuan pesat dalam bidang AI, banyak sistem AI yang memanfaatkan data pribadi untuk meningkatkan efisiensi, akurasi, dan personalisasi dalam layanan yang mereka tawarkan. Namun, di balik potensi manfaat tersebut, ada isu-isu penting yang terkait dengan privasi, keamanan data, dan etika penggunaan data pribadi.

1. Apa itu Data Pribadi dalam Konteks AI?

Data pribadi merujuk pada informasi yang dapat digunakan untuk mengidentifikasi individu secara langsung atau tidak langsung. Dalam konteks AI, data pribadi bisa mencakup:

- **Data identitas** : Nama, alamat, nomor identitas, atau data yang secara langsung mengidentifikasi seseorang.
- **Data demografis** : Usia, jenis kelamin, status perkawinan, pekerjaan, dll.
- **Data perilaku** : Riwayat penelusuran web, pembelian, aktivitas media sosial, preferensi, dll.
- **Data biometric** : Sidik jari, pengenalan wajah, suara, atau pola perilaku lainnya.
- **Data sensori** : Data yang dikumpulkan dari perangkat pintar seperti smartwatch atau sensor kesehatan.

Dalam AI, data pribadi ini digunakan untuk melatih model, memberikan rekomendasi, dan mengoptimalkan pengalaman pengguna.

2. Bagaimana Data Pribadi Digunakan dalam Algoritma AI?

Algoritma AI berfungsi untuk menganalisis, memproses, dan menarik kesimpulan dari data yang diberikan. Dalam konteks data pribadi, penggunaan ini terbagi dalam beberapa tahap:

a. Pengumpulan Data

Sistem AI sering mengumpulkan data pribadi melalui berbagai saluran, seperti aplikasi, perangkat pintar, situs web, dan interaksi dengan pengguna. Data ini bisa didapatkan langsung dari pengguna atau melalui pihak ketiga yang memantau perilaku pengguna secara online.

b. Pembersihan dan Penyaringan Data

Setelah data terkumpul, tahap berikutnya adalah pembersihan dan penyaringan untuk menghilangkan data yang tidak relevan atau rusak. Data yang sudah bersih akan lebih mudah dianalisis oleh algoritma AI.

c. Pelatihan Model AI

Model AI (seperti pembelajaran mesin atau deep learning) memerlukan data pribadi untuk "belajar" dari pola yang ada dalam data tersebut. Misalnya, algoritma yang digunakan dalam rekomendasi film akan mempelajari preferensi pengguna berdasarkan data perilaku mereka, seperti film yang sering ditonton atau di-klik.

d. Prediksi dan Personalisasi

Setelah model AI dilatih, ia dapat digunakan untuk membuat prediksi atau personalisasi berdasarkan data pribadi pengguna. Contoh nyata adalah personalisasi iklan, rekomendasi produk, atau bahkan diagnosis medis berbasis AI yang membutuhkan data kesehatan pribadi.

e. Optimasi dan Pembelajaran Berkelanjutan

Model AI dapat terus belajar dan berkembang dari data baru yang dikumpulkan seiring waktu. Hal ini memungkinkan sistem untuk semakin akurat dan relevan dalam memberikan hasil atau rekomendasi berdasarkan data pribadi yang terus diperbarui.

3. Keuntungan Penggunaan Data Pribadi dalam AI

Penggunaan data pribadi dalam AI menawarkan berbagai manfaat yang signifikan, di antaranya:

a. Personalisasi Layanan

Data pribadi memungkinkan sistem AI untuk memberikan pengalaman yang lebih dipersonalisasi. Sebagai contoh, aplikasi streaming musik seperti Spotify menggunakan data pendengaran pengguna untuk menyarankan lagu atau playlist yang sesuai dengan selera musik pengguna.

b. Peningkatan Efisiensi dan Akurasi

AI yang dilatih dengan data pribadi dapat meningkatkan efisiensi dalam proses pengambilan keputusan. Dalam bidang medis, misalnya, AI yang menggunakan data riwayat medis pasien dapat

membantu dokter dalam diagnosis penyakit dengan tingkat akurasi yang lebih tinggi.

c. Penyempurnaan Layanan Pelanggan

Banyak perusahaan menggunakan AI untuk meningkatkan pengalaman pelanggan melalui chatbot, analisis sentimen, atau layanan pelanggan otomatis yang menggunakan data pribadi untuk memahami kebutuhan dan preferensi pelanggan.

d. Inovasi dalam Produk dan Layanan

AI yang menggunakan data pribadi membuka peluang untuk menciptakan produk dan layanan yang lebih inovatif dan relevan. Misalnya, dalam dunia e-commerce, AI dapat menggunakan data pribadi untuk memperkenalkan produk yang lebih sesuai dengan kebutuhan dan keinginan pengguna.

4. Risiko dan Tantangan Penggunaan Data Pribadi dalam AI

Meskipun ada banyak keuntungan, penggunaan data pribadi dalam AI juga membawa risiko dan tantangan yang harus dihadapi, seperti:

a. Masalah Privasi

Salah satu masalah terbesar adalah pelanggaran privasi. Pengumpulan, penyimpanan, dan penggunaan data pribadi sering kali dilakukan tanpa pemahaman yang jelas mengenai bagaimana data tersebut digunakan atau siapa yang mengaksesnya. Ini bisa menyebabkan penyalahgunaan data pribadi, seperti pencurian identitas atau pengungkapan informasi sensitif tanpa izin pengguna.

b. Keamanan Data

Keamanan data pribadi yang digunakan dalam AI adalah masalah kritikal. Jika data tidak dilindungi dengan baik, maka dapat terjadi kebocoran data, yang dapat mengekspos individu kepada ancaman keamanan, seperti peretasan atau penggunaan data pribadi yang tidak sah.

c. Diskriminasi dan Bias

Algoritma AI yang dilatih dengan data pribadi rentan terhadap bias. Jika data yang digunakan untuk melatih model tidak representatif atau mengandung bias tertentu, maka hasil yang dihasilkan oleh AI dapat diskriminatif. Misalnya, algoritma perekrutan berbasis AI yang dilatih dengan data historis dapat memperkuat bias gender atau rasial yang ada dalam data tersebut.

d. Pengawasan dan Otomatisasi yang Berlebihan

Penggunaan data pribadi dalam AI juga dapat berisiko menciptakan sistem pengawasan yang berlebihan. Ketika data pribadi digunakan untuk memantau perilaku individu secara terus-menerus, hal ini dapat mengurangi tingkat kebebasan dan privasi individu dalam masyarakat.

5. Regulasi dan Etika dalam Penggunaan Data Pribadi dalam AI

Untuk memastikan penggunaan data pribadi dalam AI tidak merugikan pengguna atau melanggar hak privasi mereka, berbagai regulasi dan pedoman etika telah diterapkan di banyak negara. Beberapa hal yang perlu dipertimbangkan antara lain:

a. Regulasi Perlindungan Data Pribadi

Undang-Undang Perlindungan Data Pribadi, seperti GDPR (General Data Protection Regulation) di Uni Eropa, memberikan perlindungan yang lebih ketat terhadap data pribadi. GDPR mengharuskan perusahaan untuk meminta izin eksplisit dari pengguna sebelum mengumpulkan data pribadi, serta memberikan hak bagi individu untuk mengakses, mengubah, atau menghapus data pribadi mereka.

b. Transparansi dan Kontrol Pengguna

Prinsip transparansi menuntut perusahaan atau organisasi yang menggunakan AI dengan data pribadi untuk memberikan penjelasan yang jelas tentang bagaimana data dikumpulkan, digunakan, dan dilindungi. Pengguna juga harus diberikan kontrol atas data pribadi mereka, seperti hak untuk menarik persetujuan atau menonaktifkan

pengumpulan data.

c. Etika Penggunaan AI

Penerapan AI harus didasarkan pada prinsip-prinsip etika, seperti keadilan, transparansi, dan akuntabilitas. Penggunaan data pribadi dalam AI harus dilakukan dengan cara yang adil, tanpa menimbulkan kerugian atau ketidaksetaraan bagi individu atau kelompok.

E. Tantangan Privasi yang Dihadapi oleh AI

Tantangan privasi yang dihadapi oleh kecerdasan buatan (AI) semakin kompleks seiring dengan semakin meluasnya penerapan teknologi ini dalam berbagai sektor kehidupan. AI, yang mengandalkan pengumpulan dan analisis data pribadi dalam jumlah besar untuk melatih model dan memberikan layanan yang dipersonalisasi, menimbulkan kekhawatiran serius terkait dengan pelanggaran privasi. Salah satu tantangan utama adalah pengumpulan data pribadi yang sering kali dilakukan tanpa transparansi yang memadai. Banyak aplikasi dan layanan yang mengumpulkan informasi pengguna tanpa memberikan penjelasan yang cukup mengenai jenis data yang dikumpulkan, tujuan pengumpulan, dan bagaimana data tersebut akan digunakan. Pengguna sering kali tidak memiliki kontrol penuh atas data pribadi mereka, dan seringkali tidak diberi pilihan untuk mengelola atau menghapus data yang sudah terkumpul, yang dapat berujung pada potensi penyalahgunaan data.

Selain itu, AI dapat menimbulkan masalah terkait penyalahgunaan data pribadi. Data yang terkumpul dari berbagai platform sering digunakan untuk tujuan yang lebih luas, seperti iklan bertarget atau analisis perilaku, yang terkadang tidak sepenuhnya disetujui oleh pengguna. Hal ini berisiko mengarah pada eksploitasi data pribadi untuk keuntungan komersial tanpa memperhatikan hak privasi individu. Penyalahgunaan ini semakin diperburuk dengan potensi kebocoran data, baik akibat peretasan atau kelalaian dalam pengelolaan data oleh penyedia layanan. Keamanan data yang buruk dalam sistem AI dapat mengakibatkan akses tidak sah oleh pihak ketiga, yang bisa mengekspos

individu pada risiko pencurian identitas atau penipuan.

Masalah lain yang muncul adalah bias dalam algoritma AI. Jika data yang digunakan untuk melatih model AI tidak representatif atau mengandung bias, maka hasil dari AI bisa memperburuk ketidaksetaraan atau diskriminasi terhadap individu atau kelompok tertentu. Misalnya, algoritma rekrutmen yang dilatih dengan data historis yang mencerminkan ketidaksetaraan gender atau rasial dapat menghasilkan keputusan yang diskriminatif, memperburuk ketidakadilan dalam dunia kerja. Selain itu, pengenalan wajah dan teknologi pelacakan lainnya dapat digunakan untuk mengumpulkan data biometrik secara terus-menerus, menambah risiko pengawasan massal yang dapat mengurangi kebebasan individu.

Regulasi terkait dengan privasi data pribadi dalam AI, meskipun ada kemajuan, masih sering tertinggal dibandingkan dengan perkembangan teknologi itu sendiri. Beberapa wilayah, seperti Uni Eropa dengan penerapan GDPR (General Data Protection Regulation), telah menetapkan aturan ketat tentang perlindungan data pribadi. Namun, implementasi yang tidak konsisten di tingkat global dan celah hukum dalam banyak negara lainnya masih memungkinkan penyalahgunaan data terjadi. Oleh karena itu, untuk mengatasi tantangan privasi dalam AI, perlu adanya pendekatan yang lebih komprehensif yang mencakup regulasi yang lebih tegas, transparansi yang lebih besar dari perusahaan yang menggunakan data pribadi, serta peningkatan kesadaran dan kontrol bagi pengguna terhadap data mereka.

Seiring dengan semakin banyaknya aplikasi kecerdasan buatan (AI) dalam kehidupan sehari-hari, tantangan terkait privasi menjadi isu yang semakin mendesak. Privasi data dalam AI mencakup berbagai aspek, mulai dari pengumpulan data pribadi hingga bagaimana data tersebut digunakan, disimpan, dan dibagikan. Penggunaan data pribadi untuk melatih model AI menawarkan banyak keuntungan, seperti personalisasi layanan, prediksi yang lebih akurat, dan efisiensi yang lebih tinggi. Namun, proses tersebut juga menimbulkan berbagai tantangan yang perlu ditangani secara hati-hati untuk menghindari pelanggaran privasi dan penyalahgunaan data.

1. **Pengumpulan Data yang Tidak Transparan**

Salah satu tantangan terbesar dalam konteks privasi adalah pengumpulan data pribadi yang sering kali dilakukan tanpa transparansi yang memadai. Banyak aplikasi, layanan, dan perangkat yang mengumpulkan data pribadi pengguna secara otomatis. Pengguna sering kali tidak diberi informasi yang jelas mengenai jenis data yang dikumpulkan, bagaimana data tersebut digunakan, atau siapa yang memiliki akses ke data tersebut. Hal ini menimbulkan kekhawatiran mengenai ketidaktahuan pengguna atas penggunaan data mereka, yang bisa berpotensi disalahgunakan oleh pihak yang tidak bertanggung jawab. Misalnya, data yang awalnya dikumpulkan untuk satu tujuan bisa digunakan untuk tujuan lain yang tidak disetujui pengguna, seperti untuk iklan yang lebih tertarget atau untuk analisis perilaku yang invasif.

2. **Penyalahgunaan Data Pribadi**

Penyalahgunaan data pribadi adalah risiko besar dalam penggunaan AI. Meskipun banyak sistem AI mengandalkan data untuk meningkatkan pengalaman pengguna, ada kemungkinan data tersebut jatuh ke tangan pihak yang salah. Dalam beberapa kasus, data pribadi yang sensitif, seperti riwayat kesehatan, data keuangan, atau informasi pribadi lainnya, bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk tujuan yang merugikan individu. Misalnya, dalam kasus pelanggaran data, peretas dapat mengakses informasi pribadi yang digunakan oleh AI, yang kemudian bisa dieksploitasi untuk kejahatan seperti pencurian identitas, penipuan, atau manipulasi harga. Penggunaan algoritma AI dalam sistem yang tidak aman atau kurang terlindungi dapat menyebabkan kebocoran data yang merugikan individu dan masyarakat secara keseluruhan.

3. **Penggunaan Data Tanpa Izin atau Persetujuan**

Dalam banyak situasi, data pribadi yang digunakan untuk melatih model AI diambil tanpa izin eksplisit dari individu yang datanya dikumpulkan. Meskipun beberapa aplikasi meminta izin

pengguna, seringkali proses pemberian izin ini tidak jelas atau membingungkan bagi pengguna. Kadang-kadang, pengguna tidak diberi pilihan yang jelas untuk menolak atau memilih jenis data yang akan mereka bagikan. Hal ini dapat menyebabkan masalah privasi, terutama ketika data pribadi yang dikumpulkan digunakan dalam skala besar untuk tujuan yang tidak pernah dibayangkan atau disetujui oleh pengguna.

Regulasi seperti GDPR (General Data Protection Regulation) di Uni Eropa mencoba mengatasi masalah ini dengan mengharuskan perusahaan untuk mendapatkan persetujuan eksplisit dari pengguna dan memberikan kontrol penuh atas data pribadi mereka. Namun, di banyak bagian dunia, penerapan dan kepatuhan terhadap regulasi ini masih terbatas, yang memperburuk masalah privasi data dalam AI.

4. Bias dan Diskriminasi dalam Pengolahan Data

Salah satu tantangan yang sering dihadapi oleh algoritma AI terkait dengan privasi adalah adanya bias dalam data yang digunakan untuk melatih model. Data pribadi yang digunakan dalam AI sering kali mencerminkan ketidaksetaraan atau diskriminasi yang ada dalam masyarakat. Misalnya, algoritma yang dilatih dengan data historis dapat memperkuat bias rasial, gender, atau sosial yang sudah ada, sehingga menghasilkan keputusan yang tidak adil atau diskriminatif. Sebagai contoh, dalam algoritma rekrutmen berbasis AI, data historis yang cenderung merefleksikan preferensi atau kecenderungan bias terhadap jenis kelamin atau ras tertentu dapat menghasilkan rekomendasi yang memperburuk ketidaksetaraan di dunia kerja.

Bias ini menjadi masalah privasi karena dapat memperburuk posisi kelompok tertentu dalam masyarakat dan memperlebar kesenjangan sosial. Di samping itu, diskriminasi yang terintegrasi dalam model AI dapat menyebabkan individu atau kelompok menjadi lebih rentan terhadap pelanggaran privasi atau eksposur yang tidak proporsional terhadap data pribadi mereka.

5. Kurangnya Kontrol atas Data Pribadi

Privasi data dalam AI juga terancam oleh kurangnya kontrol

yang dimiliki individu atas data mereka. Banyak perusahaan atau organisasi yang mengumpulkan data pribadi tidak memberikan pengguna kontrol yang memadai untuk mengelola atau menghapus data mereka. Dalam beberapa kasus, pengguna mungkin tidak tahu bagaimana cara mengakses data mereka yang telah dikumpulkan atau bahkan bagaimana cara menghapusnya dari sistem. Ini menjadi masalah yang signifikan karena individu kehilangan kendali atas data mereka yang telah tersebar di berbagai platform digital.

Selain itu, data yang telah dikumpulkan untuk tujuan tertentu mungkin digunakan untuk tujuan lain tanpa sepengetahuan individu tersebut. Tanpa regulasi yang ketat dan mekanisme yang jelas, data pribadi dapat dipergunakan oleh pihak ketiga yang tidak terkait dengan tujuan awal pengumpulannya, meningkatkan risiko penyalahgunaan dan pelanggaran privasi.

6. Risiko Pengawasan Massal

AI yang diintegrasikan dengan teknologi pengenalan wajah, pelacakan lokasi, atau analisis perilaku dapat membuka potensi untuk pengawasan massal yang invasif. Dalam beberapa kasus, algoritma AI digunakan untuk memantau pergerakan individu atau kelompok dalam ruang publik dengan menggunakan data pribadi mereka tanpa sepengetahuan atau persetujuan. Misalnya, sistem pengawasan yang menggunakan AI dapat menganalisis video atau gambar yang diambil di tempat umum untuk melacak individu berdasarkan data biometrik mereka. Meskipun pengawasan ini dapat dianggap bermanfaat dalam beberapa konteks (seperti keamanan publik), hal ini menimbulkan kekhawatiran besar terkait pelanggaran privasi dan kebebasan individu.

Pengawasan massal yang menggunakan AI dapat mengarah pada masyarakat yang lebih terkendali dan terbatas kebebasannya, di mana individu terus-menerus dipantau dan dianalisis berdasarkan data pribadi mereka. Hal ini menimbulkan perdebatan tentang keseimbangan antara keamanan dan privasi dalam dunia yang semakin digital.

7. Keterbatasan dalam Regulasi dan Kepatuhan

Meskipun ada sejumlah regulasi yang diterapkan untuk melindungi data pribadi, seperti GDPR di Uni Eropa atau CCPA (California Consumer Privacy Act) di Amerika Serikat, penerapan aturan tersebut belum sepenuhnya merata di seluruh dunia. Negara-negara yang tidak memiliki regulasi yang ketat terkait dengan perlindungan data pribadi dapat menghadapi kesulitan dalam melindungi privasi individu yang menggunakan layanan berbasis AI. Selain itu, perusahaan besar yang mengembangkan teknologi AI seringkali beroperasi secara global, yang berarti mereka mungkin tidak selalu mematuhi hukum privasi lokal, mengingat kompleksitas regulasi di berbagai negara.

Regulasi yang ada pun sering kali terlambat dalam mengantisipasi perkembangan teknologi yang pesat. Banyak perusahaan dan penyedia layanan AI dapat memanfaatkan celah hukum atau mengembangkan praktik yang tidak sepenuhnya sesuai dengan semangat perlindungan privasi, sehingga menambah tantangan bagi upaya untuk mengatasi masalah privasi ini.

Tantangan privasi yang dihadapi oleh AI sangat kompleks dan memerlukan perhatian yang serius dari semua pihak yang terlibat, termasuk pengembang teknologi, regulator, dan pengguna. Meskipun AI memiliki potensi besar untuk meningkatkan efisiensi dan personalisasi layanan, masalah terkait privasi dan penyalahgunaan data tidak dapat diabaikan. Penting untuk memastikan bahwa data pribadi digunakan dengan cara yang transparan, aman, dan etis, serta memberikan pengguna kendali yang lebih besar atas informasi pribadi mereka. Selain itu, regulasi yang lebih ketat dan penerapan kebijakan yang lebih tegas perlu diterapkan untuk mencegah penyalahgunaan teknologi AI dalam konteks privasi. Ke depannya, kolaborasi antara pemerintah, industri, dan masyarakat akan menjadi kunci dalam menciptakan ekosistem AI yang dapat memberikan manfaat bagi semua pihak tanpa mengorbankan hak-hak individu.

F. Regulasi dan Etika Penggunaan AI dalam Pengolahan Data

Regulasi dan etika dalam penggunaan kecerdasan buatan (AI) dalam pengolahan data pribadi adalah isu yang semakin mendesak seiring dengan pesatnya perkembangan teknologi ini. AI, yang mengandalkan data dalam jumlah besar untuk melatih model dan menghasilkan keputusan otomatis, sering kali memanfaatkan informasi pribadi yang sensitif, seperti data kesehatan, finansial, atau perilaku online. Oleh karena itu, regulasi yang ketat dan prinsip etika yang kuat diperlukan untuk memastikan bahwa penggunaan AI dalam pengolahan data pribadi tidak merugikan individu dan menjaga hak-hak privasi mereka. Salah satu regulasi penting dalam hal ini adalah General Data Protection Regulation (GDPR) di Uni Eropa, yang memberikan kontrol lebih besar kepada individu atas data pribadi mereka. GDPR mewajibkan perusahaan untuk mendapatkan persetujuan eksplisit dari pengguna sebelum mengumpulkan data, menyediakan hak untuk mengakses, memperbaiki, atau menghapus data, serta memastikan bahwa data pribadi diproses secara transparan dan aman. Di Amerika Serikat, California Consumer Privacy Act (CCPA) juga memberikan hak kepada konsumen untuk mengetahui data apa yang dikumpulkan tentang mereka, serta hak untuk menghapusnya atau menolaknya untuk dijual kepada pihak ketiga. Namun, meskipun regulasi ini memberikan kerangka yang lebih jelas, tantangan terbesar adalah implementasi yang konsisten di seluruh dunia, mengingat negara-negara lain mungkin belum memiliki regulasi yang seketat GDPR.

Di sisi lain, prinsip etika sangat penting untuk membimbing penggunaan AI yang adil dan transparan. Salah satu isu etika utama adalah transparansi, di mana individu harus diberi informasi yang jelas dan mudah dipahami mengenai bagaimana data mereka dikumpulkan, digunakan, dan dianalisis oleh sistem AI. Pengguna juga harus memiliki kontrol atas data pribadi mereka, termasuk hak untuk mengakses, mengoreksi, atau menghapus data mereka, yang sejalan dengan prinsip privasi by design. Selain itu, penting untuk memastikan bahwa sistem AI tidak memperburuk bias yang ada dalam masyarakat, sehingga masalah keadilan dan non-diskriminasi menjadi kunci. Jika data yang digunakan untuk melatih model AI mengandung bias historis—seperti bias gender,

rasial, atau etnis—maka AI dapat memperkuat ketidaksetaraan dan menghasilkan keputusan yang diskriminatif. Oleh karena itu, pengembang AI harus memastikan bahwa data yang digunakan untuk melatih algoritma mencakup representasi yang adil dari berbagai kelompok, dan algoritma harus dirancang untuk meminimalkan bias. Akuntabilitas juga menjadi prinsip etika yang tak kalah penting. Organisasi yang mengembangkan atau menggunakan AI harus bertanggung jawab atas keputusan yang diambil oleh sistem, termasuk dampak sosial dan ekonomi yang ditimbulkan, seperti ketidaksetaraan atau pelanggaran privasi.

Meskipun regulasi dan prinsip etika ini memberikan panduan yang jelas, tantangan utama terletak pada ketidaksesuaian antara perkembangan teknologi yang sangat cepat dan kemampuan regulasi untuk mengimbanginya. Teknologi AI, seperti pengenalan wajah atau pelacakan perilaku, terus berkembang, sementara regulasi sering kali tertinggal, sehingga menciptakan celah hukum yang dapat dimanfaatkan untuk penyalahgunaan. Oleh karena itu, dibutuhkan pendekatan yang lebih dinamis dan proaktif dalam merumuskan regulasi dan standar etika yang dapat menyesuaikan dengan laju inovasi teknologi. Secara keseluruhan, regulasi yang ketat dan prinsip etika yang jelas sangat diperlukan untuk memastikan bahwa penggunaan AI dalam pengolahan data pribadi dilakukan dengan cara yang dapat dipercaya, adil, dan menghormati hak individu, serta untuk menghindari potensi dampak negatif yang bisa ditimbulkan dari penyalahgunaan data pribadi.

Regulasi dan etika dalam penggunaan kecerdasan buatan (AI) dalam pengolahan data pribadi adalah isu yang semakin penting di tengah pesatnya perkembangan teknologi AI. Sebagai teknologi yang mengandalkan pengumpulan dan analisis data dalam jumlah besar untuk melatih model dan memberikan layanan yang lebih cerdas, AI dapat mempengaruhi berbagai aspek kehidupan, mulai dari keputusan bisnis hingga layanan kesehatan, pendidikan, dan keamanan publik. Namun, dengan potensi besar yang dimilikinya, muncul berbagai tantangan terkait dengan perlindungan privasi, keadilan, dan transparansi. Oleh karena itu, penting untuk memiliki regulasi yang jelas dan prinsip etika yang solid untuk mengatur bagaimana data pribadi digunakan dalam

konteks AI.

1. Regulasi Perlindungan Data dalam Konteks AI

Regulasi yang mengatur penggunaan data pribadi dalam pengolahan AI bertujuan untuk melindungi hak individu serta mencegah penyalahgunaan data. Beberapa regulasi utama yang telah diterapkan secara global termasuk General Data Protection Regulation (GDPR) di Uni Eropa dan California Consumer Privacy Act (CCPA) di Amerika Serikat.

1) General Data Protection Regulation (GDPR) : GDPR, yang diberlakukan pada tahun 2018, adalah salah satu regulasi perlindungan data pribadi yang paling ketat di dunia. GDPR memberikan hak yang lebih besar kepada individu atas data pribadi mereka, termasuk hak untuk mengakses, memperbaiki, menghapus, atau membatasi penggunaan data pribadi. Salah satu aspek penting dari GDPR adalah prinsip "privacy by design", yang mengharuskan organisasi untuk merancang sistem dan aplikasi dengan mempertimbangkan privasi sejak awal. Regulasi ini juga mengharuskan perusahaan untuk meminta izin eksplisit dari pengguna sebelum mengumpulkan dan memproses data pribadi mereka, serta memberikan transparansi terkait dengan tujuan dan cara penggunaan data.
2) California Consumer Privacy Act (CCPA) : CCPA, yang mulai berlaku pada tahun 2020, memberikan hak kepada konsumen di California untuk mengetahui data pribadi apa yang dikumpulkan tentang mereka, untuk mengakses data tersebut, serta untuk meminta agar data pribadi mereka dihapus. CCPA juga mengharuskan perusahaan untuk memberitahukan kepada pengguna jika data mereka akan digunakan untuk tujuan komersial, serta memberikan hak untuk menolak penjualan data pribadi mereka kepada pihak ketiga.

Namun, meskipun regulasi seperti GDPR dan CCPA telah memberikan kerangka kerja yang kuat untuk melindungi data pribadi, tantangan masih tetap ada dalam hal implementasi yang konsisten, terutama di negara-negara yang belum memiliki regulasi yang setara.

Selain itu, teknologi AI terus berkembang dengan cepat, dan regulasi sering kali kesulitan untuk mengikuti perkembangan tersebut, sehingga menyebabkan celah hukum yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.

2. Etika Penggunaan AI dalam Pengolahan Data

Selain regulasi formal, prinsip etika juga memainkan peran penting dalam menentukan bagaimana AI harus digunakan dalam pengolahan data pribadi. Etika AI mengacu pada seperangkat nilai yang mengarah pada penggunaan teknologi AI yang adil, transparan, dan bertanggung jawab. Beberapa isu etika utama dalam konteks pengolahan data oleh AI meliputi:

a. Transparansi dan Akuntabilitas

Transparansi adalah prinsip etika yang penting dalam penggunaan AI. Pengguna dan individu yang datanya digunakan untuk melatih model AI berhak mengetahui bagaimana data mereka dikumpulkan, digunakan, dan dianalisis. Hal ini juga mencakup keterbukaan dalam cara algoritma AI bekerja, terutama dalam keputusan yang mempengaruhi kehidupan individu, seperti dalam sistem perekrutan berbasis AI atau penilaian kredit. Organisasi harus memberikan informasi yang jelas mengenai proses penggunaan data dan memberikan penjelasan yang dapat dipahami tentang bagaimana keputusan dibuat oleh sistem AI.

Akuntabilitas juga sangat penting. Meskipun AI dapat mengambil keputusan secara otomatis, organisasi yang mengembangkan atau menggunakan teknologi AI harus bertanggung jawab atas keputusan yang diambil oleh sistem tersebut. Ini termasuk bertanggung jawab atas dampak sosial dan ekonomi dari keputusan AI, seperti diskriminasi atau bias yang mungkin terjadi dalam hasil yang diberikan oleh model AI.

b. Keadilan dan Non-Diskriminasi

Penggunaan data pribadi dalam AI harus dilakukan dengan cara yang adil dan tidak diskriminatif. Model AI yang dilatih dengan data historis dapat memperkuat bias yang sudah ada dalam masyarakat,

seperti bias gender, rasial, atau etnis, yang dapat menghasilkan keputusan yang tidak adil atau bahkan merugikan kelompok tertentu. Misalnya, dalam proses seleksi pekerjaan berbasis AI, data yang tidak representatif atau mengandung bias terhadap gender atau ras dapat menyebabkan algoritma menghasilkan rekomendasi yang cenderung mendiskriminasi kandidat dari kelompok tertentu.

Prinsip fairness (keadilan) mengharuskan bahwa data yang digunakan untuk melatih model AI mencerminkan keberagaman dan representasi yang tepat dari populasi yang lebih luas. Selain itu, algoritma harus dirancang sedemikian rupa sehingga tidak memperburuk ketidaksetaraan yang ada, dan pengguna harus diberi kesempatan untuk menantang keputusan yang dihasilkan oleh sistem AI jika mereka merasa keputusan tersebut tidak adil.

c. Privasi dan Keamanan

Privasi adalah salah satu isu etika yang paling signifikan dalam penggunaan data pribadi oleh AI. Pengumpulan dan pemrosesan data pribadi harus dilakukan dengan izin eksplisit dari individu yang bersangkutan, dan data pribadi yang dikumpulkan harus dijaga dengan cara yang aman. Dalam konteks AI, data sensitif seperti informasi kesehatan, keuangan, atau biometrik memerlukan perlindungan yang lebih ketat karena potensi dampak yang lebih besar jika data tersebut jatuh ke tangan yang salah. Selain itu, penggunaan teknologi seperti enkripsi dan anonymization (pengaburan data) adalah penting untuk memastikan bahwa data pribadi tetap terlindungi meskipun digunakan dalam proses pengolahan oleh AI.

Selain itu, model AI harus dirancang dengan pertimbangan privacy by design (privasi sejak awal). Artinya, prinsip-prinsip perlindungan privasi harus diperhitungkan sejak tahap perancangan dan pengembangan teknologi AI, bukan sebagai tambahan setelah sistem selesai dibangun. Hal ini mencakup pengumpulan data yang minimal dan hanya untuk tujuan yang sah serta penyimpanan data yang aman.

d. Pengawasan dan Kontrol Pengguna

Dalam sistem AI yang melibatkan data pribadi, penting untuk memberikan pengguna kontrol yang lebih besar atas data mereka. Pengguna harus memiliki hak untuk mengakses, memperbarui, atau bahkan menghapus data pribadi mereka yang ada di sistem. Hal ini tidak hanya memberikan transparansi, tetapi juga memberi individu kendali atas bagaimana data mereka digunakan dan apakah mereka ingin berpartisipasi dalam sistem AI tertentu. Pengawasan terhadap bagaimana data pribadi digunakan oleh sistem AI juga penting, agar perusahaan atau organisasi yang mengembangkan AI dapat mempertanggungjawabkan setiap keputusan yang dibuat oleh sistem mereka.

3. Tantangan dalam Mengintegrasikan Regulasi dan Etika AI

Mengintegrasikan regulasi dan prinsip etika dalam penggunaan AI tidak selalu mudah. Salah satu tantangan utama adalah kurangnya standar internasional yang seragam untuk mengatur penggunaan data pribadi dalam pengolahan AI. Negara-negara yang berbeda memiliki pendekatan yang berbeda terhadap perlindungan data pribadi, yang dapat menimbulkan tantangan bagi perusahaan global yang mengoperasikan AI di banyak wilayah. Misalnya, meskipun GDPR memberikan pedoman yang jelas di Eropa, banyak negara di luar Eropa yang belum memiliki regulasi serupa, dan beberapa negara bahkan mungkin lebih longgar dalam hal perlindungan privasi.

Selain itu, perkembangan teknologi AI yang sangat cepat juga menambah kesulitan dalam merumuskan regulasi yang selalu relevan dan up-to-date. Regulasi yang ada saat ini sering kali tertinggal dibandingkan dengan kemampuan teknologi AI yang berkembang pesat. Sebagai contoh, teknologi pengenalan wajah dan pelacakan biometrik menghadirkan tantangan besar dalam hal privasi dan pengawasan massal, tetapi regulasi yang ada masih belum cukup kuat untuk mengatur penggunaan teknologi tersebut secara efektif.

Regulasi dan etika dalam penggunaan AI untuk pengolahan data pribadi sangat penting untuk memastikan bahwa teknologi ini digunakan secara bertanggung jawab, adil, dan transparan. Regulasi seperti GDPR dan CCPA memberikan kerangka hukum yang kuat

untuk perlindungan data pribadi, tetapi tantangan implementasi dan adaptasi terhadap perkembangan teknologi AI tetap ada. Etika dalam penggunaan AI, yang meliputi transparansi, keadilan, privasi, dan akuntabilitas, harus menjadi dasar dalam merancang dan menggunakan sistem AI yang melibatkan data pribadi. Pengguna harus diberikan kontrol lebih besar atas data mereka, dan perusahaan harus bertanggung jawab atas dampak sosial dan etika dari penggunaan AI. Dengan pendekatan yang tepat dalam regulasi dan etika, teknologi AI dapat dimanfaatkan secara maksimal tanpa mengorbankan hak-hak individu atau memperburuk ketidaksetaraan dalam masyarakat.

G. Studi Kasus Data Pribadi Dan Teknologi Kecerdasan Buatan

Pemanfaatan teknologi kecerdasan buatan (AI) dalam bidang pendidikan terus berkembang pesat, memfasilitasi pengajaran yang lebih personal, penilaian otomatis, serta pembelajaran berbasis data yang lebih efisien. Namun, penggunaan AI juga menghadirkan tantangan besar terkait dengan pengelolaan dan perlindungan **data pribadi** siswa. Data pribadi yang dikumpulkan untuk tujuan pembelajaran, seperti riwayat akademik, preferensi belajar, serta data perilaku online, harus dikelola dengan sangat hati-hati untuk menghindari pelanggaran privasi dan penyalahgunaan informasi. Dalam konteks ini, berikut adalah contoh studi kasus penggunaan AI dalam pendidikan serta solusi untuk mengatasi tantangan yang muncul.

1. Penggunaan AI dalam Penilaian dan Pemantauan Pembelajaran

a. Kasus: Penggunaan Sistem Pembelajaran Cerdas (Intelligent Tutoring Systems - ITS)

Sistem Pembelajaran Cerdas (ITS) adalah salah satu aplikasi AI yang semakin banyak digunakan di bidang pendidikan. ITS menggunakan data siswa, seperti jawaban dalam kuis, waktu yang dihabiskan pada setiap topik, serta pola perilaku belajar, untuk memberikan rekomendasi yang dipersonalisasi dan menyesuaikan materi pembelajaran berdasarkan kebutuhan siswa. Contohnya,

platform seperti Khan Academy menggunakan AI untuk menyesuaikan tingkat kesulitan soal yang diberikan kepada siswa berdasarkan kecepatan dan cara belajar mereka.

Namun, meskipun ITS bisa meningkatkan efisiensi pendidikan dan memberikan pengalaman belajar yang lebih personal, teknologi ini memerlukan pengumpulan data pribadi dalam jumlah besar untuk dapat berfungsi dengan baik. Data yang dikumpulkan mencakup hasil ujian, kebiasaan belajar, bahkan data sensitif terkait dengan latar belakang siswa, yang menimbulkan kekhawatiran terkait dengan privasi dan keamanan data.

b. Tantangan:

1) Privasi Data Siswa: Data yang dikumpulkan oleh sistem AI seringkali mengandung informasi yang sangat sensitif, terutama ketika digunakan untuk menyesuaikan pengalaman pembelajaran atau memberi penilaian. Penggunaan data pribadi tanpa izin eksplisit atau transparansi yang cukup dapat melanggar privasi siswa.
2) Keamanan Data: Dalam beberapa kasus, platform pembelajaran berbasis AI belum memiliki sistem keamanan yang memadai untuk melindungi data pribadi siswa dari potensi kebocoran atau pencurian data. Kebocoran data ini dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab, seperti dalam kasus peretasan platform edukasi atau penyalahgunaan data untuk tujuan komersial.
3) Bias dalam Model AI: Sistem AI yang digunakan dalam pendidikan, jika tidak dirancang dengan hati-hati, dapat mengandung bias berdasarkan data historis yang tidak representatif. Misalnya, sistem yang dilatih dengan data dari kelompok siswa tertentu (misalnya, siswa dengan latar belakang pendidikan tertentu) mungkin tidak akurat ketika diterapkan pada kelompok siswa yang lebih beragam.

c. Solusi untuk Mengatasi Tantangan:

1) Penerapan Kebijakan Perlindungan Data yang Ketat

Salah satu solusi utama untuk mengatasi masalah privasi adalah dengan memastikan bahwa penggunaan data pribadi siswa mematuhi regulasi perlindungan data yang ketat, seperti General Data Protection Regulation (GDPR) di Eropa atau Family Educational Rights and Privacy Act (FERPA) di Amerika Serikat. Kebijakan ini memastikan bahwa data siswa hanya digunakan untuk tujuan yang jelas dan sah, serta memberikan kontrol yang lebih besar kepada siswa dan orang tua atas data mereka. Misalnya, sebelum mengumpulkan atau menganalisis data, platform AI pendidikan harus meminta izin eksplisit dari siswa atau orang tua untuk mengakses dan memproses data pribadi mereka.

Pendidikan tentang hak privasi bagi siswa dan orang tua juga harus menjadi bagian dari kebijakan pendidikan, agar mereka memahami pentingnya memberikan persetujuan terhadap penggunaan data pribadi mereka serta hak mereka untuk menarik persetujuan tersebut kapan saja.

2) Penggunaan Teknologi Keamanan yang Lebih Baik

Untuk melindungi data pribadi, platform pendidikan berbasis AI perlu menerapkan teknologi enkripsi yang kuat untuk menyimpan dan mentransmisikan data. Penggunaan teknologi blockchain untuk keamanan data juga semakin mendapat perhatian, karena dapat menyediakan cara yang transparan dan terdesentralisasi untuk melacak dan melindungi data. Selain itu, pengembang teknologi AI harus memastikan bahwa sistem mereka secara teratur diuji untuk kerentanannya dan dilindungi dari potensi ancaman dunia maya, termasuk penetration testing dan pembaruan sistem yang terus-menerus.

Selain itu, institusi pendidikan dapat mengadopsi kebijakan penghapusan data secara otomatis setelah jangka waktu tertentu, untuk mengurangi risiko kebocoran data yang

disebabkan oleh penyimpanan data yang lama.

3) Penghindaran Bias melalui Desain yang Inklusif

Untuk mengatasi masalah bias dalam AI, penting untuk memastikan bahwa data yang digunakan untuk melatih sistem pendidikan berbasis AI mencakup populasi siswa yang beragam. Pengembang AI harus secara aktif mencari dan mengatasi bias yang ada dalam data dengan memastikan bahwa data representatif dari berbagai kelompok siswa, termasuk siswa dengan latar belakang etnis, ekonomi, dan geografi yang berbeda.

Selain itu, algoritma AI perlu dirancang dengan prinsip transparansi dan akuntabilitas yang tinggi, di mana setiap keputusan yang dibuat oleh AI dapat dipertanggungjawabkan, dan kesalahan atau bias dalam penilaian dapat diidentifikasi dan diperbaiki. Lembaga pendidikan dapat melakukan audit AI secara rutin untuk memeriksa apakah algoritma tersebut menghasilkan hasil yang adil dan tanpa bias.

4) Penerapan Prinsip 'Privacy by Design' dan 'Data Minimization'

Sebagai langkah preventif untuk menjaga privasi, prinsip Privacy by Design harus diterapkan dalam pengembangan teknologi AI untuk pendidikan. Artinya, pengembang AI harus merancang sistem yang meminimalkan pengumpulan data pribadi dan hanya mengumpulkan informasi yang benar-benar diperlukan untuk tujuan pembelajaran yang sah. Data yang tidak diperlukan untuk tujuan tersebut harus dihapus atau tidak dikumpulkan sama sekali.

Selain itu, anonymization atau pengaburan data juga bisa digunakan untuk mengurangi risiko pelanggaran privasi. Dengan mengaburkan informasi pribadi secara efektif, data yang digunakan untuk melatih model AI bisa tetap berguna untuk tujuan pendidikan tanpa mengungkapkan identitas individu siswa.

5) Peningkatan Pengawasan dan Kebijakan Regulasi dalam Pendidikan

Institusi pendidikan dan pengembang teknologi perlu bekerja sama dengan regulator untuk memastikan bahwa penggunaan AI dalam pendidikan sesuai dengan pedoman etika dan hukum yang ada. Pemerintah dan organisasi internasional perlu menetapkan pedoman yang jelas mengenai penggunaan AI dalam pengolahan data pribadi siswa, termasuk menetapkan standar keamanan data yang wajib dipatuhi oleh semua platform pendidikan berbasis AI. Selain itu, mereka harus memperbarui regulasi secara berkala untuk mengikuti perkembangan teknologi yang cepat dan memastikan bahwa regulasi tetap relevan dan efektif.

Penggunaan AI dalam pendidikan memiliki potensi yang sangat besar untuk meningkatkan pengalaman belajar, memberikan pembelajaran yang dipersonalisasi, serta meningkatkan efisiensi dan akurasi penilaian. Namun, penerapan AI dalam pengolahan data pribadi siswa juga membawa tantangan besar terkait dengan privasi, keamanan data, dan bias algoritma. Untuk memastikan bahwa AI digunakan secara bertanggung jawab dan tidak merugikan siswa, penting untuk mengadopsi regulasi yang ketat, mengimplementasikan prinsip etika yang kuat, serta memanfaatkan teknologi keamanan yang canggih. Dengan pendekatan yang tepat, penggunaan AI dalam pendidikan dapat memberikan manfaat maksimal tanpa mengorbankan hak privasi dan keadilan bagi siswa.

H. Referensi

Artikel jurnal

Mittelstadt, B. D., et al. (2016). "The ethics of algorithms: Mapping the debate." Big Data & Society, 3(2), 2053951716679679.

Tufekci, Z. (2015). "Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency." Colorado Technology Law Journal, 13(2), 203-218.

Schneier, B. (2018)."Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World." W. W. Norton &

Company.

Buku

O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown Publishing Group.

Zeng, D., et al. (2021). Artificial Intelligence and Privacy Protection: A Global Perspective. Springer.

Dastin, J. (2018). The Ethics of Artificial Intelligence and Robotics. Cambridge University Press.

Regulasi dan Laporan Kebijakan

European Commission (2016). General Data Protection Regulation (GDPR).

U.S. Federal Trade Commission (2012). Privacy and Security in a Digital Age: A Framework for the Digital Economy.

California Consumer Privacy Act (CCPA), 2018.

Artikel Berita dan Laporan Industri

O'Flaherty, K. (2020). "AI, big data, and privacy: How the tech industry is reshaping data protection." Wired.

AI Now Institute (2018). Discriminating Systems: Gender, Race, and Power in AI.

The World Economic Forum (2020). The Future of Privacy: Data and Artificial Intelligence in the Digital Age.

Artikel dan Publikasi Online

Kuner, C. (2020). "The General Data Protection Regulation: A Commentary." Oxford University Press.

Harari, Y. N. (2018). "The rise of the data religion." The Guardian.

Gibson, J. (2021). "AI and Privacy: Navigating Data Protection Challenges." The Conversation.

Website dan Platform Pembelajaran

European Commission: Artificial Intelligence and Data Protection [https://ec.europa.eu/info/business-economy-euro/banking-and-

finance/financial-services-consumers/ai-and-data-protection_en](https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-services-consumers/ai-and-data-protection_en)

AI Ethics Guidelines Global Inventory https://algorithmswatch.org/

BAB 8

KEBIJAKAN PERUSAHAAN DALAM PENGELOLAAN DATA PRIBADI

Moh. Muniri, S.H., M.Kn.

(Asmi Citra Nusantara Banjarmasin)

A. Pendahuluan

Di tengah perkembangan kemajuan teknologi digital seperti saat ini, Data Pribadi menjadi salah satu aset paling berharga bagi perusahaan. Data Pribadi ini dimaknai sebagai data tentang orang perorangan yang terinditifikasi atau dapat diindentifikasi secara tersendiri atau kombnasi dengan informasin lainnya baik secara langsung maupun tidak langsung maupun tidak langsung melalui sistem elektronik atau non elektronik, Data Pribadi dapat digunakan untuk mengidentifikasi orang perorangan, seperti nama, alamat, nomor identitas, nomor telepon, status perkawinandan bahkan kebiasan seseorang dalam bersosial media. Dalam Pemrosesan Data Pribadi melibatkan banyak pihak sebagaimana diatur dalam Undang – undang Nomor 27 tahun 2022 Tentang Perlindungan Data Pribadi antara lain setiap orang yang mengacu pada oran perorangan dan korporasi, badan publik dan organisasi internasional yang bertindak sendiri – sendiri atau bersama – sama dalam melakukan pemrosesasn data pribadi atas nama pengendali data pribadi sehingga mengharuskan pengelola / pemroses data harus hati – hati dalam mengelola data pribadi tersebut untuk menjaga data pribadi disalahgunakan oleh pihak – pihak yang tidak bertanggung jawab.

Di era digital seperti sekarang ini yang semakin terhubung, data pribadi menjadi sesuatu yang sangat bermanfaat bagi Perusahaan dalam mengelola karyawan, bisnis dan berinovasi agar perusahaan tetap eksis dalam persaingan yang kian kompetitif, namun pada saat yang sama juga membawa potensi risiko yang sangat besar apabila data pribadi ini tidak dilindungi secara maksimal, salah satu yang menjadi ancaman adalah

penyalahgunaan data pribadi atau pelanggaran terhadap hak-hak karyawan yang dapat menyebabkan dampak yang merugikan, baik bagi karyawan maupun perusahaan itu sendiri. Untuk itu, kebijakan yang mengatur bagaimana perusahaan mengumpulkan, menggunakan, menyimpan, dan melindungi data pribadi sangat diperlukan. Tanpa kebijakan yang jelas dan konsisten, perusahaan berisiko melanggar peraturan perundang – undangan yang berlaku serta berpotensi kehilangan kepercayaan dari pelanggan dan mitra kerja.

Kebijakan Pengelolaan data pribadi oleh Perusahaan sebagai Korporasi yang diatur dalam Peraturan perundang – undangan tidak hanya diperlukan untuk melindungi Karyawan dan Pelanggan namun juga menciptakan reputasi yang baik bagi perusahaan serta juga untuk mengetahui dan memastikan apakah perusahaan sudah mematuhi berbagai peraturan yang mengatur pengelolaan data pribadi, baik di tingkat global ataupun ditingkat nasional, ditingkat global ada regulasi seperti General Data Protection Regulation (GDPR) yang berlaku di Uni Eropa, Di Indonesia Perlindungan Data Pribadi diatur dalam beberapa Peraturan Perundang - undangan antara lain : Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, Undang – undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik dan Peraturan Menteri Komunikasi Dan Informatika Republik Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik yang mewajibkan setiap perusahaan atau korporasi untuk menjaga privasi dan keamanan data pribadi orang perorangan atau warga negara.

Dengan adanya bebertapa regulasi diatas, perusahaan baik yang bertindak sebagai Pengendali atau Pengolah Data diharapkan tidak hanya berfokus pada keuntungan yang bersifat komersial, tetapi juga fokus pada perlindungan data pribadi orang perongan atau warga negara, Kepatuhan terhadap hukum ini bukan hanya sebagai kewajiban yang diatur dalam perundang – undangan tetapi juga merupakan bentuk tanggung jawab perusahaan untuk menciptakan kepercayaan dan reputasi perusahaan dimata karyawan dan mitra kerja atau pelanggan.

Pengelolaan data pribadi selain mencakup langkah-langkah untuk memastikan data tersebut aman dari potensi ancaman mengingat ancaman terhadap data pribadi bisa datang dari berbagai sumber, baik internal maupun eksternal, seperti peretasan, pencurian identitas, atau penggunaan data untuk tujuan yang tidak sah. Juga harus mencakup prosedur untuk mencegah kebocoran data khususnya kepada pihak – pihak yang tidak bertanggung jawab dengan penggunaan enkripsi, autentikasi ganda, dan pembatasan akses ke data hanya pada pihak yang berwenang saja, Selain itu, perusahaan harus memiliki mekanisme yang memungkinkan individu untuk mengetahui dan mengontrol bagaimana data pribadi mereka diperlakukan. Prinsip transparansi dalam pengelolaan data sangat penting, di mana perusahaan wajib memberikan informasi yang jelas kepada individu mengenai jenis data yang dikumpulkan untuk tujuan apa saja penggunaan data tersebut, dan bagaimana mereka dapat mengakses atau meminta penghapusan (retensi) data pribadi mereka yang sudah dikumpulkan oleh Perusahaan.

Dalam Penulisan ini penulis hanya fokus pada Perusahaan sebagai Korporasi yang Mengumpulkan dan Mengelola Data Pribadi Karyawan atau Pelanggan sebagaimana yang diatur dalam Undang – undang no 27 Tahun 2022 tentang Perlindungan Data Pribadi untuk memastikan perlindungan dalam pengelooolaan data Perusahaan perlu menunjuk Karyawan atau pihak yang bekerja sama dengan perusahaan, Karyawan atau Perusahaan dimaksud bertugas untuk memastikan kebijakan dan prosedur yang diterapkan perusahaan sesuai dengan standar perlindungan data yang berlaku. Selain itu, perusahaan juga perlu melakukan audit dan pemantauan secara berkala untuk menilai apakah kebijakan ini diterapkan dengan efektif dan sesuai dengan perkembangan teknologi serta regulasi yang berlaku.

Secara keseluruhan, kebijakan perusahaan dalam pengelolaan data pribadi adalah upaya untuk menjaga keseimbangan antara kebutuhan bisnis untuk memanfaatkan data pribadi dalam operasionalnya dan kewajiban untuk melindungi hak-hak individu. Kebijakan ini tidak hanya memberikan perlindungan hukum bagi perusahaan, tetapi juga membangun kepercayaan Karyawan dan Pelanggan untuk keberlanjutan dan pertumbuhan perusahaan dalam jangka panjang terutama dalam

kompetisi yang semakin sengit seiring dengan perkembangan tehnologi digital.

B. Pembuatan Kebijakan Privasi Perusahaan

Pembuatan kebijakan privasi perusahaan adalah proses penting yang harus dilakukan oleh setiap Perusahaan yang mengumpulkan, menyimpan, atau memproses data pribadi Karryawan dan pelanggan. Kebijakan ini berfungsi sebagai pedoman yang mengatur bagaimana data pribadi dikumpulkan, digunakan, dilindungi, dan dibagikan oleh perusahaan, dengan tujuan utama untuk menjaga privasi individu dan memastikan kepatuhan terhadap peraturan yang berlaku. Sebuah kebijakan privasi yang baik harus disusun dengan jelas, transparan, dan mudah dipahami, sehingga pelanggan atau pengguna layanan perusahaan dapat mengetahui bagaimana informasi pribadi mereka diperlakukan.

Pembuatan Kebijakan Privasi ini adalah salah satu upaya dalam perlindungan data pribadi yang didefiniskan dalam Undang – undang No 27 tahun 2022 Tentang perlindungan Data Pribadi Pasal 1 angka 2 yang menyatakan bahwa Perlindungan Data Pribadi adalah Keseluruhan Upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin Hak Konstitusional Subjek Data Pribadi sedangkan perlindungan data Pribadi dalam sistem elektonik yang diatur dalam Permen Komunikasi dan informasi no 20 tahun 2016 Tentang Perlindungan data pribadi dalam sistem elektronik mencakup perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpan, penampilan pengumumman, pengiriman, penyebarluasan dan pemusnahan data pribadi;

Menurut Dwi Safitri "Kebijakan privasi adalah dokumen resmi yang menjelaskan bagaimana perusahaan mengumpulkan, menggunakan, menyimpan, dan melindungi data pribadi pengguna. Kebijakan ini biasanya mencakup informasi tentang jenis data yang dikumpulkan, tujuan penggunaan data tersebut, pihak ketiga yang mungkin memiliki akses ke data, serta hak-hak pengguna terkait data mereka. Kebijakan privasi adalah alat penting untuk transparansi dan kepatuhan terhadap regulasi perlindungan data".

Ada beberapa langkah yang harus dilakukan dalam membuat Kebijakan Privasi terhadap data yang ada yang pertama adalah mengidentifikasi Jenis Data Pribadi yang akan dikumpulkan. Ada 2 data jenis data yang dapat digolongkan yaitu Data Pribadi yang bersifat spesifik dan data pribadi yang bersifat umum Data pribadi yang bersita spesifik mencakup Informasi Kesehatan, Biometrik, genetika, catatan kejahatan, data anak, data keungan pribadi dan data lain yang sesuai dengan peraturan perundang – undangan. Dan data pribadi yang bersifat umum meliputi : Nama Lengkap, Jenis Kelamin, Kewarnagnegaraan, Agama, Status Perkawinan dan data Pribadi yang dikombinasikan untuk mengindentifikasi seseorang, Setiap jenis data pribadi yang dikumpulkan harus dijelaskan secara rinci dalam kebijakan privasi, termasuk tujuan pengumpulannya. Misalnya, data dikumpulkan untuk Menetukan tunjangan karyawan, memberikan layanan Kesehatan diperusahaan, atau untuk tujuan penentuan strategi pasar dan marketing.. Selain itu, perusahaan juga harus memberikan informasi jelas mengenai bagaimana dan kapan data tersebut akan digunakan, serta jika data akan dibagikan dengan pihak ketiga, seperti mitra atau penyedia layanan kesehatan atau asuransi, dan dengan alasan yang sah.

Penting untuk menjelaskan langkah-langkah yang diambil oleh perusahaan untuk melindungi data pribadi tersebut, baik dari pencurian, kebocoran, atau akses yang tidak sah. Keamanan data menjadi aspek kunci dalam kebijakan privasi, yang mencakup penggunaan teknologi enkripsi, pengelolaan akses yang ketat, dan penerapan prosedur untuk mendeteksi serta merespons pelanggaran data. Perusahaan juga perlu menginformasikan kepada pengguna tentang hak-hak mereka terkait data pribadi, seperti hak untuk mengakses data, memperbaiki informasi yang salah, atau menghapus data yang sudah tidak diperlukan lagi. Selain itu, kebijakan privasi harus mencakup bagaimana perusahaan menangani permintaan pengguna untuk menarik persetujuan mereka dalam penggunaan data pribadi dan bagaimana perusahaan akan menanggapi permintaan tersebut sesuai dengan hukum yang berlaku.

Dalam hal penyimpanan data, kebijakan privasi harus jelas tentang durasi penyimpanan data pribadi dan alasan mengapa data tersebut disimpan selama periode tertentu. Data pribadi hanya boleh disimpan

selama diperlukan untuk tujuan yang sah dan sesuai dengan kebijakan yang ada. Perusahaan juga harus memastikan bahwa pengguna diberi informasi terkait perubahan kebijakan privasi, dengan cara yang mudah dipahami dan sesuai dengan regulasi yang berlaku. Mengingat kebijakan privasi ini adalah dokumen yang hidup, perusahaan perlu secara rutin meninjau dan memperbarui kebijakan tersebut untuk menyesuaikan dengan perkembangan teknologi dan perubahan peraturan secara berkala seperti setiap setahun sekali dengan melibatkan peran aktif dari pemilik data pribadi contoh karyawan perusahaan dimana setiap setahun diminta untuk meng update data karyawan setiap awal tahun.

Secara keseluruhan, pembuatan kebijakan privasi oleh Perusahaan bukan hanya untuk memastikan kepatuhan terhadap peraturan perlindungan Data, Pribadi seperti Undang – undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi dan peraturan perundang – undangan lainnya yang ada kaitannya dengan data pribadi tetapi juga sebagai langkah untuk membangun trust/ kepercayaan karyawan dan pelanggan namun juga untuk menjaga hubungan yang baik dengan pelanggan atau mitra kerja perusahaan. Kebijakan ini menunjukkan bahwa perusahaan menghargai hak privasi individu dan berkomitmen untuk mengelola data pribadi dengan penuh tanggung jawab.

Pengaturan Pembuatan Kebijakan Privasi oleh Perusahaan atau Korporasi diatur dalam beberapa peraturan perundang – undangan antara lain Pasal 28G ayat (1) Undang – undang Dasar 1945, Pasal 65 dan Pasal 68 Undang – undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi dan Pasal 281 Kitab Undang – undang Hukum Pidana/KUHP.

Dalam Pasal 28G ayat (1) Undang – undang Dasar 1945 amandemen kedua yang menyatakan bahwa "Setiap orang berhak atas perlindungan 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 yang merupakan dasar dari dikeluarkan peraturan perundang – undangan yang mengatur tentang perlindungan data pribadi yaitu Undang – undanag no 27 tahun 2022

C. Praktik Baik dalam Pengelolaan Data Pribadi

Praktik baik dalam pengelolaan data pribadi merujuk pada serangkaian langkah dan kebijakan yang diterapkan perusahaan untuk memastikan bahwa data pribadi yang dikumpulkan, diproses, dan disimpan dikelola dengan aman, transparan, dan sesuai dengan peraturan yang berlaku. Salah satu praktik utama yang harus diterapkan adalah transparansi. Perusahaan wajib memberi tahu individu secara jelas tentang jenis data yang dikumpulkan, tujuan pengumpulannya, dan bagaimana data tersebut akan digunakan. Hal ini termasuk memberikan informasi yang mudah dimengerti dalam kebijakan privasi, yang harus tersedia dan mudah diakses oleh pengguna kapan saja. Selain itu, perusahaan juga harus menerapkan prinsip minimalisasi data, yang berarti hanya mengumpulkan data yang diperlukan untuk tujuan yang spesifik, tanpa mengumpulkan informasi yang berlebihan atau tidak relevan.

Keamanan data adalah praktik baik lainnya yang tidak boleh diabaikan. Data pribadi yang dikelola perusahaan harus dilindungi dengan sistem yang kuat, seperti enkripsi untuk data sensitif, kontrol akses yang ketat, serta perlindungan terhadap ancaman dari pihak ketiga yang tidak sah. Penggunaan sistem keamanan canggih dan pembatasan akses internal untuk karyawan atau pihak lain yang tidak perlu mengetahui data pribadi juga sangat penting untuk mencegah kebocoran atau penyalahgunaan data. Selain itu, perusahaan harus secara aktif melakukan audit dan pengujian berkala untuk memastikan bahwa langkah-langkah keamanan yang diterapkan masih efektif dan sesuai dengan perkembangan ancaman teknologi.

Praktik baik lainnya adalah memberikan kontrol penuh kepada pengguna atas data pribadi mereka. Pengguna harus memiliki hak untuk mengakses data mereka kapan saja, memperbarui informasi yang tidak akurat, dan menghapus data pribadi jika sudah tidak diperlukan lagi. Hal ini sejalan dengan prinsip hak atas data, yang juga mencakup hak untuk menarik persetujuan penggunaan data tanpa mempengaruhi layanan yang diberikan. Dalam hal ini, perusahaan harus menyediakan saluran yang mudah diakses bagi pengguna untuk mengajukan permintaan terkait data mereka, serta menjamin proses yang cepat dan transparan

dalam memenuhi permintaan tersebut.

Penting juga untuk memastikan bahwa data pribadi tidak disimpan lebih lama dari yang diperlukan untuk tujuan yang sah. Praktik penghapusan data yang tidak diperlukan secara berkala sangat penting dalam mengurangi risiko kebocoran data dan menjaga integritas sistem pengelolaan data perusahaan. Selain itu, perusahaan harus memperbarui kebijakan privasi mereka secara rutin untuk menyesuaikan dengan perubahan peraturan atau teknologi, serta memberi tahu pengguna tentang perubahan tersebut. Terakhir, pembinaan dan pelatihan kepada karyawan tentang bagaimana menangani data pribadi dengan aman dan sesuai kebijakan perusahaan juga merupakan praktik yang sangat dianjurkan. Semua langkah ini membentuk dasar dari praktik baik dalam pengelolaan data pribadi yang tidak hanya membantu perusahaan dalam mematuhi regulasi yang berlaku, tetapi juga dalam membangun kepercayaan dan menjaga hubungan yang baik dengan pengguna.

Pengelolaan data pribadi yang baik dan bertanggung jawab adalah salah satu elemen kunci dalam menjaga privasi individu serta membangun kepercayaan antara perusahaan dan pengguna atau konsumen. Praktik baik dalam pengelolaan data pribadi tidak hanya mencakup aspek kepatuhan terhadap peraturan perlindungan data yang berlaku, tetapi juga mencerminkan komitmen perusahaan untuk melindungi hak privasi dan meningkatkan transparansi dalam penggunaan data. Berikut adalah beberapa praktik terbaik yang harus diterapkan oleh perusahaan dalam pengelolaan data pribadi antara lain : Kepatuhan terhadap Peraturan perundang – undangan yang berlaku, Transparansi dalam Pengumpulan Data, Pengumpulan Data yang Minimal, Pengamanan Data yang Kuat, Hak Akses dan Pengontrolan Data, Pembatasan Akses Internal, Penghapusan Data yang Tidak Diperlukan, Penyuluhan dan Pendidikan Pengguna, valuasi dan Pembaruan Berkala dan Membangun Kepercayaan dan Komunikasi yang Terbuka

D. Audit dan Pengawasan Internal terhadap Data Pribadi

Audit dan Pengawasan internal terhadap Data Pribadi diperusahaan merupakan kegiatan yang wajib dilaksanakan untuk

menjaga reputasi, keamanan, dan kepatuhan dalam pengelolaan data pribadi di perusahaan. Audit berfungsi untuk memeriksa secara independen apakah perusahaan sudah mengikuti kebijakan privasi dan prosedur yang benar dalam mengumpulkan, menggunakan, menyimpan, dan menghapus data pribadi diperusahaan serta memastikan bahwa langkah-langkah pengamanan yang diperlukan sudah diterapkan secara efektif audit dapat dilakukan dengan internal audit atau eksternal audit, internal audit dilakukan oleh divisi khusus dalam perusahaan yang bertugas dan bertanggung jawab dalam melakukan audit diperusahaan dan sebagai fasilitator untuk berkomuniasi dengan ekternal auditor serta mendampingi auditee bila diaudit oleh eksternal auditor, audit dilaksanakan secara berkala atau secara isidentil bila diperlukan.

Internal audit dimulai dengan perencanaan dengan menentukan lead auditor dan auditor yang berkompoten dan mempunyai sertifikasi, auditor akan menentukan area mana yang perlu diaudit, sistem dan prosedur apa terkait dengan mengumpulan, penyimpanan, pengolahan dan penghapusan data pribadi, bagaimana kontrol akses terhadap data pribadi dan bagaimana sistem keamanan yang digunakan. Auditor kemudian mengumpulkan informasi yang relevan, seperti kebijakan privasi dan dokumen yang berkaitan dengan pengelolaan data pribadi baik berupa buku manual, prosedur, instruksi kerja dan form yang terkait dengan Data pribadi, untuk memastikan bahwa audit dilaksanakan dengan baik, benar auditor terlebih dahulu membuat cheklist atau pertanyaan audit yang terkait dengan Data Pribadi dan memastikan auditee atau pihak yang diaudit adalh pihak yang mempunyai kewenangan dalam pengumpulan, penyimpann, pengolahan dan pengendalian data pribadi di perusahaan. auditor harus memastikan pengumpulan data sesuai dengan tujuan yang sah dan sesuai dengan peraturan perundang – undangan yang berlaku, Hasil dari audit akan dituangkan dalam laporan non conformity (laporan ketidaksesuaian) yang berisi temuan ketidaksesuaian yang terdiri atas temuan yang bersifat major, minor atau nearmiss dan rekomendasi apa saja untuk perbaikan terhadap temuan dan memberikan batasan waktu kapan temuan itu akan diperbaiki.

Hasil audit akan di bawa pada pertemuan manajemen yang

melibatkan direksi dan karyawan yang terkait dengan audit yang dinamakan Manajemen review meeting yang nantinya dari hasil audit dan pemenuhan audit dijadikan bahan evaluasi bagi manajemen untuk melakukan perubahan dan peningkatan berkelanjutan (Continuous improvement) terhadap sistem dan organisasi perusahaan untuk mempertahankan eksistensi perusahaan terhadap persaingan yang lebih kompetitif

Sementara itu, pengawasan internal adalah proses berkelanjutan yang bertujuan memastikan bahwa kebijakan dan prosedur yang telah disetujui oleh manajemen terus diikuti dalam jangka panjang. Pengawasan internal tidak hanya mencakup pengawasan terhadap langkah-langkah pengamanan data pribadi, tetapi juga terhadap implementasi kebijakan privasi dan kepatuhan terhadap hukum yang berlaku. Tim pengawasan internal ini dibentuk oleh manajemen berdasarkan kompetensi yang dimiliki dengan Surat Keputusan Direksi dan merupakan Divisi yang berada langsung di bawah Direksi setingkat dengan Kepala Divisi atau Manajer yang tugasnya secara rutin memantau apakah Data Pribadi dikelola dengan baik, apakah akses ke Data Pribadi dibatasi hanya kepada pihak yang berwenang, dan apakah sistem keamanan Data ribadi terus di up date untuk menghadapi ancaman yang kian berkembang. Salah satu aspek penting dalam pengawasan internal adalah memastikan bahwa sistem operasional prosedur penanganan pelanggaran datapribadi dijalankan dengan cepat dan efisien, sesuai dengan prosedur yang telah ditetapkan oleh manajemen perusahaan.

Pengawasan internal ini mencakup pemantauan terhadap training/ pelatihan karyawan dan juga memastikan apakah karyawan memahami pentingnya dalam menjaga kerahasiaan data pribadi yang dikumpulkan dan disimpan oleh perusahaan dan dapat ppula merespons potensi pelanggaran dengan cepat dan tepat. Dengan audit dan pengawasan internal yang terintegrasi perusahaan tidak hanya mampu mendeteksi dan memperbaiki masalah secara cepat dan responsif namun juga dapat membangun kepercayaan karyawan dan pelanggan serta mengurangi risiko hukum yang dapat timbul dikemudian hari akibat pengelolaan data pribadi yang tidak aman atau tidak sah.

Audit dan Pengawasan Internal terhadap Data Pribadi merupakan bagian penting dalam perusahaan untuk memastikan bahwa pengelolaan data pribadi dilakukan dengan baik, benar, aman, dan sesuai dengan peraturan perundang – undangan yang berlaku. Proses ini bertujuan untuk memantau, mengevaluasi, dan memperbaiki sistem pengelolaan data pribadi di dalam suatu Perusahaan, dengan fokus utama pada keamanan, kepatuhan hukum, serta perlindungan terhadap hak privasi individu sebagai subjek data pribadi yang dilindungan undang - undang. Melalui audit dan pengawasan internal yang tepat, perusahaan dapat mencegah potensi pelanggaran terhadap data pribadi dan memastikan bahwa kebijakan serta prosedur yang diterapkan diperusahaan berjalan sesuai dengan tujuan yang diinginkan oleh perusahaan.

Proses Audit dalam Pengelolaan Data Pribadi melibatkan serangkaian kegiatan untuk memeriksa dan menilai bagaimana data pribadi dikumpulkan, digunakan, disimpan, dan dilindungi oleh perusahaan. tahapan umum dalam proses audit data pribadi adalah sebagai berikut : Perencanaan Audit (penunjukan auditor dan area yang akan diaudit, menyusun checklist atau pertanyaan audit), Opening Audit dengan mengumpulkan manajemen dan staf sebagai auditee, Pengumpulan Data dan Pemeriksaan Dokumen (Buku Manual sistem, sistem operasional prosedur, instruksi kerja dan form), Evaluasi Kepatuhan terhadap Kebijakan Privasi dan Peraturan perundang – undangan, Pemeriksaan Keamanan Data, Identifikasi Risiko dan Celah Keamanan dalam sistem data pribadi, Closing Audit dengan memaparkan temuan Audit, Tindak Lanjut dan batas pemenuhan audit, Manajemen Review Meeting sebagai upaya perbaikan berkelanjutan dalam organisasi / perusahaan.

Pengawasan Internal dalam Pengelolaan Data Pribadi fokus pada pemantauan dan evaluasi berkelanjutan terhadap praktik pengelolaan data pribadi di dalam perusahaan. Pengawasan ini dapat dilakukan melalui berbagai cara, seperti pemantauan rutin terhadap kebijakan dan sistem operasional prosedur yang berhubungan dengan pengelolaan data, serta melakukan pengecekan berkala terhadap penerapan sistem keamanan data pribadi, ada beberapa aspek penting dalam pengawasan internal terhadap data pribadi : Monitoring Kepatuhan Secara Rutin,

Pengecekan dan Evaluasi Sistem Keamanan, Audit Keberlanjutan dan Evaluasi Proses, Pelaporan Insiden dan Pelanggaran Data

Manfaat Audit dan Pengawasan Internal dalam Pengelolaan Data Pribadi, Melalui audit dan pengawasan internal yang efektif, perusahaan dapat memperbaiki kekurangan dalam sistem pengelolaan data pribadi, meningkatkan keamanan data, serta memastikan bahwa praktik pengelolaan data sesuai dengan standar hukum yang berlaku. Kedua proses ini memberikan gambaran yang jelas tentang area mana yang membutuhkan perbaikan, mengurangi risiko kebocoran data, dan membantu perusahaan untuk mematuhi regulasi yang semakin ketat. Selain itu, audit dan pengawasan internal juga berperan penting dalam membangun kepercayaan karyawan dan pelanggan, karena mereka merasa yakin bahwa data pribadi mereka diperlakukan dengan cara yang aman dan sesuai dengan peraturan perundang – undangan yang berlaku.

E. Refrensi

Peraturan Perundang – undangan

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Undang – undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Peraturan Pemerintah Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik

Regulation (EU) 2016/679 of the European Parliament and of the Council. (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union.

Buku - Jurnal

Kuner, C. (2017). The General Data Protection Regulation: A Commentary. Oxford University Press.

Solove, D. J., & Schwartz, P. M. (2021). Information Privacy Law (7th ed.). Aspen Publishers.

Harris, R. M., & Liu, H. (2019). Privacy and Data Protection in the Cloud: Legal, Regulatory and Technical Issues. Springer.

Cavoukian, A. (2012). Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario.

Mayer-Schönberger, V., & Cukier, K. (2013). Big Data: A Revolution That Will Transform How We Live, Work, and Think. Houghton Mifflin Harcourt.

European Commission. (2018). The EU General Data Protection Regulation (GDPR): A Practical Guide.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review, 4(5), 193-220.

Binns, R. (2018). "Cybersecurity and the Protection of Personal Data: Legal Frameworks and Industry Practices". Information Security Journal: A Global Perspective, 27(4), 202-213.

Information Commissioner's Office (ICO). (2020). Guide to Data Protection.

Rainer, M. (2017). Data Privacy and the Ethics of Personal Information. Routledge.

Pellegrini, A., & Peterson, P. (2018). Managing Privacy: Data Protection in Practice. Wiley.

Toth, C., & Allen, J. (2019). Data Privacy and Corporate Governance: A Strategic Perspective. Springer.

Denton, D. W. (2014). The Law of Data Security and Privacy. Aspen Publishers.

Dwi Safitri, (2024), csirt.teknokrat.ac.id. Pentingnya Kebijakan Privasi dalam Pengelolaan Data Pengguna

TENTANG PENULIS

Dr. Kurniawan Tri Wibowo., SH., MH

(Universitas Islam Negeri Prof. Saifudin Zuhri Purwokerto)

Penulis lahir di lahir di Kota Bekasi tanggal 29 Oktober 1987. Penulis adalah advokat, penulis buku dan dosen di Universitas Islam Negeri Prof. Saifudin Zuhri Purwokerto. Menyelesaikan pendidikan S1 pada program studi ilmu hukum di Fakultas Hukum UNSOED, S2 pada Magister Hukum UNSOED dan Pendidikan Doktor Hukum/ S3 di Universitas Islam Sultan Agung Semarang (UNISSULA).

Muhammad Alfian Dj

Penulis lahir di Lhokseumawe, Oktober 1978, setelah menyelesaikan pendidikannya di Madrasah Muallimin Muhammadiyah Yogyakarta kemudian melanjutkan ke Fakultas Syariah IAIN Sunan Kalijaga, S2 Ilmu Hukum di Universitas Gajah Mada dilanjutkan program Doktoral (S3) Ilmu Hukum pada Universitas Islam Indonesia. Profesi saat ini sebagai Staf Pengajar Madrasah Muallimin Muhammadiyah Yogyakarta

Karya penulis banyak di publikasikan di berbagai media seperti: Era Siaran TV Digital, Hak Pemirsa Televisi Terabaikan, Pandemi dan Bencana Putus Sekolah, Dana BOS, ,Netralitas ASN, Survei Lingkungan Belajar. Menanti ‘ Kado tahun Baru’ PPN 12 %, Melindungi Profesi Guru. ‘Politik Rangkul” ala Prabowo. Regulasi Batasan Usia Minimum Bermedia sosial. Revisi UU Penyiaran. Asa Kebebasan Pers. Pendidikan Politik Pemilih Pemula. Ikhtiar Semesta Merawat Lingkungan. Kampanye di Sekolah. Arah Baru UU Kesehatan THR antara Hak dan Kewajiban

Dr. Abdul Karim, S.T., M.M.

Global Institute of Technology and Business

Penulis lahir di Makassar tanggal 15 Oktober 1973. Penulis adalah dosen tetap pada Fakultas Teknologi Informasi, Institut Teknologi dan Bisnis, Bina Sarana Global. Penulis menyelesaikan pendidikan S1 pada program studi Teknik Informatika di Institut Teknologi Bandung (ITB) pada tahun 1996, Pendidikan S2 Manajemen di Universitas IPWIJA pada tahun 2006 dan S3 Ilmu Manajemen di Universitas Brawijaya pada tahun 2021, saat ini sedang menempuh Pendidikan Magister Hukum dengan fokus penelitian pada Hukum Siber.

Penulis juga adalah professional di bidang Teknologi Informasi, Data Sistem dan Bisnis Proses Operasional di beberapa Perusahaan Nasional dan Multi-nasional dengan pengalaman lebih dari 27 tahun. Selain sebagai Professional dan Dosen, Penulis juga adalah jurnalis dan kontributor di salah satu media hukum nasional dan fasilitator beberapa pelatihan tingkat nasional serta pembicara di beberapa event dan seminar di tingkat nasional dan internasional di bidang Big Data, Data Analytic dan Manajemen Resiko Digital.

Dr. Abdul Karim, S.H.,M.Ikom, Banjarbaru

(Sekolah Tinggi Ilmu Hukum Sultan Adam Banjarmasin)

Penulis lahir di Barabai (Kalsel) tanggal 13 Juli 1963. Penulis adalah dosen tetap pada Program Studi Magister Ilmu Hukum Sekolah Tinggi Ilmu Hukum Sultan Adam Banjarmasin. Menyelesaikan Pendidikan S1 Ilmu Hukum di Sekolah Tinggi Ilmu Hukum Sultan Adam Banjarmasin (2006), Pendidikan S2 pada program studi Ilmu Komunikasi di Universitas Mercubuana Jakarta (2014), Pendidikan S3 Ilmu Hukum Universitas Brawijaya Malang (2020). Bekerja di PT Telekomunikasi Indonesia, Tbk sejak 1983 sampai 2019 dan Menjadi Sekretaris Jenderal Serikat Karyawan Telkom 2016-2019. Pernah menjadi Kepala Sekolah SMK Telkom Banjarbaru (Kalsel) 2012-2015.

Di samping sebagai dosen tetap STIH Sultan Adam Banjarmasin Penulis aktif di beberapa organisasi. Menjadi Ketua Yayasan Pendidikan Pondok Darul Hijrah Putri Martapura, Penasihat Ikatan Sarjana Nahdatul Ulama Kota Banjarbaru, Ketua Bidang Advokasi dan Organisasi Yayasan Lestari Anggrek Nusantara, dan menjabat sebagai Ketua RT 02/RW 04 Kelurahan Mentaos Banjarbaru, juga sebagai Ketua Komunitas Informasi Masyarakat Kelurahan Mentaos - Banjarbaru Kalsel.

Latar belakang profesi/pekerjaan Penulis berpengaruh kepada pemilihan topik karya llmiah selama menempuh studi mulai S1 hingga S3. yaitu di seputar penggunaan teknologi informasi. Skripsi di S1 berjudul Perlindungan Konsumen Dalam Transaksi E-commerce. Tesis

S2 berjudul Dinamika Komunikasi Personal Jarak Jauh Antara Anak dan Orang Tua Dengan Menggunakan Teknologi Media Baru. Disertasi S3 berjudul Kewenangan Pemerintah Dalam Penyelenggaraan Telekomunikasi Untuk Mewujudkan Kemandirian Teknologi Informasi dan Komunikasi Yang Berkeadilan.

Penulis sempat menulis buku "Dua Puluh Tahun Serikat Karyawan Telkom Meretas Kesejahteraan. Berisi seputar perjuangan para aktivis Serikat Pekerja. Di samping itu ada beberapa book chapter antara lain Tindak Pidana Korporasi Dalam KUHP Baru. Perkembangan Teknologi Mendorong Perubahan Sosial dan Hukum Global.

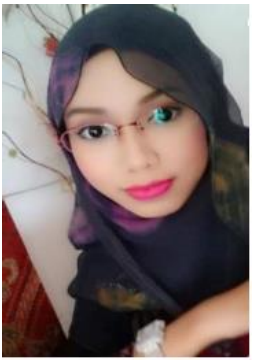
Rizki Syafril, SHI, M.Si,

Penulis yang biasa di panggil dengan Unchu Rizki, lahir di Bukittingi, Kamis, tanggal 03 Desember 1987, seorang santri yang mengenyam pendidikan di pesantren selama 6 tahun di Pondok Pesantren Ibnul Qoyyim (2000-2006) di Yogyakarta, kemudian dilanjutkan Pendidikan S1 di STAIN Sjech M. Djamil Djambek Bukittinggi dan S2 di Universitas Andalas Padang.

Aktifitas sekarang sebagai seorang pengajar di Departemen Ilmu Administrasi Negara Fakultas Ilmu Sosial Universitas Negeri Padang. Fokus mengajar terkait dengan bidang Hukum, Politik dan Kebijakan. Sebelum menjadi seorang Pengajar, bekerja di dalam instansi pemerintahan yang juga terfokus pada hukum dan regulasi.

Selama menempuh perkuliahan juga aktif dalam organisasi kemahasiswaan seperti Himpunan Mahasiswa Islam dan Pers Kampus. Telah mengikuti berbagai macam pelatihan dari semenjak perkuliahan sampai menjadi seorang pengajar yang bertujuan untuk meningkatkan kapasitas diri dan bermanfaat untuk semua.

Sebagai seorang pengajar juga aktif dalam dua Pusat Riset yaitu Pusat Riset Kebijakan, Hukum dan Politik (Policy, Law and Political Research Center) dan Pusat Riset Masyarakat Hukum Adat Indonesia (Indonesian Tradisional Law Community Research Center)



Dr. Ma'rifah, S.H., M.H.

Penulis menyelesaikan pendidikan Strata 1- Sarjana Ilmu Hukum Fakultas Hukum Universitas Lambung Mangkurat (ULM), Strata 2- Magister Ilmu Hukum Program Pasca Sarjana Fakultas Hukum Universitas Lambung Mangkurat (ULM), dan Strata 3- Doktor Ilmu Hukum Program Pasca Sarjana Fakultas Hukum Universitas Airlangga (UNAIR). Penulis Tesis yang berjudul "Lembaga Jaminan Perorangan *Borgtocht* Dalam Pembiayaan Perbankan Syariah" (2009) dan penulis Disertasi berjudul "Prinsip Proporsionalitas Pengelolaan Pertambangan Minyak Dan Gas Bumi"-*Principles of Mining Management Proportionality Oil and Gas* (2018) dipublikasikan *AUNILO Libraries of ASEAN University Network*, melalui http://aunilo.uum.edu.my/Find/Record/id-langga.80529, Penulis buku Hukum Pengelolaan Sumber Daya Alam (2020), Hubungan Hukum Internasional (Hukum Internasional & Hukum Perdata Internasional), dan *Prophetic Intelligence as Therapeutical AntiThesis for Scientific Writing* serta beberapa artikel penelitian dan pengabdian kepada masyarakat yang dilakukan secara mandiri dan kolaborasi. Fokus penelitian penulis pada kajian kerangka berpikir secara Teoritis dan Filsafat hukum meliputi :

2. bidang Hukum Bisnis yang meliputi Hukum Hubungan Internasional (Hukum Perdata/Perdagangan Internasional dan Hukum Internasional), Hukum Kontrak, Hukum Perusahaan, Hukum Ketenagakerjaan/Perburuhan;
3. bidang Hukum Administrasi yang meliputi Hukum Lingkungan, Hukum Pengelolaan/Penegakan Sumber Daya Alam, Hukum Pertambangan dan Hukum Kehutanan/Perkebunan.

Professional Appointments sebagai Editor in Chief jurnal "*DE JURE Critical Laws Journal*" by Lembaga Pendidikan Dan Publikasi Riset

Ilmu Hukum (LP2RIH), https://myjournal.id/index.php/jwh, Editor jurnal "*The Journal International Review of Social Research"* by Institute of Industry and Academic Research Incorporated (IIARI), https://iiari.org/journals/irssr, dan Advisor "*Australia Pacific Publisher*", https://australiapacificpublisher.com/our-advisors/. Penulis terhubung sebagai Assistant Professor Program Magister Ilmu Hukum Sultan Adam Banjarmasin, South Kalimantan-Indonesia @ marifah@stihsa.ac.id, drriefa@gmail.com;

Dr. H. Muhammad Syaukani, S.T., S.H., M.Cs, M.Kom

(Rektor – Institut Teknologi Bisnis dan Bahasa "Dian Cipta Cendikia")

Penulis lahir di Banjarmasin tanggal 17 April 1973. Penulis adalah dosen tetap dengan jabatan fungsional Lektor Kepala pada Program Sistem Informasi, Fakultas Ilmu Komputer Institut Teknologi Bisnis dan Bahasa 'Dian Cipta Cendikia' Bandar Lampung. Menyelesaikan Pendidikan S1 pada program studi Teknik Informatika Universitas Ahmad Dahlan Tahun 2003, S1 program studi Ilmu Hukum Universitass Sain Cut Nyak Dien Tahun 2024, S2 Ilmu Komputer Universitas Gadjah Mada Tahun 2009, S2 Teknik Informatika Universita Islam Indonesia Tahun 2014, S3 Ilmu Komputer Universitas Gadjah Mada Tahun 2018.

Pengalaman Jabatan sebagai Anggota Badan Penyelesaian Sengketa Konsumen (BPSK) Kota Banjarmasin Periode (2011-2016) dan Periode (2018-2023), Ketua STMIK Indonesia Banjarmasin Periode (2018-2020), Komisaris Utama BPR Tapin Periode (2020-2025), Anggota Komisioner Penyiaran Indonesia Daerah (KPID) Provinsi Kalimantan Selatan Periode (2021-2024), Rektor Institut Teknologi Bisnis dan Bahasa 'Dian Cipta Cendikia' Bandar Lampung Periode (2024 – 2028).

Moh. Muniri, S.H., M.Kn.

(Asmi Citra Nusantara Banjarmasin)

Penulis lahir di Sampang tanggal 14 September 1982. Penulis adalah dosen tetap pada Program Studi Manajemen Bisnis, Akademi Sekretaris dan Manajemen Citra Nusantara (Asmi Cinus) Banjarmasin. Tutor Online Pada Universitas Terbuka, dan Dosen Terbang Pada ITBA Lampung, Penulis Menyelesaikan pendidikan S1 pada program studi Ilmu Hukum Universitas Airlannga Surabaya Tahun 2005, S2 Pada Magister Kenotariatan Universitas Gadjah Mada Tahun 2012 dan Sekarang sedang menempuh Program Doktor Hukum di Universitas Lambung mangkurat Banjarmasin, Kalimantan Selatan

Buku dengan judul “Hukum Digital dan Privasi Data” ini disusun untuk memberikan wawasan mendalam tentang isu-isu hukum yang berkaitan dengan perkembangan pesat teknologi digital, khususnya mengenai privasi data dalam konteks global yang semakin terhubung. Ditulis oleh tujuh orang praktisi pendidikan dan hukum yang memiliki pengetahuan serta pengalaman mumpuni di bidangnya, buku ini menawarkan analisis kritis mengenai tantangan hukum yang muncul seiring dengan pemanfaatan teknologi digital yang semakin luas. Dalam setiap bab, para penulis berbagi pandangan yang didasarkan pada pemahaman hukum yang mendalam, serta perspektif yang berbasis pada praktik nyata dalam menghadapi dinamika dunia digital.

Di era digital yang serba cepat ini, privasi data menjadi salah satu isu yang paling relevan dan penting untuk diperhatikan. Buku ini menyelami berbagai dimensi hukum yang terkait dengan pengelolaan dan perlindungan data pribadi, baik dari sudut pandang regulasi nasional maupun internasional. Dengan pertumbuhan pesat teknologi seperti internet of things (IoT), kecerdasan buatan (AI), dan media sosial, perlindungan data pribadi kini menghadapi tantangan yang jauh lebih kompleks daripada sebelumnya. Para penulis berusaha mengurai dengan jelas bagaimana hukum dapat mengimbangi perkembangan teknologi tanpa mengesampingkan hak privasi individu.

Penerbit CV. Al-Haramain Lombok
Anggota IKAPI (No. 012/NTB/2022)
Jl. Gunung Tambora, Mataram, NTB.
alharamainlombok.com | 085-338-949-261 (WA)

Hukum Digital

ISBN 978-634-7095-05-3