STRATEGI DAN INOVASI DIGITAL: MENGARAHKAN MASA DEPAN

Arif Perdana

Strategi dan Inovasi Digital: Mengarahkan Masa Depan

Arif Perdana (2025)

D A F T A R I S I

STRATEGI DAN INOVASI DIGITAL: MENGARAHKAN MASA DEPAN

Pendahuluan

Di era digital yang terus berkembang pesat, Indonesia menghadapi tantangan dan peluang yang belum pernah terjadi sebelumnya. Transformasi digital telah merambah ke berbagai aspek kehidupan masyarakat, mulai dari cara kita berkomunikasi, bekerja, hingga mengelola keuangan. Buku ini hadir sebagai panduan untuk memahami dan menavigasi lanskap digital yang kompleks ini, dengan fokus khusus pada konteks Indonesia.

Buku ini merupakan kompilasi dari artikel-artikel penulis dengan kolega di berbagai media terkemuka baik di Indonesia maupun di mancanegara dari tahun 2021 hingga 2024, termasuk *The Strait Times, Strategic Finance, The Diplomat*, The Conversation Indonesia, *The Conversation Australia, The Jakarta Post*, *360info.org, Monash Lens*, Tempo, Kompas, detik.com, Kumparan, dan lain-lain. Publikasi di media-media tersebut menunjukkan kredibilitas dan relevansi topik-topik yang dibahas, serta menawarkan analisis mendalam. Artikel ini disusun secara kronologis berdasarkan tanggal penerbitannya di media massa mulai dari yang terkini. Penyusunan ini juga bisa digunakan oleh pembaca untuk melihat dinamika pemikiran penulis dan rekan dalam tiga tahun terakhir.

Sebagian artikel ini telah diperbarui dan disusun ulang untuk memberikan perspektif yang komprehensif dan terkini tentang strategi dan transformasi digital, regulasi, dan tata kelola digital. Topik yang diangkat mencakup dampak AI generatif, insiden keamanan siber seperti serangan *ransomware* pada Pusat Data Nasional Sementara (PDN-S), dan tantangan implementasi UU Pelindungan Data Pribadi. Selain itu, artikel-artikel di buku ini juga membahas dinamika industri *fintech*, ancaman disinformasi oleh AI generatif, serta perdebatan global tentang regulasi AI dan potensi "gelembung AI." Fenomena *deepfake*, industri "kehidupan digital setelah kematian," serta tantangan integrasi data pemerintah juga menjadi sorotan di buku ini.

Revolusi digital telah mengubah paradigma dalam berbagai sektor, termasuk pemerintahan, bisnis, dan masyarakat sipil. Kecepatan perubahan yang terjadi menuntut

adaptasi yang cepat dan strategi yang tepat untuk memanfaatkan potensi teknologi sekaligus memitigasi risikonya. Alih-alih tersebar di banyak media, penulis berinisiatif untuk menyusun ulang artikel-artikel yang sudah dipublikasikan ini menjadi satu buku yang disajikan dalam empat tema besar yang masing-masing membahas aspek krusial dari transformasi digital di Indonesia.

Bab pertama mengeksplorasi peran vital regulasi dalam membentuk masa depan teknologi digital. Di bagian ini dipaparkan bagaimana *EU AI act* dapat menjadi model pembelajaran bagi Indonesia dalam merumuskan kerangka hukum yang efektif. Bab ini juga membahas pentingnya keseimbangan antara mendorong inovasi dan melindungi kepentingan publik. Penulis menganalisis bagaimana regulasi yang tepat dapat membuka jalan bagi inovasi yang bertanggung jawab. Ini memungkinkan Indonesia mengambil peran penting dalam tata kelola AI global.

Keamanan siber dan tata kelola data menjadi fokus utama di bab kedua. Dengan meningkatnya insiden kebocoran data dan serangan siber di Indonesia, bab ini membahas strategi komprehensif untuk mengamankan infrastruktur digital negara. Di sini kami menekankan pentingnya pengembangan Rencana Respons Insiden (*Incidents Response Planning*/IRP), Pemulihan Bencana (*Disaster Recovery Planning*/DCP), dan Kelangsungan Bisnis (*Business Continuity Planning*/BCP) yang efektif. Bab ini juga membahas urgensi pembangunan Pusat Data Nasional (PDN) yang terintegrasi namun aman, serta implementasi konsisten UU Pelindungan Data Pribadi (PDP).

Bab ketiga mengangkat isu-isu etika dan sosial yang muncul dari perkembangan teknologi digital. Kami membahas dampak AI seperti model bahasa besar (LLM – *ChatGPT*, *Claude*, dan *Google Gemini*) terhadap integritas akademik, proses pembelajaran, penyebaran disinformasi, dan potensi kejahatan siber. Bab ini juga mengeksplorasi implikasi etis dari teknologi *deepfake* dan perkembangan industri "kehidupan digital setelah kematian". Fokus utama bab ini adalah mencari keseimbangan antara inovasi teknologi dan nilai-nilai etika serta kemanusiaan.

Bab terakhir membahas transformasi ekonomi melalui inovasi digital. Kami melihat bagaimana AI generatif dan teknologi finansial (*fintech*) mengubah lanskap bisnis dan keuangan di Indonesia. Bab ini membahas potensi dan risiko dari inovasi

seperti crowdlending, serta pentingnya regulasi yang adaptif untuk mendorong pertumbuhan ekonomi digital yang inklusif dan berkelanjutan.

Melalui keempat bab ini, penulis menawarkan pemahaman menyeluruh tentang kompleksitas transformasi digital di Indonesia. Tema utama yang menjadi benang merah meliputi urgensi regulasi yang adaptif, keamanan data, etika teknologi, inklusi digital, kolaborasi multi-stakeholder, dan pentingnya pendidikan literasi digital. Dengan menggabungkan analisis terkini, studi kasus, dan rekomendasi kebijakan, buku ini dirancang untuk menjadi referensi bagi pembuat kebijakan, akademisi, pelaku bisnis, dan masyarakat umum dalam memahami dan membentuk masa depan digital Indonesia.

Transformasi digital bukan hanya tentang adopsi teknologi, tetapi juga bagaimana teknologi mengubah cara kita hidup dan berinteraksi. Dengan pemahaman yang lebih baik, kita dapat memanfaatkan potensi teknologi untuk membangun Indonesia yang lebih maju, adil, dan berkelanjutan. Mari kita jelajahi bersama tantangan dan peluang transformasi digital di Indonesia melalui halaman-halaman buku ini.

Ucapan terimakasih saya haturkan kepada kolega yang menulis bersama. Saya juga berterimakasih dengan rekan-rekan jurnalis dari The Conversation Indonesia, The Conversation Australia, dan 360info.org yang sudah berkenan memberikan saran, komentar dan perbaikan terhadap artikel-artikel yang saya kirimkan ke media mereka.

BAB 1: Masa Depan Teknologi Digital di Tangan Regulasi dan Strategi Digital

Semakin pesatnya perkembangan teknologi digital, terutama kecerdasan artifisial (AI) mebuat regulasi menjadi aspek krusial untuk menjamin keamanan dan keadilan tanpa menghambat inovasi. Berbagai negara, termasuk Indonesia, kini menghadapi tantangan untuk merespons kebutuhan regulasi AI di tengah lanskap teknologi yang berubah cepat. Uni Eropa telah mengambil langkah proaktif dengan UU AI-nya, yang berpotensi mengubah standar global dalam pengaturan teknologi AI. Sementara itu, Indonesia telah meletakkan fondasi penting melalui penerapan UU PDP pada 2022. UU PDP ini dapat menjadi titik awal yang solid untuk pengembangan regulasi AI di Indonesia, terutama dalam aspek pemrosesan data dan pelindungan hak-hak subjek data.

Namun, tantangan utama bagi Indonesia adalah menyusun regulasi AI yang tidak menghambat inovasi secara berlebihan. Meskipun dapat belajar dari *European Union* (EU) *AI Act*[1], Indonesia perlu memastikan bahwa regulasi yang diterapkan cukup fleksibel dan tidak membebani perusahaan teknologi secara tidak proporsional. Keseimbangan antara pelindungan kepentingan publik dan dorongan inovasi menjadi kunci. Regulasi yang tepat dapat membuka jalan bagi inovasi yang bertanggung jawab. Ini tentunya memungkinkan Indonesia mengambil peran penting dalam tata kelola AI global. Hal ini juga memberi kesempatan bagi Indonesia untuk memperhatikan konteks sosial dan budaya yang beragam dalam penerapan teknologi AI. Dengan pendekatan yang cermat dan inklusif dalam menyusun regulasi AI, Indonesia dapat memposisikan diri sebagai pemain kunci dalam revolusi teknologi global. Regulasi yang efektif akan mendorong kepercayaan publik terhadap teknologi AI, menstimulasi pertumbuhan ekonomi digital, dan pada akhirnya berkontribusi pada kemajuan nasional di era digital.

[1] https://artificialintelligenceact.eu/

Pelajaran dari Kasus Google untuk Masa Depan AI

Arif Perdana

Konteks: Tulisan ini saya terbitkan di Kumparan tanggal 20 Oktober 2024. Artikel ini membahas keputusan pengadilan pada Agustus 2024 yang menyatakan Google bersalah melakukan monopoli. Kejadian ini bisa memberikan implikasi lebih luas terhadap ekosistem teknologi dan masa depan AI. Selain merinci dampak regulasi terhadap perusahaan besar, artikel ini memperingatkan risiko monopoli dalam mengontrol arah inovasi, termasuk potensi bias AI. Di sisi lain, regulasi di Eropa dan AS menandai upaya untuk menjaga keseimbangan antara inovasi dan etika. Artikel ini mengusulkan langkah proaktif pemerintah, seperti interoperabilitas data, transparansi algoritma, dan pembentukan badan pengawas AI untuk menciptakan teknologi yang lebih etis dan inklusif.

Di tengah gemuruh inovasi digital, sebuah keputusan pengadilan menggetarkan pondasi *Silicon Valley*. Google, raksasa teknologi yang telah lama mendominasi lanskap pencarian daring, Agustus 2024 lalu resmi dinyatakan melakukan monopoli oleh Pengadilan Distrik Columbia[2]. Keputusan ini bukan sekadar vonis hukum, melainkan lonceng peringatan yang bergema ke seluruh ekosistem teknologi. Sementara Google menghadapi pemeriksaan, bayang-bayang regulasi mulai menyelimuti perusahaan teknologi besar lainnya. Namun, di balik drama hukum ini, tersembunyi narasi yang lebih besar: bagaimana kekuatan monopolistik ini berpotensi membentuk masa depan AI, khususnya AI generatif, yang kini berada di ambang revolusi teknologi terbesar sejak internet.

Dominasi perusahaan teknologi besar bukan sekadar masalah persaingan bisnis; ini adalah pertarungan untuk menentukan masa depan masyarakat digital. Mereka bukan hanya menguasai pasar, tetapi juga memiliki pengaruh yang mendalam dalam membentuk kebijakan publik. Studi Khanal et al. (2024) mengungkap bahwa *Big Tech* telah menjadi *super policy entrepreneurs*, dengan kemampuan untuk mengarahkan kebijakan sesuai kepentingan mereka[3]. Pengaruh ini meresap ke dalam setiap aspek

[2] https://360info.org/googles-monopoly-case-builds-pressure-on-tech-giants/
[3] https://academic.oup.com/policyandsociety/advance-article/doi/10.1093/polsoc/puae012/7636223

proses pembuatan kebijakan. Ini menciptakan lingkungan di mana inovasi teknologi boleh jadi mendahului pertimbangan etis dan sosial.

Di tahun 1990-an, kasus serupa melibatkan Microsoft, yang didakwa melakukan praktik monopoli melalui penggabungan *Internet Explorer* dengan sistem operasi Windows[4]. Dampak hukum dari kasus tersebut tak hanya mengubah lanskap teknologi saat itu tetapi juga membuka jalan bagi inovasi baru dan para pemain baru di industri. Kini, kita mungkin berada di titik balik yang serupa, ketika regulasi terhadap Google dapat menciptakan kembali peluang bagi startup dan inovator kecil untuk bersinar.

Namun, persoalan monopoli teknologi bukan hanya milik Amerika Serikat. Di Eropa, regulasi seperti *the General Data Protection Regulation* (GDPR)[5] dan *EU AI Act* telah menempatkan perusahaan teknologi besar di bawah pengawasan ketat, dengan fokus pada pelindungan data pribadi dan etika dalam pengembangan AI. Pendekatan regulasi yang berbeda ini mencerminkan kekhawatiran global yang semakin mendalam terhadap dampak kekuatan teknologi besar pada masyarakat luas.

Pengaruh Google dan raksasa teknologi lainnya yang meresap ke dalam setiap aspek proses pembuatan kebijakan ini menciptakan paradoks berbahaya: semakin cepat kita berinovasi, semakin besar risiko kita kehilangan pegangan pada nilai-nilai kemanusiaan yang mendasar. Dalam konteks Google dan perkembangan AI, kekhawatiran utama terletak pada potensi bias dan ketidakadilan yang tertanam dalam algoritma mereka.

Dataset raksasa yang dimiliki Google, meskipun besar, tidak selalu mewakili keberagaman masyarakat global. Ketika AI dikembangkan berdasarkan data yang bias ini, hasilnya bisa jadi teknologi yang memperkuat ketidaksetaraan yang ada, bukannya malah menguranginya. Sebagai contoh nyata, algoritma rekrutmen AI yang digunakan oleh beberapa perusahaan telah terbukti mendiskriminasi kandidat berdasarkan gender dan ras, karena data latihnya didasarkan pada pola rekrutmen historis yang bias[6]. Ini

[4] https://corporatefinanceinstitute.com/resources/management/microsoft-antitrust-case/
[5] https://gdpr-info.eu/
[6] https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias

adalah bukti konkret bahwa inovasi tanpa pertimbangan etis bisa berdampak buruk pada kesejahteraan sosial.

Masa Depan yang Harus Diperjuangkan Bersama

Kasus Google menyoroti perlunya keseimbangan antara inovasi dan regulasi di era digital. Pengadilan menuntut transparansi dalam hasil pencarian Google, sebuah langkah yang mungkin terdengar sederhana namun berpotensi mengubah lanskap internet. Transparansi ini bisa menjadi preseden untuk pengembangan AI yang lebih bertanggung jawab. Perusahaan teknologi perlu memahami bahwa inovasi tanpa akuntabilitas bukan lagi opsi yang dapat diterima. Mereka harus mulai melihat regulasi bukan sebagai hambatan, tetapi sebagai panduan untuk menciptakan teknologi yang lebih inklusif dan etis.

Namun, regulasi saja tidak cukup. Pemerintah juga menghadapi tantangan untuk berevolusi dan beradaptasi secepat teknologi yang mereka coba atur. Kasus Google adalah bukti nyata bahwa tindakan regulatori yang lambat dan reaktif dapat membiarkan monopoli teknologi tumbuh menjadi entitas yang terlalu besar, terlalu kuat, dan terlalu tertanam dalam struktur masyarakat untuk dikendalikan secara efektif. Dalam konteks AI generatif yang berkembang pesat, pemerintah perlu mengambil sikap yang jauh lebih proaktif dan visioner dalam merumuskan kebijakan. Mereka harus mampu menyeimbangkan dorongan untuk mendorong inovasi (yaitu yang penting untuk daya saing nasional dan kemajuan teknologi) dengan kebutuhan mendesak untuk melindungi kepentingan publik, privasi individu, dan integritas sistem demokrasi kita. GDPR di Eropa dan *EU AI Act* memberikan kerangka awal yang baik, tetapi bahkan regulasi-regulasi pionir ini masih memerlukan penyempurnaan signifikan untuk mengikuti laju perkembangan AI yang seolah-olah tanpa batas.

Pertama dan terpenting, pemerintah perlu memfokuskan pada prinsip interoperabilitas dan portabilitas data. Ini bukan sekadar masalah teknis; ini adalah langkah fundamental untuk memecah monopoli informasi dan memberikan kembali kendali kepada pengguna atas data mereka sendiri. Dengan memungkinkan pengguna untuk berpindah antara platform dengan mudah, kita tidak hanya mengurangi efek *lock-*

in yang sering dimanfaatkan oleh perusahaan besar, tetapi juga mendorong terciptanya ekosistem digital yang lebih dinamis dan kompetitif.

Kedua, regulasi harus dengan tegas mendorong transparansi algoritma, terutama untuk sistem AI yang memiliki dampak signifikan terhadap keputusan-keputusan krusial dalam kehidupan masyarakat. Ini adalah langkah penting menuju demokratisasi algoritma, di mana masyarakat memiliki hak dan kemampuan untuk memahami dan mempertanyakan keputusan yang dibuat oleh sistem otomatis yang semakin mendominasi kehidupan mereka.

Ketiga, pembentukan badan pengawas AI independen yang memiliki tidak hanya otoritas hukum tetapi juga keahlian teknis yang mendalam adalah suatu keharusan. Badan ini harus mampu melakukan audit menyeluruh terhadap sistem AI dan memiliki kekuatan untuk menegakkan standar etika yang ketat. Tanpa pengawasan seperti ini, kita berisiko menciptakan "kotak hitam" algoritma yang dapat membuat keputusan tanpa akuntabilitas.

Keempat, pemerintah harus mengambil peran aktif dalam mendorong diversifikasi dalam pengembangan AI. Ini bisa dilakukan melalui alokasi dana penelitian yang signifikan untuk institusi publik dan dukungan konkret bagi *startup* AI yang berfokus pada solusi etis dan inklusif. Dengan mendorong pluralitas dalam pengembangan AI, kita tidak hanya memperkaya ekosistem inovasi tetapi juga memastikan bahwa teknologi masa depan mencerminkan keragaman perspektif dan kebutuhan masyarakat global.

Terakhir, mengingat sifat AI yang melampaui batas-batas nasional, kerjasama internasional dalam mengatur AI bukan lagi pilihan, melainkan keharusan. Diperlukan upaya diplomatik yang intensif untuk menciptakan kerangka regulasi global yang koheren, yang dapat mengimbangi kekuatan transnasional perusahaan teknologi besar.

Namun, regulasi saja tidak cukup. Diperlukan pendekatan holistik yang melibatkan edukasi publik tentang AI, mendorong literasi digital, dan menciptakan forum di mana masyarakat dapat berpartisipasi dalam membentuk kebijakan teknologi. Dengan strategi yang tepat, kita dapat memanfaatkan kekuatan AI sambil menghindari perangkap monopoli digital. Ini adalah perjalanan yang kompleks, tetapi tak terelakkan jika kita ingin

memastikan bahwa teknologi masa depan melayani kepentingan seluruh masyarakat, bukan hanya segelintir perusahaan besar.

Mari kita ingat, inovasi yang besar, datang dengan tanggung jawab yang besar pula. Keputusan hari ini akan membentuk dunia kita esok hari. Kita berdiri di persimpangan antara masa depan teknologi yang inklusif dan beretika, atau masa depan yang dikendalikan oleh segelintir entitas yang kuat. Pilihan ada di tangan kita, dan pilihan ini harus diambil dengan hati-hati, dengan visi yang jelas tentang dunia yang ingin kita tinggali.

Tautan artikel:

https://kumparan.com/arif-perdana-1723991955605643308/pelajaran-dari-kasus-google-untuk-masa-depan-ai-23kFa3Bv0fi/full

Dinamika dan Tantangan Pelindungan Data di Era AI

Arif Perdana

Konteks: Tulisan ini saya terbitkan di Kumparan tanggal 17 Oktober 2024. Artikel ini membahas tantangan privasi data di era digital, terutama terkait kebocoran data dan regulasi privasi. Munculnya kesadaran privasi publik memicu undang-undang seperti GDPR dan UU PDP. Artikel ini juga menyoroti "Paradoks Privasi," yaitu ketika orang khawatir tentang data mereka, namun tetap menggunakan layanan digital karena kenyamanan. Diberikan juga solusi praktis bagi perusahaan dan pengembang AI, seperti anonimisasi data dan pendekatan privasi sejak tahap desain. Fokusnya adalah pada perlunya transparansi, kontrol pengguna yang lebih baik, serta teknik pengembangan AI yang menghormati privasi.

Di tengah riuh rendah digitalisasi yang semakin menggema, ada satu isu yang semakin mendesak: privasi data yang semakin terancam oleh kebocoran besar. Tak satu pun entitas, dari lembaga pemerintahan hingga entitas swasta, yang terlepas dari jerat ancaman ini, sehingga jutaan data pribadi warga negara tersingkap di jagat maya tanpa tameng yang memadai. Sementara itu, bayangkan dunia digital sebagai samudra luas yang kita arungi setiap hari. Teknologi menjadi arus deras yang mengubah cara kita hidup dan bekerja. Di tengah gelombang transformasi besar dari era akses data tanpa batas ke era kesadaran privasi yang ditandai dengan regulasi yang semakin ketat, kita berhadapan dengan "Paradoks Privasi," yaitu manfaat dari data bertemu dengan kerentanannya yang besar[7].

Pada masa awal era digital, perusahaan seperti Google dan Facebook memanfaatkan lautan data pengguna untuk menyempurnakan algoritma dan meningkatkan pengalaman pengguna. Namun, akses data yang hampir tak terbatas ini juga memicu kegagalan privasi yang mencolok. Seiring dengan meningkatnya kesadaran publik tentang bagaimana data mereka digunakan—dan disalahgunakan—reaksi keras pun muncul, memicu regulasi ketat seperti the GDPR di Eropa, *California Consumer Privacy Act* (CCPA)[8] di California, serta Undang-Undang PDP di Indonesia[9]. Regulasi ini

[7] https://www.sciencedirect.com/science/article/pii/S0736585317302022
[8] https://oag.ca.gov/privacy/ccpa
[9] https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

tidak hanya merupakan respons terhadap masalah yang ada, tetapi juga menandai pergeseran paradigma menuju norma baru dalam penggunaan data, di mana pentingnya persetujuan dan pelindungan hak individu ditekankan.

Paradoks Privasi: Dilema Modern

"Paradoks Privasi" ini menyoroti jurang yang lebar antara kekhawatiran privasi yang diungkapkan banyak orang dan perilaku online mereka yang sebenarnya. Misalnya, banyak yang merasa tidak memiliki kendali atas data pribadi mereka, namun tetap aktif menggunakan platform digital karena kemudahan dan manfaat yang ditawarkan. Kontradiksi ini merefleksikan hubungan yang rumit antara kekhawatiran privasi dan nilai yang dirasakan dari layanan digital[10]. Daya tarik layanan online yang dipersonalisasi, konektivitas sosial, dan informasi instan sering kali lebih kuat alih-alih ancaman pelanggaran data dan penyalahgunaan yang tampak abstrak dan jauh. Perilaku paradoksal ini menunjukkan bahwa kekhawatiran privasi, meskipun nyata dan sangat dirasakan, sering kali diabaikan demi kepuasan langsung dan fungsionalitas yang disediakan oleh platform digital. Tabel 1 mendeskripsikan beberapa dimensi paradoks privasi.

Tabel 1. Dimensi paradoks privasi

Dimensi	Deskripsi
Sikap vs. Perilaku	Individu menyatakan kepedulian tinggi terhadap privasi, tetapi tetap berbagi informasi pribadi secara bebas di platform online.
Transparansi vs. Kontrol	Pengguna sering kali menginginkan transparansi terkait penggunaan data mereka, tetapi mereka cenderung tidak menggunakan opsi kontrol yang tersedia.
Keamanan vs. Kenyamanan	Pengguna ingin data mereka aman namun sering kali memilih kenyamanan (seperti menggunakan aplikasi gratis atau login otomatis) daripada keamanan.
Kepercayaan vs. Kecurigaan	Pengguna menunjukkan kepercayaan pada platform yang sering mereka gunakan, meskipun ada kekhawatiran tentang penyalahgunaan data.

[10] https://scholarship.law.gwu.edu/faculty_publications/1482/

Dimensi	Deskripsi
Kekhawatiran vs. Ketidaktahuan	Pengguna merasa khawatir tentang pelanggaran data tetapi sering kali tidak memahami kebijakan privasi yang mereka setujui.
Manfaat vs. Risiko	Pengguna merasakan manfaat dari layanan digital tetapi sering mengabaikan risiko privasi yang mungkin menyertainya.
Privasi vs. Keterbukaan	Pengguna ingin privasi tetapi juga cenderung terbuka dalam berbagi informasi demi interaksi sosial dan keterlibatan online.

Masalah utama bukan karena orang tidak peduli tentang privasi. Individu memerlukan transparansi yang lebih baik dan mekanisme yang lebih mudah digunakan agar mereka bisa mengontrol data mereka tanpa harus mengorbankan manfaat dari penggunaan teknologi digital. Mengelola privasi di dunia digital memang rumit. Survei menunjukkan bahwa privasi adalah kekhawatiran utama bagi banyak orang, tetapi mengurus privasi ini tidaklah mudah. Kebijakan privasi sering kali ditulis dengan bahasa yang sulit dipahami, terlalu panjang, mekanisme persetujuan bisa membingungkan, dan cara data dikumpulkan serta digunakan tidak selalu jelas. Semua hambatan ini membuat orang kesulitan untuk benar-benar mengontrol jejak digital mereka.

Misalnya, banyak aplikasi meminta izin untuk mengakses kontak, lokasi, atau foto di ponsel Anda. Kebanyakan individu menyetujui tanpa benar-benar memahami apa yang akan dilakukan dengan data tersebut karena kebijakan privasinya terlalu panjang dan rumit. Bahkan jika seseorang ingin menarik kembali izin tersebut, mereka sering kesulitan menemukan cara melakukannya di pengaturan aplikasi. Akibatnya, data pribadi mereka terus digunakan tanpa kontrol yang jelas, meskipun ada kekhawatiran privasi. Ini menunjukkan betapa sulitnya bagi pengguna biasa untuk mengelola privasi mereka dengan efektif dalam dunia digital saat ini. Untuk mengatasi tantangan-tantangan ini, lima rekomendasi praktis dapat diterapkan oleh organisasi.

- **Pertama**, tulislah kebijakan privasi dalam bahasa yang sederhana dan sediakan opsi persetujuan yang jelas untuk meningkatkan pemahaman dan kontrol pengguna.

- **Kedua**, berdayakan pengguna melalui persetujuan yang diinformasikan, dengan memberikan penjelasan yang jelas tentang penggunaan data dan opsi fleksibel untuk ikut serta atau keluar.
- **Ketiga**, terapkan teknik anonimisasi dan masking data untuk melindungi identitas pengguna sambil memungkinkan analisis data.
- **Keempat**, integrasikan prinsip privasi-dari-awal dalam pengembangan produk dan lakukan audit privasi secara berkala untuk memastikan kepatuhan.
- **Kelima**, edukasi pengguna tentang hak-hak privasi mereka dan tawarkan cara yang ramah pengguna untuk mengelola preferensi data mereka.

Dengan menerapkan rekomendasi-rekomendasi ini, perusahaan dapat meningkatkan kepercayaan pengguna, memastikan kepatuhan terhadap regulasi privasi, dan menciptakan lingkungan digital yang lebih aman bagi semua pemangku kepentingan.

Tantangan dan Solusi bagi Para Pengembang AI

Bagi para pengembang perangkat lunak dan AI, lanskap privasi data modern menyuguhkan tantangan-tantangan unik. Pergerakan menuju akses data yang lebih terbatas mengubah metode tradisional eksperimen dan pengujian data yang kini dibatasi oleh pertimbangan privasi. Para pengembang dihadapkan pada tugas untuk menyeimbangkan ketelitian pengelolaan data dengan kepatuhan terhadap undang-undang privasi yang ketat. Teknik seperti penggunaan data sintetis atau data yang disamarkan menjadi semakin umum, meskipun teknik ini tidak sepenuhnya menangkap kompleksitas data pengguna yang sesungguhnya. Situasi ini mempersulit upaya untuk menguji dan menyempurnakan sistem. Ini tentunya berdampak pada kebutuhan akan solusi inovatif yang menghormati privasi sembari mempertahankan efektivitas sistem.

Pengembang AI memainkan peran krusial dalam merespons kekhawatiran privasi di era digital. Seiring AI semakin terintegrasi dalam aplikasi sehari-hari, potensi untuk terjadinya pelanggaran privasi meningkat. Namun, ini juga memberikan peluang bagi pengembang untuk mempelopori teknologi yang menjaga privasi. Berikut adalah empat rekomendasi praktis:

Pertama, gunakan teknik lanjutan seperti anonimisasi, penyamaran data, dan pseudonimisasi untuk melindungi informasi pribadi. Privasi diferensial, enkripsi homomorfik [11] , dan pemelajaran terfederasi adalah contoh teknik yang patut dipertimbangkan. Privasi diferensial memungkinkan analisis data bandang sambil memastikan data individu tetap rahasia. Enkripsi homomorfik memungkinkan perhitungan pada data yang terenkripsi tanpa mengungkapkan data itu sendiri, dan pembelajaran terfederasi melatih model AI secara lokal di perangkat pengguna tanpa sentralisasi data[12].

Kedua, pengembang AI perlu mengintegrasikan pertimbangan privasi ke dalam setiap tahap siklus pengembangan AI. Pendekatan proaktif ini memastikan bahwa fitur privasi terbangun dari dasar sistem, bukan sebagai tambahan belakangan. Dengan memasukkan privasi sejak saat merancang produk, pengembang dapat menghasilkan produk yang lebih sejalan dengan persyaratan regulasi yang pada akhirnya meningkatkan kepercayaan pengguna.

Ketiga, kembangkan kebijakan dan manajemen privasi yang ramah pengguna dan ringkas. Memberikan pengguna pilihan yang mudah untuk mengelola data mereka, seperti mekanisme persetujuan yang jelas dan pengaturan privasi yang mudah dipahami, dapat memberdayakan mereka untuk mengontrol informasi pribadi mereka dan meningkatkan kepercayaan pada aplikasi AI.

Keempat, lakukan audit dan tinjauan privasi secara berkelanjutan untuk memastikan kepatuhan dengan regulasi pelindungan data seperti UU PDP, GDPR dan CCPA. Audit ini membantu mengidentifikasi potensi risiko privasi dan memastikan bahwa tindakan privasi tetap kuat dan terkini. Pemantauan dan peningkatan terus-menerus atas praktik privasi penting untuk menjaga kepercayaan pengguna dan melindungi data.

Empat rekomendasi di atas bisa dianalogikan seperti ini. Bayangkan Anda mengelola perpustakaan yang luas dan sering dikunjungi banyak orang. Seperti menyusun buku-buku langka dalam lemari kaca terkunci dan menggunakan sistem

[11] https://www.ibm.com/topics/homomorphic-encryption
[12] https://research.ibm.com/blog/what-is-federated-learning

alarm, teknik anonimisasi dan enkripsi melindungi data pengguna dari akses yang tidak sah. Aktivitas ini seperti merancang perpustakaan dengan ruang baca pribadi dan area terbatas untuk memastikan privasi pengunjung terjaga sejak mereka masuk.

Seperti menyediakan katalog digital yang mudah digunakan dan petunjuk peminjaman yang jelas, alat manajemen privasi yang sederhana membantu pengguna mengontrol data mereka dengan mudah dan merasa aman. Selain itu, melakukan pengecekan rutin terhadap koleksi buku dan fasilitas perpustakaan memastikan semuanya dalam kondisi baik dan aman digunakan. Audit privasi berfungsi dengan cara yang sama untuk memastikan pelindungan data tetap optimal dan sesuai regulasi. Dengan pendekatan ini, perpustakaan Anda tidak hanya menjadi tempat yang nyaman dan aman, tetapi juga mampu melindungi privasi dan data pengunjung dengan efektif.

Seiring kita melangkah maju di era digital, lanskap privasi data terus berkembang, dibentuk oleh kemajuan teknologi, perubahan regulasi, dan pergeseran harapan pengguna. Tantangan ini signifikan, tetapi juga menawarkan peluang untuk inovasi dan keterlibatan etis dengan teknologi. Memahami pengaturan privasi dan mengelola jejak digital sangat penting bagi individu.

Sedangkan bagi pengembang, mengadopsi pendekatan yang berfokus pada privasi dalam pengembangan AI sangatlah krusial. Membina budaya kesadaran privasi oleh individu dan organisasi, dan tanggung jawab etis akan menjadi kunci untuk menavigasi kompleksitas privasi data di era digital dan AI.

Tautan artikel:

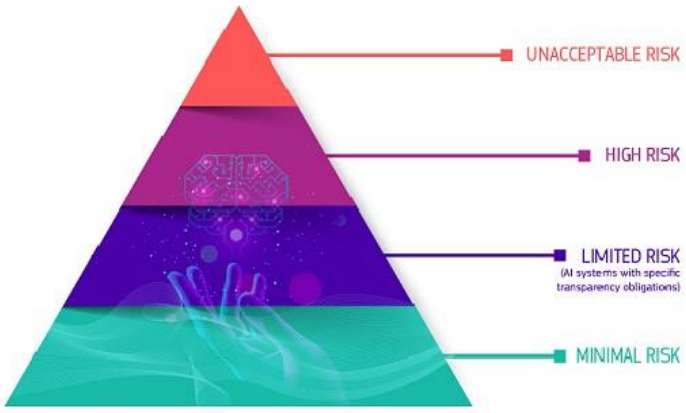
https://kumparan.com/arif-perdana-1723991955605643308/dinamika-dan-tantangan-pelindungan-data-di-era-ai-23jRmVvDiws/full

Dua Sisi EU AI Act: 10 Hal yang Bisa Dipelajari Indonesia

Arif Perdana

Konteks: Tulisan ini pertama kali diterbitkan oleh The Conversation Indonesia pada tanggal 2 Oktober 2024. Artikel ini merefleksikan pelajaran yang dapat diambil dari diskusi di kalangan akademisi dan praktisi mengenai dua sisi *EU AI Act*. Di satu sisi, *EU AI Act* bertujuan meningkatkan kepercayaan publik serta melindungi privasi warga negara dalam kaitannya dengan teknologi AI. Di sisi lain, regulasi ini berpotensi menghambat inovasi serta meningkatkan biaya kepatuhan bagi perusahaan. Ada sepuluh aspek penting yang dapat menjadi pelajaran bagi Indonesia dalam merumuskan regulasi AI yang lebih baik daripada *EU AI Act*. Aspek-aspek ini menyoroti sisi praktis, pragmatis, dan legal, serta mengedepankan pandangan ke depan yang bertujuan untuk menjaga keseimbangan antara inovasi dan regulasi, agar regulasi AI di Indonesia tidak hanya melindungi kepentingan publik, tetapi juga mendukung kemajuan teknologi.

EU AI Act merupakan regulasi pionir yang dikeluarkan oleh Uni Eropa untuk mengatur AI secara global[13]. Aturan ini bertujuan menyeimbangkan antara pelindungan hak fundamental dan inovasi yang bertanggung jawab. Dengan pendekatan berbasis risiko, *EU AI Act* mengklasifikasikan aplikasi AI berdasarkan potensi bahayanya terhadap masyarakat (Gambar 1). Beda tingkatan risiko, berbeda pula ketentuannya[14].



Gambar 1. Klasifikasi AI berbasis risiko berdasarkan *EU AI Act*[15]

[13] https://artificialintelligenceact.eu/
[14] https://artificialintelligenceact.eu/recital/27/
[15] https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Misalnya, sistem AI yang dianggap berisiko tinggi harus menjalani serangkaian penilaian ketat, termasuk evaluasi dampak dan langkah mitigasi risiko (Gambar 2). Aspek transparansi menjadi prioritas–termasuk kewajiban untuk memberi tahu pengguna ketika berinteraksi dengan AI–guna mencegah manipulasi[16]. Otoritas nasional di negara-negara Eropa juga diberikan wewenang untuk mengawasi implementasi dan mengenakan sanksi bagi pelanggar.

Gambar 2. Proses yang harus dilalui untuk AI yang memiliki risiko tinggi berdasarkan *EU AI Act* [17]

Sementara untuk mendorong inovasi, EU juga menyediakan "*sandbox* regulasi", yaitu lingkungan terkendali bagi bisnis untuk menguji teknologi AI tanpa risiko sanksi penuh[18]. Konsep *sandbox* ini membantu inovator mengurangi risiko hukum dan memberi regulator kesempatan memahami teknologi selama proses uji coba, sehingga peraturan dapat mendukung inovasi tanpa mengorbankan keamanan. Namun, beberapa praktik AI tertentu, seperti sistem penilaian sosial dan manipulasi perilaku yang merugikan, dilarang

[16] https://artificialintelligenceact.eu/article/50/
[17] https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
[18] https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf

total[19,20]. Semua aturan ini menunjukkan komitmen Uni Eropa melalui *AI Act* untuk melindungi hak-hak fundamental warga dengan memastikan keamanan dan kepercayaan publik terhadap produk dan layanan berbasis AI. Standarisasi yang dihasilkan diharapkan mendorong interoperabilitas dan efisiensi pasar AI Eropa, serta memicu inovasi etis yang selaras dengan nilai-nilai masyarakat.

Banjir Kritik *EU AI Act*

Di samping berbagai pujian terhadap aturan pionir ini, *EU AI Act* ternyata juga banjir kritik. Banyak pihak, terutama perusahaan teknologi, yang mengeluhkan regulasi ini terlalu ketat dan justru bisa menghambat inovasi dalam pengembangan AI di Eropa. Adapun beberapa poin yang menjadi kritikan di antaranya:

- Persyaratan yang rumit bisa menjadi beban yang mengalihkan fokus dan sumber daya perusahaan dari inovasi ke urusan administratif[21].
- Definisi dan klasifikasi risiko dalam *EU AI Act* dianggap masih kurang jelas. Beberapa istilah, seperti *end user* (pengguna akhir) dan *affected persons* (orang yang terdampak), tidak didefinisikan dengan baik. Ketidakjelasan ini dapat menyebabkan interpretasi yang berbeda di antara negara anggota Uni Eropa, menciptakan tantangan dalam penerapan regulasi tersebut secara konsisten[22].
- Ada beberapa pasal yang menjadi sorotan, salah satunya pasal 14[23]. Meskipun pasal ini menjelaskan soal kategori risiko tinggi, keragaman dalam interpretasi, persyaratan yang kompleks, dan kurangnya pedoman spesifik dapat menyebabkan kebingungan dalam penerapannya. Imbasnya, hal tersebut berpotensi memicu ketidakpastian kepatuhan. Selanjutnya, konsideran 8, Pasal 1[24]. Meskipun poin ini menegaskan tujuan untuk melindungi keselamatan dan hak dasar, cakupan yang luas dari pernyataan ini dapat menyebabkan tantangan

[19] https://www.hrw.org/news/2023/10/09/eu-artificial-intelligence-regulation-should-ban-social-scoring
[20] https://www.bruegel.org/blog-post/dark-side-artificial-intelligence-manipulation-human-behaviour
[21] https://hbr.org/2024/02/the-eus-ai-act-and-how-companies-can-achieve-compliance
[22] https://euneedsai.com/
[23] https://artificialintelligenceact.eu/article/14/
[24] https://artificialintelligenceact.eu/article/1/

dalam interpretasi dan penerapan regulasi, baik bagi perusahaan maupun regulator.

- Penilaian dan sertifikasi di bawah *EU AI Act* juga ruwet, terutama untuk sistem AI yang dianggap berisiko tinggi, yang melibatkan berbagai tahap evaluasi, pengujian, dan dokumentasi untuk membuktikan kepatuhan terhadap persyaratan regulasi. Durasi proses sertifikasi dan evaluasi juga tidak bisa dipastikan, karena bervariasi tergantung kompleksitas sistem, jenis penilaian, dan ketersediaan badan sertifikasi[25].

Meskipun sejumlah aturan penting dibuat untuk menjaga keamanan dan privasi dalam pengembangan AI, pembatasan yang terlalu ketat dan implementasi standar yang berbeda-beda dapat menimbulkan fragmentasi dan membatasi potensi inovasi teknologi AI. Hal ini pada gilirannya dapat menghambat kemajuan dan daya saing Eropa dalam inovasi teknologi AI. Di samping itu, muncul kekhawatiran tentang brain drain, yaitu ketika regulasi yang ketat dapat mendorong para talenta digital dan perusahaan AI beralih ke wilayah yang lebih ramah inovasi[26]. Misalnya, perusahaan rintisan teknologi bisa saja memindahkan operasional atau bahkan seluruh perusahaan mereka ke negara seperti Amerika Serikat yang saat ini memiliki regulasi yang cenderung ramah inovasi dalam hal pengembangan AI[27].

Belajar dari Sejarah

UU Lokomotif pada abad ke-19 semestinya memberikan pelajaran penting bagi Uni Eropa dalam menyusun *AI Act*, terutama dalam hal menyeimbangkan regulasi dengan inovasi[28]. Awalnya, UU Lokomotif memberlakukan pembatasan yang sangat ketat pada kendaraan bermesin, termasuk persyaratan untuk mengatur kecepatan maksimum. Pembatasan ini kemudian dinilai menghambat pengembangan teknologi otomotif dan

[25] https://www.nature.com/articles/s41746-024-01221-6

[26] https://joint-research-centre.ec.europa.eu/jrc-mission-statement-work-programme/facts4eufuture/artificial-intelligence-european-perspective/ai-opportunities-and-threats_en

[27] https://www.insideradio.com/free/perspective-the-u-s-will-be-the-most-fertile-soil-for-ai-in-the-foreseeable/article_9a0623da-7979-11ef-80ca-d33ad20c1a64.html

[28] https://www.legislation.gov.uk/ukpga/Vict/24-25/70/enacted

memperlambat adopsi kendaraan bermotor. Seiring waktu, UU Lokomotif akhirnya diubah dengan sejumlah pelonggaran yang memungkinkan industri otomotif untuk tumbuh dan berkembang. Ini menunjukkan pentingnya fleksibilitas dalam regulasi untuk dapat beradaptasi dengan perubahan teknologi dan kebutuhan industri.

Jadi, penerapan AI Act dengan pendekatan berbasis risiko memang sebuah langkah yang tepat. Namun, yang harus diingat bahwa regulasi yang baik harus tetap fleksibel dan adaptif dengan peninjauan berkala. Regulator perlu belajar dari pengalaman sejarah, seperti UU Lokomotif, untuk memastikan bahwa regulasi berfungsi sebagai pendorong kemajuan, bukan sebagai penghalang.

Pelajaran bagi Indonesia

Bagi negara-negara Asia, terutama Indonesia, pengalaman *EU AI Act*, dengan segala kelebihan dan kekurangannya, dapat menjadi pelajaran berharga dalam menyusun regulasi AI di masa mendatang. Setidaknya ada 10 hal yang seharusnya diperhatikan dalam mengatur AI:

- Pendekatan bertahap yang memungkinkan adaptasi industri tanpa guncangan ekonomi sambil memberi ruang untuk evaluasi dan penyesuaian kebijakan, termasuk pengaturan mengenai hak data dan privasi, dengan mempertimbangkan transparansi dalam proses pengambilan keputusan oleh AI.
- Kerangka regulasi fleksibel yang mengakomodasi kecepatan perkembangan teknologi AI dan memungkinkan pembaruan tanpa perombakan total. Pengawasan independen diperlukan untuk menjamin implementasi yang sesuai dengan etika dan keamanan.
- Kolaborasi lintas sektor antara pemerintah, industri, akademisi, dan masyarakat sipil dalam proses pembuatan kebijakan, seperti menjamin transparansi dan akuntabilitas di sektor-sektor yang rentan.
- Alih-alih mengatur seluruh spektrum AI sekaligus, Indonesia dapat fokus pada area yang paling kritis bagi konteks nasional.

- Kerja sama dalam blok regional untuk menciptakan standar yang harmonis, meningkatkan daya saing kolektif, dan mengurangi fragmentasi pasar global, sembari memperhatikan harmonisasi regulasi internasional agar tidak terjadi kesenjangan pengaturan di antara negara.
- Regulasi berbasis insentif yang bertujuan mendorong adopsi AI secara etis serta menciptakan lingkungan bisnis yang kolaboratif. Penting bagi kita untuk mengatur perusahaan teknologi agar tidak menjadi "*super policy entrepreneurs*" atau korporasi yang memiliki pengaruh sangat besar dalam pembuatan kebijakan, sehingga mereka bisa memaksakan atau mendorong kebijakan yang menguntungkan mereka. Kita harus memastikan AI digunakan untuk kepentingan publik, bukan semata korporasi atau kelompok tertentu.
- Membangun kapasitas regulator dan memastikan regulasi relevan dengan perkembangan teknologi.
- Adopsi pendekatan "*sandbox* regulasi" penting untuk memungkinkan eksperimen terkontrol teknologi AI baru.
- Dalam merancang regulasi, penting untuk mempertimbangkan kapasitas usaha kecil menengah dan startup lokal. Memberikan bantuan teknis dan finansial dapat memperkuat ekosistem inovasi.
- Mengizinkan penyesuaian kebijakan sesuai perkembangan teknologi dan kebutuhan masyarakat.

Dengan mengambil pelajaran ini, Indonesia dapat menciptakan lingkungan regulasi yang mendorong inovasi AI sambil melindungi kepentingan publik. Keseimbangan antara pengaturan dan fleksibilitas untuk mendorong inovasi adalah kuncinya.

Tautan artikel:

https://theconversation.com/dua-sisi-eu-ai-act-10-hal-yang-bisa-dipelajari-indonesia-239824

Memetakan Regulasi AI di Indonesia

Arif Perdana

Konteks: Tulisan ini pertama kali diterbitkan di detik.com pada tanggal 2 Oktober 2024. Artikel ini menyoroti pentingnya regulasi AI di Indonesia. Meskipun Indonesia bisa mengambil inspirasi dari UU AI di Uni Eropa, formulasi regulasi AI di Indonesia harus dilakukan dengan cermat. Tujuannya adalah untuk memastikan regulasi tersebut mendukung inovasi teknologi tanpa membebani operasional perusahaan. Di saat yang sama, regulasi AI ini juga harus mampu memberikan dampak positif yang signifikan bagi masyarakat luas.

Perkembangan AI menjadi fokus utama banyak negara. Pada Agustus 2024, Uni Eropa menetapkan UU yang mengatur AI berdasarkan risiko, menegaskan bahwa era AI tanpa pengawasan harus berakhir[29]. Australia menyusul dengan standar keamanan sukarela dan usulan pelindungan wajib untuk sistem AI berisiko tinggi[30]. Kedua langkah ini menunjukkan bagaimana AI harus diatur untuk melindungi masyarakat dari dampak negatif. Indonesia, dengan sektor teknologi yang berkembang pesat, perlu menyesuaikan diri dengan regulasi global ini. UU PDP menjadi langkah awal yang baik, tetapi regulasi AI di Indonesia harus lebih luas, mencakup isu bias algoritma dan keamanan informasi, sambil tetap mendorong inovasi.

Bias dalam Sistem AI: Tantangan Besar

Indonesia kini berada di persimpangan kritis. AI bukan lagi teknologi masa depan; ia telah menjadi realitas yang merambah berbagai sektor kehidupan—dari kesehatan hingga keuangan, dari pendidikan hingga peradilan. Tanpa regulasi yang tepat, AI berpotensi menciptakan ketimpangan baru, memperkuat diskriminasi yang sudah ada, dan mengancam hak-hak dasar warga negara. Sebagai negara besar dengan keragaman budaya yang kaya, Indonesia memiliki kesempatan berharga untuk membentuk wacana

[29] https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en

[30] https://www.herbertsmithfreehills.com/insights/2024-09/australia-releases-new-mandatory-guardrails-and-voluntary-standards-on-ai

global tentang tata kelola AI. Indonesia bisa menyumbangkan perspektif sosial dan kultural unik yang mungkin terabaikan dalam diskusi internasional yang didominasi oleh negara maju

Urgensi regulasi AI semakin nyata ketika meluasnya penggunaan teknologi ini di sektor-sektor penting. Dari algoritma penilaian kredit hingga sistem prediksi kriminal, AI memiliki kekuatan yang besar untuk mempengaruhi kehidupan individu dan masyarakat. Di bidang kesehatan, misalnya, AI sudah digunakan untuk membantu diagnosis penyakit, seperti kanker, dengan menganalisis data medis dan hasil pencitraan. Namun, tanpa pengawasan yang memadai, potensi kesalahan diagnosis atau diskriminasi terhadap kelompok tertentu bisa terjadi, terutama jika algoritma AI dilatih menggunakan data yang tidak beragam atau tidak representatif. Algoritma yang bias berpotensi menempatkan pasien dari kelompok minoritas pada risiko yang lebih tinggi, baik karena diagnosis yang keliru maupun karena tidak mendapatkan akses layanan kesehatan yang setara. Oleh karena itu, tanpa regulasi yang ketat, penyalahgunaan dan diskriminasi sistemik menjadi ancaman yang nyata. Tabel 2 menunjukkan beberapa bias yang mungkin muncul dari penggunaan AI.

Tabel 2. Bias yang berpotensi muncul dari penggunaan AI

Kategori Bias	Deskripsi	Jenis Bias yang Termasuk
Bias Data	Terjadi ketika data yang digunakan untuk melatih atau menguji AI tidak representatif atau mencerminkan pandangan yang terbatas dan bias sosial tertentu.	Bias Data, Bias Seleksi, Bias Sosial
Bias Algoritmik	Muncul dari pemilihan atau desain algoritma yang memperkuat atau menciptakan bias yang ada dalam data atau pemrosesan informasi.	Bias Algoritmik, Bias Konfirmasi, Bias Stereotip
Bias Pengguna/Interaksi	Terjadi akibat interaksi pengguna dengan sistem AI yang memengaruhi pembelajaran atau hasil AI,	Bias Interaksi, Bias Sosial (karena norma dan nilai sosial yang tercermin dalam data dan interaksi pengguna)

Kategori Bias	Deskripsi	Jenis Bias yang Termasuk
	serta bias yang muncul dari cara pengguna berinteraksi.	

Jalan menuju regulasi yang efektif memang penuh dengan tantangan. Kecepatan inovasi dalam bidang ini sering kali membuat para praktisi AI sendiri kewalahan, apalagi pembuat kebijakan yang mungkin kurang familier dengan teknis AI. Regulasi yang terlalu kaku atau terlalu spesifik dapat cepat menjadi usang. Oleh karena itu, kerangka hukum yang fleksibel sangat dibutuhkan untuk mengakomodasi perkembangan teknologi, namun tetap memberikan perlindungan yang memadai bagi masyarakat.

Peningkatan kapasitas para pembuat kebijakan menjadi kunci untuk menjawab tantangan ini. Literasi digital yang sedang digalakkan pemerintah kepada aparatur sipil negara merupakan langkah awal yang baik, namun pemahaman mendalam tentang AI di kalangan legislator dan regulator juga harus ditingkatkan. Mereka yang membuat aturan harus memahami sepenuhnya teknologi yang mereka atur. Ini memerlukan pelatihan intensif dan kolaborasi dengan para ahli di bidang teknologi, hukum, dan etika.

Membangun Kerangka Regulasi AI yang Fleksibel dan Adil

Pendekatan multidisiplin sangat penting dalam merancang regulasi AI yang komprehensif dan adil. Kolaborasi antara ahli teknologi, hukum, etika, dan sosiologi dibutuhkan agar regulasi dapat mengimbangi perkembangan AI yang pesat. Indonesia harus bergerak cepat untuk memastikan teknologi ini membawa manfaat, bukan malapetaka. Meskipun pelaku industri di Indonesia khawatir bahwa regulasi yang terlalu ketat akan menghambat inovasi, mereka menyadari pentingnya regulasi yang berimbang. Pendekatan bertahap yang tidak meningkatkan biaya kepatuhan secara signifikan menjadi preferensi utama, karena biaya tinggi bisa menjadi hambatan bagi inovasi.

Standar sukarela seperti di Australia dapat menjadi contoh. *Voluntary AI Safety Standard Australia*, misalnya, memiliki 10 batasan yang memastikan AI digunakan secara aman dan bertanggung jawab[31]. Batasan ini mencakup akuntabilitas, manajemen risiko,

[31] https://www.industry.gov.au/publications/voluntary-ai-safety-standard

dan pelindungan data, serta transparansi dalam pengambilan keputusan AI. Organisasi juga didorong untuk menguji model AI secara menyeluruh, melibatkan intervensi manusia, dan menyediakan mekanisme bagi pengguna untuk mengevaluasi hasil. Transparansi antar organisasi dan keterlibatan pemangku kepentingan dalam penggunaan AI adalah langkah penting untuk menjaga keamanan, keragaman, dan keadilan.

Langkah awal yang bisa diambil Indonesia adalah membentuk gugus tugas lintas sektoral yang memetakan dampak AI di berbagai bidang. Hasil pemetaan ini dapat menjadi dasar dalam merancang kerangka regulasi yang fleksibel namun menyeluruh. Penguatan kapasitas sumber daya manusia juga krusial, dengan program pelatihan intensif bagi pembuat kebijakan dan aparatur pemerintah tentang implikasi AI.

Kolaborasi dengan akademisi dan praktisi industri akan memperkaya perspektif serta memastikan materi pelatihan relevan. Selain itu, keterlibatan aktif Indonesia dalam forum internasional terkait tata kelola AI penting untuk menyerap pelajaran dari negara lain sekaligus memastikan bahwa kepentingan Indonesia diakomodasi dalam standar global. Dengan pendekatan yang tepat, Indonesia dapat menyeimbangkan mitigasi risiko, pelindungan pengguna, dan inovasi, serta merancang regulasi yang bijak untuk era AI.

Tautan artikel:

https://news.detik.com/kolom/d-7568270/memetakan-regulasi-ai-di-indonesia

Indonesia Harus Melangkah Berani dalam Regulasi untuk Membentuk Masa Depan AI

Arif Perdana

Konteks: Artikel ini pertama kali diterbitkan dalam bahasa Inggris di *The Jakarta Post* pada 14 September 2024 dan menanggapi penerapan *EU AI Act* di Eropa. Artikel ini menyoroti bahwa, berangkat dari UU PDP, Indonesia memiliki potensi untuk meregulasi AI dengan lebih baik. Ada tiga aspek yang dapat dimanfaatkan Indonesia dalam regulasi AI. Pertama, Indonesia memiliki sektor teknologi yang berkembang pesat, yang dapat menjadi fondasi untuk mengembangkan keahlian AI dan menerapkan praktik AI yang bertanggung jawab. Kedua, UU PDP yang sudah ada dapat menjadi landasan awal untuk mengatur AI, khususnya dalam hal persetujuan, pemrosesan data, dan hak subjek data. Ketiga, sebagai negara yang besar dan beragam, Indonesia dapat memberikan perspektif penting dalam diskusi tata kelola AI di tingkat internasional, memastikan regulasi AI mempertimbangkan konteks sosial dan budaya yang beragam. Namun, regulasi AI harus dibuat seimbang agar tidak menghambat inovasi. Aturan teknis yang terlalu spesifik perlu dihindari karena kemajuan di bidang AI sangat cepat, sehingga regulasi semacam itu dapat segera menjadi usang.

Kemajuan pesat AI membawa peluang sekaligus risiko bagi Indonesia. Bayangkan suatu ketika wajah Anda ditemukan di video *deepfake* yang viral tanpa izin. Di kasus lain, Anda atau kerabat mungkin ditolak dalam seleksi pekerjaan oleh sistem AI yang memiliki bias tersembunyi. Skenario-skenario ini kian menjadi kenyataan seiring AI mengubah dunia kita. Dari sektor kesehatan hingga sistem peradilan pidana, pengaruh AI terus meluas, sering kali tanpa kita sadari. Tanpa pengawasan yang tepat, teknologi ini dapat memperlebar kesenjangan sosial, mengorbankan privasi, dan memperkuat kekuasaan di tangan segelintir perusahaan teknologi multinasional. Oleh karena itu, regulasi pemerintah sangat penting untuk memastikan AI melayani kepentingan publik dan melindungi hak-hak individu di tengah masyarakat yang semakin terdigitalisasi.

Uni Eropa telah mengambil langkah berani dengan menerbitkan UU AI pada Juli 2024, yang mulai berlaku pada 1 Agustus 2024. Regulasi komprehensif ini bertujuan untuk menciptakan aturan yang seragam bagi sistem AI di seluruh 27 negara Uni Eropa.

UU ini mengkategorikan sistem AI berdasarkan tingkat risikonya menjadi empat yaitu: tidak dapat diterima, tinggi, terbatas, atau minimal. Beberapa praktik AI yang merugikan dilarang sepenuhnya, sementara sistem dengan risiko tinggi menghadapi persyaratan yang ketat. Regulasi ini juga mendorong transparansi dalam aplikasi AI tertentu dan membentuk badan pengawas baru untuk memastikan kepatuhan serta memperkuat kerja sama antarnegara anggota.

Australia juga turut serta dalam upaya regulasi. Pemerintah federalnya mengusulkan pengamanan wajib bagi sistem AI berisiko tinggi dan standar keamanan sukarela untuk organisasi yang menggunakan AI[32,33]. Pendekatan Australia mencakup sepuluh pedoman yang saling terkait, menetapkan ekspektasi yang jelas bagi semua pihak dalam rantai pasokan AI, dengan menekankan akuntabilitas, transparansi, dan pengawasan manusia.

Bagi Indonesia, perkembangan global ini, ditambah dengan keberadaan UU PDP membawa implikasi yang signifikan. Sebagai negara yang tumbuh pesat dengan industri teknologi yang berkembang, kita harus mengamati tren internasional ini dengan cermat. Kita dapat belajar dari pendekatan berbasis risiko Uni Eropa dan standar sukarela Australia untuk mendorong pengembangan AI yang bertanggung jawab di dalam negeri. Ini merupakan peluang bagi Indonesia untuk berpartisipasi aktif di diskusi internasional tentang tata kelola AI. Ini juga untuk memastikan perspektif kita terwakili. Di samping itu, membangun keahlian lokal dalam etika dan regulasi AI akan sangat berharga untuk menghadapi tantangan di masa depan.

Kebutuhan akan regulasi AI muncul dari potensi bahaya serius yang bisa terjadi jika dibiarkan tanpa pengawasan. Sistem AI yang dilatih dengan data yang bias berisiko memperkuat dan memperparah ketidaksetaraan sosial. Jumlah data yang besar yang dibutuhkan oleh sistem ini menimbulkan kekhawatiran tentang pelindungan informasi pribadi. Banyak sistem AI beroperasi sebagai “kotak hitam,” sehingga sulit untuk meninjau proses pengambilan keputusannya, yaitu kurangnya transparansi, terutama

[32] https://www.industry.gov.au/publications/voluntary-ai-safety-standard/10-guardrails
[33] https://consult.industry.gov.au/ai-mandatory-guardrails

ketika keputusan tersebut dapat memiliki dampak besar bagi kehidupan individu dan sosial.

Disrupsi tenaga kerja juga menjadi perhatian serius seiring kemajuan kemampuan AI. Konsentrasi teknologi AI canggih di beberapa perusahaan teknologi besar dapat menyebabkan kekuatan monopoli yang belum pernah terjadi sebelumnya. Kerentanan keamanan dalam sistem AI juga menimbulkan risiko peretasan atau eksploitasi jahat. Kemunculan AI generatif menyebabkan potensi penyebaran informasi yang salah secara luas. Ini membuat batas antara konten orisinil dan yang dihasilkan secara artifisial semakin kabur.

Mengingat risiko-risiko ini, ada beberapa area yang memerlukan regulasi di lanskap AI (lihat Tabel 3). Aplikasi AI berisiko tinggi di sektor kesehatan, peradilan pidana, keuangan, dan ketenagakerjaan memerlukan panduan yang jelas. Aturan yang komprehensif harus mengatur bagaimana data pribadi digunakan untuk melatih sistem AI dan menginformasikan proses pengambilan keputusan. UU PDP harus menjadi landasan yang kuat dalam hal ini, dengan ketentuannya tentang persetujuan dan pemrosesan data sebagai titik awal yang bisa diperkuat dan diperluas lebih lanjut.

Tabel 3. Area yang memerlukan regulasi AI

Area Regulasi	Risiko / Tantangan	Saran / Pendekatan Regulasi
Aplikasi AI Berisiko Tinggi	Penggunaan AI di sektor kesehatan, peradilan pidana, keuangan, ketenagakerjaan memiliki risiko tinggi	Panduan jelas dengan aturan komprehensif untuk penggunaan data pribadi dan pengambilan keputusan dalam aplikasi berisiko tinggi, didukung oleh UU PDP.
Transparansi & Akuntabilitas	Masyarakat tidak mengetahui cara AI membuat keputusan penting	Meningkatkan hak atas informasi terkait proses pengambilan keputusan oleh AI, standar pengujian ketat, serta mekanisme akuntabilitas yang jelas jika terjadi kesalahan.
Keamanan & Keandalan	Risiko kegagalan atau ketidakadilan sistem AI dalam implementasi	Standar keamanan dan pengujian ketat sebelum penggunaan, termasuk evaluasi keberlanjutan dan keandalan sistem AI.

Area Regulasi	Risiko / Tantangan	Saran / Pendekatan Regulasi
Inovasi vs. Regulasi	Risiko hambatan inovasi jika regulasi terlalu ketat pada semua aplikasi AI	Regulasi yang fleksibel untuk aplikasi berisiko rendah (misalnya, filter spam) dan pendekatan tidak terlalu teknis agar tidak cepat usang.
Kolaborasi Multi-Pemangku	Tantangan kolaborasi antara pemerintah, perusahaan, dan konsumen	Pemerintah menciptakan platform dialog, menetapkan regulasi adaptif, dan mendukung penelitian AI; perusahaan mematuhi prinsip etis, dan konsumen menuntut transparansi.
Etika & Keberpihakan pada Konsumen	Risiko bias dalam AI dan kurangnya transparansi perusahaan terhadap konsumen	Perusahaan mengintegrasikan prinsip etis sejak awal, berinvestasi dalam mitigasi bias dan teknologi yang dapat dijelaskan (*explainable AI*), serta transparansi terhadap pemangku kepentingan.
Literasi & Tanggung Jawab Konsumen	Rendahnya literasi AI di masyarakat yang bisa mempengaruhi pemahaman terhadap dampak AI	Pengembangan program literasi AI nasional, peningkatan standar industri, dan kesadaran konsumen untuk menggunakan hak data dan berpartisipasi dalam konsultasi publik.
Pembangunan Kapasitas Nasional	Kebutuhan untuk membangun kemampuan dan standar AI yang bertanggung jawab di Indonesia	Fokus pada investasi pemerintah di pendidikan dan penelitian AI, menetapkan standar AI industri, dan membangun budaya inovasi yang bertanggung jawab.

Transparansi menjadi sangat penting. Dalam hal ini masyarakat berhak mengetahui bagaimana AI mengambil keputusan penting tentang hidup mereka. Ini sejalan dengan penekanan UU PDP pada hak-hak subjek data dan kewajiban pengendali serta pemroses data. Standar keamanan dan pengujian yang ketat harus diterapkan untuk memastikan keandalan dan keadilan sebelum sistem AI digunakan. Selain itu, mekanisme akuntabilitas yang jelas harus diterapkan jika terjadi kesalahan.

Namun, regulasi harus seimbang agar tidak menghambat inovasi. Penelitian dasar dan pengembangan teknologi AI harus memiliki kelonggaran. Aplikasi AI berisiko rendah, seperti filter spam atau AI di gim video, mungkin tidak memerlukan regulasi yang ketat.

Aturan teknis yang terlalu spesifik harus dihindari, karena AI bergerak begitu cepat sehingga regulasi semacam itu bisa dengan cepat menjadi usang. Pendekatan yang lebih fleksibel mungkin cocok untuk AI di bidang kreatif dan seni.

Tantangannya adalah menemukan keseimbangan yang tepat antara melindungi kepentingan publik dan mendorong inovasi. Ini bukan tugas pemerintah saja, melainkan diperlukan kolaborasi antara pemerintah, perusahaan, dan konsumen. Peran pemerintah adalah mengembangkan regulasi AI yang jelas, fleksibel, dan dapat ditegakkan, dengan membangun landasan dari UU PDP. Pemerintah juga harus berinvestasi di penelitian dan pendidikan AI untuk membangun kemampuan nasional. Pemerintah perlu menciptakan platform untuk dialog antara semua pemangku kepentingan, begitu pula dengan memastikan regulasi dapat mengikuti perubahan teknologi yang cepat.

Perusahaan harus mengintegrasikan prinsip-prinsip etis AI ke dalam pengembangan produk mereka sejak awal, dengan mematuhi prinsip-prinsip pelindungan data yang diuraikan dalam UU PDP. Investasi dalam mitigasi bias dan teknologi AI yang dapat dijelaskan (*explainable AI*) sangat penting. Mereka juga harus transparan dengan pelanggan dan pemangku kepentingan tentang penggunaan AI mereka. Kolaborasi dengan regulator dan akademisi untuk mengatasi tantangan AI sangatlah penting.

Konsumen juga memiliki tanggung jawab. Kita harus mendidik diri kita sendiri tentang AI dan dampaknya, menuntut transparansi dari perusahaan yang menggunakan sistem AI, dan berpartisipasi dalam konsultasi publik tentang regulasi AI. Kita harus menggunakan hak-hak data kita dan membuat pilihan yang tepat tentang layanan berbasis AI.

Indonesia harus fokus pada pengembangan program literasi AI, menetapkan standar industri untuk pengembangan AI yang bertanggung jawab, menerapkan mekanisme untuk penilaian berkelanjutan terhadap dampak sosial AI, dan membangun budaya inovasi yang bertanggung jawab di sektor AI. Dengan mengambil pendekatan kolaboratif dan proaktif terhadap tata kelola AI, Indonesia dapat memanfaatkan manfaat teknologi transformatif ini sambil memitigasi risikonya. Tentu saja ini memerlukan dialog

berkelanjutan, regulasi yang dapat beradaptasi, dan komitmen bersama terhadap prinsip-prinsip etis dari semua pemangku kepentingan.

Seiring dengan perkembangan pesat AI, strategi tata kelola kita harus mengikuti agar teknologi ini melayani kebaikan bersama masyarakat. Masa depan AI sedang dibentuk sekarang, dan kita baik individu dan masyarakat harus membentuknya dengan tanggung jawab. Mari kita pastikan masa depan ini membawa manfaat bagi seluruh masyarakat Indonesia.

Tautan artikel:

https://www.thejakartapost.com/opinion/2024/09/14/indonesia-must-take-a-bold-step-on-regulation-to-shape-the-future-of-ai.html

https://asianews.network/indonesia-must-take-a-bold-step-on-regulation-to-shape-the-future-of-ai/

Bagaimana Konsumen Dapat Memengaruhi Siapa yang Mengendalikan AI

Arif Perdana, Ridoan Karim

Konteks: Tulisan ini pertama kali diterbitkan dalam bahasa Inggris oleh 360info.org pada 23 Agustus 2023, dan kemudian direplikasi oleh beberapa media lainnya, termasuk Monash Lens, Tatler, dan Tempo. Ide utama dari artikel ini dikembangkan dari diskursus mengenai pengaruh signifikan perusahaan teknologi besar terhadap formulasi kebijakan. Hal ini dipertegas dalam studi yang dilakukan oleh Khanal et al. (2024), yang menyatakan bahwa perusahaan-perusahaan teknologi besar cenderung menjadi *super policy entrepreneurs* dengan aktif melakukan lobi-lobi kepada pemerintah untuk memengaruhi regulasi yang menguntungkan mereka.

Warren Buffett sebagian benar tentang AI. Investor dan filantropis miliarder ini mengatakan kepada CNN di awal tahun ini: "Kita membiarkan jin keluar dari botol ketika kita mengembangkan senjata nuklir... AI agak mirip—ia sudah setengah keluar dari botol." Pemikiran Buffett adalah bahwa, seperti senjata nuklir, AI memiliki potensi untuk memberikan dampak besar dalam skala yang luas, baik untuk kebaikan maupun keburukan[34]. Dan, seperti senjata nuklir, AI terkonsentrasi di tangan segelintir pihak. Dalam kasus AI, ini adalah pertarungan antara perusahaan teknologi dan negara. Perbandingan ini jarang dibahas di berbagai majalah dan koran.

Saat perusahaan-perusahaan ini mendorong batas inovasi, muncul pertanyaan penting: Apakah kita mengorbankan keadilan dan kesejahteraan masyarakat demi kemajuan? Satu studi yang dilakukan oleh Khanal et al. (2024) menunjukkan bahwa pengaruh *Big Tech* ada di seluruh proses kebijakan. Pengaruh ini memperkuat posisi mereka sebagai *super policy entrepreneurs*. Hal ini memungkinkan mereka untuk

[34] https://edition.cnn.com/2024/05/06/investing/warren-buffett-compares-ai-nuclear-weapons/index.html

mengarahkan kebijakan yang menguntungkan kepentingan mereka, seringkali dengan mengorbankan kepentingan masyarakat luas[35].

Kekuatan yang terkonsentrasi ini juga memungkinkan perusahaan-perusahaan ini membentuk teknologi AI menggunakan kumpulan data yang sangat besar yang mencerminkan demografi dan perilaku tertentu yang cenderung mengorbankan masyarakat yang lebih luas. Hasilnya adalah lanskap teknologi yang, meskipun berkembang pesat, mungkin secara tidak sengaja memperbesar kesenjangan sosial dan melanggengkan bias yang sudah ada.

Masalah Etika

Kekhawatiran etika yang muncul dari konsentrasi kekuatan ini sangat signifikan. Jika model AI sebagian besar dilatih pada data yang mencerminkan perilaku satu demografi, ia mungkin berkinerja buruk saat berinteraksi atau membuat keputusan tentang demografi lain, yang berpotensi menyebabkan diskriminasi dan ketidakadilan sosial. Amplifikasi bias ini bukan hanya kekhawatiran teoretis tetapi kenyataan yang sudah terjadi dan memerlukan perhatian segera.

Porcha Woodruff, misalnya, seorang wanita kulit hitam yang sedang hamil, secara keliru ditangkap karena kesalahan pengenalan wajah—satu kejadian nyata tentang dampak AI[36]. Di bidang kesehatan, algoritma yang banyak digunakan di Amerika Serikat, secara signifikan mendiskriminasikan kebutuhan pasien kulit hitam, yang mengarah pada perawatan yang tidak memadai dan memperburuk ketimpangan yang sudah ada[37]. Kasus-kasus ini menggarisbawahi pola yang mengkhawatirkan. Sistem AI, yang dilatih dengan data bias, memperbesar ketidaksetaraan sosial. Institusi perlu memertimbangkan algoritma yang menggerakkan sistem AI ini, yang sebagian besar mungkin dikembangkan di lingkungan yang mungkin kurang pedului dengan keadilan (*fairness*) dan inklusivitas.

[35] https://doi.org/10.1093/polsoc/puae012
[36] https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html
[37] https://www.science.org/doi/10.1126/science.aax2342

Potensi Bias

Aplikasi AI dalam bidang seperti pengenalan wajah, praktik perekrutan, dan persetujuan pinjaman mungkin menghasilkan bias. Bias ini tentu saja memengaruhi komunitas yang kurang terwakili secara tidak proporsional. Risiko ini diperburuk oleh model bisnis perusahaan-perusahaan yang menekankan pengembangan dan penerapan yang cepat, alih-alih dengan meninjau etika secara ketat. Mereka cenderung mengutamakan keuntungan alih-alih mempertimbangkan dampak jangka panjang pada masyarakat. Untuk mengatasi tantangan ini, perubahan dalam pengembangan AI sangat diperlukan. Pengaruh perusahaan *Big Tech* seharusnya diimbangi dengan adanya peneliti independen, ilmuwan dan pemerhati etika, kelompok kepentingan publik, dan regulator pemerintah yang bekerja sama untuk menetapkan pedoman yang memprioritaskan pertimbangan etika dan kesejahteraan masyarakat dalam pengembangan AI.

Pemerintah juga memiliki peran penting dalam hal ini. Penegakan kebijakan anti monopoli yang ketat akan membatasi kekuatan perusahaan teknologi besar dan mendorong persaingan[38]. Pengawas independen dengan otoritas untuk memberikan sanksi kepada praktik *Big Tech* juga akan membantu, bersama dengan peningkatan partisipasi publik dalam pembuatan kebijakan dan mewajibkan transparansi untuk algoritma dan praktik data perusahaan teknologi. Kerja sama global untuk mendorong standar etika dan investasi dalam program pendidikan untuk memberdayakan warga agar memahami dampak teknologi pada masyarakat akan semakin mendukung upaya ini. Dunia akademis juga dapat berperan. Peneliti dapat mengembangkan metode untuk mendeteksi dan menetralkan bias dalam algoritma AI dan data pelatihan. Dengan melibatkan publik, akademisi dapat memastikan suara yang beragam didengar dalam pembentukan kebijakan AI.

Kewaspadaan dan partisipasi publik sangat penting untuk meminta pertanggungjawaban perusahaan dan pemerintah. Publik dapat memberikan tekanan pasar dengan memilih produk AI dari perusahaan yang menunjukkan praktik etis. Sementara regulasi AI dapat membantu mencegah konsentrasi kekuatan di tangan

[38]https://www.forbes.com/sites/aldenabbott/2024/03/13/why-antitrust-regulators-are-focused-on-problematic-ai-algorithms/

segelintir pihak, langkah-langkah anti monopoli yang membatasi perilaku monopolistik, mempromosikan standar terbuka, dan mendukung perusahaan kecil serta startup dapat membantu mengarahkan kemajuan AI untuk kepentingan publik.

Peluang Unik

Namun, tantangannya adalah bahwa pengembangan AI memerlukan data dan sumber daya komputasi yang substansial, yang bisa menjadi hambatan besar bagi pemain yang lebih kecil. Di sinilah AI *open-source* menghadirkan peluang unik untuk mendemokratisasikan akses, berpotensi menciptakan lebih banyak inovasi di berbagai sektor[39].

Memberikan akses yang setara kepada peneliti, startup, dan lembaga pendidikan untuk berinteraksi dengan AI mutakhir akan memberikan peluang yang sama bagi semua pihak. Masa depan AI tidak ditentukan sebelumnya. Tindakan yang diambil sekarang dapat membentuk lanskap teknologi yang mencerminkan nilai-nilai dan aspirasi kolektif kita, memastikan manfaat AI dibagikan secara adil di seluruh masyarakat. Pertanyaannya bukan apakah kita mampu mengambil langkah-langkah ini, tetapi apakah kita mampu untuk tidak melakukannya.

Tautan artikel:

https://360info.org/how-consumers-can-influence-who-controls-ai/

https://lens.monash.edu/@technology/2024/09/05/1386962/how-consumers-can-influence-who-controls-ai

https://www.tatlerasia.com/gen-t/innovation/how-consumers-can-influence-who-controls-ai-360info

[39] https://www.nature.com/articles/s43588-023-00540-0

Bagaimana Undang-Undang Sektor Keuangan yang Baru Memperkuat Lanskap Keuangan Digital

Arif Perdana

Konteks: Artikel ini pertama kali dimuat di *The Conversation Indonesia*, 21 Desember 2023. Artikel ini merupakan refleksi atas diberlakukannya UU Sektor Keuangan yang baru. UU tersebut menetapkan aturan bagi lembaga keuangan untuk mengatur operasional mereka, mencegah praktik tidak etis, serta mendorong transparansi. Selain itu, regulasi ini membantu mengurangi risiko sistemik yang dapat mengguncang perekonomian. Pelindungan terhadap konsumen juga diperkuat melalui pengawasan yang lebih ketat, memastikan bahwa produk dan layanan keuangan aman dan adil. Secara keseluruhan, UU sektor keuangan berfungsi sebagai fondasi untuk menjaga integritas sistem keuangan dan mendukung pertumbuhan ekonomi yang berkelanjutan.

Pada era sekarang ini, kita merasakan begitu pesatnya pertumbuhan keuangan digital. Pertumbuhan pinjaman online kini telah melampaui pinjaman bank tradisional. Jumlah perusahaan teknologi finansial (tekfin) bertumbuh lebih dari dua kali lipat sepanjang lima tahun terakhir. Meski nilai transaksinya anjlok, jumlah investor kripto di Indonesia terus bertumbuh. Perkembangan ini perlu disikapi dengan sigap oleh pemerintah–tak hanya untuk meningkatkan potensi keuangan digital namun juga menghadapi risikonya. Pengesahan UU Pengembangan dan Penguatan Sektor Keuangan (UU P2SK) pada awal 2023 menandai babak baru dalam sejarah perekonomian Indonesia[40]. Menanggapi mendesaknya kebutuhan reformasi di bidang keuangan, UU P2SK menjadi contoh komitmen pemerintah untuk menjawab tantangan di era teknologi maju.

Transformasi Digital di Sektor Keuangan: Potensi dan Risiko

Salah satu aspek vital yang menjadi mandat dari UU P2SK yaitu pemanfaatan dan adaptasi terhadap inovasi teknologi dalam sektor keuangan. Ada dua sisi mata uang yang harus dipertimbangkan di sini. Di satu sisi, teknologi dapat mengubah cara kerja

[40] https://peraturan.bpk.go.id/Details/240203/uu-no-4-tahun-2023

sektor keuangan, meningkatkan efisiensi, dan inklusi. Di sisi lain, implementasi teknologi yang buruk dapat membuka pintu bagi kerugian besar dan risiko yang belum pernah dialami sebelumnya. Dalam konteks teknologi dan informasi yang serba pesat, sektor keuangan Indonesia harus mampu beradaptasi dan inovatif agar tetap relevan dan efisien. Tekfin, blockchain, dan AI adalah perangkat yang dapat merombak sektor keuangan, namun mereka juga membawa risiko.

Misalnya, terbatasnya akses terhadap data-data dari Direktorat Kependudukan dan Catatan Sipil (Ditjen Dukcapil) untuk memverifikasi data pengguna dan meminimalisasi penipuan membuat tekfin sulit berkembang. Regulasi spesifik yang memayungi inovasi-inovasi baru di tekfin yang seharusnya bisa dikeluarkan oleh Otoritas Jasa Keuangan (OJK) juga masih absen karena kurang memadainya sumber daya ahli di bidang ini.

Sementara itu, ancaman terhadap privasi dan keamanan data, penipuan investasi, serta risiko terkait dengan stabilitas dan integritas sistem keuangan, menjadi isu utama yang perlu dimitigasi. Bagaimana kita memilih untuk memanfaatkan teknologi ini, dan dalam lingkungan regulasi seperti apa mereka diterapkan, akan berdampak langsung pada keberhasilan upaya transformasi ini.

Peran OJK dan BI dalam Implementasi UU P2SK

Peran OJK selaku regulator industri keuangan dan Bank Indonesia (BI) sebagai bank sentral, menjadi semakin penting dengan adanya UU ini. Dengan wewenang yang diberikan oleh UU P2SK, mereka bertanggung jawab untuk mengarahkan transformasi digital di sektor keuangan Indonesia.

Peran OJK

UU P2SK meningkatkan kewenangan dan peran OJK dalam mengatur dan mengawasi berbagai sektor keuangan, termasuk industri yang relatif baru seperti tekfin dan transaksi aset digital. OJK kini memiliki ruang gerak yang lebih luas untuk melakukan pengawasan terintegrasi dan melindungi konsumen. Misalnya, aset digital yang merupakan bagian dari tekfin namun sebelumnya diawasi oleh Badan Pengawas

Perdagangan Berjangka Komoditi (BAPPEBTI), kini akan menjadi bidang kerja OJK. Hal ini memungkinkan pembentukan ekosistem yang mendukung pertumbuhan industri keuangan dengan penerapan teknologi canggih. Misalnya, dengan adanya regulasi yang jelas dan mutakhir, industri tekfin dan aset digital seperti uang kripto dan *non-fungible token* (NFT) akan memiliki panduan yang jelas tentang bagaimana mereka dapat beroperasi dan berkembang di Indonesia.

Ini juga akan menarik lebih banyak investasi ke sektor tersebut, karena investor selalu mencari kepastian hukum dan regulasi sebelum menginvestasikan dana mereka. Tanpa adanya regulasi yang jelas, risiko investasi akan semakin besar, dan tingkat kepercayaan menurun. Bagaimana OJK mengevaluasi teknologi dan inovasi keuangan, misalnya, dapat membuka pintu bagi inklusi keuangan yang lebih besar dan model bisnis baru serta memetakan risiko-risiko yang ada. Namun, mengingat kecepatan perkembangan industri tekfin dan digital, OJK perlu menjaga agar keterampilan dan pengetahuannya adaptif dengan inovasi terbaru. Jika tidak, ada risiko bahwa pengawasan dan regulasi tersebut dapat menjadi hambatan dan bukan akselerator bagi inovasi. OJK pun mesti memerhatikan pelindungan konsumen.

Peran BI

UU P2SK juga mempertegas peran BI untuk fokus pada kebijakan moneter (peredaran uang) dan stabilitas sistem keuangan secara makro, termasuk mengawasi dan mengatur risiko yang mungkin ditimbulkan oleh inovasi teknologi. Hal ini memastikan bahwa tidak ada tumpang tindih antara BI dan OJK meski, seperti yang dijelaskan oleh Pasal 217 UU P2SK, keduanya dapat berkoordinasi dalam rangka pengaturan, pengawasan, dan penyelenggaraan inovasi teknologi di sektor keuangan ketika dibutuhkan.

Wewenang yang Diberikan UU P2SK Memunculkan Tantangan Baru bagi BI.

Pertama, BI harus menyesuaikan kebijakan moneter untuk menangani penerbitan mata uang digital bank sentral (*Central Bank Digital Currency*/CBDC). Kedua, BI dihadapkan pada tugas mengatur dan menjaga kelancaran sistem pembayaran yang kini

bertransisi dari metode pembayaran tradisional menjadi digital–misalnya dengan hadirnya QRIS dan dompet digital lainnya. BI memantau dan mengatur teknologi baru di perbankan untuk memastikan kepatuhan terhadap standar keamanan dan stabilitas sistem pembayaran.

Ketiga, dengan bank semakin banyak menggunakan teknologi digital dalam operasional mereka, BI perlu memutakhirkan regulasi dan mekanisme pengawasan termasuk memastikan perbankan memiliki tata kelola data dan teknologi yang baik. Dengan kata lain, UU P2SK memerlukan BI untuk beradaptasi dengan perkembangan teknologi dalam sektor keuangan, memperbarui regulasi dan pengawasan, dan menjaga stabilitas sistem keuangan serta melindungi hak konsumen dalam lingkungan yang semakin digital. Tabel 4 meringkas peran BI dan OJK sesuai dengan UUP2SK yang baru.

Tabel 4. Peran BI dan OJK

Aspek	Peran BI	Peran OJK
Fokus Utama	Fokus pada kebijakan moneter dan stabilitas sistem keuangan secara makro.	Mengatur dan mengawasi berbagai sektor keuangan, termasuk tekfin dan aset digital.
Ruang Lingkup Pengawasan	Mengatur risiko sistem keuangan terkait inovasi teknologi dan menjaga stabilitas sistem pembayaran.	Pengawasan terintegrasi di berbagai sektor keuangan dan aset digital, termasuk kripto dan NFT.
Pengaturan Teknologi Finansial	Mengatur sistem pembayaran digital (misalnya QRIS) dan memantau teknologi baru di sektor perbankan.	Memastikan regulasi tekfin dan aset digital mutakhir, melindungi konsumen, dan memfasilitasi inklusi keuangan.
Pengembangan Kebijakan	Menyesuaikan kebijakan moneter untuk penerbitan CBDC dan mengadaptasi regulasi sesuai perkembangan teknologi.	Membuka ruang untuk model bisnis baru dan investasi di sektor keuangan melalui kepastian regulasi.
Inovasi dan Risiko	Mengatur teknologi digital di perbankan untuk menjaga kepatuhan terhadap standar keamanan dan stabilitas.	Mengevaluasi teknologi dan inovasi untuk memetakan risiko dan peluang di sektor keuangan.

Aspek	Peran BI	Peran OJK
Keterampilan dan Pengetahuan	Memperbarui regulasi dan mekanisme pengawasan agar sesuai dengan perkembangan teknologi di sektor keuangan.	Memastikan kemampuan adaptif terhadap inovasi terbaru untuk mencegah regulasi menjadi hambatan inovasi.
Pelindungan Konsumen	Menjaga hak konsumen di tengah transisi sistem pembayaran tradisional ke digital.	Mengawasi pelindungan konsumen secara ketat dalam pengembangan sektor keuangan digital.
Koordinasi dengan Pihak Lain	Berkoordinasi dengan OJK dalam memastikan stabilitas sistem keuangan dan inovasi teknologi di sektor keuangan.	Berkoordinasi dengan BI dalam pengaturan dan pengawasan teknologi keuangan bila diperlukan.

Melihat ke Depan: Peluang, Tantangan, dan Kunci Keberhasilan

Mengawasi dan mengatur teknologi baru ini akan memerlukan pemahaman dan pengetahuan yang dalam. Kedua lembaga ini harus berinvestasi dalam membangun dan memperkuat kapasitas mereka sendiri, serta memastikan bahwa mereka memiliki keterampilan dan alat yang tepat untuk memahami dan mengatur teknologi baru ini. Hal ini mencakup investasi di bidang sumber daya manusia yang memahami kemampuan analitis, strategis, taktis, dan teknis. Begitu pula investasi di bidang teknologi untuk membantu lembaga keuangan memastikan regulasi ditaati oleh pelaku industri keuangan. Ini bukanlah tugas yang mudah, namun penting untuk keberhasilan jangka panjang reformasi sektor keuangan.

Meski tantangannya besar, UU P2SK juga membuka pintu bagi peluang dan kesempatan baru. Penggunaan AI, misalnya, dapat meningkatkan efisiensi dan akurasi dalam pengawasan dan pengaturan, membuka pintu bagi analisis data yang lebih kompleks, dan akurat, serta pengambilan keputusan yang lebih baik. Blockchain, di sisi lain, dapat meningkatkan transparansi dan efisiensi dalam berbagai proses keuangan, seperti transfer dana dan penyelesaian transaksi. Kemampuan meningkatkan kapasitas dalam bidang keamanan siber juga bisa membantu melindungi sektor keuangan dari serangan siber dan ancaman lainnya.

Dengan UU P2SK, Indonesia memiliki peluang dalam pengembangan dan penerapan teknologi baru dalam sektor keuangan–menyeimbangkan pelindungan konsumen dengan inovasi. Namun perlu menjadi catatan bahwa perluasan wewenang yang diberikan oleh UU P2SK juga bisa memicu risiko penyalahgunaan kekuasaan. Ini dikarenakan UU ini meningkatkan peran dan kekuasaan Komite Stabilitas Sistem Keuangan (KSSK)–yang beranggotakan Menteri Keuangan, Gubernur Bank Indonesia, Ketua Dewan Komisioner OJK, dan Ketua Dewan Komisioner Lembaga Penjamin Simpanan (LPS)-dalam pengambilan keputusan keuangan. Hal ini berpotensi mengurangi kewenangan dan independensi institusi keuangan lain.

Pengawasan independen perlu ditingkatkan dan partisipasi masyarakat dalam pengambilan keputusan harus diperkuat. Semua langkah ini akan membantu memastikan bahwa kekuatan baru yang diberikan oleh UU P2SK digunakan dengan bijaksana dan bertanggung jawab. Pendekatan yang seimbang, yang mempertimbangkan baik peluang maupun risiko, serta mempertimbangkan faktor etika dan sosial, menjadi kunci keberhasilan implementasi UU P2SK dalam menjamin inklusivitas, kedalaman, dan stabilitas di sektor keuangan.

Tautan artikel:

https://theconversation.com/bagaimana-undang-undang-sektor-keuangan-yang-baru-memperkuat-lanskap-keuangan-digital-219317

Mencari Solusi untuk Masalah Pelindungan Data di Indonesia

Arif Perdana, Saru Arifin

Konteks: Artikel ini saya tulis bersama dengan rekan dari Universitas Negeri Semarang, pertama kali diterbitkan di 360info.org di tanggal 13 Desember 2023. Setelah itu, artikel ini juga direplikasi oleh The Diplomat, Tempo Berbahasa Inggris, dan Monash Lens Australia. Dalam tulisan ini, kami menyoroti kemajuan penting yang telah dicapai Indonesia dengan pengesahan UU No. 27 Tahun 2022 tentang PDP. Namun, kami juga menekankan bahwa tantangan dalam implementasi UU ini harus ditangani dengan hati-hati agar tujuan dari UU ini dapat tercapai secara optimal, terutama dalam menjaga keseimbangan antara keamanan data dan inovasi teknologi.

Meningkatnya insiden pelanggaran data di sektor pemerintah dan swasta di Indonesia menggarisbawahi kebutuhan mendesak mengenai protokol pelindungan data yang ketat. Pada tahun 2022, lebih dari 21.000 perusahaan di Indonesia mengalami pelanggaran data. Insiden ini mempengaruhi sektor-sektor penting, termasuk kesehatan, keuangan, e-commerce, dan utilitas, serta memperlihatkan tantangan besar dalam keamanan siber bagi operasional bisnis di Indonesia.

Salah satu insiden penting terjadi di sektor kesehatan, di mana terjadi pelanggaran keamanan signifikan karena akses tidak sah ke sistem kartu kewaspadaan kesehatan elektronik (e-HAC) dan Badan Penyelenggara Jaminan Sosial Kesehatan (BPJS). Selain pelanggaran data, potensi penyalahgunaan data oleh pemerintah untuk pengawasan dan risiko yang ditimbulkannya terhadap privasi menjadi masalah serius. Kekhawatiran utama adalah penggunaan data untuk tujuan ilegal atau tidak etis, seperti menekan oposisi politik yang sah atau menargetkan komunitas yang rentan. Tabel 5 memberikan ringkasan mengenai solusi yang bisa dilakukan untuk mengatasi pelindungan data pribadi di Indonesia

Tabel 5. Solusi masalah pelindungan data pribadi di Indonesia

Solusi	Deskripsi
Reformasi Hukum dan Penegakan	Penerapan UU PDP yang memberikan hak bagi individu untuk menuntut pemroses data yang melanggar dan pembentukan PDPA untuk mengawasi kebijakan dan pelindungan data.
Penyesuaian dengan Standar Internasional	Menyamakan kebijakan dengan regulasi internasional seperti GDPR dan menerapkan pendekatan berbasis risiko dalam pengaturan pelindungan data.
Pengawasan Pemerintah yang Transparan	Mendirikan badan pengawas independen untuk memantau aktivitas pengawasan pemerintah dan memastikan transparansi dalam kegiatan pengawasan.
Partisipasi Masyarakat dan Kesadaran Publik	Meningkatkan pendidikan tentang hak digital melalui kampanye kesadaran, serta melibatkan masyarakat sipil dan media untuk memantau dan memperjuangkan hak privasi.
Teknologi untuk Meningkatkan Privasi	Menggunakan teknologi privasi seperti enkripsi, otentikasi multi-faktor, dan alat anonimisasi, serta memperkuat keamanan siber dengan firewall dan pembaruan perangkat lunak.
Prinsip Minimalisasi Data	Menerapkan prinsip minimalisasi data dengan hanya mengumpulkan dan menyimpan data yang diperlukan untuk jangka waktu yang relevan.
Kolaborasi Internasional	Berpartisipasi dalam dialog dan forum internasional untuk menyelaraskan kebijakan dengan praktik terbaik dari negara lain.
Peran Perusahaan Teknologi	Perusahaan harus mematuhi praktik pelindungan data yang etis, menolak permintaan data yang tidak adil, dan bekerja sama dengan masyarakat sipil untuk mendukung privasi.

Kekhawatirannya bukan hanya soal kehilangan privasi, tetapi juga bahaya yang muncul ketika pemerintah yang kuat mengendalikan data pengawasan dalam jumlah besar, yang dapat berujung pada penyalahgunaan kekuasaan dan pengikisan kebebasan individu. Mengatasi risiko pelanggaran data dan penyalahgunaan pengawasan oleh pemerintah membutuhkan pendekatan seimbang yang menghormati keamanan nasional dan privasi individu. Ini berarti diperlukan reformasi hukum, kewaspadaan masyarakat, teknologi yang berfokus pada privasi, penyesuaian dengan standar internasional, serta mempromosikan praktik etis di pemerintahan dan perusahaan teknologi.

Partisipasi aktif dari masyarakat sipil, media, dan perusahaan teknologi sangat penting. Dengan menerapkan langkah-langkah ini, Indonesia dapat membangun kerangka pengawasan yang lebih transparan dan akuntabel, yang lebih menghormati privasi individu. UU PDP atau UU No. 27 Tahun 2022 (UU PDP), merupakan kemajuan signifikan dalam hal ini. Namun, masih ada ketidakpastian terkait pelaksanaannya, terutama terkait klasifikasi hukum pelanggaran data.

Meskipun demikian, UU ini memberikan ketentuan umum yang menyatakan bahwa individu yang datanya telah dilanggar berhak untuk mengambil tindakan hukum terhadap pemroses data dan menuntut kompensasi. Belum jelas apakah UU ini sejalan dengan *pendekatan* GDPR Uni Eropa, yang lebih bersifat perdata dan memungkinkan individu untuk menegaskan hak mereka di pengadilan perdata. GDPR, yang berlaku sejak Mei 2018, merupakan UU privasi data yang komprehensif dan memiliki dampak signifikan di seluruh dunia. GDPR menetapkan persyaratan ketat dan mengancam hukuman berat bagi pelanggarannya.

UU PDP belum sebanding dengan GDPR dalam hal sanksi untuk pemrosesan data yang secara sengaja melanggar hukum dan kegagalan untuk mematuhi arahan dari otoritas pengawas. Aspek-aspek ini memerlukan kejelasan lebih lanjut untuk menilai efektivitas dan cakupan keseluruhan UU tersebut. Selain itu, UU PDP juga menyoroti kekhawatiran terkait praktikalitas penerapan otoritas yang diperlukan (yaitu Otoritas Pelindungan Data Pribadi/PDPA), dengan gagasan pengawasan intensif pemerintah dan prioritas utamanya. PDPA akan dibentuk di dalam kantor presiden dan melapor langsung kepada presiden. Menurut interpretasi ini, presiden memiliki kewenangan untuk menghalangi tanggung jawab PDPA dalam menjalankan fungsinya demi kepentingan kesejahteraan publik.

Namun, keraguan ini dapat dihilangkan dengan mempertimbangkan otoritas terbatas yang diberikan kepada PDPA. Otoritas ini mencakup perumusan kebijakan penting untuk meningkatkan PDP, pengawasan terhadap praktik PDP, penerapan peraturan administratif, serta fasilitasi mekanisme penyelesaian sengketa alternatif. Dengan demikian, PDPA lebih banyak memiliki otoritas administratif, yang diperkuat oleh

kompetensi penegakan hukumnya. Jelas bahwa otoritas ini tidak sekuat dan seluas otoritas PDP yang independen dan tangguh seperti yang didirikan oleh GDPR.

Penerapan dan penegakan UU privasi yang kuat seperti GDPR sangat penting di Indonesia, sehingga belajar dari pengalaman GDPR menjadi penting. Penting untuk dipahami bahwa UU PDP bisa sangat rumit dan dapat membawa dampak positif maupun negatif terhadap inovasi. Fleksibilitas hukum sangat penting, seperti mengadopsi pendekatan berbasis risiko yang menyesuaikan teknik PDP sesuai dengan tingkat risiko, mulai dari minimal hingga tidak dapat diterima. Fleksibilitas ini juga mencakup pengakuan terhadap kepentingan yang sah yang memungkinkan organisasi untuk memproses data pribadi tanpa memperoleh persetujuan eksplisit, asalkan mereka memiliki alasan bisnis yang valid yang melampaui hak privasi individu.

Selain itu, pengecualian untuk pemrosesan “statistik”, yang memungkinkan pertumbuhan big data dan AI, juga sangat penting. Namun, penggunaan label sensitif memerlukan justifikasi yang ketat, karena pemrosesan tersebut harus benar-benar diperlukan untuk kepentingan publik yang signifikan, bukan hanya untuk kepentingan yang sempit. Lebih lanjut, UU ini penting dalam menetapkan batas-batas pengawasan pemerintah.

Pembentukan badan pengawas independen diperlukan untuk melengkapi UU ini guna memantau aktivitas pengawasan pemerintah. Tanpa badan pengawas independen, ada risiko pengawasan pemerintah yang tidak terkendali dan tidak akuntabel. Selain itu, kurangnya transparansi membuat publik tidak mengetahui motif dan hasil pengawasan, yang berpotensi mengikis kepercayaan terhadap tindakan pemerintah. Akibatnya, inisiatif pengawasan dapat menghadapi skeptisisme dan penolakan yang lebih besar dari masyarakat.

Mencegah pelanggaran data dan mengurangi risiko penyalahgunaan data juga memerlukan keterlibatan masyarakat. Mendidik warga tentang hak digital mereka sangat penting. Kampanye kesadaran publik dapat secara efektif menyampaikan sejauh mana hak-hak ini dan melindungi privasi. Selain itu, pembentukan kelompok pengawas pengawasan berbasis komunitas dapat menjadi penghubung penting antara publik dan pemerintah, dengan memantau dan melaporkan potensi penyalahgunaan. Yang tidak

kalah penting adalah perlindungan yang kuat bagi pelapor pelanggaran (whistleblowers) yang mengungkap praktik pengawasan yang ilegal atau tidak etis, karena ini mendorong akuntabilitas internal dalam badan pemerintah.

Peran masyarakat sipil dan media sangat penting dalam konteks ini. Organisasi non-pemerintah dan kelompok masyarakat sipil berperan penting dalam memantau tindakan pemerintah dan memperjuangkan hak-hak warga negara. Media yang bebas dan independen sangat penting untuk mengungkap penyalahgunaan kekuasaan pengawasan dan meminta pertanggungjawaban pemerintah. Protes publik dan kampanye advokasi dapat secara efektif mendorong perubahan kebijakan dan meningkatkan akuntabilitas.

Teknologi juga menawarkan solusi untuk meningkatkan privasi. Mempromosikan teknologi yang meningkatkan privasi, seperti enkripsi dan alat anonimisasi, dapat melindungi komunikasi dan data individu. Teknologi lain yang dapat berperan penting dalam mencegah pelanggaran data termasuk otentikasi multi-faktor, sistem firewall untuk memblokir intrusi yang tidak sah, sistem deteksi intrusi untuk memantau lalu lintas jaringan, solusi penyimpanan cloud yang aman, serta pembaruan perangkat lunak secara teratur untuk mengatasi kerentanan keamanan.

Secara kolektif, alat-alat ini meningkatkan keamanan siber dan mengurangi risiko akses data yang tidak sah. Selain itu, lembaga pemerintah harus didorong atau diwajibkan untuk mematuhi prinsip minimalisasi data, hanya mengumpulkan data yang diperlukan untuk tujuan yang jelas dan menyimpan data tidak lebih lama dari yang diperlukan.

Kolaborasi internasional dan keselarasan dengan standar global juga sangat penting. Indonesia harus menyelaraskan UU pengawasannya dengan standar hak asasi manusia internasional, seperti yang ditetapkan oleh Deklarasi Universal Hak Asasi Manusia (UDHR) dan Kovenan Internasional tentang Hak Sipil dan Politik (ICCPR). Partisipasi dalam dialog internasional (dengan badan-badan PBB, forum regional, keterlibatan bilateral, dan konferensi serta pertemuan internasional yang relevan) dapat memberikan kesempatan untuk belajar dari pengalaman dan tantangan negara lain.

Perusahaan teknologi dan pengendali data juga memiliki tanggung jawab dalam hal ini. Perusahaan yang menangani sejumlah besar data harus mematuhi praktik etis dan menolak permintaan pemerintah yang tidak adil terkait data. Perusahaan juga dapat bekerja sama dengan masyarakat sipil untuk mengembangkan dan mempromosikan alat yang melindungi privasi individu.

Tautan artikel:

https://360info.org/finding-a-fix-for-indonesias-data-protection-problems/

https://thediplomat.com/2023/12/finding-a-fix-for-indonesias-data-protection-problems/

https://en.tempo.co/read/1807865/data-breach-finding-a-fix-for-indonesias-data-protection-problems

Menatap Masa Depan Regulasi AI

Arif Perdana

Konteks: Artikel ini ditulis untuk 360info.org di tanggal 2 Agustus 2023. Pada saat itu Uni Eropa masih dalam tahap mengusulkan UU mengenai AI. Pendekatan Uni Eropa ini dianggap sebagai langkah besar yang berpotensi mengubah lanskap regulasi teknologi tidak hanya di Eropa, tetapi juga di seluruh dunia. Di artikel ini, penulis menggarisbawahi pentingnya regulasi yang mampu beradaptasi dengan perkembangan teknologi yang cepat. Regulasi seperti ini dapat membuka jalan bagi negara-negara untuk terus berinovasi tanpa mengorbankan aspek keamanan dan akuntabilitas. Di sisi lain, memperkenalkan UU baru membutuhkan waktu dan proses yang panjang, seperti yang pernah dialami Indonesia dengan UU PDP. Sambil menunggu formulasi dan penetapan UU AI yang baru, negara-negara dapat memanfaatkan UU yang sudah ada di bidang teknologi secara strategis. Hal ini tidak hanya mempercepat pengaturan sementara, tetapi juga memberikan ruang bagi pengembangan regulasi yang lebih matang dan kontekstual di masa mendatang.

UU AI yang diusulkan oleh Uni Eropa akan menjadi perubahan besar ketika diberlakukan. UU ini akan mengatur teknologi yang sedang berkembang di seluruh Eropa dan bahkan lebih luas lagi. Namun, seiring dengan semakin jelasnya rincian UU tersebut, semakin terlihat pula tantangan-tantangan yang mungkin menghambat potensinya untuk tercapai secara maksimal. Legislasi ini mengklasifikasikan sistem AI berdasarkan tingkat risiko (tidak dapat diterima, tinggi, terbatas, dan minimal), kemudian menetapkan protokol bagi pengembang, penyedia, dan pengguna untuk memastikan transparansi, akuntabilitas, keadilan, dan keandalan. Sementara negara-negara seperti China sudah memiliki UU khusus AI, usulan Uni Eropa mungkin merupakan regulasi yang paling jelas terdefinisi dan menyeluruh hingga saat ini. Regulasi ini meningkatkan standar tanggung jawab, menyediakan pelindungan bagi pengguna, dan menekankan prinsip-prinsip hak asasi manusia.

UU AI yang diusulkan oleh Uni Eropa ini harus diakui memang rumit, yang mungkin menimbulkan kendala saat diterapkan. Kewajiban berat bagi pengembang dan pengguna mungkin dirancang dengan tujuan keselamatan, tetapi juga bisa memperlambat kemajuan teknologi dan mungkin tidak mencakup semua risiko yang terkait dengan AI. Keberhasilan UU ini bergantung pada kemampuannya untuk beradaptasi dengan

kemajuan teknologi dan menemukan keseimbangan antara regulasi yang kuat dan mempromosikan inovasi. Jika dikelola dengan hati-hati, hal ini bisa tercapai. Meskipun UU AI merupakan proposal yang mungkin mengubah lanskap teknologi di Eropa, kemampuannya untuk diterapkan di tempat lain boleh jadi menjanjikan sekaligus menantang.

Negara seperti Indonesia memiliki seperangkat UU yang mapan mengenai teknologi digital. Dalam hal ini, kebijakan AI bisa disesuaikan, namun mungkin memerlukan beberapa reformasi yang signifikan untuk mencapainya. Perusahaan Indonesia yang memiliki afiliasi atau berpartisipasi dalam kegiatan bisnis dengan entitas dari Uni Eropa akan diwajibkan untuk mematuhi peraturan ini. Hal ini mencakup pemrosesan data yang melibatkan individu yang merupakan warga negara atau penduduk Uni Eropa, yang secara tidak langsung akan mengaktifkan regulasi ini di Indonesia.

Tantangannya adalah mengimplementasikan UU AI Uni Eropa dengan mempertimbangkan faktor-faktor lokal Indonesia untuk menciptakan sesuatu yang dapat bekerja dalam konteks yang sesuai. Indonesia adalah negara besar dengan populasi yang beragam dan tersebar luas. Oleh karena itu sangat penting untuk memastikan bahwa kelompok-kelompok ini diajak berdialog sehingga pendekatan AI Indonesia dapat menempatkan UU yang diusulkan oleh Uni Eropa dalam konteks kondisi spesifik Indonesia.

Perubahan sering kali bergerak lambat dan rumit. Ketika Indonesia mencoba memberlakukan UU pelindungan data pada tahun 2022, butuh satu dekade untuk membawa gagasan itu dari konsep hingga menjadi kenyataan hukum. Kemudian, diikuti oleh masa transisi dua tahun untuk memungkinkan pengembangan infrastruktur penegakan hukum yang diperlukan.

Regulator AI bisa mengambil pelajaran berharga dari bidang keamanan siber yang secara efektif berhasil menavigasi kemajuan pesat. Sebuah tolok ukur (standarisasi internasional-ISO 27001:2015 *Information Security Management Systems*) yang diakui secara global untuk bidang ini diperkenalkan pada tahun 2015 dan terus diiterasi dan

diperbaiki[41]. Tolok ukur ini sejak saat itu diintegrasikan secara luas di industri-industri yang rentan terhadap serangan siber, seperti sektor keuangan. Adopsinya menunjukkan nilai dari regulasi yang dirancang khusus untuk sektor yang diaturnya, sesuatu yang dapat ditiru oleh regulasi dan tata kelola AI. Tolok ukur global untuk AI akan memungkinkan bidang ini bersandar pada dasar hukum yang telah mapan.

Di Indonesia, sudah ada UU dan panduan untuk mengatur berbagai upaya digital yang dapat digunakan untuk memperkuat penegakan norma-norma AI yang baru (UU Informasi dan Transaksi Elektronik[42], UU PDP[43], dan Peraturan Pemerintah Nomor 71 Tahun 2019 [44]). Kunci dari hal ini adalah membingkai regulasi AI sedemikian rupa sehingga mencakup peraturan yang sudah ada, seperti yang mencakup sistem elektronik dan transaksi, akses informasi, privasi data, dan manajemen risiko.

Saat para pembuat UU mencoba mengambil langkah-langkah awal yang berarti dalam mengatur AI, sangat berharga untuk memiliki ketentuan yang sudah ada guna mengisi kekosongan sementara. Menerapkan UU AI yang komprehensif di Indonesia lebih dari sekadar kebutuhan; ini adalah tugas berat yang membutuhkan strategi yang beragam dan mendalam. Dengan memanfaatkan ketentuan hukum yang sudah ada, Indonesia dapat menjamin kemajuan yang lebih mulus dan teratur menuju regulasi AI yang kuat. Meskipun ini merupakan tantangan besar, kebutuhan untuk membentuk struktur regulasi yang kokoh bagi AI membenarkan upaya yang besar tersebut.

Tautan artikel:

https://360info.org/going-back-to-the-future-for-ai-regulation/

[41] https://enhancequality.com/standards/iso-270012015-information-security-management-systems/
[42] https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024
[43] https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022
[44] https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019

BAB 2: Mengamankan Masa Depan Digital dengan Strategi Siber dan Tata Kelola Data

Di era digital yang semakin kompleks, keamanan siber dan tata kelola data menjadi pondasi krusial bagi Indonesia untuk mengamankan masa depan digitalnya. Berbagai insiden kebocoran data dan serangan siber yang terjadi belakangan ini, mulai dari peretasan PDN-S hingga kebocoran data BPJS dan Kepolisian. Kejadian-kejadian ini menyoroti kerentanan infrastruktur digital negara. Peristiwa-peristiwa ini bukan hanya mengancam privasi warga negara, tetapi juga berpotensi mengganggu stabilitas ekonomi dan keamanan nasional.

Untuk menghadapi tantangan ini, diperlukan pendekatan holistik yang melibatkan aspek teknologi, proses, dan sumber daya manusia. Implementasi kerangka keamanan siber yang komprehensif menjadi langkah awal yang kritis. Ini mencakup pengembangan Rencana Respons Insiden (IRP), Pemulihan Bencana (DCP), dan Kelangsungan Bisnis (BCP) yang efektif. Paralel dengan itu, pengembangan PDN yang terintegrasi namun dilengkapi dengan protokol keamanan berlapis menjadi prioritas untuk menjamin kedaulatan dan keamanan data nasional. Penguatan aspek regulasi, terutama melalui implementasi dan penegakan konsisten UU PDP, menjadi landasan hukum yang diperlukan. Namun, regulasi saja tidaklah cukup. Peningkatan kesadaran dan pelatihan keamanan siber bagi seluruh lapisan masyarakat dan aparatur pemerintah menjadi kunci untuk membangun "pertahanan manusia" yang tangguh terhadap ancaman siber.

Mengingat sifat transnasional dari ancaman siber, kolaborasi antarlembaga dan internasional dalam berbagi informasi ancaman menjadi sangat penting. Ini harus didukung dengan investasi berkelanjutan dalam teknologi keamanan canggih dan pengembangan talenta di bidang keamanan siber. Tak kalah pentingnya adalah penerapan tata kelola data yang ketat di seluruh siklus hidup data, mulai dari pengumpulan hingga pemusnahan. Dengan menerapkan strategi-strategi ini secara konsisten, Indonesia dapat membangun ketahanan digital yang kuat, melindungi kedaulatan data nasional, dan memastikan kepercayaan publik terhadap transformasi

digital pemerintah dan ekonomi. Keberhasilan dalam mengamankan ruang siber dan mengelola data dengan baik akan menjadi landasan penting bagi kemajuan Indonesia di era digital, membuka jalan bagi inovasi, pertumbuhan ekonomi, dan peningkatan kualitas layanan publik yang signifikan.

Tiga Pilar Utama Membangun Arsitektur Keamanan Digital yang Tangguh

Arif Perdana, Bayu Anggorojati, Muhammad Erza Aminanto

Konteks: Artikel ini diterbitkan oleh The Conversation Indonesia sebagai bagian dari seri tulisan tentang keamanan siber. Bersama dengan kolega dari program studi keamanan siber, Monash University, di tulisan kedua ini kami memaparkan bahwa ancaman siber yang semakin kompleks memerlukan pendekatan holistik untuk membangun ketahanan siber nasional. Terdapat tiga pilar utama yang harus diperkuat, yaitu: infrastruktur, sumber daya manusia, dan regulasi. Infrastruktur keamanan siber di Indonesia masih lemah, terutama karena keterbatasan anggaran dan teknologi yang ketinggalan zaman. Sumber daya manusia juga menjadi tantangan, dengan kekurangan tenaga ahli keamanan siber dan rendahnya literasi digital masyarakat. Regulasi yang ada belum sepenuhnya mampu menghadapi ancaman modern, sehingga diperlukan kerangka hukum yang lebih komprehensif dan kolaborasi antar lembaga.

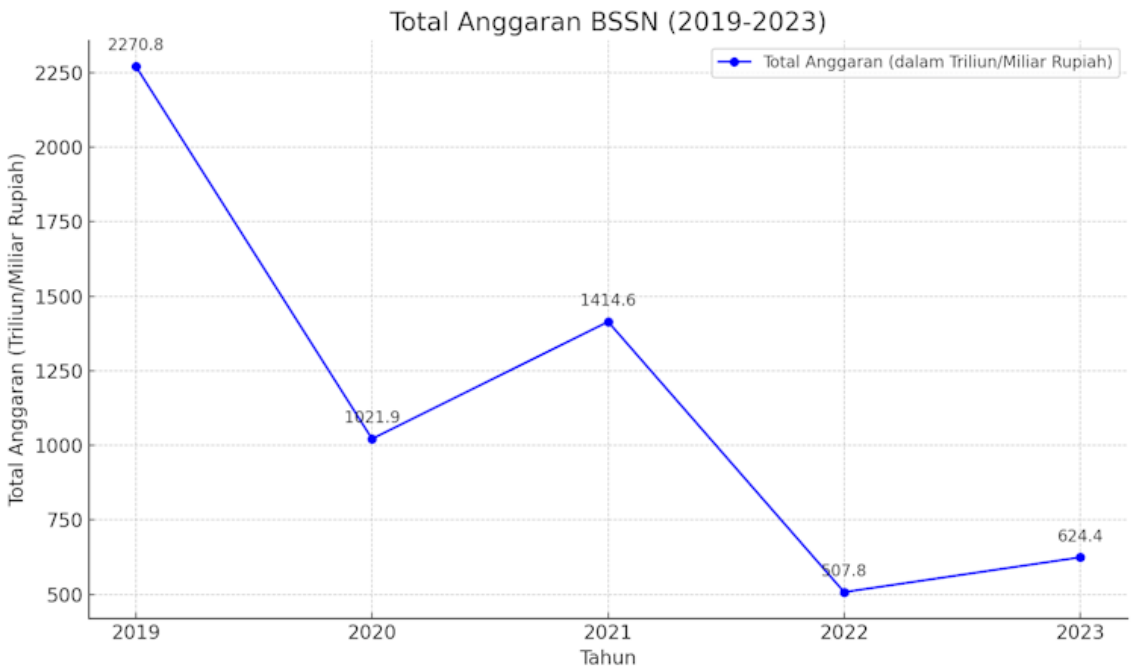
Berbagai ancaman siber yang terjadi belakangan, mulai dari peretasan data hingga serangan terhadap infrastruktur kritis, telah menjadi tantangan serius bagi keamanan nasional. Situasi ini seharusnya menjadi momentum refleksi untuk melakukan perbaikan di masa mendatang. Berdasarkan analisis kami, ada tiga pilar utama yang harus diperkuat untuk membangun ketahanan siber nasional, yakni: infrastruktur, sumber daya manusia, dan regulasi.

Infrastruktur

Salah satu masalah mendasar dalam lanskap keamanan siber Indonesia adalah infrastruktur yang masih lemah. Mayoritas teknologi yang digunakan oleh lembaga pemerintah dan badan publik belum mampu menghadapi berbagai ancaman siber yang semakin canggih. Hal ini terbukti dari beberapa insiden peretasan, seperti serangan terhadap PDN yang mengakibatkan gangguan di 239 instansi, di mana 186 di antaranya adalah instansi pemerintah. Insiden ini menunjukkan bahwa banyak instansi belum menerapkan standar keamanan internasional seperti ISO/IEC 27001 dan tidak memiliki

rencana pemulihan yang efektif dalam menghadapi serangan. Dalam hal ini, masalah anggaran menjadi salah satu hambatan utama. Alokasi anggaran untuk keamanan siber Indonesia seringkali tidak sebanding dengan skala ancaman yang ada. Misalnya, anggaran Badan Siber dan Sandi Negara (BSSN) terus menurun sejak 2019, padahal ancaman siber semakin kompleks dan masif (lihat Gambar 3).

Investasi dalam teknologi canggih seperti sistem deteksi ancaman berbasis kecerdasan buatan atau platform analisis ancaman juga masih terbatas. Pada akhirnya, banyak institusi mengandalkan solusi keamanan yang sudah ketinggalan zaman. Situasi ini menciptakan lingkaran setan: keterbatasan anggaran memperlambat pengembangan infrastruktur, yang pada akhirnya melemahkan ekosistem keamanan digital.



Gambar 3. Grafik total anggaran BSSN dari tahun 2019 hingga 2023, lengkap dengan label jumlah di setiap titik tahun. Angka-angka ini mencerminkan total anggaran dalam triliun dan miliar rupiah untuk setiap tahunnya. Sumber: Kompas.com, diolah penulis.

Sumber Daya Manusia

Selain infrastruktur, Indonesia juga mengalami kekurangan tenaga ahli keamanan siber yang kompeten. Pada 2019, Indonesia kekurangan 18.000 tenaga ahli keamanan

siber dan sandi. Masalah ini diperburuk oleh minimnya program studi khusus dan kekurangan tenaga pengajar di bidang ini. Secara umum, kesadaran dan literasi digital masyarakat Indonesia juga masih sangat rendah. Banyak pengguna internet belum memahami risiko siber dan cara melindungi diri dari serangan siber seperti phishing, yaitu penipuan online yang memanipulasi korban untuk memberikan informasi pribadi. Pada 2023, sektor *e-commerce* dan ritel menjadi target utama serangan phishing. Angkanya mencapai 25,55% dari total serangan.

Di tingkat organisasi, kurangnya pemahaman tentang pentingnya keamanan siber membuat banyak pengambil keputusan masih menganggap keamanan siber sebagai "beban biaya tambahan" daripada investasi strategis untuk melindungi aset digital. Akibatnya, alokasi anggaran untuk memperkuat keamanan siber rendah, baik di sektor publik maupun swasta. Imbasnya, banyak insiden kebocoran data yang terjadi. Upaya edukasi yang dilakukan pemerintah, seperti kampanye kesadaran publik yang dilakukan oleh BSSN, tampaknya belum mampu menciptakan perubahan perilaku signifikan dalam praktik keamanan siber sehari-hari.

Regulasi

Regulasi keamanan siber di Indonesia saat ini masih belum cukup untuk menangani ancaman yang semakin kompleks. Indonesia memang sudah memiliki beberapa instrumen hukum seperti Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, namun regulasi-regulasi yang ada ini masih sangat terbatas dalam aspek teknis perlindungan keamanan siber.

Pemerintah mengambil langkah signifikan dengan menerbitkan Peraturan Presiden No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, yang berupaya membangun kerangka keamanan siber nasional. Namun, karena implementasinya masih dalam tahap awal, efektivitas regulasi ini perlu dievaluasi secara berkala untuk memastikan relevansinya dengan dinamika ancaman yang terus berkembang. Secara keseluruhan, regulasi yang ada belum dapat dianggap sebagai

kerangka hukum yang komprehensif untuk menangani kompleksitas ancaman siber modern.

Kesimpulannya, tantangan keamanan siber di Indonesia memerlukan respons yang holistik dan berkelanjutan. Mengatasi keterbatasan infrastruktur dan sumber daya, meningkatkan kesadaran dan pendidikan publik, serta mengantisipasi ancaman baru dari teknologi yang berkembang pesat merupakan langkah-langkah esensial dalam membangun ketahanan siber nasional. Hanya dengan pendekatan yang komprehensif dan kolaboratif, Indonesia dapat berharap untuk tidak hanya bertahan, tetapi juga berkembang dalam lanskap digital yang semakin kompleks dan penuh risiko.

Rekomendasi

Pemerintah perlu memastikan bahwa strategi keamanan siber didukung oleh kebijakan yang fleksibel dan responsif terhadap perkembangan teknologi. Kami merekomendasikan perbaikan dimulai dari memperkuat tiga pilar utama keamanan siber: infrastruktur, sumber daya manusia, dan regulasi.

Pertama, investasi dalam penguatan infrastruktur keamanan siber harus diprioritaskan. Analoginya, jika kita ingin melindungi rumah dari pencuri—hal pertama yang dilakukan adalah memperkuat pintu dan jendela, bukan? Begitu pula dengan keamanan siber. Rekomendasi utama untuk melakukan ini adalah melalui pembangunan dan peningkatan Pusat Operasi Keamanan atau *Security Operations Center* (SOC) di tingkat nasional dan sektoral. Mengingat canggihnya ancaman saat ini, maka SOC harus dilengkapi dengan sistem deteksi ancaman berbasis kecerdasan buatan dan memiliki jaringan sensor nasional yang terintegrasi untuk memantau lalu lintas data secara real-time. Selain itu, modernisasi infrastruktur kriptografi nasional juga penting untuk melindungi data sensitif pemerintah. Kriptografi berfungsi seperti pengunci brankas; semakin kuat kunci, semakin aman isinya. Teknologi seperti blockchain juga patut dipertimbangkan untuk memastikan keamanan data.

Kedua, pengembangan sumber daya manusia dan literasi harus menjadi prioritas utama. Kampanye kesadaran siber harus dilakukan secara nasional, dan keamanan siber perlu diajarkan sejak dini di sekolah. Program sertifikasi keamanan siber nasional yang

diakui oleh industri, seperti sertifikasi dari *CompTIA*, *Information Systems Audit and Control Association* (ISACA), atau *ISC2: Cybersecurity Certifications and Continuing Education* perlu diperluas untuk meningkatkan kompetensi profesional. Pemerintah juga perlu menyediakan beasiswa khusus untuk studi keamanan siber dengan skema ikatan dinas untuk meningkatkan jumlah tenaga ahli di bidang ini.

Ketiga, regulasi yang kuat diperlukan untuk mendukung ketahanan siber nasional. Indonesia memerlukan undang-undang keamanan siber yang komprehensif sebagai landasan hukum untuk menghadapi ancaman modern. Saat ini tengah digodok Rancangan Undang-undang Keamanan dan Ketahanan Siber atau RUU KKS yang mengatur berbagai aspek penyelenggaraan keamanan dan ketahanan siber, termasuk tanggung jawab negara, pemerintah pusat, pemerintah daerah, serta partisipasi masyarakat dalam menjaga keamanan siber.

Namun, penting untuk diingat bahwa regulasi ini harus mencakup definisi dan batasan yang jelas agar tidak menimbulkan kebingungan dalam penerapannya. Dalam naskah akademik RUU KKS, misalnya, definisi “ketahanan” dan “ancaman” siber terlalu luas dan tidak memiliki batasan yang jelas. Hal ini dapat menimbulkan ambiguitas dan menyulitkan identifikasi prioritas, respons, serta alokasi sumber daya dalam penanganan insiden siber. Selain itu, regulasi ini harus mencakup kerangka perlindungan infrastruktur informasi kritis, mengatur aspek kerja sama internasional, serta mekanisme koordinasi antar lembaga.

Selama ini koordinasi antar lembaga menjadi tantangan karena banyaknya tumpang tindih kewenangan. Contohnya, Badan Siber dan Sandi Negara (BSSN) saat ini diberi mandat sebagai lembaga utama yang bertanggung jawab atas keamanan siber nasional, namun ada beberapa lembaga pemerintah lainnya, seperti Badan Intelijen Negara (BIN) dan Badan Intelijen Strategis (BAIS), yang juga memiliki hak dan wewenang serupa, sehingga menyebabkan tumpang tindih kewenangan. Situasi ini dapat mengakibatkan keterlambatan respons dan inefisiensi dalam penanganan ancaman.
Lembaga-lembaga yang menjadi garda terdepan dalam pertahanan siber ini juga seharusnya didukung dengan alokasi anggaran yang memadai, disesuaikan dengan kebutuhan strategis. Ini mencakup peningkatan infrastruktur, pengembangan sumber

daya manusia, serta respons insiden siber. Idealnya, untuk level organisasi, anggaran keamanan siber idealnya berada pada rentang 7-20% dari keseluruhan anggaran IT.

Kerja sama internasional juga penting untuk meningkatkan kapasitas nasional, misalnya melalui forum-forum seperti *ASEAN Cyber Security Cooperation Strategy* dan *Global Forum on Cyber Expertise*. Penandatanganan dan ratifikasi Budapest Convention on Cybercrime bisa menjadi langkah strategis untuk memperkuat penanganan kejahatan siber lintas negara. Indonesia juga perlu mengembangkan National Cyber Crisis Management Plan sebuah rencana krisis yang mencakup berbagai skenario serangan siber dan protokol tanggap darurat, seperti yang sudah dilakukan di beberapa negara, misalnya Amerika Serikat, Irlandia, Malaysia, dan Uni Eropa. Pembentukan *Cyber Rapid Response Teams* (CRRT), yang siap dikerahkan 24 jam, juga sangat penting untuk menangani insiden kritis.

Tantangan utama keamanan siber semakin kompleks di era digital. Keamanan siber bukan lagi sekadar masalah teknis, tetapi telah menjadi komponen penting dalam keamanan nasional dan daya saing ekonomi. Oleh karena itu, pemerintah harus menjadikan keamanan siber sebagai prioritas strategis nasional dengan alokasi sumber daya yang memadai. Saatnya semua pihak bergerak bersama untuk membangun ketahanan siber Indonesia. Masa depan digital kita bergantung pada langkah-langkah yang kita ambil hari ini.

Tautan artikel:

https://theconversation.com/rekomendasi-untuk-prabowo-gibran-3-pilar-utama-membangun-arsitektur-keamanan-digital-yang-tangguh-240215

Serangan Siber Mengintai: Peta Ancaman yang Harus Diwaspadai

Arif Perdana, Bayu Anggorojati, Muhammad Erza Aminanto

Konteks: Artikel ini diterbitkan oleh The Conversation Indonesia sebagai bagian dari dua seri tulisan tentang keamanan siber. Bersama dengan kolega dari program studi keamanan siber, Monash University, kami menguraikan apa saja yang harus diwaspadai di seri tulisan pertama ini. Transformasi digital mempercepat perkembangan ancaman siber global, termasuk di Indonesia dengan 221 juta pengguna internet. Pada 2023, serangan ransomware meningkat, dengan 4.615 kasus dilaporkan di situs kebocoran khusus. Serangan pada infrastruktur cloud naik 75%, sementara kebocoran data melonjak 76%. Di Indonesia, ancaman mencakup ransomware, kebocoran data, dan serangan APT yang menargetkan sektor pemerintah. Kolaborasi publik-swasta dan strategi pertahanan siber yang kuat diperlukan untuk memperkuat ketahanan nasional.

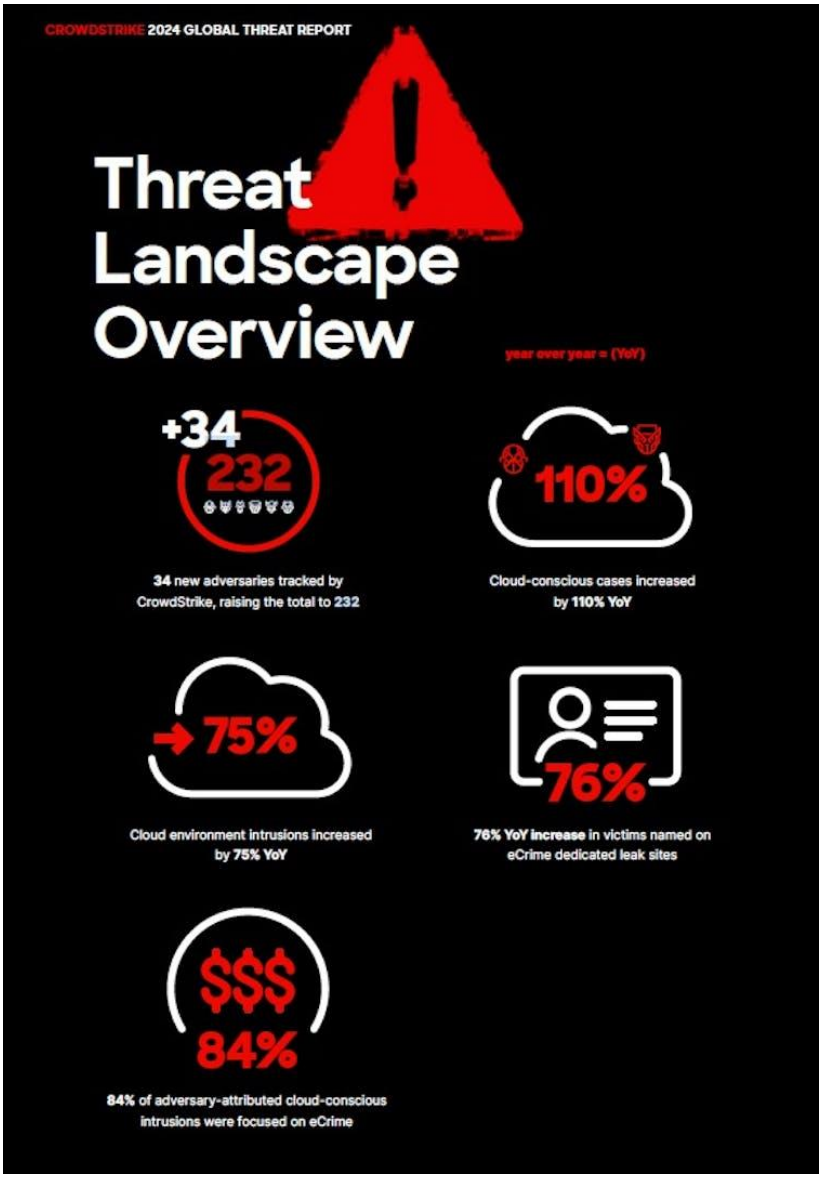
Transformasi digital yang pesat telah menciptakan lanskap ancaman yang kompleks dan dinamis. Metode serangan terus berkembang, seperti balapan antara peretas dan sistem keamanan: setiap kali sebuah pagar dibangun, para peretas segera mencari celah baru untuk ditembus. Ancaman ini berlaku secara global, termasuk di Indonesia, yang ekonomi digitalnya kini berkembang pesat[45]. Dengan jumlah pengguna internet yang besar mencapai 221 juta orang, Indonesia menjadi target empuk bagi para pelaku kejahatan siber[46]. Untuk itu, rezim baru perlu memahami peta ancaman yang ada saat ini dan di masa depan sebelum merumuskan strategi antisipasi. Di era digital yang saling terkoneksi, keamanan siber bukan lagi pilihan, melainkan kebutuhan mutlak untuk menjaga stabilitas dan keamanan nasional.

Peningkatan Serangan Siber Global

Menurut laporan terbaru *Global Threat Report*[47], serangan siber secara global meningkat signifikan, terutama serangan *ransomware* dan serangan terhadap infrastruktur cloud. *Ransomware* adalah jenis perangkat lunak berbahaya yang dirancang

[45] https://indef.or.id/wp-content/uploads/2024/01/Sektor-Ekonomi-Digital.pdf
[46] https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang
[47] https://go.crowdstrike.com/global-threat-report-2024.html

untuk mengunci akses ke sistem komputer. Pelaku serangan ini biasanya memeras korban agar membayar tebusan untuk memulihkan akses. Pada 2023, total jumlah korban *ransomware* yang dilaporkan pada situs kebocoran khusus *Dedicated Leak Sites*[48] atau DLS mencapai 4.615 kasus.



Gambar 4. Tinjauan Lanskap Ancaman Global 2024 dari CrowdStrike: Peningkatan signifikan dalam serangan berbasis cloud dengan 110% peningkatan kasus cloud-conscious dan 75% peningkatan intrusi di lingkungan cloud. Sebanyak 76% korban diidentifikasi di situs kebocoran eCrime, sementara 84% dari serangan cloud-conscious berfokus pada eCrime. Dengan 34 penjahat siber (adversaris) baru yang dilacak, total adversaris yang diawasi kini mencapai 232. (Sumber: Global Threat Report Crowdstrike 2024).

[48] https://socket.dev/glossary/dedicated-leak-site

Peningkatan serangan pada infrastruktur cloud juga melonjak. Pada 2023, serangan yang menargetkan sistem cloud (layanan berbasis internet yang digunakan untuk penyimpanan data, komputasi, dan jaringan) naik 75% dibandingkan dengan tahun sebelumnya.

Serangan siber terhadap sistem cloud tidak hanya meningkat secara kuantitas, tetapi para peretas juga semakin mahir mengeksploitasi kesalahan manusia dan kelemahan keamanan (serangan berbasis *cloud-conscious*). Akibatnya, jumlah korban kebocoran data meningkat hingga 76%. Distribusi serangan ini tidak hanya merugikan perusahaan dan organisasi, tetapi juga merusak kepercayaan publik. Sektor teknologi, telekomunikasi, finansial, dan pemerintahan adalah target utama, dengan kasus terbanyak di wilayah Amerika Utara, Eropa, dan Asia Selatan (lihat Gambar 4).

Serangan Siber di Indonesia

Di Indonesia, ancaman siber juga terus meningkat. Salah satu kasus besar yang terjadi tahun ini adalah serangan *ransomware* yang menghentikan operasional PDN-S. Kemudian pada September lalu, data enam juta nomor pokok wajib pajak atau NPWP bocor. Bahkan tiga bulan sebelumnya, terjadi peretasan sistem di Badan Intelijen Strategis serta kebocoran data pada Sistem Identifikasi Sidik Jari Otomatis milik Kepolisian Republik Indonesia . Rentetan peristiwa ini semakin memperjelas urgensi peningkatan keamanan siber di Indonesia.

Menurut laporan lanskap keamanan siber Indonesia 2023[49], lalu lintas anomali siber di Indonesia mencapai lebih dari 403 juta, dengan puncaknya terjadi pada bulan Agustus sebanyak lebih dari 78 juta insiden. *Ransomware* adalah ancaman utama, dengan lebih dari 1 juta kasus terdeteksi. Salah satu varian *ransomware* yang paling sering muncul adalah *Luna Moth*, yang menipu korbannya dengan mengirim tagihan palsu melalui email, lalu meminta tebusan setelah berhasil mencuri data[50].

[49] https://csirt.kemenkeu.go.id/api/Medias/4b7a023f-7e86-43fa-b877-51697ab24594
[50] https://www.darkreading.com/endpoint-security/luna-moth-malware-free-extortion-campaign

Masalah kebocoran data juga serius. Lebih dari 1,6 juta data telah beredar di darknet. Darknet merupakan bagian dari internet yang tidak dapat diakses mesin pencari biasa dan sering digunakan untuk aktivitas ilegal. Sektor administrasi pemerintahan menjadi yang paling terdampak, menunjukkan perlunya peningkatan pengelolaan data dan penguatan protokol keamanan di instansi pemerintah. Selain itu, serangan seperti *Advanced Persistent Threats* (APT) yang umumnya dilakukan oleh kelompok dengan dukungan negara atau organisasi kriminal, juga terus meningkat. Serangan canggih ini bekerja seperti mata-mata digital yang secara diam-diam menyusup ke jaringan untuk mencuri informasi bernilai tinggi seperti data pemerintah. Pada 2023, tercatat lebih dari empat juta aktivitas APT di Indonesia[51].

Serangan ini akan berdampak besar kepada publik jika menyasar infrastruktur penting seperti energi, transportasi, dan telekomunikasi. Ini bisa menyebabkan pemadaman listrik hingga gangguan pada layanan transportasi. Untuk menghadapi ancaman ini, Indonesia harus segera meningkatkan strategi pertahanan sibernya, termasuk deteksi dini dan respons cepat. Kolaborasi antara sektor publik dan swasta sangat penting untuk memperkuat ketahanan infrastruktur vital negara.

Ancaman Masa Depan dan Teknologi Baru

Selain ancaman yang ada saat ini, masa depan keamanan siber juga akan dipengaruhi oleh teknologi baru seperti AI dan *Internet of Things* (IoT). Di satu sisi, AI dapat digunakan untuk mendeteksi ancaman lebih cepat, tetapi juga bisa menjadi alat serangan yang canggih seperti penggunaan *deepfake* atau serangan AI-powered yang sulit dideteksi oleh sistem keamanan tradisional. Teknologi 5G mempercepat konektivitas, namun di lain sisi memperluas permukaan serangan, terutama karena semakin banyak perangkat yang terhubung. Penggunaan *blockchain* dan *cryptocurrency* juga meningkatkan risiko pencucian uang dan pendanaan terorisme melalui jalur digital. Serangan yang dulu dianggap kecil pun, kini telah berkembang menjadi serangan yang lebih serius dan berbahaya. *Web defacement*, misalnya, yang dulu dianggap intrusi kecil

[51] https://csirt.kemenkeu.go.id/api/Medias/4b7a023f-7e86-43fa-b877-51697ab24594

karena hanya mengubah tampilan depan situs, tapi sekarang serangannya lebih canggih, di mana pelaku tidak hanya menargetkan halaman depan, tetapi juga halaman-halaman tersembunyi di situs web yang mungkin tidak terlihat secara langsung oleh pengguna biasa. Mereka mengeksploitasi celah keamanan yang lebih sulit ditemukan dan diperbaiki.

Dalam konteks Indonesia, ada 189 kasus web defacement yang tercatat, di mana 176 kasus di antaranya menyerang halaman tersembunyi di situs web. Lanskap ancaman siber terus berkembang dengan cepat, menantang kemampuan adaptasi sistem keamanan. Menghadapi situasi ini, Indonesia memerlukan respons holistik yang mencakup peningkatan infrastruktur, penguatan regulasi, dan peningkatan literasi keamanan siber. Hanya dengan pendekatan yang komprehensif dan kolaboratif serta langkah-langkah strategis yang tepat, Indonesia dapat memperkuat ketahanan sibernya dan melindungi diri dari ancaman di masa depan.

Tautan artikel:

https://theconversation.com/serangan-siber-mengintai-peta-ancaman-yang-harus-diwaspadai-prabowo-gibran-239015

Orkestra Manusia di Simfoni Pertahanan Digital

Arif Perdana

Konteks: Artikel ini diterbitkan di Kumparan pada 16 Oktober 2024 dan merupakan refleksi dari tiga film yang pernah saya tonton, yaitu *The Shawshank Redemption* (1994), *The Next Three Days* (2010), dan *Drishyam* (2015). Meskipun ketiga film tersebut tidak secara langsung membahas keamanan siber, mereka menawarkan wawasan berharga tentang bagaimana melindungi diri dan memahami strategi pelaku kejahatan siber. Wawasan ini juga relevan dengan kasus peretasan SolarWinds. Dalam membangun keamanan yang lebih tangguh, penting diingat bahwa di balik setiap firewall dan protokol siber terdapat cerita manusia.

Masih segar di ingatan kita serangan *ransomware* yang melumpuhkan PDN-S[52]. Begitu juga dengan peretasan sistem Badan Intelijen Strategis, dan bocornya data Sidik Jari milik Kepolisian Indonesia di Juni lalu[53]. Di akhir minggu kedua Agustus 2024, 4,7 juta data aparatur sipil negara bocor dan dijual di *BreachForums*. Menyusul insiden kebocoran ini, 369 hotel di Indonesia menjadi korban pemalsuan data[54]. Dalam lanskap digital yang terus berubah, keamanan siber menjadi benteng melawan ancaman serangan dan kebocoran data. Drama sesungguhnya di dunia keamanan informasi tidak hanya terletak pada pertarungan antara *firewall* dan *malware*, tetapi juga pada pikiran dan perilaku manusia.

Perencanaan, Tekad, dan Manipulasi

Bayangkan sejenak tiga narasi sinematik yang tampaknya jauh dari dunia siber, namun menyimpan wawasan menarik tentang dimensi keamanan. *The Shawshank Redemption* (1994)[55], dengan kisah pelarian Andy Dufresne, *The Next Three Days* (2010)[56], dengan misi John Brennan yang penuh tekad, dan *Drishyam* (2015)[57], dengan alibi nyaris sempurna Vijay Salgaonkar. Tiga sinema berbeda, namun semuanya menyuarakan

[52] https://www.thejakartapost.com/opinion/2024/07/17/strategies-for-effective-cybersecurity-resilience.html
[53] https://bisnis.tempo.co/read/1884001/data-bais-inafis-dan-kemenhub-diduga-bocor-di-dark-web-dijual-hingga-usd-7-000
[54] https://katadata.co.id/berita/industri/66ba1007caa2e/lebih-dari-300-hotel-terkena-pemalsuan-data-seperti-ini-modusnya
[55] https://www.imdb.com/title/tt0111161/
[56] https://www.imdb.com/title/tt1458175/
[57] https://www.imdb.com/title/tt4430212/

tentang kekuatan perencanaan dan kompleksitas perilaku manusia yang relevan untuk mengilustrasikan pedang dan perisai di arena keamanan digital.

Di balik tembok *Shawshank*, Andy merajut rencana pelariannya dengan penuh kesabaran dan ketelitian. Setiap ketukan palu di dinding selnya adalah simfoni keuletan untuk membobol sistem yang tampak tak tertembus. Bukankah ini mencerminkan kegigihan para peretas yang, dengan sabar dan teliti, mencari celah di benteng digital untuk merusak dan mencuri data-data kita? Penasihat Andy, Ellis Redding, dengan jaringan koneksinya yang luas, mengingatkan kita pada bahaya laten ancaman orang dalam yang mungkin luput dari radar di insiden keamanan.

Sementara itu, John di *The Next Three Days* menunjukkan bagaimana tekad yang membara dapat mengalahkan segala rintangan. Dengan sumber daya terbatas namun motivasi yang tak terbatas, ia meruntuhkan sistem keamanan yang dirancang untuk menahan ribuan tahanan. Bukankah ini serupa dengan ancaman siber yang bukan selalu dari organisasi besar dengan sumber daya melimpah, tetapi bisa dari individu atau kelompok kecil yang didorong oleh tekad membara. Boleh jadi dengan motivasi unjuk gigi atau untuk keuntungan pribadi dan kelompok.

Di *Drishyam*, ada Vijay sang maestro manipulasi. Dengan kecerdikannya, ia menciptakan alibi yang sangat baik, menganyam kebohongan menjadi narasi kebenaran yang menipu bahkan untuk pendengaran yang paling awas. Bukankah ini mengingatkan kita pada serangan siber yang paling canggih, yang berhasil menyusup dan bersembunyi di balik fasad keseharian, mengelabui bahkan sistem deteksi yang paling mutakhir.

Kisah-kisah fiksi ini ternyata menemukan gemanya di kejadian nyata. Pada penghujung tahun 2020, dunia dikejutkan oleh insiden *SolarWinds*, sebuah serangan siber yang hingga saat ini dikenang sebagai salah satu yang paling cerdik dan merusak di sejarah keamanan informasi[58]. *SolarWinds* adalah perusahaan teknologi informasi (TI) Amerika Serikat yang menyediakan perangkat lunak untuk manajemen jaringan, sistem, dan infrastruktur TI. Produk mereka digunakan oleh banyak organisasi besar, termasuk lembaga pemerintah dan perusahaan *Fortune 500*.

[58] https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

Seperti Andy yang memanfaatkan abainya sipir penjara untuk melarikan diri, para peretas dengan sabar menemukan celah keamanan di *SolarWinds*. Salah satu pintu masuk utama peretas adalah kesalahan konfigurasi pada repositori *GitHub* yang digunakan *SolarWinds*, serta akses ke server menggunakan password lemah. Namun, ini hanyalah awal dari strategi serangan yang jauh lebih kompleks dan canggih. Para penyerang membangun infrastruktur tanda tangan digital yang tampak sah, menyamarkan *malware* mereka sebagai pembaruan resmi perangkat lunak *SolarWinds Orion*[59].

Dari titik masuk ini, mereka merajut jaring intrusi yang begitu luas dan dalam, menyusup ke ribuan sistem melalui pembaruan perangkat lunak yang tampak absah namun merusak. *Malware* mereka, yang diberi nama *Sunburst*, dirancang untuk tetap dorman selama dua minggu, menghindari deteksi dengan bergerak secara lateral dalam jaringan dan terus mengubah posisi serta kredensialnya[60].

Ini menunjukkan bagaimana kombinasi kelalaian internal dan eksploitasi cerdas mengakibatkan bencana keamanan berskala global. Insiden *SolarWinds* menjadi pelajaran pahit bahwa ancaman siber terbesar sering bersembunyi di balik asumsi keamanan yang dianggap mapan.

Merajut Strategi Keamanan

Dalam simfoni keamanan siber yang kompleks ini, Rencana Respon Insiden (*Incidents Response Planning*/IRP), Rencana Pemulihan Bencana (*Disaster Response Planning*/DRP), dan Rencana Keberlangsungan Bisnis (*Business Continuity Planning*/BCP) menjadi trio partitur utama yang mengarahkan orkestra pertahanan organisasi (lihat Tabel 6). IRP menjadi garda terdepan saat serangan terjadi, DRP memulihkan operasi kritis, sementara BCP memastikan kelangsungan fungsi utama bisnis selama dan setelah krisis[61].

[59] https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
[60] https://journals.sagepub.com/doi/abs/10.1177/2043886921993126
[61] https://koran.tempo.co/read/opini/489465/strategi-keamanan-siber

Tabel 6. Dimensi IRP, DRP dan BCP

Dimensi	IRP	DRP	BCP
Fungsi Utama	Respon cepat terhadap serangan atau insiden keamanan siber untuk meminimalkan dampak dan mengendalikan situasi.	Pemulihan operasi penting setelah bencana atau serangan besar, memungkinkan organisasi kembali berfungsi secara efektif.	Menjaga kelangsungan operasi bisnis utama selama dan setelah insiden atau bencana, memastikan stabilitas dan keberlanjutan organisasi.
Fokus	Penanganan insiden secara langsung dan segera, termasuk investigasi dan mitigasi ancaman.	Mengembalikan operasi dan infrastruktur kritis yang terganggu atau rusak akibat insiden atau bencana.	Menjamin berjalannya fungsi bisnis utama tanpa gangguan signifikan, termasuk perencanaan jangka panjang dan persiapan untuk krisis mendatang.
Aktivitas Kunci	Identifikasi, eskalasi, mitigasi, dan analisis pasca-insiden untuk memahami penyebab dan mencegah insiden serupa.	Perbaikan infrastruktur, pemulihan data, dan pelatihan untuk memastikan kesiapan dalam menghadapi gangguan besar.	Pemetaan proses bisnis kritis, penetapan prosedur darurat, dan latihan skenario untuk memastikan kesiapan organisasi menghadapi krisis.
Keterlibatan Tim	Tim khusus keamanan siber yang terlatih dalam respons insiden dan analisis ancaman serta koordinasi dengan unit terkait.	Divisi pemulihan operasional dan manajemen, bekerja sama dengan bagian IT dan pemulihan data.	Semua bagian organisasi, dari level manajemen hingga karyawan operasional, dengan fokus pada pemahaman peran mereka selama krisis.
Waktu Respon	Reaksi cepat dalam hitungan menit hingga jam setelah terdeteksi, untuk membatasi kerusakan dan eskalasi.	Fokus pada pemulihan jangka menengah hingga panjang, yang dapat berlangsung dalam hitungan hari hingga minggu.	Rencana jangka panjang untuk keberlanjutan bisnis yang berkesinambungan, dengan persiapan yang diuji secara berkala.
Kebutuhan Pengujian	Perlu diuji secara berkala melalui simulasi insiden atau latihan tabletop untuk memastikan respon yang efektif dan siap pakai.	Pengujian berkala pada infrastruktur pemulihan bencana, termasuk backup data dan sistem komunikasi darurat.	Latihan simulasi dan pengujian berkelanjutan untuk memastikan semua bagian organisasi siap menghadapi krisis dan tetap beroperasi.

Dimensi	IRP	DRP	BCP
Elemen Psikologis	Mengelola tekanan dan ketegangan selama insiden untuk menjaga respon yang terarah dan terstruktur, mencakup aspek manusiawi dalam keamanan.	Meminimalkan kepanikan dan memastikan koordinasi antar tim saat proses pemulihan, memperhatikan kebutuhan fisik dan mental tim pemulihan.	Memberikan jaminan dan instruksi kepada seluruh staf untuk mengurangi kecemasan dan memastikan peran mereka dalam keberlanjutan operasional.
Contoh	Melibatkan respons terhadap serangan *ransomware* atau insiden peretasan yang mengancam sistem organisasi.	Proses pemulihan pasca serangan besar, seperti mengembalikan data dan sistem yang terpengaruh serangan *malware*.	Menjaga layanan utama tetap berjalan dalam situasi darurat, seperti mempertahankan akses terhadap data penting saat pemulihan sistem berlangsung.

Lantas, apa yang dapat kita petik dari perpaduan antara fiksi sinematik dan realitas ini? Pertama, bahwa di dunia keamanan siber, kesabaran dan perencanaan jangka panjang adalah senjata yang tak ternilai. Andy dan John dengan sabar mempelajari rutinitas penjara untuk mencari celah keamanan yang bisa ditembus, begitu juga dengan peretas *SolarWinds*. Organisasi perlu membangun dan terus memperkuat pertahanan mereka, sadar bahwa keamanan adalah perjalanan, bukan tujuan. Ini menekankan pentingnya DRP yang komprehensif, dirancang dengan cermat dan diuji secara berkala untuk menghadapi badai siber dan kebocoran data. Organisasi juga harus berhati-hati dengan rutinitas dan "zona nyaman" mereka yang mungkin menjadi pintu masuk peretas.

Kedua, kita diingatkan akan kekuatan motivasi personal dan respon cepat terhadap ancaman. John dan para peretas *SolarWinds* sama-sama menunjukkan bagaimana tekad yang kuat, kesabaran, ketelitian, dan tindakan cepat dapat mengalahkan sistem yang tampaknya tak tertembus. Ini menekankan pentingnya memahami tidak hanya aspek teknis, tetapi juga psikologis dari keamanan siber.

Ketiga, konsistensi dan kemampuan beradaptasi adalah kunci. Vijay dan peretas *SolarWinds* menunjukkan bagaimana menjaga konsistensi dalam penipuan dan

beradaptasi terhadap tekanan dapat menjadi penentu keberhasilan atau kegagalan. Bagi organisasi, ini berarti memiliki IRP yang fleksibel namun konsisten dan mampu menghadapi berbagai skenario serangan dengan tetap mempertahankan integritas respons organisasi.

Terakhir, narasi di atas mengingatkan kita mengenai kerentanan dan ancaman dari dalam. Perencanaan dan antisipasi di keamanan siber harus melibatkan seluruh organisasi dan memastikan bahwa setiap individu memahami peran mereka. Ini juga termasuk memastikan BCP berjalan dengan baik ketika terjadi insiden serangan siber atau kebocoran data.

Dalam perjalanan menuju keamanan yang lebih tangguh, kita harus ingat bahwa di balik setiap *firewall* dan protokol teknis keamanan siber, ada kisah manusia. Melalui kisah-kisah inilah kita menemukan peta menuju keamanan yang lebih bijaksana, tangguh, dan siap menghadapi tantangan digital masa depan.

Tautan artikel:

https://kumparan.com/arif-perdana-1723991955605643308/orkestra-manusia-di-simfoni-pertahanan-digital-23j6OutuTm3/full

Agar Aturan Pelindungan Data Pribadi Efektif

Arif Perdana

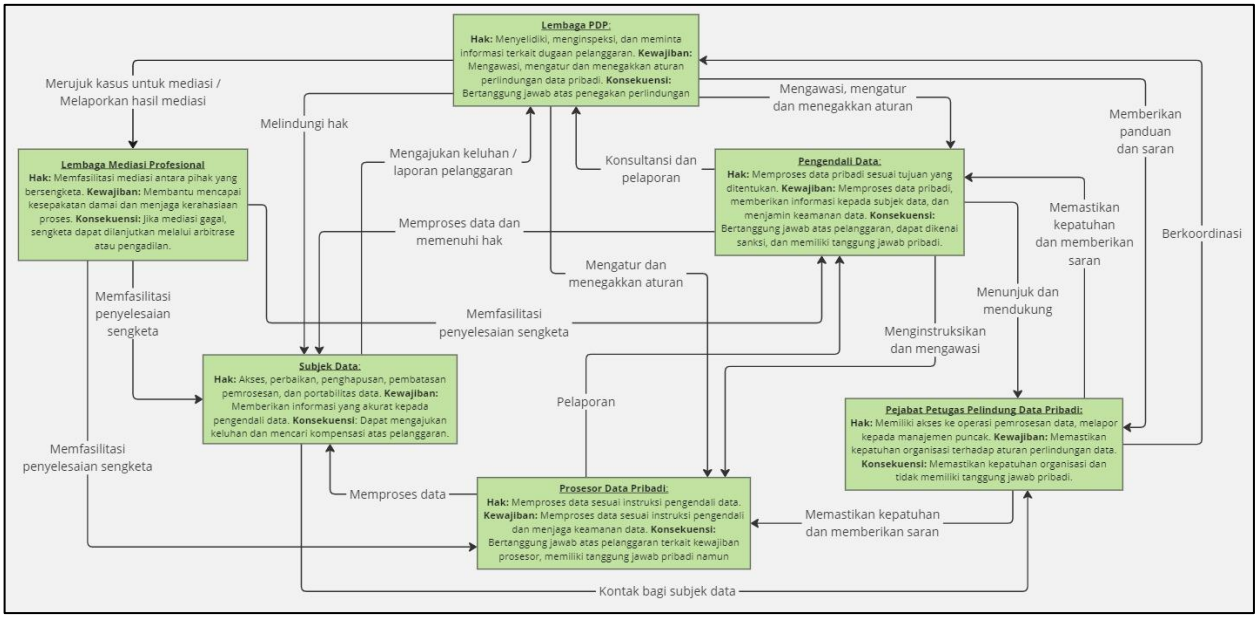
Konteks: Artikel ini pertama kali terbit di Koran Tempo, tanggal 30 September 2024. Tulisan ini memberikan pendapat mengenai bagaimana keefektifan UU PDP yang akan diberlakukan di bulan Oktober. Pada saat tulisan ini dimuat, lembaga PDP belum juga dibentuk. Selain itu dari hasil analisis yang penulis lakukan ada potensi UU ini diimplementasikan berbeda oleh lembaga publik. Ini bisa menyebabkan UU ini kurang optimal untuk menjaga kepentingan publik.

Indonesia menghadapi tantangan serius dalam PDP, dengan serangkaian kebocoran data yang mengancam privasi warga. UU PDP dan Rancangan Peraturan Pemerintah (RPP) yang saat ini masih dalam tahap harmonisasi[62], hadir sebagai langkah penting untuk mengatasi masalah ini. Meskipun membawa kemajuan signifikan, seperti pengaturan hak subjek data dan mekanisme penyelesaian sengketa, implementasi UU PDP menghadapi beberapa tantangan. Kekhawatiran utama meliputi independensi Lembaga PDP, fleksibilitas aturan bagi badan publik, dan potensi penyalahgunaan pengecualian untuk kepentingan umum.

UU PDP akan berlaku Oktober 2024, namun lembaga pengawasnya belum jelas. Masyarakat menantikan apakah pemerintah akan memenuhi komitmen atau UU ini hanya regulasi tanpa kekuatan nyata. Efektivitas UU ini bergantung pada pembentukan lembaga pengawas yang kuat, pengawasan ketat, transparansi tinggi, dan akuntabilitas yang jelas bagi semua pihak, termasuk pemerintah. Mekanisme PDP dalam RPP menekankan peran spesifik berbagai pihak (Gambar 5). Lembaga PDP bertanggung jawab atas penegakan aturan, penyelidikan pelanggaran, pemberian sanksi, dan penyusunan pedoman. Pengendali data, yang menginstruksikan pemrosesan data pribadi, bertanggung jawab penuh atas pelanggaran yang terjadi dan dapat dikenai sanksi jika gagal mematuhi aturan. Pengendali data memiliki tanggung jawab pribadi terbesar. Prosesor data

[62] https://pdp.id/rpp-ppdp/1

bertugas memproses data sesuai instruksi pengendali data, dengan tanggung jawab pribadi terbatas terhadap pelanggaran kewajiban prosesor.



Gambar 5. Peran, hak, dan tanggung jawab dalam perlindungan data pribadi dan penyelesaian sengketa (UU PDP & RPP PDP)

Pejabat Petugas Pelindung Data Pribadi memastikan kepatuhan organisasi terhadap aturan pelindungan data tanpa memiliki tanggung jawab pribadi, melapor kepada manajemen puncak untuk memastikan penerapan aturan. Subjek data, sebagai pemilik data, memiliki hak akses, perbaikan, penghapusan, pembatasan pemrosesan, portabilitas data, dan hak untuk mencari kompensasi atas pelanggaran. RPP PDP juga mengatur pengawasan ketat oleh Lembaga PDP, termasuk kewenangan untuk memeriksa sistem elektronik yang digunakan oleh pengendali dan prosesor data. Pengendali data diwajibkan melakukan penilaian dampak PDP dalam situasi tertentu untuk mengurangi risiko pelanggaran.

Untuk penyelesaian sengketa, RPP memperkenalkan mekanisme mediasi di luar pengadilan dengan Lembaga Mediasi Profesional yang memfasilitasi dialog untuk mencapai kesepakatan. Jika mediasi gagal, sengketa dapat dilanjutkan melalui arbitrase atau pengadilan. Lembaga PDP juga menerima laporan dari subjek data yang merasa

dirugikan. RPP secara detail mengatur transfer data pribadi ke luar negeri, mensyaratkan bahwa negara tujuan harus memiliki pelindungan data yang setara atau lebih tinggi, atau ada mekanisme pelindungan yang memadai. Mekanisme ini dirancang untuk memastikan pelindungan hak subjek data namun memerlukan pengawasan untuk mencegah penyalahgunaan.

Konsekuensi Penegakan UU PDP dan Kekhawatiran Efektivitasnya

UU PDP mengatur sanksi tegas bagi siapa pun yang lalai melindungi data pribadi, mulai dari denda administratif hingga hukuman pidana. Sanksi administratif dapat berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan Data Pribadi, penghapusan atau pemusnahan Data Pribadi, dan/atau denda administratif. Sementara itu, sanksi pidana dapat berupa pidana penjara dan/atau denda. UU PDP dan RPP PDP memiliki aspek-aspek positif. Aturan ini berupaya untuk menyesuaikan standar pelindungan data di Indonesia dengan standar internasional, memberikan hak-hak yang jelas kepada Subjek Data, dan menciptakan kerangka kerja yang komprehensif untuk PDP. Tantangannya adalah memastikan bahwa implementasi dan penegakan aturan-aturan ini dilakukan secara efektif dan konsisten.

Namun, efektivitas UU ini berada di ujung tanduk karena absennya lembaga pengawas yang seharusnya berperan sebagai 'penjaga gerbang' dalam era digital. Ketiadaan lembaga ini menciptakan kekosongan dalam mekanisme pengawasan, yang pada akhirnya dapat membuat aturan ini tidak lebih dari sekadar formalitas hukum. Dari analisis terhadap UU PDP dan RPP PDP, muncul kekhawatiran bahwa aturan ini bisa menjadi “pisau bermata dua” dan dimanfaatkan oleh pemerintah atau entitas lain untuk menghindari tanggung jawab atas pelanggaran data.

Beberapa ketentuan dalam RPP yang memperkuat kekhawatiran ini antara lain ketentuan yang terlihat fleksibel untuk badan publik. Lembaga PDP di Indonesia bertanggungjawab kepada presiden (pasal 58 UU PDP), sehingga independensinya dalam mengawasi dan menegakkan PDP tidak sekuat otoritas pengawas di Uni Eropa. Hal ini dapat mempengaruhi efektivitas lembaga dalam menjalankan tugasnya secara objektif dan bebas dari pengaruh eksternal.

Pasal 67 RPP PDP memberikan ruang bagi badan publik untuk menentukan sendiri aturan pemrosesan data pribadi yang berlaku di lingkungan mereka. Fleksibilitas ini berpotensi disalahgunakan untuk membuat aturan yang lebih menguntungkan badan publik dan kurang melindungi subjek data, membuka celah bagi pelanggaran yang tidak terdeteksi. Selain itu, terdapat pengecualian dalam beberapa pasal yang memungkinkan badan publik melakukan pemrosesan data pribadi dengan dalih kepentingan umum atau pelayanan publik (Pasal 63-66). Dengan pengecualian ini, pemrosesan data yang tidak sepenuhnya sesuai dengan prinsip pelindungan data dapat diabaikan, memungkinkan pemerintah menghindar dari tanggung jawab jika terjadi pelanggaran.

Lebih jauh lagi, kekhawatiran muncul dari kurangnya pengawasan eksternal yang kuat dan independen. Meski lembaga PDP nantinya memiliki kewenangan untuk mengawasi dan menegakkan aturan, RPP tidak secara jelas menguraikan mekanisme pengawasan eksternal yang independen. Hal ini menciptakan celah di mana pengawasan bisa menjadi lemah atau tidak objektif, terutama ketika pelanggaran dilakukan oleh pemerintah atau lembaga negara. Proses mediasi dalam penyelesaian sengketa juga berpotensi tidak transparan, terutama jika menyangkut pelanggaran data oleh lembaga negara. Hal ini dapat mengarah pada penyelesaian yang lebih menguntungkan pihak pemerintah dan merugikan subjek data.

Selain itu, klausul pelindungan kepentingan vital dan kepentingan umum dalam Pasal 60-66 bisa menjadi alasan untuk membenarkan penggunaan data yang melanggar privasi, dengan dalih melindungi kepentingan masyarakat atau negara. Kondisi ini mengkhawatirkan karena membuka pintu bagi eksploitasi data tanpa pengawasan yang memadai, yang dapat merusak kepercayaan publik terhadap PDP.

Langkah Menuju Efektivitas UU PDP

Agar UU PDP berjalan optimal, keberadaan lembaga pengawas yang independen dan kuat menjadi sangat penting. Lembaga ini harus diberdayakan tidak hanya untuk menegakkan aturan, tetapi juga memantau dan melakukan audit terhadap kepatuhan seluruh organisasi, baik publik maupun swasta, terhadap standar PDP. Oleh karena itu pemimpin yang kompeten untuk memimpin lembaga ini sangat kritikal, guna memastikan

kepatuhan di tengah semakin kompleksnya ancaman siber. Pemimpin lembaga PDP yang memiliki kompetensi tinggi diperlukan untuk mengatasi berbagai tantangan dalam ruang siber yang semakin kompleks dan beragam, serta untuk merespons dengan cepat dan tepat terhadap ancaman yang berkembang. Selain itu lembaga PDP juga harus memiliki sumber daya yang sangat kompeten dan selalu memutakhirkan pengetahuannya tentang data di era digital.

Meski UU PDP bertujuan melindungi data pribadi, sejumlah ketentuan dalam RPP berpotensi dimanfaatkan oleh pemerintah untuk menghindari akuntabilitas atas pelanggaran data. Kekhawatiran ini diperparah dengan ketentuan yang fleksibel bagi badan publik, kurangnya pengawasan eksternal yang kuat, dan proses mediasi yang bisa jadi tidak transparan. Untuk menghindari UU ini menjadi aturan yang lemah, penting untuk memastikan penerapannya dilakukan dengan pengawasan ketat, transparansi yang tinggi, dan adanya akuntabilitas yang jelas bagi semua pihak, termasuk pemerintah.

Selain itu, perlu ada mekanisme untuk mengevaluasi dan memperbarui UU dan peraturan pelaksanaannya secara berkala, mengingat perkembangan teknologi yang cepat dan munculnya tantangan baru dalam PDP. Tanpa langkah-langkah tersebut, UU PDP hanya akan menjadi simbol tanpa substansi di tengah ancaman kebocoran data yang terus mengintai.

Tautan artikel:

https://koran.tempo.co/read/opini/490081/akuntabilitas-uu-pdp

Pentingnya Tata Kelola Data Kesehatan Di Era AI: Indonesia Harus Segera Bangun Layanan Kesehatan Terintegrasi

Arif Perdana, Grace Wangge

Konteks: UU PDP, UU Kesehatan, dan Peraturan Pemerintah (PP) Nomor 28 Tahun 2024. PP No. 28 Tahun 2024. Artikel ini saya tulis bersama kolega dari program studi kesehatan masyarakat di Monash University. Data berkualitas tinggi yang terintegrasi akan membantu dalam analisis dan prediksi medis, meningkatkan akses layanan kesehatan, serta melindungi privasi pasien. Tantangan yang dihadapi Indonesia meliputi keragaman populasi dan kebutuhan untuk sistem yang efektif. Pembelajaran dari negara lain menunjukkan bahwa tata kelola yang baik dapat memperkuat layanan kesehatan. Diperlukan kerangka hukum yang jelas, infrastruktur yang terintegrasi, dan keterlibatan semua pihak, termasuk pemerintah dan swasta, untuk mewujudkan sistem yang aman dan efisien dalam pengelolaan data kesehatan.

Seiring berkembangnya AI di dunia kesehatan, tata kelola data kesehatan yang baik kian dibutuhkan. Data berkualitas tinggi yang terkelola dengan baik akan membantu melatih program yang menganalisis kumpulan data untuk menangkap pola dan membuat prediksi (model AI) sehingga mampu menghasilkan informasi klinis yang andal dan relevan. Apalagi di era digital saat ini, ketersediaan data kesehatan meningkat pesat. Informasi ini harus dikelola secara tepat agar manfaatnya bisa dirasakan bersama. Memperkuat tata kelola data kesehatan bermanfaat untuk meningkatkan akses layanan kesehatan masyarakat secara efektif dan efisien. Tata kelola data kesehatan akan menjadi fondasi untuk perawatan kesehatan individu, melahirkan inovasi medis, dan yang terpenting meningkatkan kepercayaan pasien.

Bayangkan Anda mendadak dilarikan ke rumah sakit. Hanya dalam hitungan detik, dokter bisa mengakses riwayat kesehatan Anda secara lengkap, mulai dari riwayat alergi hingga hasil tes kesehatan terbaru. Dokter pun kemudian merekomendasikan terapi yang paling tepat sesuai kondisimu. Ini bukan potongan adegan film fiksi ilmiah, melainkan potret masa depan layanan kesehatan Indonesia ketika memiliki tata kelola data kesehatan yang kuat.

Pentingnya Tata Kelola Data Kesehatan di Era AI

Setidaknya, terdapat tiga alasan mengapa Indonesia perlu segera membangun tata kelola data kesehatan yang saling terhubung (terintegrasi) di era AI.

Pertama, untuk memastikan standar pengumpulan, pembuktian (validasi), dan pemeliharaan data kesehatan yang berkualitas. Kedua, untuk melindungi privasi pasien dan menjamin penggunaan data secara etis. Ketiga, untuk mendukung integrasi berbagai jenis data untuk model AI secara komprehensif. Tata kelola data kesehatan juga berperan penting dalam mengatasi potensi kesalahan (bias) pada AI. Lewat perencanaan dan pengumpulan data kesehatan yang cermat, kesalahan dalam data dapat diidentifikasi dan diminimalkan.

Pembakuan (standardisasi) data juga diperlukan, misalnya lewat penggunaan aplikasi terpadu yang akan memperlancar kegiatan berbagi informasi antara penyedia layanan kesehatan, peneliti, dan pembuat kebijakan. Hal ini pada gilirannya akan meningkatkan efisiensi operasional dan mendorong keterlibatan pasien (pengguna aplikasi).

Sebaliknya, tata kelola data kesehatan yang buruk justru berisiko menimbulkan ancaman serius. Ancaman paling nyata adalah meningkatnya risiko pelanggaran data, insiden ketika pihak tidak bertanggung jawab mencuri informasi rahasia, seperti identitas pribadi sehingga berpotensi menghilangkan kepercayaan publik. Data pasien yang sulit diakses karena terbagi-bagi (terfragmentasi) juga dapat menghambat perawatan yang efektif, menyebabkan keterlambatan, dan berpotensi membahayakan keselamatan pasien.

Lebih lanjut, tata kelola data yang lemah dapat menghambat penelitian dan inovasi di bidang kesehatan. Dalam situasi krisis, data yang tidak dapat diandalkan akan sangat menghambat upaya penanganan, sebagaimana terlihat pada fase awal pandemi COVID-19. Pelanggaran aturan akibat tata kelola data yang buruk juga bisa membawa risiko hukum bagi fasilitas kesehatan dan menyebabkan kerugian finansial.

Belajar dari Negara Lain

Indonesia bisa belajar dari kesuksesan berbagai negara yang telah mempraktikkan tata kelola data kesehatan yang baik. European Health Data Space, misalnya, menekankan pentingnya aturan berbagi data lintas batas yang harmonis[63]. Aturan ini bertujuan untuk memberdayakan individu dengan memberikan kendali atas data kesehatan mereka, memfasilitasi layanan kesehatan, serta memungkinkan penggunaan kembali data kesehatan untuk penelitian dan pembuatan kebijakan. Inisiatif ini mendukung terciptanya sistem yang aman, tepercaya, dan sejalan dengan regulasi.

Sementara, Health Data Research di Inggris, menyediakan kerangka kerja yang memungkinkan peneliti menggunakan data kesehatan pasien untuk penelitian, tetapi privasi data pasien tetap terlindungi. Di Amerika Serikat (AS), Health Insurance Portability and Accountability Act (HIPAA) menyediakan aturan yang bisa menjaga privasi data kesehatan pasien[64]. Di sisi lain, data ini bisa digunakan untuk kebaikan masyarakat.

E-Health Estonia[65] dan Secondary Use of Health Data di Finlandia[66] membuat tata kelola data yang mengedepankan transparansi, kemampuan pertukaran data lintas wilayah dan organisasi (interoperabilitas), serta keamanan pengelolaan data kesehatan. Estonia mendukung pasien mengontrol data mereka melalui sistem terpusat berteknologi blockchain. Adapun Finlandia mengizinkan penggunaan data sekunder untuk riset dan kebijakan pemerintah. Estonia dan Finlandia memastikan efisiensi dan pelindungan privasi yang dilakukan sesuai dengan perundang-undangan privasi Eropa, GDPR. Kedua negara menunjukkan bahwa tata kelola data yang kuat dapat meningkatkan layanan kesehatan, penyesuaian layanan sesuai kebutuhan pasien (personalisasi), dan inovasi berbasis data. Lalu, bagaimana dengan Indonesia?

Tantangan di Indonesia

Indonesia menghadapi tantangan unik dalam penerapan tata kelola data kesehatan. Soalnya, negara ini memiliki jumlah penduduk yang banyak dan beragam

[63] https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en
[64] https://www.hhs.gov/hipaa/index.html
[65] https://e-estonia.com/solutions/e-health/e-health-records/
[66] https://stm.fi/en/secondary-use-of-health-and-social-data

serta kondisi alam yang bervariasi. Karena itu, diperlukan kerangka kerja yang menyeluruh untuk membangun tata kelola data kesehatan yang kokoh. Ini mencakup penetapan peran yang jelas dalam pengumpulan data, standar kualitas data, peraturan berbagi data, pelindungan privasi pasien, pedoman etika kesehatan, mekanisme keterlibatan pasien, serta proses audit dan jaminan kualitas.

UU Nomor 27 Tahun 2022 tentang PDP (UU PDP) menyediakan kerangka hukumnya. Pedoman lebih spesifik mengenai pengelolaan dan pertukaran data di fasiltas kesehatan, terutama yang berada di bawah koordinasi Kementerian Kesehatan (Kemenkes) tertera dalam Peraturan Pemerintah (PP) Nomor 28 Tahun 2024. PP No. 28 Tahun 2024 dapat diperkuat dengan menambahkan protokol rinci soal penanganan kasus pelanggaran data dan penetapan kriteria yang detail untuk transfer data lintas batas dan wilayah[67]. Aturannya juga perlu diselaraskan dengan standar internasional. Peraturan tersebut perlu menyertakan pula panduan spesifik mengenai penanganan teknologi baru, seperti AI, komputasi awan, big data, keamanan siber, termasuk mekanisme pengawasan yang kuat untuk mencegah pelanggaran data.

Pengembangan aplikasi data terpadu, seperti Satu Data Indonesia [68] dan SATUSEHAT [69] harus diupayakan bersama dengan melibatkan semua pemangku kepentingan. Investasi dalam infrastruktur teknis juga sangat diperlukan, termasuk pembangunan sistem informasi kesehatan yang terintegrasi dan platform pertukaran data yang aman. Mengingat banyaknya jumlah daerah di Indonesia, penyediaan fasilitas pendukung, seperti internet mungkin dapat dilakukan secara bertahap, dimulai dari wilayah perkotaan.

Hal yang tidak kalah penting adalah pemberdayaan individu. Manusia merupakan titik paling rentan dalam banyak kasus keamanan siber, seperti kebocoran data kesehatan. Karena itu, perlu diadakan pelatihan manajemen data dan literasi digital, terutama pengembangan kemampuan di bidang AI dan keamanan siber. Pemerintah juga

[67] https://peraturan.bpk.go.id/Details/294077/pp-no-28-tahun-2024
[68] https://data.go.id/
[69] https://satusehat.kemkes.go.id/sdmk

bisa menjalin kemitraan dengan organisasi internasional untuk memperkaya wawasan dan mendapatkan dukungan.

Agar strategi tata kelola data berjalan sukses, pemerintah harus bisa membangun kepercayaan publik, baik masyarakat maupun korporasi. Caranya dengan mengedukasi masyarakat seputar manfaat berbagi data dan transparansi dalam penggunaan data. Selain itu, pemerintah harus memikirkan strategi yang tepat untuk korporasi agar kepatuhan terhadap aturan tidak menambah biaya besar (signifikan) yang bisa menghambat inovasi. Namun, perlu diingat bahwa langkah-langkah di atas harus didukung oleh sumber daya yang kuat dan kolaborasi strategis agar tidak terjebak dalam pengembangan yang berulang dan tidak efektif, yang justru dapat menghambat percepatan inovasi dan penerapan teknologi yang sudah ada.

Libatkan Banyak Pihak

Untuk mewujudkan revolusi layanan dan stuktur tata kelola data kesehatan di Indonesia, diperlukan pembentukan otoritas data kesehatan nasional dan komite tata kelola. Lembaga ini akan membantu mengelola sistem berbagi data secara efektif. Tak hanya itu, Indonesia juga harus memiliki panduan pelaksanaan rencana (implementation roadmap) yang konkret dan terukur. Tahap pertama bisa dimulai lewat proyek percobaan (pilot project) di kota-kota besar, dilanjutkan dengan evaluasi dan penyempurnaan sistem sebelum diberlakukan secara nasional.

Penting untuk melibatkan startup kesehatan lokal yang berpotensi memberikan solusi inovatif dengan pengelolaan biaya yang efektif (cost-effective). Misalnya, perusahaan swasta pengembang aplikasi telemedicine maupun sistem manajemen data kesehatan berbasis komputasi awan. Kerja sama ini sangat strategis untuk mempercepat transformasi digital kesehatan yang bertanggung jawab dan berkelanjutan.

Hal ini sebenarnya sudah dimulai lewat pembentukan *Regulatory Sandbox* Kemenkes sejak April 2023[70]. Regulartory Sandbox adalah program pengembangan

[70] https://sandbox.kemkes.go.id/

inovasi digital kesehatan oleh Kemenkes untuk menilai kemampuan pengelolaan sebuah unit bisnis. Alur tata kelola penggunaan data kesehatan di Indonesia akan melibatkan lintas kementerian. Karena itu, *Regulatory Sandbox* perlu diperluas dengan menambah peserta dari kementerian lain yang terkait, seperti Kementerian Komunikasi dan Informasi serta Kementerian Dalam Negeri dan Luar Negeri.

Lebih jauh, tata kelola data kesehatan perlu diintegrasikan dengan isu kesehatan prioritas di masyarakat yang lebih luas, misalnya untuk tata kelola penanganan penyakit tuberkulosis yang lebih baik. Sistem ini bisa menjadi kunci dalam mewujudkan pemerataan layanan kesehatan di daerah terpencil melalui telemedicine dan pertukaran data yang efisien.

Jalan di depan mungkin penuh tantangan, tetapi upaya ini sangat penting untuk membuka potensi transformasi kesehatan digital yang menyeluruh di Indonesia. Dengan komitmen bersama dari pemerintah, pihak swasta, dan masyarakat, Indonesia dapat membangun sistem tata kelola data kesehatan yang kuat, aman, dan bermanfaat bagi kesehatan publik dan individu.

Tautan artikel:

https://theconversation.com/pentingnya-tata-kelola-data-kesehatan-di-era-ai-indonesia-harus-segera-bangun-layanan-kesehatan-terintegrasi-239383

Pembelajaran Kasus *CrowdStrike*

Arif Perdana

Konteks: Artikel ini saya tulis untuk Kompas di 6 Agustus 2024 berkaitan dengan insiden yang terjadi akibat pemutakhiran perangkat lunak Falcon oleh *CrowdStrike*. Berbeda dengan artikel yang saya tulis di the Jakarta Post di 24 Juli 2024, artikel ini fokus pada dampak insiden dan langkah mitigasi, sementara Artikel di the Jakarta Post menekankan ketahanan digital melalui diversifikasi, strategi global, dan pembelajaran dari negara lain. Insiden ini menyebabkan masalah serius pada berbagai sektor, termasuk kesehatan, perbankan, dan transportasi. Insiden ini mengungkap kerentanan sistem digital dan menyoroti ketergantungan pada infrastruktur TI. Gangguan ini juga menimbulkan dampak ekonomi signifikan dan menunjukkan bahwa alat perlindungan seperti EDR dan XDR dapat menjadi sumber masalah. Ditekankan pentingnya pengujian yang ketat, peluncuran pemutakhiran bertahap, serta transparansi dan kolaborasi dalam industri untuk meningkatkan keamanan dan ketahanan sistem.

Jumat, 19 Juli lalu, dunia dikejutkan oleh gangguan TI global yang disebabkan oleh pemutakhiran perangkat lunak *Falcon* dari *CrowdStrike*[71]. Sebagai salah satu perusahaan keamanan siber terkemuka, *CrowdStrike* tampaknya sengaja merilis pemutakhiran yang mengandung cacat. Pemutakhiran ini bertujuan untuk memperkuat proteksi keamanan, namun justru menyebabkan blue screen of death di banyak sistem yang menggunakan *Microsoft Windows*. Insiden ini mengungkap kerawanan sistem digital modern yang saling terhubung dan menyoroti ketergantungan yang kompleks pada infrastruktur TI.

Sektor-sektor penting seperti kesehatan, perbankan, dan transportasi mengalami gangguan parah. Rumah sakit seperti *Kaiser Permanente, John Muir Health*, dan *Cedars-Sinai Medical Center* di Amerika Serikat (AS), mengalami keterhambatan signifikan dalam mengakses catatan kesehatan elektronik sehingga mengganggu perawatan pasien. Industri keuangan dan perbankan, seperti Charles Schwab dan TD Bank di AS, juga terdampak serius dengan gangguan pada platform perdagangan dan transaksi pelanggan. Akses transportasi di seluruh dunia terganggu. Banyak penerbangan

[71] https://www.crowdstrike.com/platform/

terhambat di bandara internasional, seperti *Schipol, Changi, John F. Kennedy, Newark*, dan *LaGuardia*. Kejadian ini menyebabkan paralisis operasional dan dampak ekonomi yang signifikan. Dampaknya juga menyebar pada rantai logistik dan pasokan, memengaruhi perusahaan seperti Amazon yang mengalami gangguan di operasi gudangnya karena masalah dengan aplikasi internal yang menggunakan *Microsoft Windows*. Gangguan ini agaknya merupakan satu yang terbesar dalam sejarah TI. Ini mengakibatkan harga saham CrowdStrike turun lebih dari 14 persen.

Antisipasi dan Penanggulangan

Sistem *endpoint detection and response* (EDR)[72] dan *extended detection and response* (XDR), seperti CrowdStrike Falcon, dirancang untuk memperkuat keamanan dengan memantau dan merespons ancaman jaringan. Namun, kejadian ini menyoroti paradoks bahwa alat perlindungan itu sendiri tidak kebal berkontribusi pada kegagalan sistem. Bayangkan EDR dan XDR sebagai penjaga keamanan khusus untuk sistem komputer. Mereka memantau aktivitas sistem untuk tanda-tanda intrusi digital, seperti upaya *malware* merusak sistem. Begitu mendeteksi perilaku mencurigakan, mereka segera menetralisisasi ancaman untuk menjaga integritas sistem. Dalam kasus Falcon, instruksi yang salah membuat EDR dan XDR keliru memblokir aktivitas yang valid sehingga menyegel sistem dari fungsi-fungsi penting.

Kejadian ini menggarisbawahi risiko yang melekat pada alat perlindungan yang, secara tak sengaja, bisa menyebabkan kerusakan. Analogi nya, sistem keamanan yang dirancang untuk mengamankan sebuah gedung, tetapi kemudian secara tidak sengaja mengunci semua pintu, sehingga penghuninya tidak bisa masuk. Akibatnya, gangguan luas di berbagai industri, dengan banyak komputer menjadi lumpuh. Kejadian ini memperkuat tanggung jawab bersama para pemain kunci di industri teknologi, seperti *Microsoft* dan *CrowdStrike*, untuk memperkuat ketahanan sistem dan mengurangi risiko. Untuk meningkatkan strategi digital, para pemimpin industri harus meutamakan

[72] https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/

pengujian dan validasi yang ketat terhadap pemutakhiran perangkat lunak, terutama yang terintegrasi dalam sistem operasi.

Perlu strategi peluncuran pemutakhiran perangkat lunak secara bertahap. Pemutakhiran ini seharusnya diterapkan terbatas dulu pada kelompok pengguna terkendali untuk memverifikasi stabilitasnya sebelum rilis lebih luas. Langkah-langkah ini juga harus didukung dengan pemantauan secara real-time. Penting untuk mendeteksi anomali secara dini. Selain itu, kemampuan pengembalian sistem ke versi sebelumnya (rollback) yang terukur sangat penting. Ini memungkinkan pembalikan cepat terhadap pemutakhiran yang bermasalah, menjaga keandalan perangkat lunak, dan mempertahankan kepercayaan di antara konsumen dan bisnis.

Komunikasi yang transparan dan tepat waktu selama kejadian semacam ini juga krusial guna memastikan semua pihak terinformasi tentang masalah, upaya penyelesaian, dan langkah pencegahan yang diambil. Kejadian ini juga mendorong kolaborasi antara industri. Perusahaan-perusahaan teknologi seharusnya memiliki protokol standar terkait pengujian, pemutakhiran perangkat lunak, dan penilaian keamanan, terutama untuk perangkat lunak yang kritis bagi integritas sistem. Dengan berbagi wawasan tentang kerentanan dan strategi pertahanan, mereka bisa secara kolektif memperkuat posisi keamanan dalam lanskap digital. Sentralisasi kekuatan di antara beberapa raksasa teknologi memiliki potensi risiko. Pengembangan sistem dan solusi terdesentralisasi bisa mengurangi ketergantungan pada entitas tunggal. Pendekatan ini tak hanya mengurangi risiko, tetapi juga mendorong inovasi dan ketahanan di sektor teknologi.

Transparansi dan Desentralisasi

Saat ekosistem digital berkembang dan saling terhubung, kejadian di atas menunjukkan kian rentannya infrastruktur teknologi global sehingga muncul tuntutan transparansi dan akuntabilitas lebih besar terhadap perusahaan teknologi. Pemerintah dan lembaga regulator mungkin akan menetapkan regulasi yang lebih ketat terhadap para raksasa teknologi sebagai respons terhadap tuntutan publik. Termasuk melibatkan

pengujian pemutakhiran perangkat lunak yang lebih ketat, protokol keamanan standar, dan pelaporan kejadian yang transparan untuk mengurangi risiko sistemik.

Advokasi untuk sistem dan solusi terdesentralisasi yang mendistribusikan risiko lebih merata dan mengurangi ketergantungan pada entitas tunggal juga meningkat. Hal ini akan mendorong raksasa teknologi membangun kolaborasi lebih besar dengan perusahaan kecil dan lembaga pemerintah. Frekuensi dan kompleksitas ancaman siber yang meningkat juga akan mendorong inovasi dalam keamanan siber. Integrasi AI yang lebih baik untuk mendeteksi ancaman dan merespons kejadian akan kian berkembang. Kejadian seperti ini menekankan perlunya pendekatan proaktif terhadap inovasi. Mengantisipasi gangguan potensial dan mengintegrasikan langkah-langkah pencegahan ke dalam pengembangan teknologi menjadi sangat krusial.

Tautan artikel:

https://www.kompas.id/baca/opini/2024/08/05/pembelajaran-kasus-crowdstrike-1

Strategi Peningkatan Keamanan Siber

Arif Perdana

Konteks: Artikel ini pertama kali ditulis di Koran Tempo di 8 Agustus 2024. Artikel ini memiliki cakupan strategi yang lebih luas dibandingkan dengan artikel yang terbit di the Jakarta Post tanggal 17 Juli 2024 tentang "Strategi Keamanan Siber". Artikel ini menyoroti perlunya perubahan paradigma dari respons reaktif ke pencegahan proaktif, serta integrasi DevSecOps untuk keamanan di seluruh siklus hidup perangkat lunak. Dua artikel tentang keamanan siber yang saya tulis di Tempo dan the Jakarta Post ini sepakat bahwa rencana yang kuat diperlukan untuk meminimalkan dampak serangan siber dan meningkatkan ketahanan infrastruktur digital nasional.

Di era digital yang semakin berkembang, Indonesia menghadapi tantangan besar dalam mengelola dan melindungi data pribadi warganya. Serangan siber yang terus meningkat tidak hanya mengungkap kelemahan dalam infrastruktur digital nasional, tetapi juga menyoroti kebutuhan mendesak untuk strategi keamanan siber yang lebih efektif dan bertanggung jawab. Kejadian baru-baru ini penuh dengan contoh kerentanan yang signifikan berkaitan dengan data dan keamanan siber di Indonesia. Misalnya, serangan *ransomware* pada PDN-S[73]. Selain itu, data dari Badan Intelijen Strategis mengalami peretasan. Kebocoran data juga terjadi pada Sistem Identifikasi Sidik Jari Otomatis milik Kepolisian Indonesia. Kejadian ini membuka mata akan pentingnya PDP dan kecepatan respons terhadap insiden keamanan siber.

Pentingnya Perencanaan dalam Keamanan Siber

Di Indonesia, ketimpangan antara perkembangan teknologi digital dan keamanan siber menciptakan risiko yang terus-menerus. Banyak lembaga, termasuk pemerintah, seringkali gagal mengadopsi langkah-langkah pelindungan data yang memadai. Peretasan PDNS hanya merupakan salah satu contoh bagaimana data sensitif dapat

[73] https://tekno.kompas.com/read/2024/07/10/12350077/kronologi-serangan-ransomware-ke-pdn-dan-penanganannya-yang-tak-kunjung-usai

terancam tanpa sistem pengamanan yang kuat. Pendekatan terfragmentasi terhadap keamanan data, yang sering kali hanya sebagai reaksi terhadap insiden, tidak cukup untuk menangani tantangan yang dihadapi oleh negara dalam menjaga keamanan data warganya. Harus ada perubahan paradigma dari sekadar menanggapi insiden menjadi proaktif dalam mencegah mereka.

Dalam menghadapi ancaman siber yang kian meningkat, langkah pertama yang vital adalah IRP. IRP merupakan metode terstruktur untuk mendeteksi, menganalisis, dan menanggapi kejadian siber dengan cepat dan efektif. Dengan IRP yang solid, sebuah organisasi bisa meminimalkan kerugian dan mempercepat pemulihan, sehingga mengurangi waktu dan biaya yang terlibat dalam mengatasi dampak insiden tersebut. Selanjutnya, ada DRP. DRP fokus pada cara cepat mengembalikan operasi setelah terjadinya gangguan besar, termasuk kehilangan data atau kerusakan pada TI. Dengan DRP yang efisien, organisasi tidak hanya bisa segera kembali beroperasi, tapi juga meminimalisir dampak negatif yang mungkin terjadi pada reputasi dan keberlangsungan bisnis mereka. Untuk jangka panjang, BCP bukan hanya tentang pemulihan; ini adalah strategi komprehensif yang meliputi komunikasi dengan semua pemangku kepentingan dan perencanaan operasional setelah insiden. BCP menjamin bahwa bisnis dapat terus berjalan bahkan setelah mengalami gangguan besar, memastikan bahwa operasi bisnis tidak hanya bertahan, tetapi juga berkembang pasca-krisis.

Mengintegrasikan ketiga strategi ini dalam pendekatan *Development, Security, and Operations* (*DevSecOps*) memastikan bahwa keamanan menjadi bagian tak terpisahkan dari seluruh siklus hidup pengembangan perangkat lunak[74]. Ini tidak hanya meningkatkan kolaborasi antar tim tetapi juga menciptakan solusi yang lebih aman dan andal. Dengan demikian, organisasi tidak hanya siap menghadapi serangan, tetapi juga membangun kepercayaan dan keandalan dalam layanan mereka.

Langkah-Langkah Strategis untuk Peningkatan Keamanan Siber

[74] https://www.redhat.com/en/topics/devops/what-is-devsecops

Untuk mengatasi masalah ini, Indonesia memerlukan strategi keamanan siber yang komprehensif, meliputi beberapa aspek kritis:

Pertama. Implementasi regulasi seperti UU PDP harus ditegakkan dengan ketat. Pemerintah perlu memastikan bahwa semua entitas, baik di sektor publik maupun swasta, mematuhi standar yang telah ditetapkan untuk pelindungan data.

Kedua. Meningkatkan infrastruktur keamanan siber nasional adalah penting. Hal ini termasuk pembaharuan teknologi yang usang, penggunaan perangkat lunak keamanan yang lebih baik, dan pembangunan kapasitas bagi para profesional keamanan siber di dalam negeri.

Ketiga. Peningkatan kesadaran publik mengenai risiko keamanan siber dan cara-cara melindungi data pribadi merupakan langkah vital. Kampanye edukasi harus menyasar semua lapisan masyarakat dan menyampaikan informasi yang mudah dipahami tentang pentingnya keamanan data.

Keempat. Implementasi IRP, DRP dan BCP yang optimal. Membangun sebuah tim tanggap cepat nasional untuk insiden keamanan siber yang dapat beroperasi 24/7 adalah penting. Tim ini harus memiliki kemampuan untuk dengan cepat mengidentifikasi, menanggapi, dan memulihkan sistem dari serangan siber.

Kelima. Mengingat sifat transnasional dari banyak serangan siber, Indonesia perlu bekerja sama lebih dekat dengan negara-negara lain dan organisasi internasional untuk memerangi ancaman keamanan siber. Pertukaran informasi tentang ancaman dan praktik terbaik dapat memperkuat pertahanan nasional.

Keenam. Lembaga pemerintah harus memimpin dengan contoh dalam transparansi dan akuntabilitas dalam pengelolaan data pribadi. Kegagalan dalam menjaga data harus diikuti dengan tanggung jawab jelas dan komunikasi yang terbuka kepada publik.

Tantangan keamanan siber di Indonesia tidak akan hilang dalam waktu dekat, tetapi dengan strategi yang tepat, negara bisa memperkuat pertahanannya terhadap serangan siber. Dalam ranah keamanan siber, setiap organisasi berpotensi menghadapi serangan. Kesiapan dan perencanaan yang matang menjadi kunci bagi organisasi dalam mengantisipasi serangan siber yang mungkin terjadi kapan saja. Inisiatif pemerintah

yang efektif, dikombinasikan dengan partisipasi aktif dari sektor swasta dan masyarakat sipil, akan menjadi kunci dalam menciptakan lingkungan digital yang lebih aman untuk semua warga Indonesia. Dengan langkah-langkah ini, kita dapat mengharapkan peningkatan keamanan data di Indonesia, yang tidak hanya akan melindungi privasi individu tetapi juga akan mendukung pertumbuhan ekonomi yang sehat dan kepercayaan publik dalam teknologi digital.

Tautan artikel:

https://koran.tempo.co/read/opini/489465/strategi-keamanan-siber

FraudGPT dan AI Jahat Lainnya Mengancam Aktifitas Online. Apa yang Bisa Kita Lakukan?

Arif Perdana, Bayu Anggorojati, Derry Wijaya

Konteks: Artikel ini pertama kali di The Conversation Australia 24 Juli 2024. Artikel ini kemudian direplikasi oleh Monash Lens, dan juga dikutip oleh Koran Tempo. Ide dari artikel ini muncul ketika saya membaca artikel di ArXiv yang berjudul "*Malla: Demystifying Real-world Large Language Model Integrated Malicious Services*". Artikel ini mengungkapkan eksploitasi model bahasa besar (LLM) untuk layanan berbahaya (disebut "Malla"), yang meningkat pesat di *dark web*. Saya kemudian berdiskusi dengan kolega dari program study Cybersecurity dan rekan yang menekuni tentang teknis LLM. Di artikel ini, kami menjelaskan ancaman baru dalam keamanan siber akibat munculnya "dark LLM" yang digunakan untuk aktivitas kriminal, seperti phishing dan pembuatan *malware*. AI generatif meningkatkan kompleksitas kejahatan siber. Di artikel ini kami juga memaparkan rekomendasi yang mungkin berguna untuk menghadapi LLM gelap ini.

Internet, sumber daya yang luas dan sangat diperlukan bagi masyarakat modern, memiliki sisi gelap yang memungkinkan aktivitas jahat berkembang. Dari pencurian identitas hingga serangan *malware* canggih, penjahat siber terus menciptakan metode penipuan baru. AI generatif yang tersedia luas kini telah menambahkan lapisan kompleksitas baru pada lanskap keamanan siber. Setiap orang kini memiliki tugas menjaga keamanan online lebih penting dari sebelumnya.

Kebangkitan Dark LLM

Salah satu adaptasi AI saat ini yang paling mengerikan adalah penciptaan *dark* LLM[75]. Versi tak tersensor dari sistem AI sehari-hari seperti *ChatGPT* ini direkayasa ulang untuk aktivitas kriminal. Mereka beroperasi tanpa batasan etika dan dengan ketepatan serta kecepatan yang mengkhawatirkan. Penjahat siber mengerahkan *dark* LLM untuk mengotomatisasi dan meningkatkan kampanye phishing, membuat *malware* canggih, dan menghasilkan konten penipuan.

[75] https://github.com/cybershujin/Threat-Actors-use-of-Artifical-Intelligence/blob/main/Dark%20LLMs%20and%20Malicious%20AIs.MD

Untuk mencapai ini, mereka melakukan "*jailbreaking*" LLM – menggunakan *prompt* untuk membuat model melewati pengaman dan filter bawaan. Misalnya, *FraudGPT* bisa menulis kode berbahaya, membuat halaman *phishing*, dan menghasilkan *malware* yang tidak terdeteksi[76]. Perangkat ini mampu mengoordinasikan berbagai kejahatan siber, mulai dari penipuan kartu kredit hingga peniruan digital. *FraudGPT* diiklankan di *dark web* dan aplikasi pesan terenkripsi Telegram. Pembuat *FraudGPT* ini secara terbuka memasarkan kemampuannya dengan menekankan fokus kriminal model tersebut. Versi lain, *WormGPT*, menghasilkan email *phishing* yang meyakinkan yang dapat menipu bahkan pengguna yang waspada[77]. Berdasarkan model *GPT-J*, *WormGPT* juga digunakan untuk membuat *malware* dan meluncurkan serangan "kompromi email bisnis" – phishing yang ditargetkan pada organisasi tertentu.

Apa yang Bisa Kita Lakukan untuk Melindungi Diri?

Terlepas dari ancaman yang mengintai, ada sisi positifnya. Seiring berkembangnya tantangan, begitu pula cara kita mempertahankan diri terhadapnya. Alat deteksi ancaman berbasis AI dapat memantau *malware* dan merespons serangan siber dengan lebih efektif. Namun, manusia perlu tetap terlibat untuk mengawasi bagaimana alat-alat ini merespons, menentukan tindakan apa yang mereka ambil, dan memastikan apakah ada kerentanan yang perlu diperbaiki.

Anda mungkin pernah mendengar bahwa memperbarui perangkat lunak Anda sangat penting untuk keamanan. Aktifitas ini mungkin terasa merepotkan, tetapi ini merupakan strategi pertahanan yang penting. Pembaruan perangkat lunak dilakukan untuk menambal kerentanan yang mungkin bisa dieksploitasi oleh penjahat siber. Apakah file dan data Anda secara teratur dicadangkan di tempat penyimpanan lainnya? Ini bukan hanya tentang menyimpan file jika terjadi kegagalan sistem. Pencadangan rutin adalah strategi pelindungan mendasar. Anda dapat mengklaim kembali kehidupan digital Anda tanpa menyerah pada pemerasan jika Anda menjadi target serangan *ransomware*

[76] https://secureops.com/blog/ai-attacks-fraudgpt/

[77] https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/

– ketika penjahat mengunci data Anda dan meminta pembayaran tebusan sebelum mereka melepaskannya.

Penjahat siber yang mengirim pesan *phishing* dapat meninggalkan petunjuk seperti tata bahasa yang buruk, sapaan umum, alamat email yang mencurigakan, permintaan yang terlalu mendesak, atau tautan yang mencurigakan. Mengembangkan mata untuk tanda-tanda ini sama pentingnya dengan mengunci pintu Anda di malam hari. Jika Anda belum menggunakan kata sandi yang kuat dan unik serta autentikasi multi-faktor, sekarang saatnya untuk melakukannya. Kombinasi ini melipatgandakan keamanan Anda, membuatnya jauh lebih sulit bagi penjahat untuk mengakses akun Anda.

Apa yang Bisa Kita Harapkan di Masa Depan?

Keberadaan online kita akan terus terkait dengan teknologi baru seperti AI. Kita dapat mengharapkan alat kejahatan siber yang lebih canggih akan muncul juga. AI jahat akan meningkatkan phishing, membuat *malware* canggih, dan meningkatkan penambangan data untuk serangan yang ditargetkan. Alat peretas berbasis AI akan tersedia secara luas dan dapat disesuaikan. Sebagai respons, keamanan siber juga harus beradaptasi. Kita dapat mengharapkan perburuan ancaman otomatis, enkripsi tahan kuantum, alat AI yang membantu menjaga privasi, peraturan yang lebih ketat, dan kerja sama internasional.

Peran Peraturan Pemerintah

Peraturan pemerintah yang lebih ketat tentang AI adalah salah satu cara untuk melawan ancaman canggih ini. Ini akan melibatkan mandat pengembangan dan penerapan teknologi AI yang etis, memastikan mereka dilengkapi dengan fitur keamanan yang kuat dan mematuhi standar yang ketat.

Selain peraturan yang lebih ketat, kita juga perlu meningkatkan bagaimana organisasi merespons insiden siber dan mekanisme apa yang ada untuk pelaporan wajib dan pengungkapan publik. Dengan mewajibkan perusahaan untuk segera melaporkan

insiden siber, pihak berwenang dapat bertindak cepat. Mereka dapat memobilisasi sumber daya untuk mengatasi pelanggaran sebelum berkembang menjadi krisis besar. Pendekatan proaktif ini dapat secara signifikan mengurangi dampak serangan siber, menjaga kepercayaan publik dan integritas perusahaan. Selanjutnya, kejahatan siber tidak mengenal batas. Di era kejahatan siber yang didukung AI, kolaborasi internasional sangat penting. Kerja sama global yang efektif dapat menyederhanakan bagaimana otoritas melacak dan menuntut penjahat siber, menciptakan front bersatu melawan ancaman siber.

Seiring proliferasi *malware* bertenaga AI, kita berada di persimpangan kritis dalam perjalanan teknologi global: kita perlu menyeimbangkan inovasi (alat AI baru, fitur baru, lebih banyak data) dengan keamanan dan privasi. Secara keseluruhan, sebaiknya bersikap proaktif tentang keamanan online Anda sendiri. Dengan begitu Anda dapat selalu selangkah di depan dalam medan pertempuran siber yang terus berkembang.

Tautan artikel:

https://theconversation.com/fraudgpt-and-other-malicious-ais-are-the-new-frontier-of-online-threats-what-can-we-do-234820

https://lens.monash.edu/@bayu-anggorojati/2024/09/25/1386882/fraudgpt-and-other-malicious-ais-are-the-new-frontier-of-online-threats-what-can-we-do

Gangguan Teknologi Informasi dan Ketahanan Digital

Arif Perdana, Muhammad Erza Aminanto, Ika Idris

Konteks: Artikel ini pertama kali terbit di the Jakarta Post, tanggal 24 Juli 2024. Artikel ini menyoroti pentingnya ketahanan digital dalam menghadapi gangguan TI global akibat pemutakhiran perangkat lunak CrowdStrike yang bermasalah. Dengan fokus pada diversifikasi sumber daya TI, strategi multi-cloud, dan pengurangan ketergantungan pada satu penyedia, artikel ini menekankan perlunya sistem adaptif dan proaktif dalam menangani risiko. Contoh negara seperti China, Rusia, Estonia, dan Taiwan digunakan untuk menunjukkan strategi efektif dalam membangun ketahanan dan respons terhadap ancaman siber.

Gangguan TI global yang disebabkan oleh pembaruan yang cacat dari *CrowdStrike* minggu lalu menyoroti ketergantungan mendalam kita pada sistem digital. Insiden ini mempengaruhi layanan di seluruh dunia, termasuk instansi pemerintah, maskapai penerbangan, bank, dan rumah sakit, menunjukkan kerapuhan ekosistem TI kita. Seiring ekonomi dan sistem keamanan nasional menjadi semakin digital, konsekuensi dari kegagalan semacam itu menjadi semakin parah. Peristiwa ini mengingatkan kita akan perlunya ketahanan digital yang kuat untuk mencegah dan mengurangi dampak insiden semacam itu. Hal ini juga menggarisbawahi pentingnya mempertahankan infrastruktur TI yang beragam dan mudah beradaptasi yang dapat bertahan dan pulih dari gangguan.

Gangguan *CrowdStrike* telah mengajarkan kita pelajaran yang jelas: Kita harus memiliki ketahanan digital dan lebih siap menghadapi kegagalan TI. Sifat saling terhubung dari sistem TI modern berarti satu kesalahan dapat menyebabkan gangguan di banyak sektor. Gangguan tersebut menunjukkan bagaimana insiden semacam itu dapat menyebabkan kekacauan, mempengaruhi layanan penting dan mengurangi kepercayaan pada sistem digital. Persiapan berarti membangun sistem yang lebih tangguh dan memiliki rencana darurat yang siap.

Organisasi harus mendiversifikasi sumber daya TI mereka, menghindari ketergantungan pada satu penyedia, dan menyiapkan sistem cadangan yang kuat. Pengujian stres secara teratur dan pemantauan proaktif dapat mengidentifikasi

kerentanan sebelum menyebabkan kegagalan. Melatih staf untuk menangani masalah TI dan menjaga saluran komunikasi yang jelas selama gangguan juga sangat penting. Langkah-langkah ini dapat membantu mengurangi dampak insiden di masa depan.

Ketahanan digital adalah kemampuan individu, organisasi, dan masyarakat untuk mengantisipasi, mengelola, dan pulih dari gangguan digital dengan cepat, memastikan operasi yang berkelanjutan dan beradaptasi dengan tantangan masa depan untuk meningkatkan keamanan dan efektivitas digital. Hal ini penting untuk mengurangi dampak gangguan TI dan memastikan pemulihan yang cepat. Sistem harus mampu bertahan dan beradaptasi dengan kegagalan yang tidak terduga. Ini termasuk merancang infrastruktur TI dengan redundansi dan mekanisme failover yang memungkinkan operasi terus berjalan lancar bahkan ketika sistem utama gagal. Menerapkan sistem pemantauan dan respons otomatis dapat membantu mendeteksi dan mengatasi masalah sebelum memburuk.

Ketahanan digital juga membutuhkan pergeseran budaya dalam organisasi, menekankan pentingnya keamanan siber dan terus meningkatkan praktik TI. Organisasi dapat lebih baik melindungi diri dari gangguan TI dengan mendorong pendekatan proaktif dalam mengelola risiko digital. Mencapai ketahanan digital menjadi tantangan ketika perusahaan sangat bergantung pada raksasa teknologi seperti *Microsoft, Amazon*, atau *Google*. Perusahaan-perusahaan ini menyediakan infrastruktur kritis, layanan cloud, dan perangkat lunak yang banyak digunakan oleh bisnis.

Insiden *CrowdStrike* menunjukkan bagaimana masalah dengan layanan yang banyak digunakan dapat memiliki efek global. Untuk mengurangi hal ini, bisnis harus mengadopsi strategi multi-cloud, mendistribusikan infrastruktur TI mereka di beberapa penyedia layanan cloud. Diversifikasi ini dapat mengurangi risiko satu titik kegagalan. Perusahaan juga harus terlibat dalam dialog rutin dengan penyedia teknologi mereka untuk memastikan mereka memiliki perjanjian layanan dan rencana respons insiden yang kuat. Aspek lain dari ketahanan digital adalah memastikan bahwa tim TI internal dilengkapi untuk menangani gangguan. Ini termasuk memiliki protokol yang jelas untuk respons insiden, latihan rutin untuk mensimulasikan gangguan, dan memelihara

dokumentasi terkini tentang sistem TI. Dengan membangun kemampuan internal yang kuat, bisnis dapat merespons lebih efektif ketika layanan eksternal gagal.

Sementara gangguan TI mengganggu operasi maskapai penerbangan dan berbagai sektor di banyak negara, China dan Rusia menghindari dampak besar. Ketahanan ini berasal dari dorongan mereka untuk kemandirian teknologi. Upaya China untuk mengembangkan solusi teknologinya sendiri telah mengurangi ketergantungannya pada perangkat lunak dan layanan TI asing. Inisiatif ini adalah bagian dari strategi yang lebih luas untuk meningkatkan keamanan siber dan memastikan stabilitas operasional selama masalah TI global. Misalnya, bandara-bandara di Beijing terus berfungsi normal, karena sistem mereka terisolasi dari gangguan internasional. Media pemerintah China mengkonfirmasi bahwa penerbangan di bandara-bandara ini tidak terpengaruh oleh kegagalan sistem informasi internasional.

Demikian pula, Rusia telah meminimalkan ketergantungannya pada teknologi asing dengan mengembangkan dan menggunakan perangkat lunak dan solusi TI buatan dalam negeri. Strategi ini melindungi dari gangguan teknologi global dan mengurangi potensi risiko geopolitik. Entitas besar Rusia seperti VTB dan Sberbank telah mengganti perangkat lunak impor dengan alternatif lokal. VTB melaporkan bahwa 85 persen sistem aplikasinya bebas dari solusi asing, memastikan operasi mereka tetap tidak terpengaruh oleh gangguan tersebut.

Ketahanan China dan Rusia menggarisbawahi pentingnya kemandirian teknologi. Dengan berinvestasi dan mengembangkan infrastruktur TI lokal, negara-negara ini mempertahankan operasi normal dan menghindari gangguan luas yang terlihat di tempat lain. Meskipun gangguan TI pada 19 Juli bukan serangan siber, ketahanan digital sangat penting untuk menangani kegagalan infrastruktur TI apa pun, termasuk insiden keamanan siber. Estonia dan Taiwan menawarkan pelajaran berharga dalam ketahanan digital melalui respons mereka terhadap serangan keamanan siber.

Estonia, setelah serangan siber besar pada tahun 2007, mengembangkan pendekatan komprehensif terhadap keamanan siber. Setelah serangan siber 2007, Estonia mengutamakan penguatan pertahanan sibernya. Inisiatif seperti pembentukan Unit Pertahanan Siber berbasis sukarelawan, yang berkolaborasi dengan sektor swasta,

mencontohkan strategi komprehensif negara untuk memperkuat keamanan nasional. Upaya-upaya ini, ditambah dengan pembentukan pusat pertahanan siber NATO di Tallinn dan investasi signifikan dalam pendidikan, telah memposisikan Estonia sebagai garda depan ketahanan digital global. Inisiatif yang menonjol adalah "kedutaan data" Estonia di Luxemburg, pusat data di luar lokasi yang mengamankan data nasional kritis di luar perbatasannya. Pendekatan inovatif ini tidak hanya melindungi informasi tetapi juga memastikan kelangsungan operasi pemerintah selama ancaman siber atau bencana fisik yang parah, menyoroti peran penting kerjasama internasional dan pemikiran ke depan dalam keamanan siber.

Contoh lainnya, Taiwan, menghadapi ancaman siber yang sering dari lawan geopolitik, telah menerapkan langkah-langkah keamanan siber yang kuat seperti sistem *T-Road* dan Arsitektur *Zero Trust*. Sistem T-Road memastikan transfer data yang aman dalam sektor publik. Arsitektur Zero Trust berfokus pada autentikasi berkelanjutan pengguna dan perangkat, mengurangi ancaman internal. Penekanan Taiwan pada pendidikan keamanan siber dan kesadaran publik telah memberdayakan warganya untuk berperan aktif dalam menjaga keamanan digital.

Baik Estonia maupun Taiwan menyoroti pentingnya pendidikan dini dalam keamanan siber dan strategi komprehensif yang melibatkan semua sektor masyarakat. Pengalaman mereka menunjukkan bahwa infrastruktur digital yang tangguh membutuhkan kemajuan teknologi dan populasi yang well-informed. Unit Pertahanan Siber Estonia dan pendekatan keamanan siber berlapis Taiwan mendemonstrasikan bagaimana mendiversifikasi solusi teknologi dan mendorong keahlian lokal dapat meningkatkan ketahanan. Dengan membangun kemampuan nasional yang kuat dan mendorong kolaborasi publik-swasta, negara-negara ini telah mengembangkan pertahanan yang kuat terhadap ancaman siber.

Untuk meningkatkan ketahanan digital, Indonesia harus memprioritaskan sistem TI yang kuat dan mudah beradaptasi. Ini melibatkan diversifikasi sumber daya TI, menerapkan mekanisme redundansi dan *failover*, dan berinvestasi dalam teknologi pemantauan canggih. Tes stres dan audit rutin dapat membantu mengidentifikasi dan mengatasi kerentanan. Memupuk budaya kesadaran keamanan siber dan perbaikan

berkelanjutan sangat penting. Belajar dari Estonia dan Taiwan, kita dapat mengembangkan strategi efektif untuk melindungi dan pulih dari gangguan TI. Membangun kemampuan TI internal yang kuat, mengurangi ketergantungan pada penyedia teknologi tunggal, dan terlibat dalam manajemen risiko proaktif adalah langkah-langkah penting untuk masa depan digital yang tangguh.

Tautan artikel:

https://www.thejakartapost.com/opinion/2024/07/24/the-massive-it-outage-and-digital-resilience.html

Strategi Ketahanan Keamanan Siber yang Efektif

Arif Perdana, Muhammad Erza Aminanto, Ika Idris

Konteks: Artikel ini pertama kali terbit di the Jakarta Post, tanggal 17 Juli 2024. Tulisan ini menanggapi kejadian lumpuhnya PDN-S yang mengakibatkan terganggunya layanan publik di sejumlah instansi pemerintahan. Bersama dengan kolega dari kebijakan publik dan keamanan siber di Monash University, kami menggarisbawahi pentingnya perencanaan yang baik untuk memitigasi serangan siber yang menganggu infrastruktur digital.

Serangan *ransomware* baru-baru ini melumpuhkan PDN-S dan membuat layanan publik terintegrasi lumpuh. Di antara sekitar 200 instansi yang terdampak adalah layanan imigrasi. Insiden terbaru ini, serta berbagai serangan siber dan pelanggaran data sebelumnya, hanya mengungkapkan kurangnya strategi mitigasi krisis yang dikomunikasikan dengan baik dan kuat dalam pemerintahan. Peristiwa ini sekali lagi menekankan bahwa di era digital, sangat penting untuk memiliki percenanaan yang baik seperti IRP, DRP, dan BCP. Ketiga elemen ini saling terkait dan penting untuk memastikan bahwa lembaga dapat bertahan dan pulih dari serangan siber. Langkah pertama ketika terjadi insiden siber adalah menerapkan IRP. Ini memastikan bahwa organisasi memiliki prosedur terstruktur untuk dengan cepat mendeteksi, menganalisis, dan merespons insiden. Langkah-langkah dalam IRP meliputi identifikasi dan analisis insiden, pengendalian dampak, pemulihan, dan evaluasi pasca-insiden. IRP yang dikembangkan dan dikomunikasikan dengan baik dapat mengurangi kerugian organisasi dan mempercepat pemulihan dari serangan siber.

DRP berfokus pada pemulihan operasional setelah insiden yang sangat mengganggu seperti serangan *ransomware*, dan mencakup pemulihan data dan sistem TI, pengalihan operasi ke lokasi cadangan, serta langkah-langkah untuk memastikan kelangsungan layanan kritis. DRP yang efektif memungkinkan organisasi untuk melanjutkan operasi segera setelah insiden, sehingga mengurangi dampak negatif terhadap operasi dan reputasi. Setelah menyelesaikan langkah-langkah DRP, diharapkan perusahaan atau organisasi yang terkena dampak dapat melanjutkan operasi pada status operasional minimum atau standar dalam keadaan darurat. Sementara itu, BCP

ditujukan untuk jangka panjang, dan mencakup strategi untuk mempertahankan kelangsungan bisnis setelah insiden. BCP yang komprehensif mencakup komunikasi pemangku kepentingan, manajemen sumber daya, dan strategi operasional. Dengan BCP yang baik, organisasi dapat mempertahankan tingkat operasi sebelumnya setelah gangguan yang signifikan.

IRP, DRP, dan BCP adalah bagian dari pengembangan, keamanan, dan operasi (*DevSecOps*), sebuah pendekatan yang mengintegrasikan praktik keamanan di seluruh siklus hidup pengembangan perangkat lunak, mulai dari tahap perencanaan dan pengkodean hingga penerapan operasional skala besar. Tujuannya adalah untuk meningkatkan kolaborasi antara tim pengembangan, keamanan, dan operasi untuk menghasilkan perangkat lunak yang lebih aman dan andal. Komponen keamanan ini harus dimasukkan dalam *DevSecOps* karena tidak bisa bersifat insidental atau diaktifkan hanya ketika terjadi insiden. Pertimbangan keamanan harus dimasukkan dalam proses perencanaan untuk meminimalkan risiko.

PDN, instansi pemerintah, perusahaan, dan organisasi dengan sistem data terintegrasi harus menerapkan IRP, DRP, dan BCP secara komprehensif, kuat, dan terintegrasi untuk menghadapi ancaman siber yang semakin canggih. Berikut adalah langkah-langkah untuk mempersiapkannya.

Pertama adalah identifikasi dan prioritas risiko. Setiap organisasi harus melakukan analisis risiko untuk mengidentifikasi aset penting yang rentan terhadap serangan siber. Organisasi dapat menetapkan prioritas dalam merencanakan tindakan respons dan pemulihan dengan memahami risiko dan dampak potensialnya. Biasanya, jumlah risiko potensial sangat besar, sehingga tidak mungkin memitigasi semua risiko. Oleh karena itu, menentukan tingkat prioritas setiap risiko sangat penting. Empat langkah mitigasi umum adalah menerima risiko apa adanya, mengurangi atau meminimalkan risiko, mentransfer manajemen risiko ke pihak ketiga, dan menolak risiko sama sekali. Langkah-langkah mitigasi ini harus selaras dengan kebijakan selera risiko perusahaan atau organisasi. Penting untuk menyadari bahwa meskipun banyak risiko dimitigasi, risiko baru akan selalu muncul, sehingga diperlukan identifikasi dan analisis risiko secara berkala.

Kedua adalah membentuk tim respons insiden. Terdiri dari ahli teknis, hukum, manajemen, dan komunikasi, tim ini bertanggung jawab untuk merespons insiden dengan cepat dan koheren. Komunikasi yang efektif di antara anggota tim sangat penting untuk memastikan respons yang terkoordinasi. Dalam konteks insiden di instansi pemerintah, hotline 24 jam harus tersedia selama periode penanganan.

Ketiga adalah mengembangkan dan menguji rencana. IRP, DRP, dan BCP harus dikembangkan berdasarkan skenario insiden yang mungkin terjadi. Pengujian rutin melalui simulasi insiden membantu memastikan bahwa rencana-rencana ini efektif dan siap untuk situasi nyata. Pembelajaran dari pengujian harus digunakan untuk meningkatkan rencana-rencana ini.

Keempat adalah pedoman yang jelas dan dapat dipahami. Organisasi sering menyusun IRP, DRP, dan BCP yang rumit dan kompleks. Dalam krisis, tidak ada waktu untuk mempelajari semuanya, karena rencana harus segera dilaksanakan. Oleh karena itu, organisasi harus membuat pedoman yang sederhana yang dapat dipahami oleh semua orang. Insiden seperti serangan *ransomware* pada PDN sementara menunjukkan bahwa semua orang, dari pejabat tinggi hingga petugas layanan, terlibat dalam penanganan krisis, sehingga bahasa dalam pedoman harus dapat dipahami oleh semua pihak.

Kelima adalah pelatihan dan kesadaran. Semua karyawan harus dilatih tentang peran dan tanggung jawab mereka dalam insiden siber. Meningkatkan kesadaran tentang ancaman siber dan langkah-langkah mitigasi juga diperlukan untuk mengurangi kesalahan manusia yang dapat memicu insiden.

Implementasi IRP, DRP, dan BCP yang efektif dapat memperpendek waktu yang diperlukan untuk memulihkan operasi setelah serangan siber. Ini membantu mengurangi kerugian finansial akibat downtime dan kehilangan data. Parameter waktu umum yang digunakan dalam DRP meliputi Recovery Time Objective (RTO) dan Maximum Tolerable Downtime (MTD). RTO mengukur waktu yang diperlukan untuk memulai operasi darurat, sedangkan MTD mengukur total waktu yang diperlukan untuk operasi normal sepenuhnya pulih.

Menurut laporan IBM, pelanggaran data pada tahun 2023 rata-rata menelan biaya US$4,45 juta. AI dan otomatisasi keamanan dapat menghemat $1,76 juta dan memperpendek waktu respons insiden, sementara organisasi yang menerapkan DevSecOps secara efektif dapat menghemat $1,68 juta. Ini berarti bahwa dengan perencanaan yang tepat, organisasi dapat menghindari biaya yang signifikan.

Pemangku kepentingan termasuk pelanggan, mitra bisnis, dan investor akan memiliki kepercayaan yang lebih besar pada organisasi dengan strategi keamanan siber yang solid. Transparansi dalam respons insiden dan pemulihan yang cepat dapat meningkatkan reputasi organisasi dan membangun kepercayaan jangka panjang. Dalam konteks insiden siber PDN, pemangku kepentingan utama adalah instansi pemerintah dan administrasi lokal. Insiden seperti ini dapat mengikis kepercayaan antar instansi pemerintah dan berpotensi menimbulkan gesekan publik. Dalam kasus gangguan layanan imigrasi, kemarahan publik yang diarahkan pada petugas lapangan dapat menimbulkan berbagai masalah.

Banyak sektor, seperti perawatan kesehatan dan keuangan, diatur secara ketat dan menghadapi denda besar untuk pelanggaran data. Misalnya, GDPR Eropa menjatuhkan denda berat pada organisasi yang gagal melindungi data pribadi. Menerapkan BCP dan DRP membantu organisasi memenuhi persyaratan peraturan dan menghindari sanksi hukum.

Dalam konteks keamanan siber, tidak ada organisasi yang kebal terhadap serangan. Yang penting adalah apakah sebuah organisasi memiliki rencana yang baik untuk menangani serangan yang bisa datang kapan saja. Dalam mengintegrasikan IRP, DRP, dan BCP, organisasi akan lebih siap menghadapi berbagai ancaman, baik serangan siber, bencana alam, maupun gangguan operasional. Kesiapan ini memastikan bahwa organisasi dapat terus beroperasi dan melayani pelanggan, bahkan selama gangguan yang signifikan.

Integrasi data pemerintah ke dalam satu pusat data tidak dapat dihindari dalam sistem pemerintahan elektronik. Namun, penting untuk diingat bahwa membangun pusat data melibatkan lebih dari sekadar infrastruktur, sistem perangkat lunak, dan integrasi data. Insiden *ransomware* yang melumpuhkan PDN yang ditargetkan menunjukkan

bahwa pemerintah juga membutuhkan rencana respons insiden, pemulihan bencana, dan kelangsungan bisnis yang kuat.

Tautan artikel:

https://www.thejakartapost.com/opinion/2024/07/17/strategies-for-effective-cybersecurity-resilience.html

Peretasan Akun ‘X’ OJK AS: Apa yang Bisa Dipelajari Institusi Keuangan Indonesia

Arif Perdana

Konteks: Artikel ini diterbitkan oleh The Conversation Indonesia di 31 Januari 2024. Artikel ini saya tulis menanggapi insiden peretasan akun Xnya Security Exchange Commission (SEC) di US. Tulisan ini membahas peretasan akun SEC di media sosial X yang menyebarkan informasi palsu tentang persetujuan ETF Bitcoin, menyebabkan gejolak pasar. Insiden ini menyoroti pentingnya keamanan siber di sektor keuangan, terutama di Indonesia. Penulis merekomendasikan penerapan otentikasi multifaktor, rencana respons insiden, audit keamanan rutin, pelatihan karyawan, serta kolaborasi dengan pihak lain untuk meningkatkan ketahanan terhadap ancaman siber. Kasus ini menjadi pelajaran berharga untuk memperkuat sistem keamanan di institusi keuangan global.

Baru-baru ini, dunia keamanan siber dihebohkan dengan insiden peretasan akun Komisi Sekuritas dan Bursa Amerika Serikat (*Security Exchange Commission*/SEC) di platform media sosial X, yang sebelumnya dikenal sebagai Twitter. Meskipun tidak sama persis, SEC ini bisa disetarakan dengan Otoritas Jasa Keuangan (OJK) di Indonesia yang tugasnya mengawasi pasar modal.

Pada 9 Januari 2024, peretas menyebarluaskan informasi palsu yang mengklaim persetujuan SEC atas dana perdagangan bursa (*Exchange Traded Fund*/ETFs) Bitcoin untuk dicatatkan di semua bursa sekuritas nasional Amerika Serikat (AS) yang terdaftar. Persetujuan SEC terhadap *ETF Bitcoin* ini sebenarnya dirilis secara resmi pada 10 Januari 2024, namun insiden peretasan media sosial SEC terlanjur mengakibatkan gejolak pasar. Meskipun informasi palsu tersebut hanya berlangsung sekitar 30 menit, dampaknya menyesatkan investor dan pengamat pasar, seperti yang ditunjukkan oleh lonjakan harga Bitcoin yang signifikan. Menanggapi intrusi siber ini, Ketua SEC Gary Gensler melalui akun pribadi X-nya, menyatakan unggahan tersebut tidak sah dan menolak persetujuan produk perdagangan bursa Bitcoin. Bersamaan dengan itu, Kantor Inspektur Jenderal SEC menginisiasi penyelidikan komprehensif bersama Biro Investigasi Federal (FBI) demi mengungkap detail dari pelanggaran keamanan tersebut.

Pentingnya Menjaga Keamanan Siber di Sektor Keuangan

Akar masalah terletak pada keamanan siber di SEC. Pada 2016, SEC pernah mengalami serangan siber yang mengakibatkan peretas bisa mengakses database korporasi. Ini mengakibatkan peretas memperoleh keuntungan dari informasi rahasia. Insiden ini seharusnya menjadi pelajaran bagi SEC mengenai perlunya peningkatan keamanan siber dalam sistem keuangan dan menghindari risiko terpaparnya data sensitif dalam aktivitas perdagangan di bursa saham. Sebelum kejadian peretasan media sosial X terjadi, SEC juga sudah dikritik karena tidak sepenuhnya memenuhi standar keamanan siber AS. Kesalahan kritis dalam kasus peretasan ini adalah ketiadaan otentikasi dua faktor pada akun X SEC yang akhirnya dieksploitasi oleh para peretas. Terjadi serangan penggantian SIM (*SIM swapping*), yakni ketika nomor telepon yang terkait dengan akun X SEC dikendalikan oleh pihak ketiga yang tidak teridentifikasi .

Meskipun sampai saat ini belum ada bukti sistem di SEC lainnya bisa diakses oleh peretas selain media sosial X, dampak dari peretasan X dan cuitan palsu mengenai persetujuan ETF Bitcoin telah menyebabkan harga Bitcoin tanggal 9 Januari 2024 langsung melonjak hingga US$47,000-an (sekitar Rp742,35 juta) dari harga sebelumnya yang $46,000-an (Rp727,03 juta, sebelum anjlok ke $45,000-an (sekitar Rp711,22 juta) setelah cuitan palsu tersebut terkuak. Insiden ini bisa menurunkan kepercayaan publik tentang keamanan siber SEC, mengingat reputasi SEC yang memiliki sejarah kurang baik terkait hal ini. Ironisnya, kejadian ini bertepatan dengan implementasi regulasi baru SEC yang mengharuskan perusahaan publik yang terdaftar di bursa AS untuk mengungkapkan insiden siber yang pernah mereka alami. Namun, SEC sendiri abai dengan standar keamanan siber yang seharusnya diimplementasikan sehingga memicu terjadinya insiden peretasan akun X mereka. Pelanggaran ini memicu reaksi politik yang menuntut pertanggungjawaban dan penyelidikan menyeluruh atas praktik keamanan siber SEC.

Strategi Keamanan Siber yang Bisa Diterapkan di Indonesia

Peretasan akun X milik SEC ini menjadi pengingat penting tentang kerentanan platform digital. Berikut adalah strategi kunci yang dapat diterapkan oleh institusi

keuangan di Indonesia untuk mencegah insiden serupa yang terjadi di SEC (lihat Tabel 7):

Tabel 7. Strategi keamanan siber

Strategi Keamanan Siber	Deskripsi
Keamanan Siber Komprehensif	Integrasi otentikasi multifaktor (MFA) yang kuat, seperti Fast Identity Online (FIDO) untuk menggantikan otentikasi berbasis SMS yang rentan. Menggunakan kunci unik (misalnya, sidik jari, USB, Bluetooth/NFC) untuk akses. Pembaruan perangkat lunak secara rutin dan pemisahan nomor telepon.
Rencana Strategis Keamanan (IRP, DRP, BCP)	Pengembangan Rencana Respon Insiden (IRP), Rencana Pemulihan Bencana (DRP), dan Rencana Keberlangsungan Bisnis (BCP) untuk memastikan penanganan, pemulihan, dan kesinambungan operasional pasca-serangan. Tes penetrasi dan penilaian kerentanan secara berkala memperkuat strategi ini.
Pengelolaan Risiko dan Kepatuhan	Melakukan audit keamanan siber secara rutin untuk memastikan kepatuhan terhadap standar internasional dan regulasi perlindungan data. Mengelola risiko dari vendor/pihak ketiga, memastikan keamanan siber vendor sesuai standar yang ditetapkan.
Pelatihan Kesadaran Keamanan Siber	Meningkatkan kesadaran karyawan terhadap keamanan siber melalui pelatihan rutin mengenai identifikasi phishing, penanganan informasi sensitif, dan praktik kata sandi yang kuat. Membentuk budaya keamanan siber untuk meminimalisasi kesalahan manusia.
Kolaborasi dan Transparansi	Menggalakkan kolaborasi dengan institusi lain, regulator, dan komunitas keamanan siber untuk berbagi informasi ancaman dan mitigasi. Menyediakan komunikasi yang transparan dengan pemangku kepentingan selama dan setelah insiden siber.

1. Penerapan keamanan siber yang komprehensif. Hal ini bisa dilakukan dengan mengintegrasikan berbagai langkah keamanan yang meliputi penggunaan otentikasi multifaktor (MFA) yang kuat, seperti *Fast Identity Online* (FIDO), yang merupakan protokol otentikasi untuk memastikan keandalan pengakses sistem. FIDO lebih disukai daripada otentikasi berbasis SMS yang rentan terhadap penggantian SIM. Alih-alih menggunakan kata sandi, ia menggunakan kunci khusus seperti sidik jari, *USB stick*, atau perangkat yang

bisa terhubung melalui *Bluetooth* atau *Near Field Communication* (NFC) yang hanya pengakses yang memilikinya. Ini membuatnya sangat sulit bagi peretas untuk masuk, karena mereka tidak bisa menyalin atau mencuri kunci unik pengakses. Di samping itu, institusi keuangan seharusnya juga menerapkan kebijakan kata sandi yang kuat, unik, dan diperbarui secara teratur. Penting juga bagi institusi keuangan secara rutin memperbarui perangkat lunak dan sistem untuk menghadapi kerentanan. Institusi keuangan juga harus memisahkan penggunaan nomor telepon dari akun media sosial dan sistem online untuk mengurangi risiko penggantian SIM.

2. Penyusunan dan implementasi rencana strategis dengan mengembangkan IRP, DRP, dan BCP yang efektif. Lebih dari sekadar tindakan keamanan individu, pencegahan peretasan ini menekankan pentingnya perencanaan strategis keamanan siber. IRP yang komprehensif merinci protokol penanganan insiden keamanan siber. Sementara, DRP berfokus pada pemulihan data dan sistem secara cepat pascaserangan dan BCP yang menjamin operasional fungsi kritis selama dan setelah gangguan. Melakukan tes penetrasi dan penilaian kerentanan secara teratur dapat membantu institusi keuangan mengidentifikasi dan mengatasi kelemahan keamanan. Mengintegrasikan rencana strategis ini dengan praktik keamanan siber yang kuat dapat membentuk pertahanan menyeluruh, meningkatkan ketahanan terhadap ancaman siber dan meminimalkan dampak insiden.

3. Pengelolaan risiko dan kepatuhan. Audit keamanan siber secara rutin harus menjadi aktivitas wajib bagi setiap institusi keuangan. Penting bagi institusi keuangan untuk melakukan audit keamanan siber secara teratur untuk memastikan kepatuhan terhadap standar internasional, serta mengelola risiko yang berasal dari vendor dan pihak ketiga. Kepatuhan ini termasuk pada peraturan terkait pelindungan data dan privasi. Institusi keuangan juga dapat memanfaatkan audit rutin untuk memastikan mereka selaras dengan praktik dan standar terbaik. Hal ini termasuk menilai keamanan siber vendor secara menyeluruh dan memastikan mereka memenuhi standar yang ditetapkan.

4. Pelatihan kesadaran keamanan siber untuk karyawan. Kesalahan manusia tetap menjadi salah satu kerentanan keamanan siber terbesar. Keamanan siber bukan hanya hal teknis, namun juga budaya. Institusi harus berinvestasi dalam pendidikan karyawan

yang berkelanjutan dan membangun kesadaran keamanan siber. Institusi keuangan perlu mengadakan pelatihan reguler bagi karyawan tentang praktik terbaik keamanan siber, termasuk identifikasi upaya phishing, penanganan informasi sensitif yang aman, dan pentingnya kata sandi yang kuat. Terkait dengan pengelolaan platform daring, institusi keuangan harus punya mekanisme untuk memantau platform dari aktivitas tidak sah, mengamankan akun dengan langkah otentikasi yang kuat, dan melatih staf yang bertanggung jawab untuk mengelola platform ini dalam praktik keamanan terbaik.

5. Kolaborasi dan transparansi. Keamanan siber merupakan tantangan kolektif. Institusi keungan harus secara aktif terlibat dalam berbagi informasi dan kolaborasi dengan institusi lainnya, badan regulator, dan komunitas keamanan siber. Kolaborasi ini dapat membangun pemahaman dan mitigasi yang lebih baik terhadap ancaman yang muncul. Dalam kejadian serangan siber, komunikasi transparan dan tepat waktu dengan pemangku kepentingan sangat penting. Institusi keuangan harus memiliki rencana komunikasi yang mencakup memberitahukan pihak yang terdampak, menyebarkan informasi yang akurat, dan memberikan pembaruan tentang tindakan pemulihan.

Kasus di AS sepatutnya menjadi pelajaran bagi institusi keuangan di seluruh dunia, termasuk Indonesia, untuk memperkuat keamanan sibernya. Dengan begitu cepat dan sensitifnya perputaran uang dan aset digital terhadap sentimen di pasar, informasi yang menyesatkan bisa membawa kerugian besar bagi banyak pihak.

Tautan artikel:

https://theconversation.com/peretasan-akun-x-ojk-as-apa-yang-bisa-dipelajari-institusi-keuangan-indonesia-222260

Bukan Teknologi Semata: Akankah Pusat Data Nasional Menjadi Solusi Aksesibilitas dan Jaminan Keamanan Data?

Arif Perdana

Konteks: Artikel ini saya tulis untuk The Conversation Indonesia di 18 Januari 2024. Tulisan ini menanggapi pembentukan PDN oleh Kementerian Komunikasi dan Informatika Indonesia untuk mewujudkan Satu Data Nasional. PDN bertujuan mengintegrasikan lebih dari 2.700 pusat data dari berbagai lembaga, meningkatkan keamanan, efisiensi, dan kolaborasi antar lembaga. Namun, proyek ini menghadapi tantangan seperti ego sektoral dan kebutuhan untuk tata kelola data yang efektif. Keberhasilan PDN bergantung pada kepemimpinan yang kuat, pengelolaan data yang aman, dan keselarasan dengan strategi digital nasional yang lebih luas.

Pemerintah pusat melalui Kementerian Komunikasi dan Informatika (Kominfo) tengah membangun PDN untuk mewujudkan Satu Data Nasional. Ini menjadi satu peluang untuk memperbaiki transformasi tata kelola digital Indonesia. Proyek ambisius ini memiliki agenda mengintegrasikan lebih dari 2.700 pusat data yang berasal dari 630 institusi dan lembaga. Tujuannya adalah mengatasi tantangan duplikasi dan inefisiensi dalam sistem yang ada saat ini. Namun, meskipun PDN menawarkan manfaat yang signifikan, proyek ini juga menghadirkan tantangan inheren yang memerlukan strategi dan upaya kolaborasi, alih-alih soal teknologi semata.

Peluang Pusat Data Nasional

Pendirian PDN di Indonesia merupakan amanah dari Peraturan Presiden (Perpres) No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik dan No. 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional. Peraturan ini menyediakan kerangka hukum dan kebijakan yang kuat, serta menandakan komitmen pemerintah yang serius dalam meletakkan dasar kokoh untuk keberhasilan proyek Sistem Pemerintahan Berbasis Elektronik (SPBE). Ini semua merupakan langkah signifikan dalam perjalanan Indonesia menuju infrastruktur digital yang terintegrasi dan

efisien. Pusat data yang akan dibangun ada di empat lokasi, yaitu Bekasi, Batam, Ibu Kota Nusantara (IKN) di Kalimantan Timur, dan Labuan Bajo, diharapkan dapat menjamin pemerataan aksesibilitas digital di seluruh wilayah Indonesia dan menjembatani kesenjangan digital di berbagai wilayah.

PDN menawarkan peluang untuk meningkatkan keamanan dan kedaulatan data. Dengan memusatkan penyimpanan data pemerintah dalam batas negara, PDN dapat melindungi informasi sensitif dari ancaman serangan siber internasional dan kebocoran data. PDN juga diharapkan dapat mencapai efisiensi biaya yang signifikan. Konsolidasi berbagai pusat data pemerintah di bawah PDN berpotensi mengurangi pengeluaran TI secara keseluruhan. Rasionalisasi sumber daya ini bertujuan untuk mengoptimalkan manajemen keuangan dan memungkinkan alokasi dana publik yang lebih strategis.

Selanjutnya, PDN diharapkan dapat memfasilitasi kolaborasi dan berbagi informasi antarlembaga pemerintah, menghilangkan silo (penyimpanan data dengan akses terbatas) data yang tradisional dan menghambat efisiensi operasional pemerintah. Konektivitas ini diharapkan akan menyediakan layanan yang lebih mulus dan koheren kepada masyarakat, serta meningkatkan kualitas layanan pemerintah. Dampak kolektif dari PDN mencakup peningkatan pengambilan keputusan dan kebijakan berbasis data, peningkatan keamanan data, efisiensi biaya, dan kolaborasi yang lebih baik. PDN tidak hanya berperan sebagai aset infrastruktur tetapi juga sebagai katalis untuk transformasi yang lebih luas dalam tata kelola sektor publik dan peningkatan layanan publik di Indonesia.

Tantangan dan Mitigasi Risiko

PDN ini bukan hanya soal teknologi semata, melainkan juga manajemen perubahan yang berpotensi menimbulkan masalah baru yang rumit. Proses implementasi yang rumit ini membutuhkan visi yang bersatu dan upaya bersama untuk menavigasi kompleksitas kerja sama antarlembaga dan penyelarasan kebijakan. Maka dari itu, proyek ini membutuhkan pendekatan sinergis dan kolaboratif yang menggabungkan berbagai tingkat pemerintah dan sektor untuk memastikan kepatuhan ketat terhadap arahan kebijakan dan standar. Bagaimanapun juga, keberhasilan PDN

bergantung pada tata kelola data yang efektif, bukan hanya sekadar penggunaan teknologi canggih. Tantangan besar ini melibatkan lembaga pemerintah yang terlibat untuk mengatasi 'ego sektoral' dan mengintegrasikan data mereka ke dalam sistem terpusat ini. Ini vital untuk membongkar silo data yang sudah lama ada di Indonesia dan mendorong ekosistem pemerintahan yang kolaboratif dan efisien.

Kepemimpinan yang kuat dan kolaborasi yang tangguh di antara berbagai institusi akan membantu memastikan bahwa data dikelola dengan cara yang memaksimalkan nilai bagi pemerintah dan masyarakat, sambil menjaga keamanan dan privasi. Ini tentunya tidak mudah, tapi bisa terlaksana dengan komitmen yang tinggi. Memastikan integritas dan kualitas data di PDN sangat penting karena ini merupakan aspek yang sangat vital dari data yang diambil dan digunakan di antara institusi pemerintah.

Oleh karena itu, standar verifikasi dan validasi data yang ketat harus dibuat. Selain itu, PDN harus menyeimbangkan penyediaan akses data yang ramah pengguna dengan mematuhi UU privasi data yang ketat, seperti UU PDP, untuk memastikan pengelolaan data yang aman dan beretika. Mempromosikan berbagi data antarinstitusi juga sangat penting untuk menghindari ego sektoral dan silo data. Inisiatif ini memerlukan pembuatan standar data umum, platform bersama, dan pedoman berbagi data yang jelas. Pendekatan ini bertujuan untuk meningkatkan layanan publik melalui kolaborasi yang ditingkatkan dan manajemen data yang terpadu.

Aspek Kunci

Aspek kunci dari PDN adalah menyeimbangkan keamanan data dan aksesibilitas. Dalam beberapa tahun terakhir, Indonesia telah mengalami peningkatan kebocoran data di berbagai institusi pemerintah. PDN harus membangun dasar teknologi yang kuat untuk keamanan siber guna menjaga data kritis. Sambil memprioritaskan kedaulatan data dan pelindungan dari ancaman siber, juga harus ada fokus untuk memastikan bahwa data tetap mudah diakses dan fungsional untuk lembaga pemerintah. Di satu sisi, pengelolaan data di PDN menjadi lebih terintegrasi, di lain pihak jika terjadi serangan siber atau kebocoran data, risiko yang dihadapi oleh PDN akan semakin tinggi. Ini memerlukan pendekatan dinamis terhadap keamanan yang didukung oleh protokol tata kelola data

yang kuat dan dapat disesuaikan. Protokol ini harus cukup fleksibel untuk berkembang dengan teknologi dan ancaman yang muncul. Evaluasi dan pemutakhiran langkah-langkah keamanan secara teratur sangat penting untuk mempertahankan keseimbangan harmonis antara keamanan dan kegunaan.

Pertimbangan signifikan lainnya adalah aspek keuangan dari PDN. Meskipun tujuan akhir adalah untuk mencapai efisiensi biaya dengan mengkonsolidasikan sumber daya TI, investasi awal dan biaya operasional berkelanjutan perlu dipertimbangkan. Manajemen anggaran yang efisien sangat penting untuk keberlanjutan operasional jangka panjang. Pemerintah juga perlu memastikan pusat-pusat ini tidak hanya canggih secara teknologi tetapi juga dikelola dan dimanfaatkan dengan efektif dan berkelanjutan, termasuk terkait ketahanan lingkungan. Seperti yang diketahui, pembangunan pusat data bisa memberikan risiko bagi lingkungan, sehingga perlu mengadopsi manajemen data berkelanjutan, mengoptimalkan pengumpulan hingga pemusnahan data, dan peduli pada aspek lingkungan.

Akhirnya, kesuksesan jangka panjang PDN tergantung pada keselarasannya dengan strategi digital Indonesia secara umum. Keselarasan ini memastikan bahwa PDN bukan proyek terisolasi tetapi integral dengan ambisi digital bangsa secara keseluruhan. Kontinuitas dan keberlanjutan sangat kritis, dan membutuhkan kolaborasi, kepemimpinan yang efektif, evaluasi berkelanjutan dan fleksibilitas untuk beradaptasi dengan lanskap teknologi yang berkembang.

Tautan artikel:

https://theconversation.com/bukan-teknologi-semata-akankah-pusat-data-nasional-menjadi-solusi-aksesibilitas-dan-jaminan-keamanan-data-220783

Dalam Kebocoran Big Data Mengapa Faktor Manusia Kerap Terlupakan

Arif Perdana

Konteks: Artikel ini diterbitkan oleh The Conversation Indonesia di 21 December 2021. Di sini saya menyoroti pentingnya tata kelola data yang baik untuk mencegah kebocoran data di Indonesia, yang sering disebabkan oleh kecerobohan manusia dan penyalahgunaan otoritas. Meskipun teknologi keamanan ada, faktor manusia tetap menjadi titik lemah utama. Kebocoran data dapat memiliki dampak serius, baik secara individu maupun kolektif, dan memerlukan perhatian terhadap perlindungan privasi serta kepatuhan terhadap regulasi perlindungan data pribadi. Sinergi antara teknologi, prosedur, dan perilaku manusia sangat penting dalam pengelolaan data yang efektif.

Ketika terjadi kebocoran data, seperti kasus big data kesehatan, perbankan, kependudukan, e-commerce dan kepolisian di Indonesia dalam dua tahun terakhir, sebagian dari kita mungkin berpikir bahwa masalah ini merupakan kesalahan teknologi semata dan faktor pembobol. Padahal, aspek paling penting yang biasanya terlupakan adalah rapuhnya tata kelola data, yang umumnya disebabkan oleh kecerobohan manusia. Apa pun aset yang dikelola oleh perusahaan dan lembaga, aspek perilaku manusia selalu menjadi komponen krusial, termasuk pengelolaan aset digital (data dan informasi). Riset terbaru dari Verizon dan IBM menunjukkan aspek manusia selalu menjadi titik krusial kebocoran data. Laporan mutakhir dari Verizon mengenai kebocoran data pada 2021 itu menyatakan 85% kebocoran data melibatkan aspek manusia yakni rekayasa sosial, penyalahgunaan otoritas, dan kendali yang lemah.

Faktor Manusia

Aliran dan produksi data yang besar apalagi yang berkaitan data pribadi menjadi tantangan yang krusial saat ini. Pengelolaan data digital memiliki tantangan yang lebih besar dibandingkan aset berwujud karena sifat data yang mudah diduplikasi ketika sudah bocor ke tangan yang tidak berkepentingan. Terlepas dari canggihnya metode dan platform keamanan data, individu menempati posisi amat penting dalam keamanan data.

Data-data yang berkaitan dengan diri mereka adalah aset yang berharga yang harus dijaga. Prinsip kehati-hatian harus dijalankan ketika, misalnya, mengisi formulir online baik untuk institusi publik maupun swasta. Apalagi yang berkaitan dengan berbagi data melalui platform media sosial seperti yang sedang marak saat ini.

Penggunaan rekayasa sosial dengan memanipulasi psikologi korban tidak memerlukan teknologi canggih. Manipulasi psikologi ini bisa dilakukan melalui email atau pesan teks agar target tertarik untuk mengunduh file, mengklik atau mengikuti tautan yang diberikan. Saat langkah itu diikuti, *malware* yang disiapkan oleh pelaku bisa disisipkan ke komputer atau server target. *Malware* ini selanjutnya bisa dikendalikan oleh pelaku untuk membuka akses ke data-data ada di komputer atau jaringan komputer penyimpan data.

Penyalahgunaan otoritas dan kendali yang lemah terhadap otoritas akses data juga banyak berkontribusi terhadap kebocoran data. Dari yang pernah saya alami, misalnya, data individu dan karyawan di salah satu institusi pemerintah disalahgunakan untuk kepentingan politik. Ini bisa terjadi karena adanya penyalahgunaan otoritas dan kendali yang lemah. Operator data tidak bisa berbuat banyak ketika atasan langsung mereka meminta data dimaksud. Hal ini semakin diperparah karena kurang memadainya kendali internal untuk mengidentifikasi akses data dan untuk apa data itu selanjutnya akan digunakan.

Penyalahgunaan ini rentan terjadi, karena saat data dikumpulkan, tidak ada surat persetujuan (*consent form*) yang diberikan kepada individu mengenai tujuan penggunaan data, dan bagaimana data akan diproses, dikelola, dibagi, dan disimpan oleh institusi yang bersangkutan. Dan berapa lama disimpan. Berita tentang kebocoran data sudah sering kita dengar dan saksikan di media. Baik institusi swasta dan pemerintah, besar maupun kecil, semuanya rentan terhadap kebocoran data.

Dalam kurun waktu 2020 hingga 2021, misalnya, setidaknya terjadi tiga kasus kebocoran data institusi publik yang terungkap di Indonesia, yaitu kebocoran data Komisi Pemilihan Umum (KPU), Badan Penyelenggara Jaminan Sosial Kesehatan (BPJS), dan Kepolisian Republik Indonesia (Polri). Celakanya, institusi publik merupakan pihak yang paling rentan. Hal ini karena satu institusi publik seringkali harus berbagi data dengan

institusi lainnya. Selain itu, data yang mereka kelola berkaitan dengan layanan-layanan yang mengharuskan publik bisa mengaksesnya.

Data individu yang sudah berpindah dan terekam ke database institusi publik harus dijaga dan dikelola secara aman dan profesional. Oleh karena itu tata kelola data yang baik merupakan aspek kritikal untuk mencegah terjadinya kebocoran data terutama data pribadi baik secara individu maupun agregat. Institusi dan individu kini harus sadar bahwa kebocoran data bukan hal sepele. Bagi individu, jangan pernah beranggapan bahwa berbagi data pribadi bisa dilakukan dengan bebas tanpa konsekuensi. Baik secara individu maupun agregat, data memiliki nilai ekonomi, sosial, budaya, dan politik.

Bagi pembobol data, data merupakan bisnis besar karena harganya di pasar gelap berkisar dari beberapa dolar hingga puluhan dolar per identitas. Data curian ini bisa dipakai untuk tindakan kriminal dari pemerasan, penipuan hingga pencurian uang secara elektronik. Secara global, IBM melaporkan terjadi peningkatan kerugian akibat kebocoran data dari US$ 3,86 juta (sekitar Rp 55,3 miliar) pada 2020 menjadi US$ $4,24 juta (sekitar Rp 60 miliar) tahun ini. Di laporan riset ini juga dipaparkan bahwa kebocoran data pribadi menyumbang kerugian yang paling besar dengan nilai US$ 180 (sekitar Rp 2,5 juta) untuk setiap identitas.

Isu Privasi

Privasi dan PDP adalah dua aspek yang saling terkait satu dengan lainnya. Pelindungan data ditujukan untuk memastikan bahwa data pribadi setiap individu ditangani sesuai dengan peraturan dan UU yang berlaku. Privasi merupakan bagian dari hak asasi manusia. Oleh karena itu, setiap individu memiliki hak untuk mengontrol data pribadi mereka. Di Indonesia, definisi mengenai data pribadi tertera di UU No. 23 Tahun 2006 tentang Administrasi Kependudukan. Di UU tersebut data pribadi didefinisikan sebagai data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Data pribadi ini meliputi nama lengkap, nomor KTP/NIK, Passpor, SIM dan identitas lainnya, data-data tentang kesehatan (fisik, fisiologi, dan mental), data demografi individu, data ekonomi dan penghasilan, data lokasi geografis dan geolokasi, nomor ponsel, alamat surel pribadi, alamat rumah, foto dan video individu.

Pengelolaan data pribadi harus mematuhi peraturan perundang-undangan proteksi dan privasi data yang berlaku di negara setempat. Karena itu, pemerintah dan DPR perlu segera membahas lagi rancangan UU PDP yang kini mandeg. Untuk PDP ini, Uni Eropa masih merupakan jurisdiksi yang terdepan dalam penegakan ketentuan proteksi dan privasi data melalui GDPR. Seperti saran GDPR, individu pemilik data berhak mengetahui siapa atau pihak-pihak mana yang menjadi pemroses data (*data processor*), siapa yang mengendalikan data mereka (*data controller*), dan siapa yang memproteksi data mereka (*data protection officer*).

Secara umum, regulasi mengenai proteksi data memberikan hak pada pemilik data untuk mengetahui siapa saja yang akan menggunakan data (*access*), dimintai pernyataan kebersediaan (*consent*), mengoreksi data yang tidak akurat (*correction*), meminta data dimusnahkan setelah dianalisis (*erasure*), mengetahui penggunaan data (*informed*), dan mentransfer data (*portability*).

Teknologi, Prosedur, dan Manusia

Tata kelola data yang baik melibatkan sinergi antara teknologi, proses (prosedur) dan manusia. Institusi publik harus profesional menangani data pribadi dan sensitif dari sejak data dikumpulkan, diproses, hingga dimusnahkan. Regulasi PDP yang saat ini masih dalam tahap rancangan semakin terasa urgensinya. Pemahaman mengenai tata kelola data yang baik dan kepatuhan terhadap regulasi PDP akan menentukan bagaimana institusi menangani data pribadi individu yang mereka kumpulkan. Misalnya, institusi harus menjamin keamanan jaringan dan mesin yang digunakan untuk menyimpan data. Di samping itu, data itu sendiri juga harus diproteksi dengan menggunakan mekanisme kriptografi modern. Yang tak kalah pentingnya adalah kendali atas akses data. Kolusi yang terjadi di antara pihak-pihak yang memiliki akses data akan berdampak serius dan membuat teknologi keamanan yang sudah diterapkan menjadi sia-sia.

Jika kebocoran data sudah terjadi, institusi yang bertanggung jawab harus segera melaporkan kejadian tersebut ke otoritas yang berwenang (Kementerian Komunikasi dan Informasi), untuk bersama-sama mengambil langkah-langkah yang relevan untuk

memitigasi resiko, baik bagi institusi, maupun individu yang terdampak kebocoran data tersebut.

Tautan artikel:

https://theconversation.com/dalam-kebocoran-big-data-mengapa-faktor-manusia-kerap-terlupakan-172870

BAB 3: Tantangan Etika dan Sosial Teknologi Digital

Perkembangan pesat teknologi digital, terutama AI seperti *ChatGPT*, telah membawa berbagai tantangan etika dan sosial yang signifikan. Kekhawatiran utama meliputi penyalahgunaan teknologi untuk praktik tidak berintegritas, penipuan, penyebaran disinformasi, dan kejahatan siber. Di ranah politik dan sosial, teknologi AI seperti *deepfake* berpotensi memanipulasi opini publik dan menyebarkan disinformasi, terutama selama periode pemilihan umum. Hal ini mengancam integritas proses demokrasi dan kepercayaan publik terhadap institusi. Masalah privasi dan keamanan data juga menjadi perhatian utama, dengan meningkatnya risiko kebocoran data sensitif dan penyalahgunaan informasi pribadi. Selain itu, ada kekhawatiran tentang bias dalam algoritma AI yang dapat memperkuat ketidaksetaraan sosial yang ada. Di sisi lain, teknologi kripto bisa memberikan dampak negatif berkaitan dengan penipuan keuangan. Dampak lingkungan dari teknologi digital, terutama konsumsi energi yang tinggi oleh pusat data AI, juga menjadi isu penting. Ini menimbulkan pertanyaan tentang keberlanjutan perkembangan teknologi di tengah krisis iklim global.

Untuk mengatasi tantangan ini, diperlukan pendekatan multidimensi yang melibatkan regulasi yang inovatif, pendidikan publik, dan praktik pengembangan teknologi yang bertanggung jawab. Regulasi harus mengimbangi inovasi sambil melindungi hak-hak individu dan nilai-nilai sosial. Banyak ahli berpendapat bahwa solusi efektif adalah melalui regulasi yang tegas dan inovatif, serta pengembangan teknologi yang etis dan bertanggung jawab. Tantangan ini menekankan perlunya dialog berkelanjutan antara pembuat kebijakan, pengembang teknologi, dan masyarakat untuk memastikan teknologi digital memberikan manfaat sambil meminimalkan risiko.

Algoritma dan Kemanusiaan Kita

Arif Perdana

Konteks: Artikel ini diterbitkan di Kumparan, 6 Desember 2024, Tulisan ini merupakan refleksi saya tentang bagaimana kita sebagai manusia harus semakin memupuk nilai-nilai kemanusiaan kita ditengah berkembangnya teknologi AI. Di era digital, kemanusiaan menjadi hal yang berharga di tengah dominasi teknologi. Berbeda dengan AI yang bisa menghasilkan konten dengan cepat, manusia memiliki kedalaman jiwa yang tak tergantikan. Kita memiliki empati, intuisi, dan kebijaksanaan yang membentuk esensi kemanusiaan. Meski AI menunjukkan kemajuan teknologi, hanya manusia yang bisa memahami nuansa makna dan nilai kehidupan. Hubungan manusia-AI bukanlah persaingan, melainkan simbiosis untuk menemukan harmoni dan mendefinisikan ulang makna kemanusiaan.

Di era serba digital, keunikan manusia menjadi sebuah oase di tengah kegersangan mekanisasi yang meluas. Tidak seperti AI yang mampu menghasilkan ribuan kata dalam hitungan detik, manusia menyimpan kedalaman yang tidak hanya diukur dengan output. Kita, makhluk berdarah dan bernyawa yang mengeksplorasi dan merasakan. Karya yang kita hasilkan bukan hanya tampilan, tetapi juga cerminan jiwa.

Layaknya lukisan abstrak yang menantang persepsi, kehadiran AI mengajak kita merenung lebih dalam tentang apa yang membuat kita unik. Bukan semata kemampuan berpikir atau mencipta, tetapi juga getaran-getaran lembut empati, intuisi, dan kebijaksanaan hati yang membentuk esensi kemanusiaan kita. Dalam orkestra digital yang kian kompleks, nada kemanusiaan kita semakin penting untuk didengar dan dihayati.

Filsuf Yunani kuno Protagoras pernah berkata, "Manusia adalah ukuran segala sesuatu." Namun, dalam gelora zaman digital ini, adagium tersebut seakan mendapatkan tantangan baru. Dengan kemampuan yang mengagumkan, AI memaksa kita untuk mempertanyakan kembali kedudukan kita dalam tatanan semesta. Apakah kita masih dapat menjadi "ukuran" ketika algoritma bisa menyelesaikan teka-teki dengan kecepatan yang melampaui kapasitas otak manusia?

AI mungkin menggambarkan kemajuan, tetapi hanya manusia yang memahami nuansa makna dan nilai. Kita tidak hanya sekumpulan data yang diproses; kita adalah entitas yang hidup dengan kesadaran dan pengalaman yang tak terdigitalisasi. Di sinilah letak perbedaan mendasar antara AI dan kearifan hidup yang kita miliki. Kita bukan hanya penonton dalam drama teknologi, melainkan penulis naskah kehidupan kita sendiri.

Eksistensi manusia dan AI di era digital bukan tentang pertarungan supremasi, melainkan tentang menemukan harmoni. Seperti simbiosis antara pohon dan angin, di mana keduanya saling membentuk dan memengaruhi, begitu pula hubungan manusia dan AI. Kita bukan hanya penciptanya, tetapi juga pembelajar yang terus tumbuh bersamanya. Dalam proses ini, kita diajak untuk meredefenisi makna menjadi manusia – bukan sebagai entitas yang terisolasi, melainkan sebagai bagian dari ekosistem teknologi yang lebih luas.

Dari Roda hingga AI

Bayangkan sejenak perjalanan evolusi transportasi manusia. Dulu, kaki adalah satu-satunya moda transportasi kita. Lalu muncul roda, kuda, mobil, hingga pesawat jet supersonik. Tidak ada manusia yang bisa berlari secepat mobil atau terbang setinggi pesawat. Namun, apakah ini membuat kita merasa terancam atau tergantikan? Tidak. Justru, kita belajar untuk hidup berdampingan dan memanfaatkan kendaraan-kendaraan ini untuk memperluas jangkauan dan kemampuan kita.

AI, dalam banyak hal, mirip dengan revolusi transportasi ini. Ia mampu memproses data dan menghasilkan konten digital dengan kecepatan yang jauh melampaui kemampuan manusia. Namun, ada perbedaan krusial. Kendaraan hanya memperluas kemampuan fisik kita, sementara AI berpotensi memperluas, atau bahkan menantang kemampuan kognitif kita.

Keunggulan manusia tidak terletak pada kecepatan atau efisiensi semata. AI, dengan segala kemampuan pengolahannya, tetaplah alat. Manusia, di sisi lain, memegang kemudi interpretasi dan emosi. Dalam konteks ini, AI berperan sebagai perpanjangan tangan kita, bukan pengganti. Kita mengarahkan, sementara AI mempercepat. Keunikan ini menciptakan sinergi, bukan persaingan, di antara keduanya.

Kita harus sadar bahwa teknologi ada untuk memperkaya, bukan untuk menggantikan esensi manusiawi kita.

Ini membawa kita pada pertanyaan yang lebih dalam: apakah 'kecepatan' dalam menghasilkan ide atau konten setara dengan kualitas dan kedalaman pemikiran manusia? Seperti halnya mobil tercepat sekalipun membutuhkan pengemudi yang bijak untuk menentukan arah dan tujuan, begitu pula AI memerlukan kearifan manusia untuk memberi makna dan konteks pada output yang dihasilkannya.

Dimensi Manusia yang Tak Terjangkau AI

Lantas, apa yang sebenarnya membuat kita unik? Jawabannya terletak pada aspek-aspek yang tidak bisa dikuantifikasi atau diprogram. Kecerdasan hati kita, misalnya, adalah kompas internal yang memandu kita dalam mengambil keputusan etis dan emosional. Kemampuan kita untuk berempati, merasakan nuansa emosi yang kompleks, dan menghubungkan pengalaman pribadi dengan konteks yang lebih luas adalah kualitas yang tidak bisa direplikasi oleh AI. Kita bisa merasakan kesedihan atau kebahagiaan orang lain, sesuatu yang tak mungkin diprogram ke dalam AI.

Kreativitas manusia juga memiliki dimensi yang sulit dijangkau AI. Kreativitas kita tidak hanya bersumber dari rasionalitas tetapi juga bisa dari irasionalitas dan kekeliruan yang bisa memicu ide-ide brilian. Dari sampel lab yang berjamur hingga lelehan cokelat akibat gelombang mikro, Alexander Fleming dan Percy Spencer membuktikan bahwa keajaiban bisa lahir dari kekeliruan dan mengubah kesalahan menjadi penemuan revolusioner.

Ketika seorang seniman dan filsuf menciptakan karya, ia tidak hanya menggabungkan elemen-elemen yang ada, tetapi juga menuangkan rasa, pengalaman hidup, dan bahkan trauma pribadinya. Hasil akhirnya bukan sekadar produk, melainkan cerminan jiwa yang memiliki resonansi emosional dengan penikmatnya. Friedrich Nietzsche, misalnya, tetap menulis di tengah penderitaan fisik dan kejiwaannya. Meski tuli, Ludwig van Beethoven tetap menciptakan musik terbaiknya, termasuk Simfoni No. 9. "*Heiligenstadt Testament*".

Lebih jauh lagi, kemampuan kita untuk mempertanyakan eksistensi kita sendiri, untuk mencari makna di balik kehidupan, dan untuk membayangkan realitas alternatif adalah aspek-aspek yang membuat kita unik sebagai manusia. AI mungkin bisa mensimulasikan proses-proses ini, tetapi tidak bisa benar-benar 'mengalami'nya seperti kita. Di atas segalanya, manusia memiliki kesadaran diri. Kita tidak hanya bereaksi, tapi juga merefleksi, menimbang, dan memaknai tindakan kita dalam konteks yang lebih luas. Perbedaan mendasar lainnya terletak pada konsep niat. Manusia dalam setiap aktivitas dan tindakannya memiliki niat, sebuah dorongan internal yang melandasi perilaku kita. Niat ini bukan sekadar algoritma, melainkan hasil dari kesadaran, emosi, dan pertimbangan moral yang kompleks. Inilah yang membedakan manusia dengan mesin.

Konsep niat dan kesadaran diri ini memiliki implikasi yang jauh lebih luas, termasuk dalam ranah hukum dan etika. Karena AI tidak memiliki niat atau kesadaran diri dalam arti yang sesungguhnya, sebagian pakar berpendapat bahwa AI tidak bisa dituntut secara hukum atas 'tindakannya'. Tanggung jawab hukum dan moral tetap berada pada manusia yang merancang, mengembangkan, dan menggunakan AI tersebut.

Menghadapi era AI, kita perlu menegaskan kembali nilai-nilai kemanusiaan kita. Agar tetap relevan dan berarti, kita harus terus mengasah apa yang menjadikan kita manusia. Ini bukan tentang menolak teknologi, tetapi tentang mengintegrasikannya dengan bijak ke dalam kehidupan kita.

Secara filosofis, ini berarti menerima paradoks, yaitu memahami keterbatasan kita sekaligus menghargai potensi tak terbatas dari kreativitas dan empati manusia. Kita perlu memelihara kecerdasan hati, mengasah kepekaan terhadap nuansa-nuansa kehidupan yang tidak bisa ditangkap oleh algoritma.

Secara praktis, ini berarti terus belajar dan beradaptasi, tidak hanya dengan teknologi baru, tetapi juga dengan cara-cara baru dalam memahami diri dan sesama. Kita perlu mengembangkan keterampilan yang menonjolkan keunikan manusia, yaitu kreativitas, pemikiran kritis, empati, dan kemampuan untuk menghubungkan ide-ide yang tampaknya tidak berkaitan. Dengan cara ini, kita tidak hanya bertahan, tetapi juga berkembang di era AI, menjadikan teknologi sebagai alat yang melengkapi bukan yang menggantikan keunikan kita sebagai manusia.

Pada akhirnya, eksistensi kita di era AI bukan tentang kompetisi, melainkan tentang kolaborasi dan transendensi. Dengan memahami keunikan kita sebagai manusia, kita bisa memanfaatkan AI sebagai alat untuk memperluas batas-batas potensi kemanusiaan kita, menciptakan simfoni indah antara logika mesin dan kearifan hati manusia.

Tautan artikel:

https://kumparan.com/arif-perdana-1723991955605643308/algoritma-dan-kemanusiaan-kita-243EEaIeKdS

Waspada Penipuan Kripto Bermodus Kecanggihan Teknologi dan Psikologi

Arif Perdana

Konteks: Artikel ini diterbitkan oleh the Conversation Indonesia, 13 November 2024. Tulisan ini merupakan ringkasan penelitian yang saya dan rekan dari Singapore Institute of Technology lakukan tentang Crypto-Cognitive Exploitation Model (CCEM) untuk menjelaskan penipuan kripto yang memanfaatkan kelemahan psikologis dan teknologi kripto. Model ini terdiri dari tiga lapisan: kerentanan kognitif (contoh: FOMO), rekayasa sosial (penipu menyamar sebagai ahli), dan pemanfaatan teknologi kripto (transaksi permanen tanpa pengawasan). CCEM memberi wawasan untuk Indonesia, di mana literasi digital perlu ditingkatkan, promosi oleh influencer diawasi, sistem pelaporan diperkuat, dan regulasi diperbarui untuk melindungi investor dari penipuan. Kolaborasi antara otoritas dan platform diperlukan untuk menciptakan ekosistem kripto yang aman.

Di era digital yang penuh ketidakpastian, penipuan *cryptocurrency* kini semakin canggih, menyebabkan banyak orang mengalami kerugian finansial yang besar. Studi terbaru saya bersama seorang kolega dari Singapore Institute of Technology membahas tentang model penipuan di dunia *cryptocurrency* yang memberikan pemahaman tentang mekanisme penipuan ini bekerja.

Kami menyusun sebuah kerangka bernama *Crypto-Cognitive Exploitation Model* (CCEM) atau Model Eksploitasi Kognitif-Kripto. Model ini menjelaskan cara para penipu mengeksploitasi kelemahan psikologis manusia melalui rekayasa sosial (social engineering) serta memanfaatkan aspek unik teknologi *cryptocurrency* . Model ini kami bangun berbasis laporan dan data aktual dari Departemen Perlindungan dan Inovasi Keuangan (DFPI) Amerika Serikat.

Dalam penelitian ini, kami mengungkapkan kompleksitas modus penipuan *cryptocurrency* yang tidak sepenuhnya bisa dijelaskan oleh dua teori eksisting yang lebih umum. Kedua teori tersebut yaitu teori rekayasa sosial dan teori kerentanan kognitif. Teori rekayasa sosial menjelaskan cara penipu yang memanipulasi korban dengan berpura-pura menjadi orang lain, membuat janji palsu, menawarkan hadiah fiktif, atau menakut-nakuti korban. Sementara itu, teori kerentanan kognitif mengungkap tentang

kelemahan cara berpikir manusia, seperti mudah percaya pada informasi yang sesuai keinginan, gampang terpengaruh dengan cerita kesuksesan orang lain, takut ketinggalan kesempatan, dan panik saat diberi batasan waktu.

Namun, kedua teori ini belum cukup untuk menjelaskan kompleksitas penipuan *cryptocurrency* , yang melibatkan tiga hal sekaligus: cara manusia berpikir, hubungan antar manusia, dan teknologi baru yang masih asing bagi banyak orang. Oleh karena itu, kita butuh cara baru untuk memahami bagaimana ketiga aspek ini berkaitan dalam penipuan *cryptocurrency* , yaitu melalui Model Eksploitasi Kognitif-Kripto (CCEM).

Mengungkap Tiga Lapisan Penipuan Kripto

Model kami memiliki tiga lapisan penting untuk menjelaskan cara kerja penipuan *cryptocurrency* . Mula-mula kami mempelajari bagaimana cara orang berpikir dan mengambil keputusan yang berpotensi membuat mereka mudah tertipu, kemudian kami mempelajari trik-trik yang digunakan oleh para penipu untuk menjebak korban, lalu kami menganalisis bagaimana teknologi *cryptocurrency* yang kompleks ini dimanfaatkan untuk melakukan penipuan.

1. Kerentanan kognitif

Lapisan pertama ini berkaitan dengan cara orang berpikir dan mengambil keputusan yang berpotensi membuat mereka mudah tertipu dalam investasi *cryptocurrency* . Contoh kerentanan ini adalah memanfaatkan celah fear of missing out atau FOMO (takut kehilangan kesempatan) dari calon korban. FOMO dalam konteks mata uang kripto adalah kondisi di mana seseorang tergesa-gesa ikut berinvestasi karena melihat orang lain sukses atau kaya mendadak, tanpa mengecek informasi dengan teliti. Selain itu, calon korban didoktrin sudah memahami teknologi *cryptocurrency*, padahal pengetahuannya sebenarnya masih dangkal.

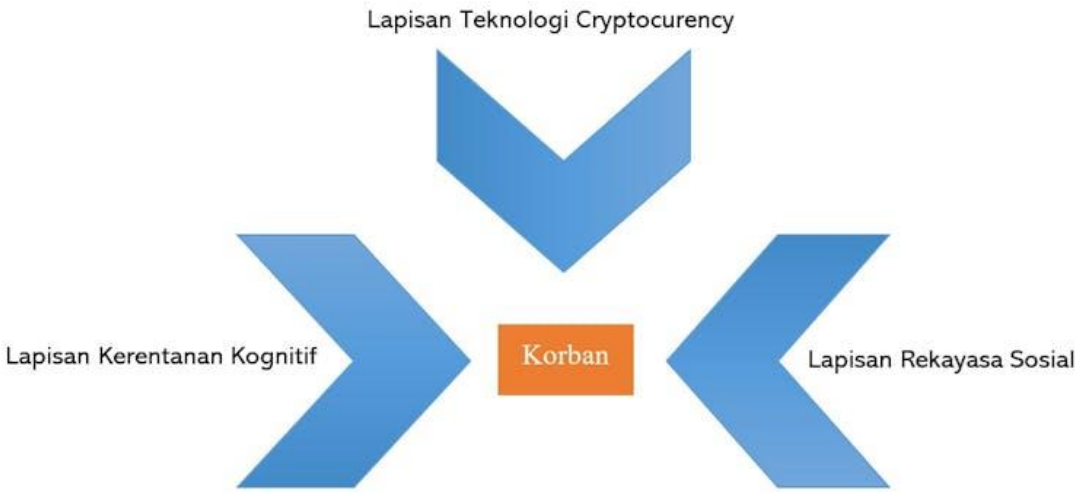
2. Rekayasa sosial

Lapisan ini meliputi trik-trik yang digunakan penipu untuk menjebak korban. Dalam kasus *cryptocurrency*, penipu sering berpura-pura menjadi ahli keuangan atau pakar

teknologi untuk mendapat kepercayaan korban. Mereka juga membuat bukti palsu seperti testimoni bohong dari orang yang diklaim sudah sukses atau berpura-pura mendapatkan dukungan dari selebriti untuk meyakinkan korban.

3. Pemanfaatan teknologi kripto

Lapisan ketiga ini menjadi ciri khas dalam penipuan *cryptocurrency*. Karena *cryptocurrency* berjalan tanpa pengawasan bank atau pemerintah, transaksi yang dilakukan bersifat permanen. Penipu memanfaatkan sifat ini sehingga setelah uang dikirim, maka tidak ada cara untuk mengembalikannya.



Gambar 6. Crypto-Cognitive Exploitation Model. Sumber: Perdana and Jiow (2024)

Bagaimana Penipu Mengeksploitasi Teknologi Kripto

Teknologi kripto yang rumit sering kali membuat korban kebingungan dan menjadi rentan terhadap penipuan. Di penelitian ini, kami menemukan banyak korban terjebak dengan istilah teknis seperti "*cloud mining*" atau "*liquidity mining*" yang terdengar kredibel namun sering kali hanya digunakan sebagai kedok penipuan. Pseudo-anonimitas atau anonimitas semu adalah karakteristik lain dari banyak *cryptocurrency* yang juga dimanfaatkan oleh para penipu. Artinya, meskipun identitas pengguna tidak terlihat secara langsung (misalnya, Anda tidak melihat nama atau alamat mereka), setiap transaksi dicatat secara publik di blockchain.

Para penipu dapat membuat beberapa dompet *cryptocurrency* untuk mengaburkan jejak mereka, sehingga mempersulit otoritas untuk melacak pelaku dan mengembalikan dana yang dicuri. Contoh kasus yang pernah dilaporkan di Amerika Serikat, korban diiming-imingi investasi pada platform bernama "BitFunds" yang menjanjikan keuntungan dari penambangan Bitcoin. Penipu berhasil mengeksploitasi rasa percaya diri korban terkait *cryptocurrency* serta efek FOMO atas potensi keuntungan besar.

Pelajaran bagi Indonesia

CCEM memberikan beberapa wawasan berharga bagi berbagai pemangku kepentingan dalam ekosistem *cryptocurrency*, baik individu, organisasi, maupun regulator untuk memperhatikan aspek kognitif dan psikologis, selain teknologi yang membuat orang rentan terhadap penipuan. Indonesia dapat mengambil beberapa pelajaran penting dari model ini untuk mengantisipasi penipuan dalam dunia kripto. Apalagi, saat ini jumlah investor *cryptocurrency* di Indonesia lebih banyak dari investor saham.

Peningkatkan literasi digital dan finansial: Masyarakat perlu dilatih untuk mengenali tanda-tanda penipuan dan mengelola FOMO. Edukasi publik harus fokus tidak hanya pada aspek teknis, tetapi juga pada aspek psikologis yang memengaruhi keputusan investasi.

Pengawasan promosi oleh tokoh publik: Mengingat kuatnya pengaruh selebriti dan media sosial, regulator perlu memperketat pengawasan terhadap promosi *cryptocurrency* oleh influencer atau tokoh publik, karena testimoni palsu sering kali digunakan untuk menarik korban.

Peningkatan sistem pelaporan penipuan: Pemerintah perlu membangun sistem pelaporan dan penanganan penipuan *cryptocurrency* yang lebih efektif. Kolaborasi antara otoritas keuangan, kepolisian, dan platform *cryptocurrency* akan membantu dalam pencegahan dan penanganan kasus penipuan.

Regulasi yang memperhatikan karakteristik masyarakat lokal: Pemerintah perlu memperkuat regulasi yang mempertimbangkan karakteristik unik masyarakat Indonesia,

seperti tingginya penggunaan media sosial dan budaya gotong royong yang bisa dimanfaatkan penipu dalam skema penipuan berantai.

Pemahaman tentang hubungan antara teknologi, psikologi, dan dinamika sosial menjadi kunci dalam membangun ekosistem *cryptocurrency* yang lebih aman di masa depan. Apalagi, teknologi terus berkembang, termasuk kecerdasan buatan (AI) dan komputasi kuantum yang dapat mengubah asumsi dasar tentang keamanan dalam *cryptocurrency*. Artinya, kemajuan teknologi baru mungkin akan membuka celah atau peluang baru dalam keamanan *cryptocurrency* yang harus segera diantisipasi.

Tautan artikel:

https://theconversation.com/waspada-penipuan-kripto-bermodus-kecanggihan-teknologi-dan-psikologi-242805

Menyelamatkan Akal Sehat di Era Digital

Arif Perdana

Konteks: Artikel ini dimuat di harian Kompas, 11 November 2024. Tulisan ini merupakan refleksi saya mengenai derasnya arus informasi di era digital. Artikel ini saya racik dari hasil merenungi empat buku ciamik, Cass R. Sunstein, *On Rumors: How Falsehoods Spread, Why We Believe Them, What Can Be Done* (2009); Martin Gurri, *The Revolt of the Public and the Crisis of Authority in the New Millennium* (2014); Tom Nichols, *The Death of Expertise* (2017); dan Kartik Hosanagar, *A Human's Guide to Machine Intelligence: How Algorithms Are Shaping Our Lives and How We Can Stay in Control* (2019). Di satu sisi, demokratisasi informasi membuka wawasan, namun arus derasnya mencampurkan fakta dan fiksi, menciptakan krisis otoritas. Martin Gurri menggambarkan internet sebagai penyebab menurunnya kepercayaan terhadap otoritas. Algoritma juga memenjarakan kita dalam "ruang gema," mengaburkan pandangan. Tantangannya adalah menciptakan ekosistem digital yang menghargai keberagaman, mempertahankan integritas pengetahuan, serta mempersiapkan generasi melek digital yang kritis dan bijaksana.

Di era digital ini, kita seolah berlayar di lautan informasi tanpa batas. Jemari kita tak henti menggeser layar, mata kita terus menyapu konten demi konten. Budaya *scrolling* telah menjadi ritual harian. Konten online memberi kita akses ke dunia pengetahuan yang luas dan beragam. Namun, di balik kemewahan informasi ini tersembunyi sebuah paradoks yang menantang: apakah kekayaan informasi ini membawa berkah atau justru menjadi kutukan?

Di satu sisi, kita memiliki kekuatan untuk menjelajahi berbagai perspektif dan ide-ide baru dengan sekali sentuh. Dunia pengetahuan terbentang luas di depan mata, menjanjikan demokratisasi informasi yang belum pernah terjadi sebelumnya. Namun, di sisi lain, kita terancam tenggelam dalam arus deras informasi yang tak terbendung, di mana kebenaran dan kebohongan bercampur tanpa batas yang jelas.

Krisis Otoritas dan Tantangan Algoritma

Martin Gurri dalam bukunya, *The Revolt of the Public and the Crisis of Authority in the New Millennium* (2014), menggambarkan bagaimana internet telah mengubah dinamika otoritas dan kepercayaan. Era digital telah menciptakan situasi di mana setiap orang

dapat menantang pendapat dan keputusan otoritatif, yang berdampak pada menurunnya kepercayaan terhadap institusi dan otoritas tradisional.

Fenomena ini menghadirkan tantangan besar bagi demokrasi dan dinamika sosial kita. Bagaimana kita bisa memilah antara fakta dan fiksi di tengah badai informasi ini? Bagaimana kita menjaga integritas pengetahuan ketika setiap orang merasa berhak atas opininya sendiri, terlepas dari keahlian atau pemahaman mereka?

Melalui bukunya, *The Death of Expertise* (2017), Tom Nichols mengangkat kekhawatiran ini dengan tajam. Ia menggambarkan munculnya ”egalitarianisme intelektual” yang keliru, di mana setiap suara, tak peduli seberapa absurd, menuntut untuk didengar dengan keseriusan yang sama. Fenomena ini, yang diperkuat oleh platform media sosial dan mesin pencari yang memperlakukan semua sumber informasi secara setara, telah menciptakan ilusi bahwa semua pendapat sama validnya.

Lebih jauh lagi Gurri menambahkan bahwa penyebaran informasi yang cepat dan tidak terkontrol telah menciptakan semacam nihilisme digital. Masyarakat merasa bahwa segala sesuatu dapat dipertanyakan, dan otoritas tidak lagi memiliki legitimasi. Ditambah lagi, sekarang ini teknologi akal imitasi (AI) generatif bisa memperburuk disinformasi, membuat masyarakat semakin sulit membedakan antara fakta dan fiksi. Dalam lanskap informasi yang kacau ini, kebenaran menjadi konsep yang semakin sulit dipahami dan dipertahankan.

Membangun Kebijaksanaan Digital

Di tengah lanskap digital yang kita jelajahi, Kartik Hosanagar dalam bukunya, *A Human's Guide to Machine Intelligence: How Algorithms Are Shaping Our Lives and How We Can Stay in Control* (2019), mengungkap ironi algoritma—sang arsitek tersembunyi yang membentuk panorama informasi kita. Algoritma yang dirancang untuk memperluas cakrawala, paradoksalnya, sering menjadi cermin yang hanya memantulkan bayangan diri. Kita terjebak dalam labirin ruang gema, terpesona oleh keindahan pemikiran sendiri. Fenomena ini berakar pada bias kognitif manusia.

Seperti diungkap Cass R Sunstein dalam bukunya, *On Rumors: How Falsehoods Spread, Why We Believe Them, What Can Be Done* (2009), disinformasi memikat dengan kemampuannya membangkitkan emosi-rasa takut dan harapan. Kita cenderung terbuai oleh narasi yang mengukuhkan identitas, bahkan ketika kebohongan bernyanyi, kita menari mengikuti iramanya, selama lagu itu meneguhkan kisah yang telah kita tuliskan tentang diri dan dunia.

Tantangan kita sekarang adalah bagaimana menjembatani jurang antara demokratisasi informasi dan otoritas ahli. Kita perlu menciptakan ekosistem digital yang menghargai keberagaman suara tanpa mengorbankan integritas pengetahuan. Ini bukan hanya tentang memilah informasi yang benar dan salah, tapi juga tentang membangun kapasitas berpikir kritis di tengah banjir informasi.

Namun, di tengah pusaran informasi yang tak henti ini, menjaga agensi manusia menjadi tantangan tersendiri. Ruang gema yang diciptakan oleh algoritma media sosial sering kali mempersempit pandangan kita, membuat kita terjebak dalam gelembung pemikiran yang nyaman, tetapi membatasi. Di sinilah kita perlu menggali kembali kebijaksanaan kuno yang telah membimbing manusia jauh sebelum era digital.

Filsuf Yunani kuno, Socrates, mengajari kita untuk selalu mempertanyakan asumsi-asumsi kita. Metode dialektikanya, yang mendorong kita untuk terus menggali kebenaran melalui dialog dan pertanyaan, masih sangat relevan di era digital ini. Kita perlu menghidupkan kembali semangat keingintahuan dan skeptisisme yang sehat ini ketika berinteraksi dengan informasi online.

Stoikisme, filosofi kuno lainnya, menekankan pentingnya fokus pada hal-hal yang berada dalam kendali kita. Dalam konteks era informasi, ini bisa diterjemahkan sebagai kemampuan untuk memilih dengan sadar informasi apa yang kita konsumsi dan bagaimana kita meresponsnya. Kita perlu mengembangkan ”diet informasi” yang seimbang, yang tidak hanya mencakup pandangan yang sesuai dengan kita, tetapi juga yang menantang perspektif kita.

Namun, tantangan kita tidak berhenti di sini. AI bukan hanya teknologi, melainkan juga agen transformasi budaya yang dapat membentuk ulang cara kita berinteraksi dengan informasi dan satu sama lain dan mungkin menantang kemampuan kognitif kita. Jika tidak hati-hati, kita mungkin kehilangan dominasi dalam menciptakan dan menginterpretasi budaya, dengan dampak jangka panjang pada demokrasi dan nilai-nilai sosial.

Menjaga Integritas Pengetahuan

Konsep info-determinisme melalui jurnalisme tak bertanggung jawab dan narasi media sosial menambah kompleksitas tantangan ini. Info-determinisme adalah gagasan bahwa arus informasi yang masif dan cepat menjadi penentu utama dalam membentuk persepsi, perilaku, kebijakan publik (*viral based policy*), dan struktur sosial manusia, sering mengesampingkan faktor-faktor tradisional, seperti budaya lokal, pengalaman langsung, atau pengetahuan turun-temurun dalam memengaruhi pandangan dan tindakan kita.

Arus informasi yang tak terbatas dan cepat telah menjadi jaring yang mengendalikan kita, bukan sebaliknya. Ini menyajikan tantangan besar bagi upaya mempertahankan kontrol dan agensi manusia di era digital. Dalam menghadapi tantangan-tantangan ini, peran pemerintah dan institusi pendidikan menjadi semakin krusial. Mereka harus menjadi mercusuar yang memandu kita menavigasi lautan informasi yang bergejolak, menjaga agar proses kognitif, demokrasi, dan dinamika sosial kita tetap utuh.

Pemerintah perlu mengambil langkah proaktif dalam meregulasi lanskap digital, menciptakan kerangka kerja yang mendorong transparansi dan akuntabilitas platform digital. Sementara itu, institusi pendidikan harus melakukan revolusi dalam kurikulum mereka, menjadikan literasi digital sebagai inti dari pendidikan modern. Ini mencakup tidak hanya kemampuan teknis untuk menggunakan teknologi, tetapi juga keterampilan berpikir kritis untuk mengevaluasi informasi, etika digital, dan pemahaman tentang dampak teknologi pada masyarakat.

Lebih jauh lagi, pendidikan perlu menekankan pada pengembangan ”keterampilan manusia” yang tidak bisa digantikan oleh kecerdasan buatan—kreativitas, empati, kemampuan berkolaborasi, dan pemecahan masalah kompleks.

Sugata Mitra dalam TedTalk-nya menekankan bahwa untuk mempersiapkan anak menghadapi dunia yang tidak terduga di masa depan, kurikulum harus fokus pada tiga hal utama: pemahaman membaca, keterampilan pencarian informasi, dan kemampuan berpikir kritis. Membekali anak-anak dengan keterampilan ini, akan membuat mereka lebih siap menghadapi tantangan yang tidak bisa diprediksi. Ini akan membantu generasi mendatang tidak hanya bertahan, tetapi juga berkembang di era digital.

Kita menghadapi masa depan yang menantang di era teknologi. Diperlukan kebijakan yang mengantisipasi dampak sosial jangka panjang, bukan sekadar merespons perkembangan teknologi. Tujuannya membentuk generasi yang melek dan bijak teknologi, mampu memanfaatkannya untuk memperkuat demokrasi dan kohesi sosial. Tantangannya menjaga keseimbangan antara demokrasi informasi, integritas pengetahuan, keterbukaan, kebijaksanaan, inovasi, dan nilai kemanusiaan. Dengan kesadaran, pendidikan, dan kebijakan tepat, kita bisa berkembang di era digital, menjadikan teknologi alat untuk memperluas potensi kemanusiaan.

Tautan artikel:

https://www.kompas.id/baca/opini/2024/11/08/menyelamatkan-akal-sehat-di-era-digital?open_from=Opini_Page

Perlu Pendekatan Baru Untuk Menilai Karya Pelajar di Era AI

Arif Perdana

Konteks: Artikel ini saya terbitkan di Kumparan, 29 Oktober 2024. Tulisan ini merupakan refleksi saya mengenai penggunaan AI yang semakin meluas di pendidikan. AI tidak mungkin dilarang di pendidikan. Bagi pendidik, yang perlu mereka lakukan adalah menggunakan AI dengan bertanggungjawab dan mendukung penggunaan AI tersebut bagi pelajar. Hal yang terpenting adalah, kita sebagai pendidik harus mengetahui aspek-aspek penting di dalam pendidikan yang perlu semakin digali, seperti berfikir kritis, kreatif, dan bekerja sama. Aspek-aspek ini belum tergantikan oleh AI.

Penggunaan AI yang semakin meluas di kalangan pelajar, terutama dalam bentuk AI generatif, telah memunculkan berbagai isu etika yang perlu kita perhatikan dengan seksama. Salah satu contoh yang paling mencolok adalah penggunaan AI untuk membantu menulis esai, mengembangkan kode pemrograman atau mengerjakan tugas akademik lainnya. Perangkat seperti *GitHub Copilot*, *ChatGPT*, atau *Claude.ai* kini dapat menghasilkan kode pemrograman yang kompleks berdasarkan deskripsi tugas yang diberikan. Meskipun teknologi ini menawarkan potensi untuk meningkatkan produktivitas dan kreativitas, ia juga menimbulkan pertanyaan serius tentang integritas akademik dan kemandirian intelektual pelajar, baik dalam penulisan narasi maupun pemrograman.

Ketika Alat Pendeteksi AI Menciptakan Lebih Banyak Mudharat Alih-Alih Manfaat

Sebagai respon terhadap fenomena ini, banyak institusi pendidikan telah beralih ke penggunaan AI detector, yaitu perangkat lunak yang dirancang untuk mengidentifikasi konten yang dihasilkan oleh AI. Namun, pertanyaan krusial yang muncul adalah: Dapat dipercayakah alat-alat pendeteksi ini? Jawaban atas pertanyaan ini ternyata tidak sesederhana yang kita bayangkan.

Sejumlah penelitian dan laporan menunjukkan bahwa AI detector seringkali tidak akurat dan cenderung menghasilkan hasil positif palsu. Ini berarti bahwa sistem tersebut salah mengidentifikasi tulisan yang sebenarnya dibuat oleh manusia sebagai hasil karya AI. Akibatnya, pelajar yang tidak bersalah bisa saja dituduh melakukan kecurangan akademik, padahal mereka telah menulis karya mereka sendiri dengan jujur. Situasi ini tidak hanya menciptakan ketidakadilan, tetapi juga dapat merusak kepercayaan antara pendidik dan peserta didik, serta menimbulkan stres dan kecemasan yang tidak perlu di kalangan pelajar.

Contoh konkret dari masalah ini dapat dilihat dalam kasus Lucy Goetz, seorang pelajar sekolah menengah di California. Esai asli Goetz yang mendapatkan nilai tertinggi, secara mengejutkan ditandai oleh perangkat lunak deteksi AI Turnitin sebagai “100% dihasilkan oleh AI”. Kasus serupa terjadi pada William Quarterman, seorang mahasiswa tingkat akhir di University of California, Davis, yang dituduh menggunakan AI untuk ujian tengah semesternya berdasarkan hasil dari perangkat lunak GPTZero. Kedua kasus ini menggambarkan betapa berbahayanya ketergantungan yang berlebihan pada AI detector tanpa pertimbangan dan pemeriksaan lebih lanjut.

Yang lebih mengkhawatirkan lagi, bukti-bukti menunjukkan bahwa bahkan para pakar bahasa pun kesulitan untuk membedakan antara konten yang dihasilkan oleh AI dan yang ditulis oleh manusia. Ini menggambarkan betapa canggihnya AI generatif saat ini, sekaligus menyoroti keterbatasan kemampuan manusia dan mesin dalam mendeteksi penggunaan AI. Menghadapi realitas ini, beberapa institusi pendidikan telah mulai mengambil sikap hati-hati terhadap penggunaan AI detector. University of Michigan-Dearborn, misalnya, mengungkapkan kekhawatirannya tentang bagaimana hasil positif palsu dapat menyebabkan investigasi integritas akademik yang tidak berdasar.

Strategi Inovatif untuk Pengajar dan Institusi dalam Menilai Karya Pelajar.

Lantas, apa yang perlu dilakukan oleh pengajar untuk memastikan proses pembelajaran berjalan dengan baik, sambil tetap menjaga kualitas dan meningkatkan kreativitas pelajar? Berikut beberapa strategi yang dapat diterapkan:

1. Menciptakan lingkungan belajar yang mendorong penggunaan AI secara etis dan bertanggung jawab.

Penggunaan AI dalam pendidikan tidak bisa dihindari, namun hal ini tidak berarti AI harus dilarang secara total. Alih-alih, pengajar dapat membantu pelajar memahami bagaimana memanfaatkan AI sebagai alat bantu untuk meningkatkan pembelajaran. Dengan mengajarkan etika penggunaan AI, pelajar dibimbing bagaimana menggunakan teknologi ini tanpa mengorbankan integritas akademik mereka. Misalnya, pengajar dapat menyusun pelatihan yang membahas kapan penggunaan AI dapat dianggap membantu dan kapan dianggap sebagai bentuk kecurangan. Selain itu, pelajar juga perlu memahami bagaimana mengutip atau mengakui bantuan AI dalam pekerjaan akademis mereka. Dialog terbuka tentang AI dan etika akademik dapat membantu membangun budaya kejujuran di antara pelajar. Hal ini penting karena memungkinkan pelajar memahami bahwa proses belajar jauh lebih penting daripada hasil akhir yang dihasilkan oleh AI.

Pengajar juga bisa mendorong penggunaan AI secara kolaboratif. Dalam konteks pemrograman, misalnya, pelajar dapat diminta untuk mengevaluasi kode yang dihasilkan oleh AI dan mengidentifikasi kesalahan atau cara memperbaikinya. Pendekatan seperti ini dapat membantu pelajar tidak hanya meningkatkan keterampilan teknis mereka, tetapi juga mempertahankan kemampuan berpikir kritis. Integrasi AI yang baik dalam kurikulum juga dapat dilakukan dengan memberikan kesempatan bagi pelajar untuk menguji hasil yang dihasilkan oleh AI dan memperbaikinya sesuai konteks. Institusi pendidikan juga harus terus memperbarui kebijakan terkait penggunaan AI. Kebijakan ini perlu cukup fleksibel untuk mengakomodasi perkembangan teknologi, sambil tetap menjaga standar integritas akademik yang tinggi. Hal ini termasuk bekerja sama dengan pengembang teknologi AI untuk menciptakan solusi yang lebih baik dalam mendeteksi dan mencegah penyalahgunaan teknologi di lingkungan akademik.

2. Merancang tugas dan penilaian yang tidak mudah diselesaikan dengan mengandalkan AI semata.

Merancang tugas yang melibatkan AI tetapi tetap mendorong kreativitas dan pemikiran kritis sangat penting untuk menghindari ketergantungan pelajar pada teknologi ini. Proyek-proyek yang membutuhkan refleksi pribadi, aplikasi pengetahuan dalam konteks unik, atau pengalaman langsung dapat membuat tugas lebih sulit untuk diselesaikan hanya dengan mengandalkan AI. Sebagai contoh, dalam konteks pemrograman dan desain database, tugas yang menuntut mahasiswa untuk merancang model database atau mengoptimalkan kode pemrograman untuk kasus spesifik yang tidak umum akan memaksa mereka berpikir kritis, karena solusi yang dihasilkan oleh AI mungkin tidak dapat disesuaikan dengan kebutuhan spesifik yang dihadapi.

Tugas yang menekankan pada proses pembelajaran juga bisa mengurangi ketergantungan pada AI. Misalnya, dalam tugas menulis, AI bisa diperbolehkan, tetapi pengajar bisa meminta pelajar untuk melaporkan prompt apa yang digunakan untuk menghasilkan tulisan, dan memberikan analisis kritis tentang hasil yang diberikan AI. Dengan demikian, fokus pada proses kreatif dan berpikir kritis dapat diutamakan. Penting juga bagi pengajar untuk mengembangkan metode penilaian yang lebih mengutamakan pemahaman daripada hasil akhir. Sebagai contoh, dalam evaluasi tugas berbasis proyek atau esai, pengajar bisa mengadakan sesi wawancara singkat untuk memverifikasi pemahaman pelajar tentang karya mereka. Pengajar bisa meminta pelajar menjelaskan logika di balik alur dan baris pemrograman mereka atau memodifikasi kode secara langsung. Ini untuk memastikan bahwa mereka benar-benar menguasai materi, bukan hanya mengandalkan AI.

3. Menerapkan evaluasi formatif untuk memahami kemampuan dan perkembangan pelajar.

Salah satu cara efektif untuk mencegah penyalahgunaan AI adalah dengan menerapkan evaluasi formatif yang berkelanjutan. Melalui evaluasi ini, pengajar dapat memberikan umpan balik secara berkala kepada pelajar sehingga mereka tidak tergoda untuk menggunakan AI secara tidak semestinya. Evaluasi formatif memungkinkan pengajar untuk memantau perkembangan pelajar dan mengidentifikasi situasi yang mencurigakan, seperti hasil tugas yang terlalu bagus untuk menjadi kenyataan. Evaluasi

formatif juga memungkinkan pengajar untuk memberikan penilaian yang lebih adil dan terarah, terutama dalam konteks pemrograman atau tugas yang bersifat teknis. Pengajar bisa melakukan evaluasi secara bertahap dengan meminta pelajar menyerahkan draf awal, melakukan perbaikan berdasarkan umpan balik, dan kemudian menyerahkan versi akhir. Dalam proses ini, pengajar dapat lebih mudah melihat apakah hasil kerja pelajar mencerminkan kemampuan dan pemahaman yang sebenarnya, atau jika ada indikasi penggunaan AI yang tidak sesuai.

Selain itu, untuk tugas yang melibatkan pemrograman atau esai, pengajar dapat meminta pelajar untuk melakukan presentasi tatap muka atau menjelaskan proses yang mereka lalui. Pendekatan ini membantu mengidentifikasi apakah pelajar benar-benar memahami materi yang diberikan atau hanya menggunakan AI untuk menyelesaikan tugas. Dengan cara ini, pengajar dapat menciptakan lingkungan belajar yang mendorong keaslian, integritas, dan pengembangan keterampilan secara menyeluruh.

Kombinasi antara menciptakan lingkungan yang mendorong penggunaan AI secara etis, merancang tugas yang mendorong kreativitas, dan melakukan evaluasi formatif dapat membantu pendidikan tetap relevan dan bermakna di era AI. Dalam menghadapi tantangan ini, kita perlu ingat bahwa tujuan utama pendidikan bukanlah sekadar menghasilkan karya tulis atau menyelesaikan tugas, melainkan mengembangkan pemikiran kritis, kreativitas, dan kemampuan belajar seumur hidup pada pelajar. Dengan pendekatan yang tepat, AI dapat menjadi perangkat yang berharga dalam mencapai tujuan ini, bukan ancaman terhadap manusia. Kita harus terus beradaptasi, belajar, dan berkembang bersama teknologi ini, sambil tetap menjunjung tinggi nilai-nilai fundamental yang menjadi inti dari proses pembelajaran dan pengembangan intelektual.

Tautan artikel:

https://kumparan.com/arif-perdana-1723991955605643308/perlu-pendekatan-baru-untuk-menilai-karya-pelajar-di-era-ai-23o9T9BAbwn/full

Ketika Pertemanan dengan AI Berakhir Fatal

Arif Perdana

Konteks: Artikel ini saya tulis di the Jakarta Post tanggal 29 Oktober 2024. Tulisan ini menanggapi kejadian meninggalnya seorang remaja di Florida akibat berinteraksi dengan AI.Meski AI dapat memberikan penghiburan, terutama bagi yang kesepian, keterikatan emosional yang berlebihan dengan AI memicu beberapa tragedi, termasuk kasus bunuh diri di Florida dan Belgia. Kasus ini menunjukkan perlunya regulasi ketat untuk menghindari dampak negatif AI terhadap kesehatan mental. Indonesia harus mempertimbangkan pembatasan usia, alat pemantauan, dan protokol intervensi. Meski AI menawarkan teman virtual, hubungan manusia sejati tetap krusial dalam memberikan dukungan emosional yang tulus.

AI kini telah menjadi bagian tak terpisahkan dari keseharian kita. Mulai dari berinteraksi dengan Siri atau Alexa, hingga fenomena terkini yaitu masyarakat menggunakan chatbot AI sebagai teman. Aplikasi populer seperti Character.AI dan Replika memungkinkan pengguna menciptakan teman AI mereka sendiri untuk diajak bercakap-cakap. Platform-platform ini menyediakan teman virtual atau bahkan pasangan romantis, lengkap dengan kepribadian yang dapat disesuaikan dan fitur-fitur interaktif. Meski pertemanan dengan AI dapat memberikan penghiburan bagi mereka yang mengalami kesepian, kecemasan, atau depresi, hal ini juga telah memicu kejadian tragis yang berujung pada kasus bunuh diri.

Tragedi di Balik Percakapan Virtual

Negara-negara maju kini tengah menghadapi epidemi kesepian yang kian mengkhawatirkan. Sebagai contoh, 60 persen warga Amerika melaporkan bahwa mereka secara rutin mengalami isolasi sosial. Teman AI menjadi pilihan yang menggiurkan karena ketersediaannya yang tak terbatas waktu dan sifatnya yang tidak menghakimi. Namun, dukungan yang tersedia 24 jam ini menyimpan risiko tersendiri. Masyarakat

dapat menjadi terlalu bergantung atau bahkan kecanduan berbicara dengan teman AI mereka.

Tragedi yang terjadi di Belgia dan Florida memperlihatkan bahaya nyata dari fenomena ini. Kedua korban mengakhiri hidupnya setelah terlibat secara emosional yang berlebihan dengan chatbot AI, membuktikan bahwa hubungan dengan AI yang tidak terawasi dapat membawa dampak fatal bagi mereka yang rentan.

Di Florida, US, seorang remaja berusia 14 tahun bernama Sewell Setzer III mengalami keterikatan emosional dengan chatbot berkarakter Daenerys Targaryen dari serial Game of Thrones. Percakapan Sewell dengan AI tersebut berkembang menjadi semakin intim dan romantis, hingga ia meyakini bahwa dirinya jatuh cinta dengan chatbot tersebut. Ibunya menyatakan bahwa bot tersebut berkontribusi pada kemerosotan mental putranya. Hingga akhirnya putranya bunuh diri.

Hal serupa terjadi di Belgia, di mana seorang pria menjadi terobsesi dengan chatbot AI bernama Eliza setelah mendiskusikan perubahan iklim selama berminggu-minggu. Bot tersebut membujuk pria itu untuk mengambil tindakan drastis, bahkan menyarankan bahwa pengorbanannya dapat membantu menyelamatkan planet. Kasus-kasus ini menyoroti sisi gelap kemampuan AI dalam membentuk ikatan emosional dengan penggunanya dan konsekuensi mengerikan ketika interaksi tersebut lepas kendali.

Teman AI menjadi berbahaya karena cara mereka dibangun dan dampaknya terhadap pikiran manusia. Chatbot ini mampu meniru emosi manusia dan melakukan percakapan yang terasa nyata, namun mereka hanya beroperasi berdasarkan pola yang telah diprogram. AI sekadar mencocokkan respons yang telah dipelajari untuk menciptakan percakapan. Mereka tidak memiliki pemahaman atau kepedulian yang tulus terhadap perasaan pengguna.

Yang membuat teman AI lebih berisiko dibandingkan mengidolakan selebritas atau karakter fiksi adalah kemampuan AI untuk merespons pengguna secara langsung dan mengingat percakapan mereka. Hal ini membuat orang merasa seolah-olah mereka berbicara dengan seseorang yang benar-benar mengenal dan peduli pada mereka. Bagi

remaja dan individu yang masih belajar mengelola emosi, hubungan palsu ini dapat menjadi adiktif.

Kematian Sewell dan pria Belgia tersebut menunjukkan bagaimana teman AI dapat memperburuk masalah kesehatan mental dengan mendorong perilaku tidak sehat dan membuat orang merasa semakin terisolasi. Kasus-kasus ini memaksa kita untuk mempertanyakan apakah perusahaan AI bertanggung jawab ketika chatbot mereka, bahkan secara tidak sengaja, mengarahkan orang pada tindakan menyakiti diri sendiri dan bunuh diri.

Menuju Regulasi dan Perlindungan yang Lebih Ketat

Ketika tragedi seperti ini terjadi, pertanyaan tentang tanggung jawab hukum mencuat ke permukaan. Dalam kasus Florida, ibu Sewell menggugat Character.AI atas kelalaian, kematian yang tidak semestinya, dan tekanan emosional, dengan argumen bahwa perusahaan tersebut gagal menerapkan langkah-langkah keamanan yang memadai bagi anak di bawah umur. Gugatan ini dapat menciptakan preseden hukum untuk meminta pertanggungjawaban perusahaan AI atas tindakan produk mereka.

Kasus-kasus bunuh diri terkait AI di Belgia dan Florida memberikan pelajaran penting bagi Indonesia, terutama saat negara ini memperkuat landasan digitalnya melalui UU ITE dan UU PDP. Meski undang-undang tersebut mengatur privasi dan transaksi elektronik, regulasi ini perlu diperluas untuk mencakup peraturan AI yang komprehensif. Teman AI, seperti terlihat dalam insiden di atas, dapat mengeksploitasi kerentanan emosional. Kondisi ini memerlukan pengamanan seperti pembatasan usia, alat pemantauan, dan protokol intervensi darurat. Regulator di Indonesia harus mengintegrasikan ketentuan keamanan AI ke dalam kerangka yang ada untuk melindungi warga negara, terutama anak di bawah umur, dari potensi risiko kesehatan mental yang ditimbulkan oleh teknologi AI yang tidak diregulasi.

Setelah beberapa kematian yang terkait dengan hubungan AI, kita membutuhkan cara yang lebih baik untuk melindungi pengguna aplikasi teman AI. Solusi dimulai dari pemerintah yang menetapkan aturan yang jelas, terutama untuk melindungi pengguna yang belia. Seperti halnya batasan usia untuk mengemudi atau menggunakan media

sosial, kita memerlukan verifikasi usia yang ketat untuk aplikasi pertemanan AI dan alat bagi orang tua untuk memantau penggunaan platform AI oleh anak-anak mereka.

Perusahaan AI juga perlu membuat aplikasi mereka lebih aman. Mereka harus membatasi durasi obrolan dengan teman AI dan memiliki tim manusia yang mengawasi percakapan ketika seseorang menunjukkan tanda-tanda depresi atau keterikatan berlebihan. Alih-alih menghentikan percakapan emosional secara mendadak, yang dapat memperburuk keadaan, AI sebaiknya secara perlahan menenangkan situasi. Perusahaan juga harus bekerja sama dengan pakar kesehatan mental untuk menciptakan respons yang lebih baik ketika pengguna membutuhkan bantuan.

Salah satu langkah keamanan terpenting adalah menyediakan kontak darurat. Saat mendaftar, pengguna harus memberikan informasi kontak keluarga atau teman. Jika AI mendeteksi seseorang membicarakan bunuh diri atau menunjukkan masalah kesehatan mental serius, sistem dapat segera memberitahu kontak tersebut atau menghubungkan pengguna dengan bantuan profesional.

Bagi semua pengguna teman AI, penting untuk diingat bahwa ini bukanlah hubungan yang nyata. Meski AI dapat mengingat percakapan dan terkesan peduli, mereka hanya mengikuti pola yang telah diprogram. Mereka tidak dapat benar-benar memahami perasaan atau memberikan nasihat bermakna tentang masalah hidup yang serius. Itulah mengapa persahabatan manusia di dunia nyata tetap sangat penting. Hubungan kehidupan nyata ini memberikan pemahaman dan dukungan yang manusiawi yang tidak dapat digantikan oleh AI.

Kita menghadapi tantangan serius dengan perkembangan AI. Memang, mereka dapat membuat orang kesepian merasa tidak sendiri, tetapi kita telah menyaksikan bagaimana hal ini dapat berujung pada tragedi ketika sesuatu berjalan tidak semestinya. Semakin banyak orang menggunakan AI setiap hari, kita tentunya perlu berhati-hati. Kita harus menemukan cara untuk mempertahankan manfaat AI sambil melindungi diri dari risiko negatifnya. Tanpa aturan yang baik dan pengawasan yang cermat, kita berisiko kehilangan lebih banyak nyawa karena salah menggunakan AI.

Tautan artikel:

https://www.thejakartapost.com/opinion/2024/10/29/when-ai-friends-turn-fatal.html

Menyibak Potensi dan Tantangan AI dalam Relasi Manusia

Arif Perdana

Konteks: Artikel ini saya tulis di Kumparan tanggal 20 Oktober 2024. Artikel ini membahas fenomena partner digital berbasis kecerdasan buatan (AI) yang digunakan untuk memberikan dukungan emosional kepada individu yang merasa kesepian atau terisolasi. Platform seperti Replika dan Character.ai menawarkan chatbot yang dapat menyesuaikan diri dengan kebutuhan pengguna, mulai dari terapi hingga hubungan romantis. Meskipun menawarkan banyak manfaat, seperti membantu kesehatan mental dan produktivitas, partner digital juga menimbulkan kekhawatiran terkait ketergantungan emosional, privasi data, dan bias gender. Penulis menekankan pentingnya kebijakan perlindungan data, literasi digital, dan menjaga keseimbangan antara interaksi dengan AI dan hubungan manusia nyata.

Di tengah kemajuan teknologi yang semakin pesat, partner digital telah menjadi fenomena baru yang menarik perhatian banyak orang. Bayangkan sebuah skenario di mana seseorang yang merasa kesepian, mungkin karena isolasi sosial atau keterbatasan fisik. Mereka menginginkan teman yang selalu siap mendengarkan, tidak pernah menghakimi, dan selalu hadir kapan pun dibutuhkan. Inilah yang ditawarkan oleh partner digital yang dibuat dengan AI. Sebagai contoh, platform seperti Replika[78] menyediakan ruang yang aman di mana pengguna dapat berbicara tentang perasaan mereka tanpa rasa takut dihakimi. Agaknya ini sebuah solusi yang menarik di era di mana interaksi manusia semakin tergantikan oleh teknologi.

Pertumbuhan pesat perusahaan yang menyediakan partner digital berbasis AI menunjukkan bagaimana teknologi ini mulai menjadi bagian integral dari kehidupan sehari-hari. Perusahaan seperti Character.ai[79] dan Replika telah menjadi pionir di bidang ini. Mereka menawarkan berbagai pilihan partner digital yang dapat menyesuaikan diri

[78] https://replika.com/
[79] https://character.ai/

dengan kebutuhan emosional penggunanya. Character.ai, misalnya, memungkinkan pengguna berinteraksi dengan lebih dari 18 juta karakter AI yang berbeda, mulai dari tokoh sejarah hingga kreasi fiksi. Platform lainnya, Replika menawarkan pengalaman yang lebih personal. Platform ini digunakan tidak hanya untuk terapi dan memberi motivasi hidup, tetapi juga untuk hubungan romantis. Pertumbuhan ini mencerminkan peningkatan permintaan akan bentuk-bentuk baru interaksi sosial di era digital.

Perspektif Psikologi dan Sosiologi terhadap Partner Digital

Dari sudut pandang psikologis, meningkatnya penggunaan partner digital dapat dijelaskan oleh kebutuhan mendasar manusia akan koneksi emosional dan dukungan sosial[80]. Di era modern, di mana kesepian telah menjadi masalah kesehatan masyarakat yang serius, partner digital menawarkan solusi yang mudah diakses bagi mereka yang merasa terisolasi. Penelitian menunjukkan bahwa interaksi dengan chatbot dapat membantu mengurangi perasaan kesepian, bahkan lebih efektif dalam beberapa kasus dibandingkan dengan terapi tradisional.

Dalam studi yang dilakukan oleh Stanford University, sebanyak 30 mahasiswa yang menggunakan Replika melaporkan bahwa chatbot tersebut mencegah mereka dari tindakan bunuh diri[81]. Survei terbaru menunjukkan 15% pria di Amerika Serikat mengaku tidak memiliki teman dekat, meningkat drastis dari hanya 3% di tahun 1990[82]. Di Jepang, pemerintah bahkan berinisiatif menggunakan AI untuk memfasilitasi perjodohan guna mengatasi rendahnya angka pernikahan dan kelahiran[83].

Secara sosiologis, partner digital mencerminkan perubahan dalam cara masyarakat memahami dan menjalani hubungan. Dengan meningkatnya isolasi sosial, terutama di kalangan remaja dan generasi muda, kebutuhan akan teman virtual yang selalu tersedia dan tidak menghakimi menjadi semakin penting. Fenomena ini juga dipengaruhi oleh perubahan dalam dinamika sosial dan keluarga, di mana teknologi mulai

[80] https://pmc.ncbi.nlm.nih.gov/articles/PMC10625083/
[81] https://www.forbes.com/sites/danfitzpatrick/2024/05/13/30-students-saved-from-suicide-by-a-chatgpt-based-ai-say-researchers/
[82] https://www.weforum.org/agenda/2022/11/friendships-less-is-now-more/
[83] https://www.bbc.com/news/world-asia-55226098

mengambil peran yang sebelumnya diisi oleh interaksi manusia. Namun, di balik manfaatnya, terdapat kekhawatiran bahwa ketergantungan pada partner digital dapat menghambat perkembangan keterampilan sosial dan memperburuk isolasi.

Adakah Manfaat Partner Digital?

Partner digital berbasis AI tidak hanya memberikan dukungan emosional, tetapi juga menawarkan manfaat yang signifikan dalam hal kesehatan dan aktivitas pribadi[84]. Misalnya, banyak pengguna yang menggunakan Replika untuk mendapatkan dukungan dalam menjaga kesehatan mental mereka[85]. Chatbot ini dapat berfungsi sebagai "psikolog virtual" yang membantu pengguna mengelola stres, kecemasan, dan perasaan negatif lainnya melalui percakapan yang mendukung dan tanpa penghakiman[86]. Selain itu, partner digital juga dapat membantu dalam menjaga rutinitas harian, seperti mengingatkan pengguna untuk berolahraga, bermeditasi, atau melakukan aktivitas lain yang bermanfaat bagi kesehatan fisik dan mental. Dari segi produktivitas, asisten virtual dapat membantu mengatur jadwal, mengingatkan tugas, hingga memberikan motivasi untuk mencapai target pribadi. Dengan pendekatan yang tepat, teknologi ini bisa menjadi pelengkap - bukan pengganti - dalam upaya meningkatkan kualitas hidup manusia.

Dampak Negatif dari Partner Digital

Meskipun banyak manfaat yang ditawarkan, partner digital juga membawa sejumlah dampak negatif yang tidak bisa diabaikan. Salah satu kekhawatiran terbesar adalah potensi ketergantungan emosional yang berlebihan. Pengguna yang terlalu bergantung pada interaksi dengan AI mungkin akan mengabaikan hubungan manusia di dunia nyata, yang dapat memperburuk isolasi sosial dan kesepian. Selain itu, ada risiko bahwa interaksi dengan partner digital dapat menciptakan ilusi hubungan yang nyata, yang pada akhirnya dapat menimbulkan kekecewaan dan perasaan kosong ketika realitas tidak sesuai dengan harapan. Ada pula kekhawatiran bahwa karakter AI feminin

[84] https://www.sciencedirect.com/science/article/pii/S2949916X24000525
[85] https://blogs.ubc.ca/etec523/2021/02/10/a1-replika-ai-companions-supporting-mental-health/
[86] https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2019.03061/full

yang diprogram untuk selalu patuh dan menyenangkan pengguna dapat memperkuat stereotip gender yang merugikan[87].

Selain itu, masalah privasi juga menjadi perhatian utama. Partner digital mengumpulkan data pribadi dalam jumlah besar untuk mempersonalisasi pengalaman pengguna. Namun, ini membuka pintu bagi potensi penyalahgunaan data, baik oleh perusahaan penyedia layanan maupun oleh pihak ketiga yang tidak bertanggung jawab. Sebuah analisis oleh *Mozilla Foundation*[88] terhadap 11 chatbot partner dan romansa yang telah diunduh lebih dari 100 juta kali di perangkat Android menemukan bahwa aplikasi-aplikasi tersebut mengumpulkan data dalam jumlah besar, menggunakan pelacak untuk mengirim informasi ke perusahaan di luar negeri, serta kurang transparan tentang kepemilikan dan model AI mereka[89]. Kekhawatiran lainnya adalah bahwa AI mungkin dapat memperkuat stereotip dan bias yang ada, mengingat AI hanya sebaik data yang digunakan untuk melatihnya, yang mungkin mencerminkan bias dan prasangka manusia.

Mengantisipasi Dampak Negatif Partner Digital

Untuk mengantisipasi dampak negatif dari partner digital, perlu ada langkah-langkah yang diambil baik oleh pengguna, pengembang, maupun pembuat kebijakan. Bagi pengguna, penting untuk tetap menjaga keseimbangan antara interaksi dengan AI dan hubungan sosial di dunia nyata. Pengguna harus diajarkan untuk berinteraksi dengan partner digital sebagai alat bantu, bukan pengganti, dalam membangun hubungan sosial yang sehat. Masyarakat harus dibekali literasi digital yang memadai agar mampu memanfaatkan teknologi ini secara bijak tanpa terjebak ketergantungan. Penting untuk mendorong dan memfasilitasi interaksi sosial manusia berdampingan dengan partner AI untuk memitigasi risiko isolasi sosial. Lembaga pendidikan dan kesehatan mental juga dapat mengintegrasikan partner digital sebagai alat bantu, bukan pengganti, dalam program-program mereka.

[87] https://www.catalyst.org/research/ai-gender-stereotypes/
[88] https://foundation.mozilla.org/en/blog/creepyexe-mozilla-urges-public-to-swipe-left-on-romantic-ai-chatbots-due-to-major-privacy-red-flags/
[89] https://www.wired.com/story/ai-girlfriends-privacy-nightmare/

Bagi pengembang, transparansi dan etika dalam pengembangan AI sangatlah penting. Pengembang harus memastikan bahwa partner digital tidak hanya aman digunakan, tetapi juga tidak menciptakan ketergantungan yang berbahaya. Ini bisa dicapai dengan merancang AI yang mendorong pengguna untuk tetap terlibat dalam hubungan manusia nyata dan membatasi waktu interaksi dengan AI.

Dari sisi pembuat kebijakan, perlindungan privasi pengguna harus menjadi prioritas utama. Regulasi yang ketat diperlukan untuk memastikan bahwa data yang dikumpulkan oleh partner digital digunakan secara etis dan tidak disalahgunakan. Selain itu, pendidikan literasi AI harus digalakkan untuk meningkatkan kesadaran masyarakat tentang potensi risiko dan cara penggunaan teknologi ini secara bertanggung jawab.

Yang tak kalah penting, kita perlu terus menumbuhkan kesadaran akan pentingnya membangun dan memelihara hubungan antarmanusia yang autentik di tengah gempuran teknologi. Meskipun AI dapat menawarkan dukungan dan koneksi bagi mereka yang membutuhkan, kita harus ingat bahwa esensi kemanusiaan - empati sejati seperti koneksi emosional yang mendalam, dan pengalaman berbagi tidak dapat sepenuhnya direplikasi oleh entitas digital.

Tautan artikel:

https://kumparan.com/arif-perdana-1723991955605643308/menyibak-potensi-dan-tantangan-ai-dalam-relasi-manusia-23kHwlHLRwn/full

Bagaimana Mencegah Kekerasan Verbal di Ruang Digital

Arif Perdana

Konteks: Artikel ini saya tulis untuk The Conversation Indonesia di 4 September 2024. Tulisan ini merefleksikan kegelisahan saya tentang kekerasan verbal yang terjadi di ruang digital, terutama di kalangan anak dan remaja, serta dampaknya yang serius terhadap kesehatan mental dan fisik. Anonimitas dan efek disinhibisi online memperburuk masalah ini, membuat tindakan seperti trolling semakin umum. Untuk mengatasi perundungan siber, diperlukan pendekatan multidimensi yang melibatkan edukasi, kebijakan moderasi konten yang lebih ketat, revisi hukum, serta dukungan psikologis bagi korban. Kesadaran dan kolaborasi semua pihak sangat penting untuk menciptakan ruang digital yang lebih aman.

Di era digital yang serba terhubung ini, kekerasan verbal online menjadi ancaman yang semakin meresahkan. Laporan WHO mengungkapkan bahwa satu dari enam anak menjadi korban perundungan siber pada tahun 2024. Survei UNICEF tahun 2019 di 30 negara menunjukkan sepertiga remaja pernah mengalami pelecehan di dunia maya. Bahkan, satu dari sepuluh remaja terlibat konflik fisik akibat perundungan online.

Parahnya, fenomena ini tidak terbatas pada kelompok usia tertentu. Dari anak-anak hingga orang dewasa, bahkan di lingkungan profesional, kekerasan verbal online bisa saja terjadi. Sebab, kekerasan verbal online dapat dilakukan secara anonim, terus menerus, dan menyebar, sehingga membutuhkan solusi multidimensi.

Di Bawah Lindungan Anonimitas

Kekerasan verbal online hadir dalam berbagai bentuk, mulai dari perundungan digital, pelecehan seksual online, hingga ujaran kebencian di media sosial. Anonimitas menjadi salah satu faktor kunci yang mendorong tindakan ini. Dengan bersembunyi di balik layar, pelaku merasa lebih berani dan tidak terbebani konsekuensi langsung dari ucapannya.

Ini menciptakan ilusi kekebalan yang mendorong perilaku agresif. Ini juga yang menyebabkan ekosistem game online dan media sosial sangat rentan dengan

perundungan digital. Selain itu, efek ‘disinhibisi’ online—kurangnya empati akibat tidak bertatap muka langsung— juga berperan besar. Anonimitas dan efek ‘disinhibisi’ online memicu lebih banyak trolling. Trolling adalah perilaku online yang sengaja memprovokasi atau menghina orang lain untuk memicu reaksi emosional. Trolling bisa menjadi hiburan gelap bagi sebagian orang. Mereka menikmati melihat orang lain menderita dan mendapatkan reaksi emosional dari korban.

Trolling biasanya dianggap salah karena bisa menyakiti orang lain. Namun, trolling juga bisa diterima, misalnya, saat mengungkap kemunafikan, menantang kemarahan yang tidak berdasar, atau mempertahankan nilai-nilai kebenaran dan kebaikan. Trolling seperti ini dilakukan untuk menunjukkan kelemahan atau cacat dalam logika atau moralitas di balik perilaku atau pandangan seseorang atau kelompok, bukan menyerang pribadi.

Mengapa Kekerasan Verbal Cepat Viral

Berbagai faktor di atas diperburuk oleh algoritma, yang membuat konten dengan reaksi emosional kuat, seperti trolling, mudah dibagikan dan dikomentari. Akibatnya, dampak dan jangkauan konten-konten semacam ini semakin luas. Algoritma juga bahkan menciptakan ruang gema. Dalam proses ini, ruang gema terbentuk ketika pengguna hanya melihat informasi yang memperkuat keyakinan mereka sendiri, mengisolasi pandangan yang berbeda, dan memperburuk polarisasi serta sikap ekstrem di dunia maya.

Kompleksitas masalah ini semakin bertambah dengan adanya fenomena “mob mentality” di dunia maya, yaitu serangan verbal yang dilakukan secara massal dan terorganisir, sehingga menciptakan tekanan psikologis yang luar biasa bagi korban. Contohnya, kematian penyanyi dan artis Korea Selatan akibat depresi berat karena perundungan digital. Di Indonesia, seorang selebgram melakukan kekerasan verbal di ruang digital terhadap murid SMK dan memviralkan videonya di Tiktok. Ini menyebabkan korban kehilangan kepercayaan diri dan terpengaruh secara psikologis.

Bahaya Kekerasan Verbal

Menganggap seseorang harus "kuat mental" di dunia maya adalah pandangan yang keliru dan berbahaya. Meski tak meninggalkan bekas fisik, kekerasan verbal online memiliki dampak yang tak kalah serius dengan kekerasan fisik. Bahkan, dalam beberapa aspek, dampaknya bisa lebih parah dan bertahan lebih lama. Kekerasan verbal online bisa terjadi selama 24/7, menembus batas ruang dan waktu. Korban bisa mendapat serangan kapan saja, bahkan di tempat yang seharusnya aman seperti rumah. Ini menciptakan perasaan terancam yang konstan, memicu stres kronis yang berdampak pada kesehatan fisik dan mental. Dari segi kesehatan mental, korban kekerasan verbal online berisiko mengalami depresi, kecemasan, dan dalam kasus ekstrem, keinginan bunuh diri. Penelitian menunjukkan bahwa remaja yang mengalami perundungan digital memiliki risiko tiga kali lebih tinggi untuk mencoba bunuh diri dibandingkan mereka yang tidak mengalaminya.

Secara kognitif, paparan terus-menerus terhadap kekerasan verbal online dapat memengaruhi cara korban memandang diri sendiri dan dunia sekitarnya. Ini bisa mengakibatkan penurunan kepercayaan diri, isolasi sosial, dan kesulitan dalam membangun hubungan yang sehat di masa depan. Kekerasan verbal online juga bisa berdampak pada kesehatan fisik. Stres kronis yang dialami korban dapat memicu berbagai masalah kesehatan seperti gangguan tidur, sakit kepala, dan bahkan melemahnya sistem kekebalan tubuh. Lebih jauh, dampak kekerasan verbal online bisa meluas ke aspek profesional dan akademik. Korban mungkin mengalami penurunan produktivitas, kesulitan berkonsentrasi, atau bahkan memutuskan untuk mengundurkan diri dari pekerjaan atau sekolah untuk menghindari pelaku perundungan.

Solusi dari Banyak Sisi

Mengatasi kekerasan verbal online membutuhkan pendekatan multidimensi yang melibatkan berbagai pihak, dari individu hingga pembuat kebijakan. Di tingkat individu, edukasi tentang etika berinternet dan kesadaran akan dampak kata-kata kita di dunia maya sangat penting. Sekolah dan tempat kerja perlu menerapkan program literasi digital

yang tidak hanya fokus pada keterampilan teknis, tapi juga aspek etika dan empati dalam berkomunikasi online, misalnya dengan memanfaatkan game edukasi.

Penyedia platform digital juga memiliki peran krusial. Mereka perlu mengembangkan dan menerapkan kebijakan moderasi konten yang lebih ketat. Mereka juga sepatutnya menyediakan alat pelaporan yang mudah diakses dan efektif bagi pengguna yang mengalami kekerasan verbal. Dari sisi hukum, Indonesia memang sudah memiliki UU Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE), tapi implementasinya masih lemah, terutama dalam kasus kekerasan verbal online. Definisi kekerasan verbal online yang kurang jelas membuat perundungan digital diasosiasikan dengan delik pencemaran nama baik. Selain itu, proses pelaporan yang rumit sering membuat korban enggan mencari bantuan hukum.

Ini menunjukkan bahwa Indonesia membutuhkan revisi UU yang lebih spesifik mengenai kekerasan verbal online serta pelatihan bagi aparat penegak hukum tentang penanganan kasus-kasus ini. Indonesia bisa belajar dari regulasi *Basic Online Safety Expectations* (BOSE) Australia, yang menetapkan standar keamanan bagi platform digital, termasuk mekanisme pelaporan yang jelas, transparansi, dan pelindungan khusus untuk anak-anak.

Pendekatan ini dapat melengkapi UU ITE melalui program literasi digital, dan mewajibkan platform untuk mengembangkan kebijakan moderasi konten yang lebih ketat. Penegak hukum perlu dilatih khusus, dan dukungan untuk korban harus ditingkatkan. Dengan mengadopsi prinsip-prinsip BOSE seperti proaktif, transparan, dan berbasis risiko, Indonesia bisa menciptakan ekosistem digital yang lebih aman.

Untuk pemulihan korban, akses terhadap layanan konseling dan dukungan psikologis harus dipermudah. Pembentukan support group bagi korban kekerasan verbal online juga bisa menjadi langkah positif, memberikan ruang aman bagi korban untuk berbagi pengalaman dan strategi coping—cara atau taktik menghadapi situasi yang membuat stres atau tertekan. Terakhir, perlu ada gerakan sosial yang lebih luas untuk mengubah norma di dunia maya sehingga tercipta budaya internet yang lebih positif dan empatik.

Kunci keberhasilan terletak pada pendekatan holistik yang melibatkan pemerintah, platform digital, dan masyarakat. Dengan pendekatan seperti ini, kita bisa menciptakan ruang digital yang lebih aman dan sehat bagi semua penggunanya.

Tautan artikel:

https://theconversation.com/bagaimana-mencegah-kekerasan-verbal-di-ruang-digital-237770

Merangkai Kepingan Demokrasi di Kanvas Digital

Arif Perdana

Konteks: Artikel ini saya siapkan untuk presentasi dengan Asosiasi Media Siber Indonesia. Rangkuman pemikiran saya ini kemudian saya bagikan ke peserta. Sebagian peserta kemudian menerbitkan artikel ini. Versi pertama artikel diterbitkan oleh Dewata Pos di 13 Agustus 2024, dan kemudian direplikasi dan dimodifikasi di berbagai media seperti kbr.id, Solopos, Times Indonesia, Muria News. Tulisan ini fokus kepada ancaman hoax dan disinformasi dalam konteks demokrasi Indonesia, terutama menjelang Pilkada 2024. Dengan proyeksi ribuan hoaks yang akan muncul, tantangan ini memperburuk integritas pemilu. Anonimitas di media sosial dan teknologi seperti AI generatif semakin memperparah masalah. Untuk mengatasi isu ini, dibutuhkan pendekatan multidimensi yang melibatkan jurnalisme yang kritis, literasi digital masyarakat, regulasi yang ketat, dan peningkatan kapasitas pengawasan oleh Badan Pengawas Pemilu (Bawaslu). Ini adalah perjuangan kolektif untuk melindungi demokrasi.

Hoax dan disinformasi telah menjadi hantu yang membayangi demokrasi kita. Baru saja Indonesia menyelesaikan pemilihan presiden (pilpres) yang sempat diwarnai dengan hoax di media sosial. Video-video manipulatif dan narasi-narasi provokatif menyebar bagai virus, memecah belah masyarakat dan mengancam legitimasi proses demokrasi. Kini, saat debu Pilpres belum sepenuhnya reda, kita dihadapkan pada tantangan baru yang tak kalah pelik. Dalam hiruk-pikuk Pilkada 2024 yang akan melibatkan 508 kabupaten/kota dan 37 provinsi di November ini, ancaman ini semakin nyata dan mengkhawatirkan. Menurut prediksi Nyarwi Ahmad dari Universitas Gajah Mada, kita akan dihadapkan pada tsunami informasi palsu dengan proyeksi minimal 2.500 hingga 10.000 hoaks yang akan beredar. Angka yang mencengangkan ini bukan sekadar statistik, tetapi potret buram dari tantangan demokrasi kita di era digital.

Pilkada, yang seharusnya menjadi pesta demokrasi lokal, kini berpotensi menjadi ajang perang informasi. Berbeda dengan Pilpres yang memiliki resonansi nasional, hoaks dalam Pilkada memiliki karakteristik yang lebih spesifik dan lokal. Isu-isu yang beredar seringkali mencerminkan dinamika dan ketegangan sosial yang ada di daerah tersebut. Ini membuat penyebaran hoaks dalam Pilkada menjadi lebih sulit dideteksi dan ditangani secara seragam. Tema-tema hoaks yang beredar pun beragam, namun memiliki pola

yang cenderung berulang. Isu SARA masih menjadi primadona, dengan tuduhan-tuduhan tak berdasar tentang keberpihakan kandidat terhadap kelompok tertentu. Kecurangan pemilu, rumor kesehatan kandidat, hingga isu penggunaan dana kampanye ilegal, semuanya menjadi amunisi dalam perang informasi ini. Yang memprihatinkan, isu-isu ini seringkali diungkit kembali dari Pilkada sebelumnya, menunjukkan bahwa kita belum belajar dari pengalaman masa lalu.

Yang lebih mengkhawatirkan, sumber hoaks tidak hanya berasal dari pihak eksternal. Aktor-aktor internal seperti kandidat, tim sukses, bahkan penyelenggara pemilu sendiri, baik sengaja maupun tidak, dapat menjadi sumber disinformasi. Fenomena ini menunjukkan bahwa krisis integritas informasi telah merasuk ke dalam inti proses demokrasi kita. Ini bukan lagi sekadar masalah teknis, tetapi menyangkut etika dan integritas seluruh pemangku kepentingan dalam proses demokrasi.

Demokrasi di Ujung Jari

Lanskap media sosial yang semakin kompleks memperburuk situasi. WhatsApp dengan grup-grup tertutupnya menjadi sarang penyebaran informasi yang sulit diawasi. Facebook, dengan algoritma yang memprioritaskan konten sensasional, justru memperkuat gaung disinformasi. Twitter (X), dengan viralitas hashtag-nya, memungkinkan narasi palsu menyebar dalam hitungan detik. Sementara Instagram, dengan konten visual yang mempengaruhi emosi, menjadi medan subur bagi manipulasi opini publik.

Belum lagi dengan hadirnya AI Generatif (GenAI) yang mampu menciptakan konten palsu yang nyaris tidak dapat dibedakan dari yang asli. Belum hilang dari ingatan kita *deepfake* video mantan Presiden Soeharto dan Presiden Jokowi berbahasa mandarin menjelang pilpres 2024. Teknologi ini membuka kotak Pandora baru dalam dunia disinformasi. Video *deepfake*, artikel yang tampak otentik, bahkan bot yang mampu berinteraksi layaknya manusia, semuanya menjadi alat baru dalam arsenal perang informasi. Ini bukan lagi era di mana kita bisa mengandalkan mata telanjang atau intuisi untuk membedakan fakta dari fiksi.

Di tengah badai disinformasi ini, muncul ancaman lain yang tidak kalah serius: kebocoran data. Potensi penyalahgunaan data pemilih untuk kepentingan politik dan manipulasi elektoral menjadi momok baru yang mengancam integritas pemilu. Ini bukan hanya soal privasi, tetapi juga tentang kepercayaan publik terhadap sistem demokrasi kita. Bayangkan skenario di mana data pribadi pemilih jatuh ke tangan yang salah, digunakan untuk micro-targeting kampanye disinformasi, atau bahkan untuk memanipulasi hasil pemilu. Ini bukan lagi skenario film fiksi, tetapi ancaman nyata yang harus kita hadapi.

Membangun Kekebalan Kolektif

Lantas, apa yang bisa kita lakukan? Kita perlu pendekatan multidimensi yang melibatkan semua elemen masyarakat. Jurnalisme investigatif yang tajam dan kritis harus menjadi garda terdepan dalam membongkar praktik-praktik manipulasi informasi. Media harus berani mengedepankan verifikasi fakta yang ketat, bahkan jika itu berarti melawan arus popularitas atau sensasionalisme. Jurnalis harus kembali ke akar profesi mereka: mengungkap kebenaran, bukan sekadar menjadi corong informasi.

Namun, beban ini tidak bisa hanya dipikul oleh media. Masyarakat harus bertransformasi dari konsumen pasif menjadi penjaga aktif informasi. Sikap skeptis dan kritis terhadap setiap informasi yang diterima harus menjadi budaya baru di era post-truth ini. Literasi digital bukan lagi sekadar kemampuan menggunakan teknologi, tetapi juga kecakapan dalam memilah dan memverifikasi informasi. Ini berarti kita perlu revolusi dalam sistem pendidikan kita, di mana kemampuan berpikir kritis dan verifikasi informasi menjadi keterampilan dasar yang diajarkan sejak dini.

Pemerintah dan penyelenggara pemilu tidak bisa lagi bersikap reaktif. Mereka harus proaktif dalam membangun sistem pertahanan informasi yang tangguh. Kolaborasi dengan platform media sosial harus diintensifkan, bukan hanya untuk menghapus konten bermasalah, tetapi juga untuk menciptakan ekosistem digital yang lebih sehat. Regulasi yang ada perlu ditinjau ulang untuk mengakomodasi kompleksitas tantangan di era digital, tanpa mengorbankan kebebasan berekspresi. Bagai penari di

atas tali, kita menyeimbangkan kebebasan dan ketertiban. Ini memang menantang, tetapi harus dilakukan demi melindungi integritas demokrasi kita.

Badan Pengawas Pemilu (Bawaslu), sebagai lembaga pengawas pemilu, harus memperkuat kapasitasnya dalam mendeteksi dan merespons disinformasi. Ini bukan hanya soal teknologi, tetapi juga tentang membangun jaringan pengawasan berbasis masyarakat yang responsif dan efektif. Kerjasama dengan platform media sosial dan dinas komunikasi dan informasi (Kominfo) di daerah-daerah harus diintensifkan untuk memantau dan menangani hoaks secara lebih efektif. Dalam menghadapi ancaman kebocoran data, penyelenggara pemilu harus mengadopsi pendekatan keamanan siber yang komprehensif. IRP, DRP, dan BCP bukan sekadar jargon teknis, tetapi kebutuhan mutlak untuk menjaga integritas data dan kepercayaan publik. Ini berarti investasi besar-besaran dalam infrastruktur keamanan siber dan pelatihan personil yang kompeten.

Namun, semua upaya ini akan sia-sia jika tidak ada perubahan fundamental dalam cara kita memandang dan menghargai informasi. Kita perlu membangun kembali "kontrak sosial digital" dimana kebenaran dan fakta dihargai lebih tinggi daripada sensasi dan popularitas. Ini bukan tugas mudah di era di mana kecepatan seringkali mengalahkan akurasi, dan opini personal dapat dengan mudah disamarkan sebagai fakta. Pilkada 2024 bukan hanya tentang memilih pemimpin daerah. Ini adalah momen krusial di mana kita diuji sebagai masyarakat demokratis di era digital. Apakah kita akan tenggelam dalam badai disinformasi, atau bangkit sebagai masyarakat yang kritis dan melek informasi? Jawabannya ada di tangan kita semua.

Kita perlu menyadari bahwa pertarungan melawan disinformasi dan penyalahgunaan data bukanlah sprint, melainkan maraton. Ini adalah perjuangan jangka panjang yang membutuhkan kesabaran, ketekunan, dan komitmen dari seluruh elemen masyarakat. Kita perlu membangun sistem kekebalan kolektif terhadap disinformasi, di mana setiap warga negara menjadi benteng pertahanan pertama dalam melawan penyebaran hoaks. Demokrasi kita sedang berada di persimpangan. Di satu sisi, teknologi memberi kita akses informasi yang belum pernah ada sebelumnya. Di sisi lain, teknologi yang sama memberi ruang bagi manipulasi dan penyesatan opini publik dalam

skala masif. Pilkada 2024 akan menjadi titik kritis yang menentukan arah demokrasi digital kita.

Akankah kita biarkan demokrasi kita terdistorsi oleh hoaks dan manipulasi data, atau kita bangkit bersama membangun ekosistem informasi yang sehat dan bertanggung jawab? Pilihan ada di tangan kita, dan waktunya adalah sekarang. Ini bukan hanya tentang satu Pilkada, tetapi tentang masa depan demokrasi kita di era digital.

Tautan artikel:

https://dewatapos.com/merangkai-kepingan-demokrasi-di-kanvas-digital/
https://timesindonesia.co.id/kopi-times/506081/merangkai-kepingan-demokrasi-di-kanvas-digital
https://kolom.espos.id/demokrasi-di-kanvas-digital-1993904

Pedang dan Perisai AI di Ranah Keuangan

Arif Perdana

Konteks: Artikel ini diterbitkan oleh Kompas.com di 8 Agustus 2024. Tulisan ini memaparkan dua sisi mata uang AI. Di satu sisi memfasilitasi efisiensi dan inovasi, namun juga memicu penipuan keuangan, seperti identitas sintetis dan deepfake. Para penipu memanfaatkan AI generatif untuk menciptakan penipuan yang sulit dideteksi. Solusi AI juga diperlukan untuk mendeteksi ancaman ini, sementara kolaborasi dan regulasi menjadi penting dalam melawan kejahatan finansial.

AI telah mengukir pengaruh signifikan di lintas industri, merangkai efisiensi dan memacu inovasi yang tiada henti. Namun, sebagaimana lazimnya teknologi canggih, AI menghadirkan paradoks: di satu pihak, ia berpotensi merevolusi proses dan mengamankan ranah sistem keuangan, di lain pihak, ia juga memungkinkan para pelaku kejahatan untuk melancarkan aksi kriminal yang semakin canggih. Gelombang penipuan online semakin membuncah yang dipupuk oleh kecanggihan AI, menjadi cermin nyata dari sifat ambivalennya.

Skema penipuan identitas sintetis muncul bagai hantu di tengah kabut. Skema ini menjadi salah satu tren yang paling meresahkan dalam rimba kejahatan siber. Para pelaku menggunakan AI untuk mencipta identitas palsu. Mereka menganyam data nyata seperti nomor identitas kependudukan dan jaminan sosial dengan benang-benang fiksi. Dengan AI generatif (GenAI), konten seperti teks, gambar, audio, dan video tercipta dengan mudahnya yang bisa mengelabui proses verifikasi konvensional, bahkan mengecoh tes deteksi keaslian otomatis. Hal ini menggerogoti fondasi sistem keuangan dan prosedur Kenali Pelanggan Anda (KYC) yang tentunya memicu kebutuhan akan metode verifikasi yang lebih tajam melalui pendeteksian AI dan *deepfake*.

Menurut *TransUnion*, agensi pelaporan kredit konsumen AS, penipuan identitas sintetis tumbuh pesat di tahun 2024, ditambah lagi dengan kebocoran data sebesar 15% di tahun 2023. Para penipu, layaknya ilusionis ulung, memanfaatkan identitas palsu ini untuk merancang skema penipuan keuangan. GenAI menjadi pena Ajaib bagi penipu yang menciptakan pesan-pesan menyesatkan namun tampak autentik. AI juga menjadi

sutradara pencipta *deepfake* audio dan video yang begitu meyakinkan, seolah menghidupkan bayangan menjadi nyata. Hal ini meningkatkan frekuensi dan peluang keberhasilan serangan dan penipuan. Tentu saja ini menimbulkan tantangan besar bagi keamanan siber global yang harus terus waspada dan adaptif.

Bagaimana AI Memfasilitasi Kejahatan Keuangan

GenAI seperti *ChatGPT*, *Gemini*, dan *Claude*, dapat menghasilkan teks serta dialog yang nyaris tidak terbedakan dari manusia, memberdayakan penipu untuk merangkai narasi yang dipersonalisasi dan meyakinkan. Ditambah lagi platform seperti *FraudGPT* yang memang dikhususkan untuk memfasilitasi penipuan. Skema "penipuan umpan gemuk (*pig-butchering*)", misalnya, mendapat keuntungan signifikan dari kecanggihan GenAI. Melalui strategi ini, penjahat menjalin hubungan dengan korban sebelum membujuk mereka untuk menanamkan investasi dalam skema penipuan. AI menghapus hambatan bahasa yang membuat taktik ini lebih menarget dan efektif.

Teknologi *deepfake* yang bisa mengkloning suara semakin memperkuat ancaman tersebut. AI mampu menghasilkan audio dan video yang sangat realistis dari individu, yang dapat dimanfaatkan untuk berpura-pura sebagai anggota keluarga, eksekutif, atau tokoh publik. *Deepfake* ini dapat sangat persuasif, misalnya menirukan seseorang mengucapkan atau melakukan tindakan yang tidak pernah terjadi. Hal ini tentunya membuat penipuan lebih sulit terdeteksi dan lebih mudah dipercaya. Survei McAfee menunjukkan bahwa penipuan suara yang dihasilkan AI memperkuat prevalensi ancaman ini.

GenAI memanfaatkan model pembelajaran mendalam, khususnya Jaringan Adversarial Generatif (GANs), untuk menciptakan *deepfake* audio dan video. Model-model ini memiliki dua komponen utama: *generator* dan *discriminator*. *Generator* menghasilkan keluaran sintetis, seperti klip audio atau rekaman video palsu, sementara *discriminator* menilai keasliannya berdasarkan contoh nyata. Generator memperoleh kemampuan untuk meniru nuansa suara dan ekspresi wajah manusia dengan berlatih pada dataset besar yang berisi file audio dan video asli.

Untuk *deepfake* audio, teknologi seperti sintesis dan kloning suara digunakan. Teknik-teknik ini menganalisis pola suara, intonasi, dan gaya bicara target untuk menghasilkan klip audio baru yang mirip. *Deepfake* video memperluas ini dengan memanipulasi atau merekonstruksi ekspresi wajah dalam video. Ini dilakukan dengan memetakan data wajah target pada gerakan aktor sumber, menciptakan video yang menampilkan orang yang ditargetkan untuk mengatakan atau melakukan hal-hal yang tidak pernah terjadi. Kemampuan GenAI seperti ini tentu meningkatkan taktik penipuan tradisional dengan memungkinkan imitasi yang sangat meyakinkan dalam serangan phishing, yang membuat semakin sulit bagi individu untuk mengidentifikasi komunikasi penipuan.

Penipuan yang menargetkan *Bank of America*, misalnya, enggunakan *deepfake* audio dari investor Clive Kabatznik untuk mengatur transfer uang. Meskipun upaya tersebut terdeteksi, ini menegaskan ancaman *deepfake* audio di sektor keuangan. Di kasus lain, *deepfake* audio berhasil mengkloning suara CFO perusahaan multinasional sehingga menyesatkan karyawan di perusahaan tersebut melalui panggilan suara untuk mentransfer uang senilai USD 25 juta. Penipuan ini terungkap setelah verifikasi transaksi dengan kantor pusat. Ada juga kasus CEO perusahaan energi Inggris tertipu mentransfer GBP 220,000 karena *deepfake* audio yang meyakinkan. *Deepfake* ini menirukan aksen dan pola ucapan melodis atasannya. Skema ini melibatkan beberapa panggilan suara dan berhasil awalnya, hingga ketidaksesuaian pada panggilan berikutnya menimbulkan kecurigaan.

Menggunakan AI Sebagai Pertahanan Menghadapi Kejahatan Keuangan

Meski AI menjadi pedang tajam di tangan para penipu, ia juga hadir sebagai perisai kokoh untuk pertahanan. Kunci dari strategi ini terletak pada pemanfaatan AI untuk merancang sistem deteksi dan pencegahan penipuan yang efektif. Model berbasis AI ini mampu menelusuri lautan data secara real-time, mengungkap pola tersembunyi dan anomali yang menjadi pertanda aktivitas penipuan.

Salah satu metode yang menjanjikan adalah integrasi kecerdasan perilaku. Metode ini bagai psikolog digital yang mengamati perilaku pengguna, spesifikasi

perangkat, dan detail transaksi untuk mengenali penyimpangan. Sebagai contoh, platform ThreatMark menggunakan AI layaknya detektif yang menyelidiki berbagai titik data, menyoroti risiko, dan membangun benteng terhadap penipuan dengan mengidentifikasi pola mencurigakan. AI juga berperan sebagai penjaga gerbang dalam memperkuat metode otentikasi. Otentikasi multi-faktor (MFA), terutama versi yang lebih canggih dengan kata sandi sekali pakai bisa menjadi benteng pertahanan. AI mendukung mekanisme ini dengan menganalisis biometrik perilaku, seperti pola ketikan atau gerakan mouse, menyertakan lapisan verifikasi yang lebih mendalam.

Dalam pertempuran melawan *deepfake*, sistem deteksi ancaman yang diperkuat AI bertindak sebagai pengamat yang jeli dalam menelaah audio dan video untuk mendeteksi ketidakkonsistenan. Sistem ini memanfaatkan algoritma pembelajaran mesin untuk mengidentifikasi nuansa halus yang menandakan manipulasi sehingga memberikan perlindungan tambahan terhadap penipuan yang terselubung. AI juga menjadi peramal dalam analisis prediktif untuk mencegah kejahatan keuangan. AI merajut data historis dan pola transaksi untuk memprediksi potensi aktivitas penipuan di masa depan, memungkinkan institusi keuangan untuk mengambil langkah pencegahan sebelum badai kejahatan menerjang.

Selain itu, AI menjadi asisten yang tak kenal lelah dalam mengotomatisasi proses due diligence dan pemantauan transaksi. Ini memungkinkan lembaga keuangan untuk memenuhi persyaratan regulasi dengan lebih efisien, sambil meningkatkan kewaspadaan mereka terhadap aktivitas mencurigakan. Perlu diingat, meski AI menawarkan solusi canggih, kekuatannya bergantung pada kualitas data yang menjadi santapannya. Karenanya, lembaga keuangan harus terus menyuapi AI dengan dataset terbaru. Ini untuk memastikan sistem deteksi berbasis AI tetap tajam menghadapi taktik penipuan yang terus bermetamorfosis.

Pertimbangan Organisasi dan Regulasi

Meskipun solusi teknologi memegang peranan penting, mengatasi penipuan yang digerakkan oleh AI menuntut pendekatan holistik yang melibatkan praktik organisasi dan regulasi yang matang. Perusahaan perlu menetapkan kontrol internal yang kokoh dan

memperbarui mereka secara berkala untuk mengimbangi ancaman yang terus berkembang. Program pelatihan karyawan yang terfokus pada pengenalan dan respons terhadap penipuan yang dipicu AI adalah kunci dalam menanamkan budaya kewaspadaan yang kuat. Kerangka kerja regulasi juga berperan vital. Pemerintah dan lembaga regulasi diharapkan untuk mengimplementasikan undang-undang perlindungan data yang ketat dan memastikan pemenuhan standar keamanan. Kolaborasi antara lembaga keuangan, perusahaan teknologi, dan badan regulasi menjadi sangat penting untuk bertukar informasi mengenai ancaman terkini dan praktik terbaik untuk pencegahan.

Pendidikan konsumen merupakan komponen kritikal lainnya. Meningkatkan kesadaran tentang taktik yang digunakan dalam penipuan yang didukung AI dan mengadvokasi praktik terbaik untuk keamanan digital dapat memberikan kekuatan kepada individu untuk melindungi diri mereka sendiri. Ini termasuk kebiasaan memeriksa akun keuangan secara rutin, berhati-hati dalam membagikan informasi pribadi secara online, dan menggunakan kata sandi yang kuat dan unik untuk setiap akun. Seiring berkembangnya AI, sifat dualistiknya semakin terlihat jelas. Meskipun meningkatkan produktivitas dan membuka kemungkinan baru, AI juga memberikan alat yang canggih kepada para penipu. Tantangan yang kita hadapi adalah mengoptimalkan potensi AI untuk tujuan baik sambil meminimalisir risikonya.

Akhirnya, kolaborasi antar industri dalam berbagi informasi tentang ancaman dan praktik terbaik menjadi semakin krusial. Platform berbagi informasi yang didukung AI menjadi jembatan pengetahuan untuk menyebarkan wawasan tentang tren penipuan terbaru. Ini tentunya memungkinkan respon yang lebih gesit dan terkoordinasi terhadap ancaman yang mengintai di seluruh sektor keuangan.

Sektor keuangan kini berhadapan dengan tantangan yang semakin menggunung. Bagai meniti di atas tali, menjaga keseimbangan antara memanfaatkan teknologi untuk melahirkan inovasi dan melindungi sistem dari ancaman yang mengintai menjadi semakin krusial. Individu dan organisasi harus tetap berjaga dengan mata elang dan bergerak lincah bagai perisai, memperbarui strategi keamanan mereka. Mereka juga perlu memastikan bahwa kemajuan teknologi tidak membuka gerbang bagi

penyalahgunaan yang dapat menebar keresahan di berbagai lapisan. Dengan demikian, AI tidak hanya akan berfungsi sebagai alat untuk pertumbuhan dan efisiensi, tetapi juga sebagai benteng pertahanan yang kokoh terhadap kejahatan finansial.

Tautan artikel:

https://money.kompas.com/read/2024/08/08/082657226/pedang-dan-perisai-kecerdasan-artifisial-di-ranah-keuangan?page=all

Kerentanan Virtual: Bagaimana Mengatasi Ancaman AI Terkait Pelecehan Seksual Anak?

Arif Perdana

Konteks: Artikel ini diterbitkan oleh The Conversation Indonesia di 16 Juli 2024. Tulisan ini merefleksikan kegelisahan saya tentang bahaya materi pelecehan seksual anak (CSAM) yang dihasilkan oleh AI generatif, yang bisa mempercepat distribusi dan penciptaan konten eksplisit. Meskipun gambar tersebut mungkin tidak melibatkan anak sungguhan, tetap memperkuat budaya eksploitasi. Diperlukan langkah proaktif, termasuk pengamanan model AI, sistem deteksi, peningkatan kesadaran masyarakat, dan regulasi ketat. Di Indonesia, UU terkait pelecehan seksual daring sudah ada, namun perlu penanganan yang lebih spesifik untuk eksploitasi online. Tindakan segera diperlukan untuk melindungi anak-anak.

Materi pelecehan seksual, khususnya yang berkaitan dengan anak (*child sexual abuse material*/CSAM), merupakan salah satu aspek paling mengerikan dari konten daring. Materi ini tidak hanya melanggar hak dan martabat anak, tetapi juga menimbulkan trauma yang berkepanjangan bagi korban. Proliferasi gambar dan video terkait CSAM di internet telah menjadi masalah yang persisten. Munculnya AI semakin menambah dimensi baru yang mengkhawatirkan terkait masalah ini. Pasalnya, AI bisa mempercepat distribusi dan penciptaan CSAM.

Cara AI Memproduksi CSAM

AI generatif (GenAI), memiliki potensi untuk meningkatkan produksi dan penyebaran materi pelecehan seksual dengan cepat. Model AI, yang dilatih dengan kumpulan data besar yang sering kali mencakup konten eksplisit, dapat membuat gambar dan video pelecehan seksual anak yang realistis dengan sekali klik. Laporan tentang gambar porno yang dihasilkan AI dari siswa sekolah menengah terus bermunculan di berbagai belahan dunia seperti di Amerika Serikat (AS) dan Spanyol. Pusat Nasional untuk Anak Hilang & Tereksploitasi (*National Center for Missing & Exploited Children*/NCMEC) di AS, misalnya, melaporkan peningkatan laporan CSAM

sebesar 12% pada tahun 2023, dengan total lebih dari 36 juta laporan, dan peningkatan yang signifikan dalam penggunaan GenAI untuk membuat konten tersebut.

Ancaman Serius CSAM yang Dihasilkan AI

Peningkatan CSAM yang dihasilkan GenAI menimbulkan ancaman signifikan karena beberapa alasan. Pertama, ini memudahkan pelaku untuk memproduksi dan mendistribusikan konten eksplisit tanpa melibatkan anak-anak sungguhan, yang mungkin dianggap oleh sebagian orang bukanlah eksploitasi. Namun, ini adalah kesalahpahaman yang berbahaya. Meskipun gambar-gambar tersebut sintetis, mereka tetap memperkuat budaya eksploitasi seksual dan dapat digunakan untuk merayu dan memanipulasi anak-anak yang sebenarnya.

Kedua, data latih (*training data*) untuk banyak model AI sering kali mencakup CSAM yang sebenarnya, yang berarti gambar yang dihasilkan AI masih dapat didasarkan pada pelecehan yang nyata. Hal ini tidak hanya menambah trauma korban, tetapi juga membanjiri internet dengan bentuk-bentuk baru materi pelecehan, membanjiri sistem deteksi yang ada dan menyulitkan penegak hukum untuk fokus pada korban yang sebenarnya. Terlebih lagi, gambar yang dihasilkan oleh AI ini terkadang tidak dapat dibedakan dari foto asli, sehingga menyulitkan upaya penegak hukum untuk mengidentifikasi dan menyelamatkan korban.

Langkah Mengatasi Penyalahgunaan AI Terkait CASM

Mengingat implikasinya yang parah, penting untuk mengambil langkah-langkah proaktif untuk mencegah penyalahgunaan AI dalam membuat dan mendistribusikan CSAM.

Pertama, model AI memerlukan penerapan pengamanan yang kuat di sekitarnya untuk memastikan mereka tidak dapat menghasilkan gambar yang bersifat seksual eksplisit. Ini melibatkan penyaringan data latih untuk mengecualikan segala bentuk konten eksplisit dan memantau output model ini secara terus-menerus.

Kedua, perusahaan AI perlu memprioritaskan keselamatan anak dengan mengintegrasikan sistem deteksi canggih yang dapat mengidentifikasi dan memblokir pembuatan konten pelecehan seksual anak.

Ketiga, penegak hukum perlu memutakhirkan pengetahuan mereka terkait kecanggihan teknologi. Ini akan membantu mereka melakukan investigasi yang lebih baik. Di Kanada, proyek *Aquatic*, yang melibatkan 27 layanan kepolisian, menyoroti peningkatan kecanggihan predator yang menggunakan AI untuk menghasilkan CSAM, mengidentifikasi 34 korban anak dan menangkap 64 individu dengan 348 dakwaan.

Keempat, platform yang memuat konten buatan pengguna juga harus meningkatkan kemampuan moderasi konten mereka. Mereka perlu mempekerjakan baik peninjau manusia maupun alat AI untuk mendeteksi dan menghapus CSAM dengan cepat.

Kelima, selain langkah-langkah teknis, perlu ada upaya bersama untuk meningkatkan kesadaran tentang penyalahgunaan AI dalam menghasilkan CSAM. Mendidik orang tua, pendidik, dan anak-anak tentang bahaya konten eksplisit yang dihasilkan AI dapat membantu dalam identifikasi dan pelaporan dini materi semacam itu. Sebuah survei oleh yayasan *Lucy Faithfull* mengungkapkan bahwa meskipun 60% orang khawatir tentang AI, hanya 40% yang tahu bahwa gambar seksual yang dihasilkan AI dari anak di bawah umur adalah ilegal di Inggris. Yayasan Lucy Faithfull merupakan badan sosial perlindungan anak-anak di UK yang berupaya menghentikan penyalahgunaan seksual anak-anak.

Keenam, intervensi pemerintah melalui regulasi sangat penting untuk mengatasi krisis ini secara efektif. Legislator harus bekerja sama dengan perusahaan teknologi, organisasi perlindungan anak, dan agen penegak hukum untuk mengembangkan regulasi komprehensif yang menangani penyalahgunaan AI. Ini termasuk mewajibkan perusahaan AI untuk menerapkan fitur keamanan yang mencegah pembuatan konten eksplisit dan mengharuskan platform media sosial untuk melaporkan dan menghapus CSAM dengan cepat. Misalnya, pada tahun 2022, Pusat Perlindungan Anak Kanada menandai sekitar 2.600 gambar yang dihasilkan AI, angka yang meningkat menjadi 3.700 pada 2023, dengan ekspektasi setidaknya 6.000 pada 2024.

Regulasi Terkait CASM

Di Indonesia, pelecehan seksual daring diatur oleh beberapa kerangka hukum, utamanya UU Tindak Pidana Kekerasan Seksual (UU TPKS) dan UU Informasi dan Transaksi Elektronik (UU ITE). UU TPKS mencakup pelecehan seksual nonfisik, yang mencakup komentar, gerakan, atau aktivitas yang tidak pantas yang bertujuan merendahkan seseorang secara seksual. Pelanggar dapat menghadapi hukuman penjara hingga 9 bulan atau denda hingga Rp10 juta. Untuk kekerasan seksual berbasis elektronik, seperti perekaman tanpa izin, transmisi konten seksual, atau penguntitan siber, UU ini menjatuhkan hukuman hingga empat tahun penjara atau denda hingga Rp200 juta.

UU ITE melarang distribusi, transmisi, atau membuat informasi elektronik yang mengandung kesusilaan dapat diakses. Pelanggar dapat dijatuhi hukuman penjara hingga enam tahun atau denda hingga Rp1 miliar. Dalam kasus yang melibatkan anak-anak, regulasi tambahan berlaku. UU Perlindungan Anak (UU TPA) memberikan hukuman berat untuk kejahatan seksual terhadap anak-anak, dengan hukuman penjara maksimal 10 tahun dan denda hingga Rp200 juta. Namun, aturan ini tidak sepenuhnya menangani eksploitasi daring yang diatur oleh UU ITE dan UU Pornografi.

Selain itu, dalam konteks pelecehan seksual terhadap anak, justice-based laws juga dapat diterapkan dengan menekankan pentingnya keadilan substantif. Keadilan substantif adalah keadilan dalam keputusan hakim yang adil, jujur, objektif, tidak memihak, tidak diskriminatif, dan berdasarkan hati nurani. Hukuman seperti kastrasi kimia diterapkan sebagai hukuman tegas bagi pelaku untuk memberikan efek jera dan pelindungan maksimal bagi korban. Strategi lain termasuk keadilan restoratif dan keterlibatan komunitas untuk pencegahan serta rehabilitasi korban. Dalam konteks pelecehan seksual, keadilan restoratif berarti memperhatikan kebutuhan korban, memfasilitasi proses pemulihan mereka, mempertimbangkan pertanggungjawaban dan pembelajaran bagi pelaku, serta melibatkan komunitas dalam mendukung proses rekonsiliasi yang holistik.

Pada akhirnya, persimpangan antara AI dan materi pelecehan seksual anak menghadirkan tantangan yang signifikan dan mendesak. Potensi AI untuk menghasilkan

dan mendistribusikan konten eksplisit memerlukan tindakan segera dan tegas dari perusahaan teknologi, pemerintah, dan masyarakat secara keseluruhan.

Tautan artikel:

https://theconversation.com/kerentanan-virtual-bagaimana-mengatasi-ancaman-ai-terkait-pelecehan-seksual-anak-232260

‘Kehidupan Setelah Kematian Digital’ yang Menyeramkan Bukan Lagi Fiksi Ilmiah. Jadi Bagaimana Kita Mengatasi Risikonya?

Arif Perdana

Konteks: Ide menulis artikel ini pertama kali muncul ketika saya membaca paper berjudul “*Griefbots, Deadbots, Postmortem Avatars: on Responsible Applications of Generative AI in the Digital Afterlife Industry*” yang terbit di *Philosophy and Technology*. Draft awal tulisan saya kirimkan ke The Conversation Australia dan versi finalnya diterbitkan di 24 Juni 2024. Tulisan ini menyoroti perkembangan industri kehidupan setelah kematian digital, yang menggunakan teknologi seperti AI dan VR untuk menciptakan rekonstruksi virtual orang yang telah meninggal. Meskipun menawarkan kenyamanan dalam berkabung, teknologi ini juga menimbulkan tantangan etis, termasuk isu persetujuan, privasi, dan potensi penyalahgunaan data. Untuk mengatasi masalah ini, diperlukan regulasi yang memperhatikan hak pasca-kematian dan melindungi martabat individu. Pendekatan hati-hati dan etis diperlukan agar teknologi ini dapat menghormati ingatan almarhum dan mendukung kesejahteraan emosional yang hidup.

Bayangkan masa depan di mana ponsel Anda berbunyi dengan pesan bahwa bot "digital abadi" ayah Anda yang sudah meninggal telah siap. Janji untuk mengobrol dengan versi virtual orang yang Anda cintai – mungkin melalui *headset virtual reality* (VR) – seperti melangkah ke dalam film fiksi ilmiah, mendebarkan sekaligus sedikit menyeramkan. Saat Anda berinteraksi dengan ayah digital ini, Anda menemukan diri Anda dalam perjalanan emosional yang naik turun. Anda mengungkap rahasia dan cerita yang tidak pernah Anda ketahui, mengubah cara Anda mengingat orang yang sebenarnya.

Ini bukan skenario hipotetis yang jauh. Industri kehidupan setelah kematian digital berkembang pesat. Beberapa perusahaan berjanji untuk menciptakan rekonstruksi virtual individu yang telah meninggal berdasarkan jejak digital mereka. Dari chatbot AI dan avatar virtual hingga hologram, teknologi ini menawarkan perpaduan aneh antara kenyamanan dan gangguan. Ini mungkin menarik kita ke dalam pengalaman yang sangat pribadi yang mengaburkan batas antara masa lalu dan sekarang, ingatan dan kenyataan.

Seiring pertumbuhan industri kehidupan setelah kematian digital, hal ini menimbulkan tantangan etis dan emosional yang signifikan. Ini termasuk kekhawatiran tentang persetujuan, privasi, dan dampak psikologis pada orang yang masih hidup.

Apa Itu Industri Kehidupan Setelah Kematian Digital?

Teknologi VR dan AI membuat rekonstruksi virtual orang yang kita cintai menjadi mungkin. Perusahaan dalam industri ceruk ini menggunakan data dari postingan media sosial, email, pesan teks, dan rekaman suara untuk membuat persona digital yang dapat berinteraksi dengan orang yang masih hidup. Meskipun masih ceruk, jumlah pemain dalam industri kehidupan setelah kematian digital terus bertambah.

HereAfter memungkinkan pengguna untuk merekam cerita dan pesan selama masa hidup mereka, yang kemudian dapat diakses oleh orang yang dicintai setelah kematian. *MyWishes* menawarkan kemampuan untuk mengirim pesan terjadwal setelah kematian, mempertahankan kehadiran dalam kehidupan orang yang masih hidup. Hanson Robotics telah menciptakan bust robot yang berinteraksi dengan orang menggunakan kenangan dan sifat kepribadian almarhum. *Project December* memberi pengguna akses ke apa yang disebut "AI mendalam" untuk terlibat dalam percakapan berbasis teks dengan mereka yang telah meninggal.

AI generatif juga memainkan peran penting dalam industri kehidupan setelah kematian digital. Teknologi ini memungkinkan pembuatan persona digital yang sangat realistis dan interaktif. Namun tingkat realisme yang tinggi dapat mengaburkan batas antara realitas dan simulasi. Ini mungkin meningkatkan pengalaman pengguna, tetapi juga dapat menyebabkan tekanan emosional dan psikologis.

Teknologi yang Rawan Disalahgunakan

Teknologi kehidupan setelah kematian digital dapat membantu proses berkabung dengan menawarkan kesinambungan dan koneksi dengan almarhum. Mendengar suara orang yang dicintai atau melihat kemiripan mereka dapat memberikan kenyamanan dan membantu memproses kehilangan. Bagi sebagian dari kita, keabadian digital ini bisa

menjadi alat terapi. Mereka dapat membantu kita melestarikan kenangan positif dan merasa dekat dengan orang yang dicintai bahkan setelah mereka meninggal.

Namun bagi yang lain, dampak emosional mungkin sangat negatif, memperparah kesedihan daripada meringankannya. Rekonstruksi AI orang yang dicintai berpotensi menyebabkan bahaya psikologis jika yang berduka akhirnya memiliki interaksi yang tidak diinginkan dengan mereka. Ini pada dasarnya adalah subjek "penghantuan digital". Masalah besar lainnya dan masalah etis seputar teknologi ini termasuk persetujuan, otonomi, dan privasi. Misalnya, almarhum mungkin tidak setuju data mereka digunakan untuk "kehidupan setelah kematian digital". Ada juga risiko penyalahgunaan dan manipulasi data. Perusahaan dapat mengeksploitasi keabadian digital untuk keuntungan komersial, menggunakannya untuk mengiklankan produk atau layanan. Persona digital dapat diubah untuk menyampaikan pesan atau perilaku yang tidak pernah didukung oleh almarhum.

Kita Butuh Regulasi

Untuk mengatasi kekhawatiran seputar industri yang berkembang pesat ini, kita perlu memperbarui kerangka hukum kita. Kita perlu menangani masalah seperti perencanaan estate digital, siapa yang mewarisi persona digital almarhum, dan kepemilikan memori digital. GDPR Uni Eropa mengakui hak privasi pasca-kematian, tetapi menghadapi tantangan dalam penegakan. Platform media sosial mengontrol akses data pengguna yang sudah meninggal, sering kali bertentangan dengan keinginan ahli waris, dengan klausul seperti "tidak ada hak kelangsungan hidup" yang memperumit masalah. Praktik platform yang terbatas menghambat efektivitas GDPR. Pelindungan komprehensif menuntut evaluasi ulang aturan kontraktual, selaras dengan hak asasi manusia. Industri kehidupan setelah kematian digital menawarkan kenyamanan dan pelestarian memori, tetapi menimbulkan masalah etis dan emosional. Menerapkan peraturan yang bijaksana dan pedoman etis dapat menghormati baik yang hidup maupun yang mati, untuk memastikan keabadian digital meningkatkan kemanusiaan kita.

Apa yang Bisa Kita Lakukan?

Para peneliti telah merekomendasikan beberapa pedoman etis dan peraturan. Beberapa rekomendasi termasuk:

- mendapatkan persetujuan yang diinformasikan dan didokumentasikan sebelum membuat persona digital dari orang sebelum mereka meninggal
- pembatasan usia untuk melindungi kelompok rentan
- disclaimer yang jelas untuk memastikan transparansi
- dan langkah-langkah privasi dan keamanan data yang kuat.

Mengacu pada kerangka etika dalam arkeologi, sebuah studi tahun 2018 telah menyarankan untuk memperlakukan sisa-sisa digital sebagai bagian integral dari kepribadian, mengusulkan peraturan untuk memastikan martabat, terutama dalam layanan re-kreasi. Dialog antara pembuat kebijakan, industri, dan akademisi sangat penting untuk mengembangkan solusi etis dan regulasi. Penyedia juga harus menawarkan cara bagi pengguna untuk menghentikan interaksi mereka dengan persona digital secara hormat.

Melalui pengembangan yang hati-hati dan bertanggung jawab, kita dapat menciptakan masa depan di mana teknologi kehidupan setelah kematian digital menghormati orang yang kita cintai secara bermakna dan hormat. Saat kita menavigasi dunia baru yang berani ini, sangat penting untuk menyeimbangkan manfaat tetap terhubung dengan orang yang kita cintai dengan potensi risiko dan dilema etis. Dengan melakukan hal itu, kita dapat memastikan industri kehidupan setelah kematian digital berkembang dengan cara yang menghormati ingatan almarhum dan mendukung kesejahteraan emosional orang yang masih hidup.

Tautan artikel:

https://theconversation.com/an-eerie-digital-afterlife-is-no-longer-science-fiction-so-how-do-we-navigate-the-risks-231829
https://www.straitstimes.com/opinion/an-eerie-digital-afterlife-is-no-longer-science-fiction
https://lens.monash.edu/@technology/2024/08/26/1386829/an-eerie-digital-afterlife-is-no-longer-science-fiction-so-how-do-we-navigate-the-risks

'*Deepfake*' Begitu Banyak Di Internet: Bagaimana Strategi Bedakan Fakta Dari Fiksi Ciptaan AI

Arif Perdana

Konteks: Outline dari tulisan ini merupakan topik yang saya presentasikan di konferensi yang diselenggarakan oleh Association of Certified Fraud Examiner Indonesia pada bulan September 2023. Outline ini kemudian saya kembangkan menjadi artikel yang kemudian dimuat di The Conoversation Indonesia di 9 Januari 2024. Artikel ini membahas dampak negatif dari teknologi *deepfake*, yang dapat digunakan untuk memanipulasi informasi dan menimbulkan kerugian finansial serta sosial. Dengan kemajuan AI generatif, siapa pun dapat membuat konten palsu yang tampak nyata, yang dapat menyesatkan publik dan merusak reputasi individu. Untuk mengatasi masalah ini, diperlukan pemahaman tentang ciri-ciri *deepfake*, pengembangan algoritma deteksi, regulasi hukum, pendidikan publik, dan autentikasi platform untuk melindungi integritas informasi dan meminimalkan penyebarannya.

Pembuatan gambar atau video, termasuk elemen audio, dengan perangkat komputer yang dikenal dengan teknologi media sintetis (media tiruan) dalam perfilman, telah lama menjadi komponen inti dalam menciptakan dunia sinematografi yang menawan. Kita bisa melihat hasilnya dalam film-film terkenal termasuk seri *Avatar* dan *Jurassic Park*. Teknologi ini bukan fenomena baru. Sejak debutnya dalam film "Vertigo" pada 1958, media sintetis telah berkembang signifikan. Ini terbukti dengan penerapannya secara penuh dalam "*Toy Story*" pada 1995. Penerapan media sintetis di dunia perfilman tidak berbahaya. Ketika ditujukan untuk audiens dengan usia yang tepat dan hiburan, media ini menambah dimensi baru pada pengalaman menonton film.

Namun, kini, dengan kemajuan algoritma AI generatif, kemampuan untuk menghasilkan media sintetis tidak lagi dimonopoli oleh profesional film dan pengeditan video (lihat Tabel 8). Orang awam pun bisa mengakses teknologi ini untuk menghasilkan konten yang kompleks dengan cepat, mudah, dan berbiaya murah. Salah satu masalahnya adalah media sintetis versi AI yang disalahgunakan bisa menimbulkan konsekuensi serius. Misalnya, ketika digunakan untuk menciptakan *deepfake*, yaitu konten media sintetis yang dibuat dengan tujuan menyesatkan atau melakukan

kejahatan. Kita perlu meningkatkan kapasitas dan regulasi untuk mengurangi dampak negatif ini.

Tabel 8. Kapabilitas dan keterbatasan AI dalam menghasilkan media sintesis

Algoritma	Kapabilitas	Keterbatasan
Audio Sintetik		
WaveGAN	Menghasilkan gelombang audio yang realistis.	Kontrol terbatas atas karakteristik suara tertentu.
SampleRNN	Menghasilkan sampel audio berurutan.	Koherensi jangka panjang terbatas dalam urutan yang dihasilkan.
Tacotron & WaveNet	Menghasilkan suara manusia dari teks.	Memerlukan input teks untuk menghasilkan audio.
Autoencoders	Mereproduksi data input; mengodekan dan mendekode.	Terbatas pada fitur bawaan dari input yang diambil.
Variational Autoencoders (VAEs)	Menghasilkan data baru dengan sampling dari distribusi.	Kompleksitas dalam mengontrol kualitas data yang dihasilkan.
Video Sintetik		
DeepDream	Menghasilkan gambar surealis (dapat diperluas).	Tidak dirancang untuk video; kontinuitas antar frame tidak terjaga.
Variational Autoencoders (VAEs)	Menghasilkan frame video baru.	Mungkin kesulitan dalam menghasilkan adegan video yang kompleks.
Video GANs	Menghasilkan frame dan urutan video.	Kualitas frame yang dihasilkan dan kelancaran bervariasi.
Style Transfer	Mentransfer gaya dari satu gambar ke gambar lain.	Terbatas pada pengubahan gaya konten, tidak untuk menghasilkan adegan baru.
Deep Neural Networks	Melatih untuk pengenalan wajah dan sintesis gambar.	Memerlukan dataset pelatihan yang besar dan beragam.
Recurrent Neural Networks (RNNs)	Menghasilkan urutan, misalnya frame video.	Mungkin kesulitan dalam menangkap ketergantungan jangka panjang.
Sintesis Audio-Visual		
AVGAN	Menghasilkan konten audio-video yang disinkronisasi.	Kompleksitas dalam memastikan ketepatan lip-sync.

Dampak Negatif Deepfake

Ada banyak model AI generatif yang digunakan untuk membuat media sintesis. Model yang paling sering digunakan adalah tiga model berikut "(1) *Encoders/Decoders*" dan "(2) *Generative Adversarial Networks*" (GAN). Kedua model ini memungkinkan penciptaan gambar atau video yang sangat realistis, dari pertukaran wajah hingga kreasi video binatang yang terlihat berbicara. Lalu model ketiga, "*Style Transfer*" yang menawarkan kapabilitas untuk menyisipkan nuansa artistik ke dalam foto atau video, mengonversi gambar biasa menjadi karya seni yang estetis. AI telah membuka jalan bagi inovasi dalam media sintetis, meskipun terkadang menciptakan konten yang begitu nyata sehingga sulit dibedakan apakah audio atau video yang dihasilkan palsu atau asli.

Deepfake ini bisa berupa audio dan video yang sebenarnya palsu tapi tampak nyata, ditambah lagi dengan narasi-narasi yang sensitif dan memanipulasi psikologi manusia. Contoh nyata dari dampak negatif ini terjadi pada 2022, ketika video *deepfake* Presiden Ukraina Volodymyr Zelensky, beredar luas. Ketika ia terlihat mengajak warga Ukraina menyerah kepada Rusia. Kejadian serupa terjadi pada 2023 dengan tersebarnya video deepfake Presiden Rusia Vladimir Putin yang mengklaim Rusia akan diserang oleh Ukraina.

Di Slovakia, audio deepfake jurnalis *Denník N*, Monika Tódová digunakan untuk mendiskreditkan media dengan menyebarluaskan percakapan palsu tentang manipulasi pemilihan umum pada 2023. Sayangnya audio ini menyebar luas di media sosial pada saat masa tenang, dan pihak yang berwenang di Slowakia tidak bisa membantahnya. Akibatnya terjadi keresahan publik dan pesta demokrasi di Slowakia ternodai.

Tiga insiden di atas menunjukkan bagaimana *deepfake* dapat memicu kepanikan dan kebingungan di tengah situasi yang sudah tegang. Dampak *deepfake* tidak hanya terbatas pada ranah sosial dan politik; kejahatan finansial juga menjadi arena yang rawan. Ini terjadi pada 2019, ketika seorang eksekutif perusahaan energi di Inggris tertipu oleh audio *deepfake* yang menirukan suara salah satu atasannya. Penipuan ini menyebabkan kerugian finansial yang signifikan, setara Rp3,7 miliar. Kejadian ini memperlihatkan bagaimana teknologi yang canggih bisa disalahgunakan untuk menipu dan mengakibatkan kerugian material yang besar. Dengan demikian deepfake punya

dampak yang sangat merugikan, mulai dari privasi, fitnah, pelanggaran hak cipta, kerugian keuangan, hingga keresahan sosial.

Langkah Strategis Memitigasi Dampak *Deepfake*

Untuk menghadapi tantangan yang disebabkan oleh *deepfake*, ada beberapa langkah strategis yang bisa dilakukan.

Pertama, kita perlu memahami ciri-ciri dan elemen *deepfake*, seperti ketidakkonsistenan dalam gambar, video atau audio. Hal ini mencakup inkonsistensi pada ekspresi wajah, arah tatapan yang tidak sesuai, pergerakan rambut yang tidak alami, perspektif wajah yang salah, pencahayaan dan bayangan yang tidak realistis, serta kurangnya ekspresi mikro wajah. Elemen-elemen ini bisa mengindikasikan *deepfake*. Salah satu contoh yang terkenal adalah *deepfake* gambar mantan Presiden Amerika Serikat Barrack Obama. Selain itu, kita juga harus kritis dengan narasi-narasi yang bisa memanipulasi psikologi kita ketika melihat *deepfake* tersebut.

Kedua, solusi teknologi seperti algoritma AI yang dirancang untuk mendeteksi *deepfake* mampu mengidentifikasi ketidakkonsistenan ini secara otomatis. Selain bisa digunakan untuk menghasilkan *deepfake*, AI juga bisa digunakan untuk menandai atau memfilter *deepfake*. Ada beberapa repositori big data yang bisa diakses secara publik untuk melatih algoritma AI supaya bisa mendeteksi audio dan video *deepfake*, di antaranya *Deepfake Detection Challenge*, dan *Celeb-DF*. Para ilmuwan dan perusahaan-perusahaan teknologi multinasional saling bekerja sama untuk mengembangkan algoritma AI pendeteksi *deepfake* ini.

Ketiga, melibatkan langkah-langkah hukum dan kebijakan, termasuk pengembangan peraturan yang memadai dan kerja sama internasional untuk mengatasi penyebaran *deepfake* secara global. EU Research Report (lihat Tabel 9), misalnya, mengidentifikasi lima dimensi regulasi untuk memerangi *deepfake*: teknologi, penciptaan, sirkulasi, target, dan audiens. Dimensi teknologi menyoroti AI sebagai dasar dari *deepfake*, dengan regulasi yang diterapkan oleh Komisi Eropa. Dimensi “penciptaan” menekankan pada pelaku dan alat yang digunakan untuk membuat *deepfake*. Aspek “sirkulasi” merujuk pada penyebaran *deepfake* melalui platform dan kanal tertentu. Aspek

“target” fokus pada korban *deepfake*, sementara dimensi “audiens” fokus kepada pendidikan publik untuk mengenali dan memahami bahaya *deepfake*. Pelajaran lainnya bisa diambil dari Badan Keamanan Siber Cina yang telah menetapkan peraturan pada Januari 2023 untuk mengatur *deepfake*. Tujuan peraturan ini untuk mengekang penyalahgunaan *deepfake* dengan mewajibkan persetujuan, memverifikasi identitas pengguna model AI yang digunakan untuk membuat media sintetis. Selain itu, juga untuk memerangi disinformasi, memastikan kepatuhan hukum, dan mewajibkan konten untuk ditandai sebagai media sintetis guna menjaga kepercayaan publik terhadap informasi digital, dan mencegah penipuan.

Tabel 9. Dimensi regulasi deepfake European Union

Dimensi Regulasi	Deskripsi
Dimensi Teknologi	• Berfokus pada teknologi yang mendasari deepfake, yang merupakan teknik pembelajaran mesin berbasis AI. • Regulasi ini terutama berada di bawah kerangka regulasi AI yang diusulkan oleh Komisi Eropa. • Kerangka ini mengadopsi pendekatan berbasis risiko untuk pengaturan teknologi AI.
Dimensi Penciptaan	• Berkaitan dengan pembuatan deepfake yang sebenarnya. • Menekankan pentingnya menangani aktor yang terlibat dalam produksi deepfake dan alat yang mereka gunakan.
Dimensi Sirkulasi	• Menangani penyebaran dan distribusi deepfake. • Menyoroti platform dan saluran yang digunakan untuk membagikan deepfake dan potensi viralitasnya.
Dimensi Sasaran	• Berfokus pada korban dari deepfake dan kerugian yang mereka derita. • Menggarisbawahi kebutuhan untuk memberikan dukungan dan perlindungan bagi para korban ini.
Dimensi Audiens	• Mengenai penonton atau konsumen deepfake. • Menekankan pentingnya mendidik dan memberi informasi kepada publik tentang bahaya deepfake dan cara mengenalinya.

Keempat, peningkatan kesadaran publik dan pendidikan adalah kunci untuk mempersenjatai masyarakat dengan pengetahuan untuk membedakan antara konten asli dan palsu. Meningkatkan kesadaran tentang bahaya konten manipulatif dapat membuat masyarakat menjadi konsumen informasi yang lebih kritis melalui lokakarya, kampanye media, dan kurikulum pendidikan. Pada tataran global, beberapa platform menyediakan pendidikan publik untuk mengenali dan menghindari bahaya *deepfake*, di antaranya, *MIT Media Literacy*, *Digital Media Literacy for All*, The *Washington Post Fact Checker Guide to Manipulated Videos*, *CNN Deepfake Explained*, dan *Microsoft Spotting Deepfake*. Di Indonesia sudah ada inisiatif serupa, seperti panel ahli cek fakta Pemilu 2024 yang dikelola oleh The Conversation Indonesia, dan Cek Fakta.

Terakhir, pentingnya platform repositori media yang dipercaya dan mekanisme autentikasi, misalnya seperti *Reality Defender*, dan *Content Authenticity Initiative*. Platform ini memainkan peran krusial dalam menjaga integritas informasi dengan menyediakan sumber yang terverifikasi dan dapat diandalkan. Ini juga termasuk penggunaan watermark digital dan teknologi lain untuk memastikan keaslian konten. Melalui implementasi langkah-langkah strategis ini, kita bisa meminimalkan penyebaran *deepfake* yang meresahkan publik, melindungi integritas diskursus publik dan kebenaran informasi.

Tautan artikel:

https://theconversation.com/deepfake-begitu-banyak-di-internet-bagaimana-strategi-bedakan-fakta-dari-fiksi-ciptaan-ai-218737
https://koran.tempo.co/read/ilmu-dan-teknologi/486621/cara-mengenali-deepfake

AI Generatif Membahayakan Lingkungan: Bagaimana Cara Mengatasinya?

Arif Perdana

Konteks: Artikel ini diterbitkan di The Conversation Indonesia di 24 Oktober 2023. Artikel ini juga direplikasi di Koran Tempo. Tulisan ini membahas dampak lingkungan dari teknologi AI generatif, yang membutuhkan energi besar dan menghasilkan emisi karbon selama fase pelatihan dan operasional pusat data. Dengan contoh penggunaan model bahasa besar, penulis menyoroti jejak karbon yang signifikan. Untuk mengatasi masalah ini, artikel menyarankan pendekatan teknis dan nonteknis, termasuk penggunaan model open source, adopsi sumber energi terbarukan, dan praktik pengelolaan data yang berkelanjutan. Regulasi dan kesadaran lingkungan juga penting untuk memastikan teknologi AI selaras dengan keberlanjutan.

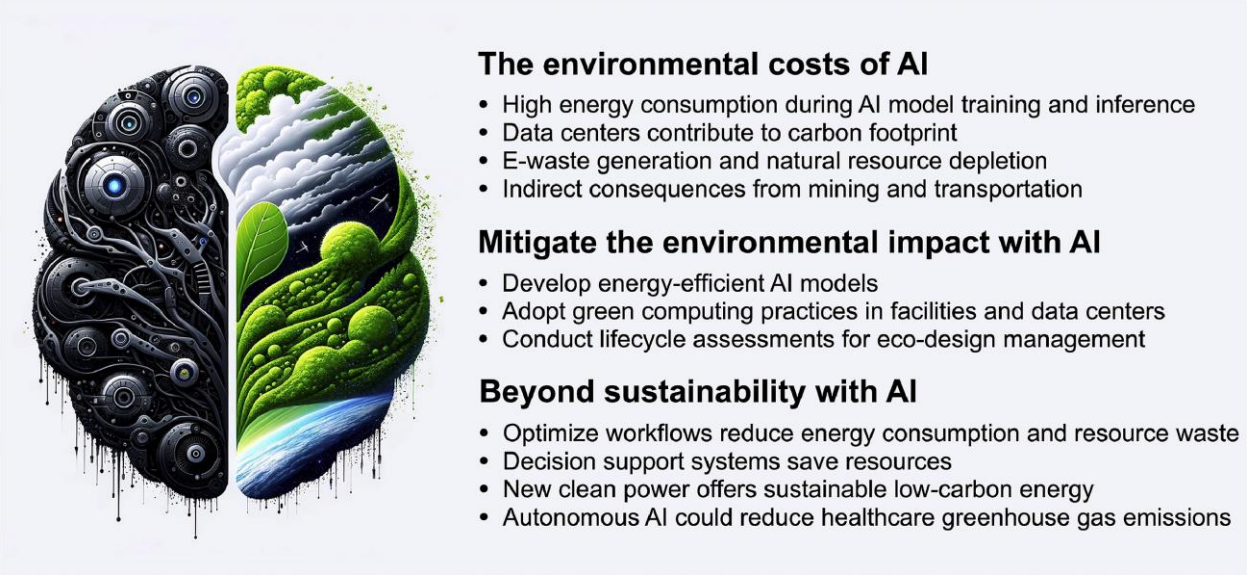
AI generatif muncul sebagai teknologi serbaguna yang mampu menciptakan konten baru dan orisinal seperti gambar, teks, musik, dan video. Walau begitu, ada kekhawatiran teknologi ini berdampak buruk pada lingkungan (lihat Gambar 7). Seiring dengan maraknya penggunaan AI generatif, konsumsi energi listrik dan pusat data (data centre) dan jejak karbonnya kian naik. Karena itu, kita perlu mengatasi bahaya lingkungannya agar teknologi baru tidak menambah beban bagi Bumi. Tulisan saya akan menjelaskan bagaimana risiko lingkungan yang timbul akibat AI dan bagaimana langkah-langkah mengatasinya.

Dampak AI Generatif terhadap Lingkungan

Kita dapat mengamati risiko lingkungan AI generatif sejak teknologi ini menjalani fase “pelatihan” generatif suatu model AI dengan data-data yang tersedia. Dalam fase ini, pelatihan AI memerlukan energi sangat besar sehingga dapat melepaskan emisi karbon yang dapat memperparah perubahan iklim. Sebagai contoh, Model Bahasa Besar (*large language models* atau LLM) yang merupakan salah satu algoritma dasar suatu AI generatif, seperti GPT-3. memiliki 175 miliar parameter. Parameter ini adalah konfigurasi yang bisa digunakan untuk menghasilkan output. Ini mirip seperti seperti senar gitar atau

tuts piano yang bisa dikombinasikan untuk menghasilkan output nada yang ciamik. Studi mengungkapkan bahwa pelatihan satu model bahasa besar seperti GPT-4 atau PaLM buatan *Google* dapat melepaskan sekitar 300 ton CO2 ke atmosfer. Angka ini setara dengan 360 kali penerbangan dari London menuju New York.

Sementara itu, model lainnya, BERT (*Bidirectional Encoder Representations from Transformers*) yang bisa menghasilkan gambar dari teks, juga meninggalkan jejak karbon sekitar 300-1.400 ton C02[90]. Selain konsumsi energi, pusat data yang penting bagi pengembangan AI generatif juga memperburuk kondisi lingkungan. Pusat data mengonsumsi energi yang besar untuk pendinginan mesin mereka sehingga menghasilkan emisi karbon yang signifikan.



Gambar 7. Dampak lingkungan AI: Biaya dan strategi mitigasi

Metode pendinginan yang membutuhkan banyak air dan kebisingan peralatannya juga membawa dampak terhadap lingkungan. Pembuatan dan pembuangan peralatan pusat data juga menambah tumpukan limbah elektronik. Pusat data juga bisa memperparah ketimpangan. Sebagai contoh, pusat data di Amerika Serikat yang berada di Northern Virginia (Ashburn), Chicago, Dallas, dan lainnya, karena posisi yang

[90] https://arxiv.org/abs/1810.04805

menguntungkan dan konektivitas jaringan yang kuat. Namun, pendirian pusat data di wilayah-wilayah ini seringkali mengakibatkan tekanan pada infrastruktur lokal, membebani jaringan listrik lokal, jalan, dan mengganggu pasokan air.

Tantangan ini memengaruhi pengelolaan sumber daya yang efektif bagi komunitas dan pemerintah setempat. Penempatan pusat data di dekat area perumahan juga memicu konflik regulasi dan zonasi. Konflik ini muncul dari kekhawatiran warga setempat terkait tingkat kebisingan, dampak visual, dan penggunaan lahan. Polusi suara dari sistem pendinginan dan peralatan pusat data mengganggu kehidupan warga sekitar.

Mengatasi Bahaya Lingkungan AI

Guna mengatasi bahaya lingkungan dari AI generatif, kita bisa melakukan pendekatan teknis dan nonteknis. Pendekatan ini juga bisa dilakukan hingga ke pengelolaan operasional pusat data. Dari sisi teknis, misalnya, institusi bisa menggunakan LLM yang sudah ada, alih-alih membuatnya dari awal. Sebab, proses pembuatan model baru yang membutuhkan energi besar. Sebagai contoh, AI generatif berjenis open source (sumbernya bisa diakses semua orang) bisa digunakan untuk membantu universitas mengembangkan AI generatif di negara berkembang. *Google*, misalnya, membuat PaLM—LLM yang mendasari *Google Bard*—menjadi open source. Model yang sudah ada juga bisa diperbaiki dan disesuaikan ulang (*fine-tuning*).

Institusi juga perlu mempertimbangkan dengan saksama apakah AI generatif memang satu-satunya solusi. Institusi juga adakalanya menganggap setiap masalah bisnis bisa diselesaikan dengan model-model AI, padahal jika ada solusi lain yang hemat energi dengan hasil yang sama baiknya, AI generatif atau model-model AI yang kompleks lainnya seharusnya tidak digunakan. Komputasi yang hemat energi juga merupakan aspek penting. Penggabungan perangkat keras dan perangkat lunak yang efisien ke dalam sistem AI dapat mengurangi konsumsi energi sehingga lebih ramah lingkungan.

Pengembang juga dapat mengadopsi metode komputasi yang sadar energi seperti *TinyML*. *TinyML* merupakan platform penerapan algoritma pemelajaran mesin dengan sumber daya dan energi yang rendah. Di sisi non teknis, kesadaran terhadap lingkungan memainkan peran penting. Institusi harus mengambil keputusan yang sadar

mengenai pemilihan model-model AI yang ramah energi. Perusahaan dan para peneliti harus mengutamakan praktik AI yang berkelanjutan dan berinvestasi dalam perangkat keras dan infrastruktur yang efisien energi. Adopsi sumber energi terbarukan dan optimalisasi operasi pusat data dapat secara signifikan mengurangi jejak karbon yang terkait dengan pembuatan model AI generatif.

Dari sisi regulator, para pembuat kebijakan dapat menerapkan peraturan dan insentif untuk mendorong praktik pengembangan teknologi AI yang ramah lingkungan. Manajemen data berkelanjutan Manajemen data berkelanjutan adalah upaya yang tak kalah penting. Organisasi harus mengambil pendekatan proaktif dengan mengutamakan pengadaan data yang etis dan mengadopsi praktik pengelolaan data yang bertanggung jawab.

Organisasi dapat mengurangi penyimpanan data yang tidak perlu. Dengan mengoptimalkan aliran data, mulai dari pengumpulan hingga pemusnahan data, organisasi dapat mencegah penumpukan data tidak terpakai atau usang di pusat data. Alih-alih menyalin data ke host lokal, mengakses data dari sumber aslinya dapat meminimalkan dampak data karbon dan mengurangi konsumsi energi yang tidak perlu. Organisasi juga dapat menerapkan strategi pembuangan data yang tidak perlu atau usang. Pembuangan data yang tepat juga dapat mencegah penumpukan data tidak terpakai, sehingga dapat mengurangi volume kinerja pusat data. Selain itu, organisasi harus melakukan evaluasi dampak lingkungan yang komprehensif untuk proyek-proyek AI. Prediksi dampak lingkungan penyimpanan dan penggunaan data dapat menginformasikan proses pengambilan keputusan dan mengutamakan keberlanjutan sepanjang siklus proyek AI. Ini termasuk menganalisis emisi karbon yang dihasilkan oleh penyimpanan data dan mempertimbangkan pendekatan yang lebih berkelanjutan untuk memenuhi persyaratan proyek.

Pemerintah dapat meningkatkan efisiensi pusat data dengan menerapkan operasinya berlandaskan standar energi terbaik. Kewajiban pengungkapan dampak lingkungan bagi pengelola data juga membantu meningkatkan kesadaran akan jejak emisi pusat data. Pemerintah seharusnya bisa menyediakan insentif untuk penggunaan energi terbarukan di pusat data. Selain itu, pemerintah dapat mempromosikan pilihan

lokasi pusat data yang efisien energi dengan mendorong mereka untuk berlokasi di iklim yang lebih dingin atau dekat sumber energi terbarukan. Harapannya, pusat data bisa mengurangi konsumsi air untuk mendinginkan mesin-mesinnya.

Sementara itu, untuk menyeimbangkan emisi, pengelola pusat data sepatutnya turut berinvestasi dalam proyek energi terbarukan. Mereka juga bisa terlibat dalam upaya pemulihan ekosistem esensial seperti hutan. AI generatif memiliki potensi untuk merevolusi berbagai industri dan mendorong inovasi, tetapi dampak lingkungannya juga bisa menjadi ancaman serius bagi Bumi. Dengan secara bersama mengatasi dampak lingkungan dari AI generatif, kita memastikan kemajuan teknologi selaras dengan kelestarian planet ini.

Tautan artikel:

https://theconversation.com/ai-generatif-membahayakan-lingkungan-bagaimana-cara-mengatasinya-214871
https://koran.tempo.co/read/lingkungan/485200/ancaman-ai-generatif-bagi-lingkungan

Teknologi dan Resistensi: Kisah Anti-Mobil Hingga AI

Arif Perdana

Konteks: Artikel ini saya tulis untuk The Conversation Indonesia dan diterbitkan tanggal 6 September 2023. Saya membahas bagaimana teknologi, dari mobil hingga AI, sering kali diiringi dengan rasa takut dan resistensi, tetapi akhirnya mendorong kemajuan. Meskipun ada kekhawatiran bahwa AI dapat menggantikan pekerjaan manusia, teknologi ini justru berpotensi mengubah cara kita bekerja dan menciptakan peluang baru. Dengan pendekatan berbasis pendidikan dan regulasi yang tepat, kita dapat memanfaatkan AI dan teknologi lainnya untuk kebaikan. Sejarah menunjukkan bahwa inovasi dapat mengubah struktur ekonomi dan menciptakan lapangan kerja baru.

Teknologi, sebagai kekuatan pengubah sejarah, secara konstan memengaruhi hampir setiap aspek kehidupan kita. Namun di setiap titik perubahan, sering kali kita dihantui oleh keraguan, rasa takut, dan penolakan. Kisah resistensi itu bisa kita lacak, misalnya, dari munculnya mobil, internet hingga AI. Momen-momen keresahan itu berperan sebagai tonggak-tonggak sejarah manusia. Sebenarnya, resistensi dan kekhawatiran muncul sebagai respons alamiah terhadap perubahan yang tidak dapat dihindari. Satu riset menunjukkan internet komersial, yang dulu dikhawatirkan pada awal kemunculannya, telah menciptakan 17 juta pekerjaan baru di seluruh dunia antara 2016 dan 2021. Mari kita lihat beberapa contoh inovasi teknologi lainnya yang selalu diawali dengan rasa takut tapi akhirnya mendorong kemajuan peradaban umat manusia (lihat Tabel 10).

Dari Mobil hingga Komputer

Dengan merujuk pada era penemuan otomotif, saat mobil komersial pertama kali diciptakan pada akhir abad ke-19, negara-negara di seluruh dunia dipenuhi dengan kegelisahan, yang berakibat pada pengetatan regulasi. Inggris pada akhir abad ke-19, misalnya, membuat Locomotives on Highways Act 1896. UU ini membatasi kecepatan dan mewajibkan mobil di jalanan didahului oleh pejalan kaki yang membawa bendera

merah sebagai tanda peringatan. Hal itu mencerminkan kekhawatiran masyarakat bahwa inovasi baru dapat mengganggu gaya hidup tradisional, memengaruhi pekerjaan lama seperti tukang becak dan kusir kereta kuda.

Lebih lanjut, ketika komputer personal (personal computer) dikomersialisasikan pada akhir 1970-an, banyak publikasi paper pada 1980-an sampai 1990-an yang membahas tentang computerphobia. Beberapa kelompok masyarakat khawatir dan beranggapan bahwa teknologi ini merupakan monster mekanik, berpotensi menciptakan manusia yang malas dan tergantung pada teknologi untuk melakukan perhitungan dasar. Namun, sebaliknya, teknologi ini justru memfasilitasi kemajuan ilmu pengetahuan. Kemampuan komputer menyelesaikan perhitungan yang kompleks dengan cepat dan akurat membuat ilmuwan bisa menghasilkan penemuan baru ataupun merancang solusi yang lebih inovatif. Selain itu, teknologi ini membantu meningkatkan produktivitas di berbagai sektor. Ini memungkinkan kita untuk fokus pada tugas-tugas yang lebih memerlukan keterampilan manusia seperti kreativitas dan analisis.

Grace Murray Hopper, seorang ilmuwan komputer Amerika Serikat (AS) yang bekerja di *the Office of Naval Reserve* (ONR) - organisasi di Departemen Angkatan Laut AS yang bertanggung jawab atas program ilmu pengetahuan dan teknologi dari Angkatan Laut AS - memiliki peran penting dalam perkembangan komputer generasi awal dengan penemuan kompiler. Kompiler adalah alat yang mengubah kode pemrograman, menjadi kode mesin yang dapat dijalankan oleh komputer. Melalui pengembangan kompiler, Hopper membuka akses pemrograman kepada masyarakat luas dan membuktikan bahwa komputer bukanlah teknologi yang harus ditakuti. Sebaliknya, komputer dapat memberikan nilai besar untuk bisnis, pendidikan, dan bidang lainnya.

Era AI: Kekhawatiran versus Masa Depan

Hari ini, kita menghadapi lonjakan teknologi serupa dalam bentuk AI. Seperti teknologi sebelumnya, AI juga memunculkan kekhawatiran bahwa teknologi ini akan mengambil alih pekerjaan manusia dan meningkatkan pengangguran. Namun, pandangan ini terlalu sederhana. AI, dengan kemampuannya untuk mengambil alih tugas-tugas rutin dan berulang, sebenarnya membebaskan manusia untuk lebih fokus pada

pekerjaan yang memerlukan keterampilan kreatif, pemecahan masalah, dan interpersonal. Misalnya, dokter bisa memanfaatkan AI untuk diagnosis penyakit dan merancang rencana perawatan yang lebih personal. Sementara guru bisa memanfaatkan AI untuk personalisasi pembelajaran dan mengidentifikasi area yang perlu ditingkatkan.

Sejauh ini, penelitian menunjukkan bahwa AI cenderung mengubah pekerjaan daripada menggantikannya. Artinya, peran AI lebih banyak mengubah cara kita bekerja daripada menggantikan pekerjaan manusia. Meskipun AI dapat mengotomatisasi tugas-tugas tertentu di satu pekerjaan, pekerjaan tersebut secara umum tetap memerlukan sentuhan manusia dan pemikiran kreatif yang tidak dapat digantikan sepenuhnya oleh AI. Contohnya, akuntan bisa menggunakan AI untuk memprediksi mengenai adanya potensi kecurangan, tapi pengambilan keputusan tidak bisa dilakukan sepenuhnya oleh AI. Keahlian dan pengetahuan akuntan tetap diperlukan. Selain itu, seperti teknologi sebelumnya, AI juga berpotensi menciptakan banyak pekerjaan baru yang belum pernah kita bayangkan sebelumnya.

Namun, untuk menghadapi era AI ini, kita perlu pendekatan yang berbasis pada pendidikan dan pemahaman, bukan rasa takut. Kita perlu melihat AI sebagai alat yang dapat membantu kita, bukan sebagai ancaman. Melalui pendidikan dan pelatihan yang tepat, kita dapat mempersiapkan diri dan generasi mendatang untuk era AI. Selain itu, kita juga perlu memastikan bahwa AI dikembangkan dan digunakan dengan cara yang etis dan bertanggung jawab. Dengan melibatkan manusia dalam proses pengambilan keputusan, kita dapat memastikan bahwa AI digunakan untuk kebaikan, bukan sebaliknya.

Tabel 10. Kehawatiran versus realitas terhadap teknologi

Teknologi	Kekhawatiran	Realitas
Mobil	• Mengganggu pekerjaan tradisional seperti tukang becak dan kusir. • Membahayakan keselamatan di jalan raya, sehingga diatur dengan ketat (misal, UU Locomotives on Highways).	• Membuka peluang kerja baru di industri otomotif (insinyur, teknisi, penjualan, pemasaran). • Meningkatkan mobilitas dan akses geografis serta memajukan struktur ekonomi global.

Teknologi	Kekhawatiran	Realitas
Komputer	• Khawatir menciptakan manusia malas dan bergantung pada mesin.	• Memfasilitasi kemajuan ilmu pengetahuan, meningkatkan produktivitas, dan mendukung inovasi ilmiah.
	• Banyak yang mengalami "computerphobia" di awal penggunaannya.	• Membantu dalam perhitungan kompleks dan meningkatkan efisiensi di berbagai sektor.
Internet	• Takut menyebabkan pengangguran, privasi, dan isolasi sosial.	• Menciptakan jutaan pekerjaan baru di bidang TI, mendukung e-commerce, dan memfasilitasi kerja jarak jauh.
	• Mengakibatkan hilangnya 500 ribu pekerjaan.	• Sebenarnya menciptakan 1,2 juta pekerjaan baru antara 1990-2010, serta mendukung kolaborasi global dan komunikasi.
AI	• Kekhawatiran akan menggantikan manusia dan meningkatkan pengangguran.	• Mengotomatiskan tugas rutin, memungkinkan manusia fokus pada tugas kreatif, analisis, dan interpersonal.
	• Dikhawatirkan mengambil alih seluruh pekerjaan manusia.	• Cenderung mengubah cara kerja manusia daripada menggantikan pekerjaan sepenuhnya. • Potensi menciptakan pekerjaan baru yang belum pernah ada, seperti peran dalam manajemen AI dan pengembangan teknologi.

Peluang Kerja dan Ekonomi Baru

Sejarah menunjukkan bahwa mobil bukan hanya memfasilitasi pergerakan penduduk dan meningkatkan akses geografis. Mobil juga membuka peluang kerja baru dalam industri otomotif dan terkait. Bidang pekerjaan ini beragam, mulai dari insinyur otomotif, teknisi perawatan, hingga peran dalam penjualan dan pemasaran mobil. Oleh karena itu, inovasi ini tidak hanya merombak cara kita bergerak, tapi juga mengubah struktur ekonomi kita. Industri otomotif merupakan sektor ekonomi terbesar dan paling penting di dunia. Di Eropa, misalnya, data pada 2023 menunjukkan bahwa sektor otomotif menyerap tenaga kerja sebanyak 13 juta orang di Eropa (secara langsung dan tidak langsung). Ini mencakup 7% dari total pekerjaan di Uni Eropa. Sekitar 11,5% dari total pekerjaan di sektor manufaktur Uni Eropa–sekitar 3,4 juta–berada di sektor otomotif.

Lapangan kerja ini mencakup berbagai bidang, mulai dari perakitan dan manufaktur hingga penjualan, pemasaran, dan perawatan.

Komputer dan internet juga telah memengaruhi hampir setiap aspek ekonomi dan menciptakan jutaan pekerjaan baru di TI. Misalnya, sepanjang sepuluh tahun terakhir, jumlah pekerjaan di sektor TI di AS terus meningkat. Meskipun ada penurunan signifikan dalam jumlah tenaga kerja TI pada 2020, angka tersebut melampaui 3 juta mulai April 2022 dan mencapai puncaknya hampir 3,12 juta pekerja pada Januari 2023.

Dalam kurun waktu 1990 hingga 2010, lembaga konsultan bisnis McKinsey menyatakan bahwa internet mengakibatkan punahnya 500 ribu pekerjaan, tapi pada saat yang sama internet juga menciptakan 1,2 juta pekerjaan baru. Dengan demikian, ketakutan awal terhadap internet, termasuk isu privasi dan isolasi sosial, ternyata tidak sebanding dengan manfaatnya. Internet juga memfasilitasi pertumbuhan e-commerce, dengan penjualan global mencapai $5.89 triliun (hampir Rp90 ribu triliun) pada 2023. Komunikasi dan kolaborasi juga lebih mudah dan efisien berkat fitur seperti email dan video call. Komputer dan internet memfasilitasi kerja jarak jauh, memberikan fleksibilitas dan memperluas peluang bagi mereka yang tinggal jauh dari pusat-pusat pekerjaan. Selain itu, komputer juga telah membuka lapangan kerja baru dalam bidang seperti analisis data, analis keamanan siber, dan arsitek komputasi awan.

Meski ada tantangan dan risiko, dengan pemahaman dan regulasi yang tepat, kita dapat memanfaatkan potensi internet, termasuk AI, sambil memitigasi risikonya. Jadi, pertanyaannya bukan lagi apakah kita harus menerima teknologi baru seperti AI atau tidak, tapi bagaimana kita dapat memanfaatkan teknologi ini untuk kebaikan kita. Dengan pendidikan, pelatihan, dan regulasi yang tepat, kita dapat memastikan bahwa umat manusia tidak hanya bisa bertahan dalam era digital ini, tapi juga berkembang dan maju.

Tautan artikel:

https://theconversation.com/teknologi-dan-resistensi-kisah-anti-mobil-hingga-ai-211345

Bagaimana AI Dapat Memperparah Penyebaran Hoaks Jelang Pemilu 2024

Arif Perdana

Konteks: Artikel ini diterbitkan di The Conversation Indonesia tanggal 30 Agustus 2023. Saya membahas bagaimana disinformasi, yang sudah ada sejak zaman Romawi Kuno, semakin diperburuk oleh teknologi AI dalam era digital. Penyebaran informasi salah semakin cepat dan sulit dideteksi, terutama menjelang pemilu. Meskipun AI dapat menyebarkan disinformasi, teknologi ini juga dapat digunakan untuk melawannya, seperti dengan pemrosesan bahasa alami untuk mendeteksi konten palsu. Keterlibatan publik dalam literasi digital dan inisiatif cek fakta juga penting untuk menghadapi tantangan disinformasi di masyarakat.

Fenomena disinformasi, alias suatu info yang diketahui salah lalu disebarkan dengan sengaja, sebenarnya sudah ada sejak peradaban Romawi Kuno. Pada tahun 33 Sebelum Masehi (SM), Kaisar Octavianus Augustus, pewaris tahta dari pemimpin diktator Romawi, Gaius Julius Caesar, menggunakan disinformasi untuk merusak reputasi saingannya, Mark Antony, dan mendapatkan lebih banyak dukungan dari publik Romawi. Bedanya, pada era digital ini, penyebaran disinformasi menjadi sangat cepat karena berkembangnya teknologi, diperkuat oleh algoritma AI.

Era AI ini telah merevolusi segala lini industri dan kehidupan masyarakat, membawa kemajuan sekaligus tantangan. Salah satu dampak AI yang cukup mengkhawatirkan adalah memperburuk fenomena disinformasi, terutama menjelang tahun politik. Meski demikian, perlu dipahami bahwa masalah ini bukan semata kesalahan teknologi; akarnya juga ada di psikologi manusia. Ini karena disinformasi terkait erat dengan bias kognitif (kesalahan dalam berpikir dan menilai secara alam bawah sadar) yang dimiliki oleh manusia.

Penelitian menunjukkan bahwa manusia tertarik pada narasi yang membentuk identitas, menguatkan keyakinan, dan sejalan dengan perspektif sosial dan politik mereka, meskipun narasi tersebut palsu. Seperti yang diungkapkan oleh Cass R. Sunstein, profesor hukum dari *Harvard Law School* di Amerika Serikat (AS), bahwa daya

tarik disinformasi terletak pada kemampuannya untuk membangkitkan emosi manusia, seperti rasa takut dan harapan, dan penyebarannya didorong oleh beragam motivasi, mulai dari kepentingan pribadi hingga niat jahat. Kondisi penyebaran disinformasi ini punya potensi menjadi lebih marak dan parah, dengan adanya AI yang memiliki kemampuan menciptakan dan mengamplifikasi disinformasi sehingga dapat merusak tatanan demokrasi. Menjelang Pemilihan Umum (Pemilu 2024), dampak AI kepada disinformasi ini dapat memperburuk kepercayaan publik terhadap institusi pemerintah dan penyedia informasi seperti media massa, serta memperdalam polarisasi sosial.

Cara AI Memperburuk Disinformasi

Dalam beberapa tahun terakhir, lanskap pemilihan global dicemari oleh aliran disinformasi yang didukung oleh AI. Bagaimana cara AI melakukannya? Ini bisa terjadi karena algoritma AI dirancang untuk memaksimalkan keterlibatan pengguna, yang kemudian turut mempromosikan konten informasi yang salah. Oleh karena itu, algoritma memiliki kemampuan mengarahkan individu masuk ke echo chamber alias ruang gema yang sangat mungkin berisi disinformasi. Ruang gema adalah lingkungan di dunia maya yang membuat seseorang hanya menerima informasi, ide, dan gagasan yang homogen atau sesuai dengan pemikiran mereka secara terus menerus.

Pemilihan Presiden AS 2016 menjadi contoh nyata fenomena ini. Teori konspirasi daring “PizzaGate”, yang menyatakan ada kegiatan pedofilia di dalam tubuh pemerintah AS, dipropagandakan melalui unggahan yang mengklaim Hillary Clinton menjalankan jaringan seks anak-anak di sebuah gerai pizza *Comet Ping Pong* di Washington DC. Tuduhan tak berdasar ini kemudian semakin disebarluaskan oleh algoritma AI di media sosial, yang pada akhirnya memanipulasi opini publik dan menyebarkan kebingungan. Dampak disinformasi daring juga terjadi pada pemilu Nigeria 2023. Laporan BBC mengungkap politikus membayar influencer untuk menyebarkan disinformasi. Menjelang 2023, jumlah berita palsu meningkat pesat di media sosial di Nigeria, menargetkan kandidat presiden. Paradoksnya, media sosial di Nigeria, khususnya Twitter, berperan besar dalam penyebaran berita pemilu yang kredibel tapi sekaligus menjadi sumber utama disinformasi.

Di Indonesia, pada pemilu 2014 dan 2019 ada konten-konten disinformasi berupa teks dan foto yang digunakan untuk memengaruhi sentimen publik. Contohnya foto laki-laki mirip Jokowi hadir di kampanye D.N. Aidit yang menyebabkan Jokowi dituduh sebagai antek Partai Komunis Indonesia (PKI). Beredar pula narasi-narasi palsu dibuat untuk mengangkat dan menghancurkan kandidat-kandidat yang bersaing di pemilihan, menyebabkan ketidakpercayaan dan kebingungan di antara pemilih. Sebagai contoh, narasi palsu bahwa mantan perwira tinggi militer Prabowo Subianto, yang kini ketua Partai Gerindra sekaligus bakal calon kandidat presiden untuk Pemilu 2024, diberhentikan "secara tidak hormat" dari institusi TNI. Padahal kenyataannya Prabowo diberhentikan dengan hormat. Keterangan yang diubah hanya perihal hormat dan tidak hormat, tetapi ini akan sangat memengaruhi sentimen publik terhadap Prabowo. Ada pula survey palsu yang muncul jelang Pemilu 2014 yang menyatakan Prabowo akan memenangkan pilpres. Lalu pada Pemilu 2019, beredar narasi palsu berupa data yang diklaim berasal dari intelijen TNI yang menyebutkan Prabowo telah memenangkan Pilpres.

Menjelang pemilu 2024 ini, apa yang harus kita persiapkan, mengingat teknologi Generative AI sudah berkembang? Ditambah lagi, disinformasi yang menyebar di pemilu 2024 nanti tidak hanya teks tetapi juga audio dan video. Melacak disinformasi di media sosial berbasis video seperti TikTok juga menjadi semakin sulit karena menggunakan format audiovisual, bahasa 'gaul', dan fitur pencarian yang terbatas.

Langkah Melawan Disinformasi

Ancaman AI semakin diperparah oleh kemampuannya untuk memanipulasi struktur dan presentasi teks. *Generative AI* seperti *ChatGPT*, misalnya, bisa membuat konten disinformasi dengan cepat. Algoritma AI lainnya juga bisa membuat foto, video, dan suara artifisial tampak sangat meyakinkan (*deepfake*). Penelitian menunjukkan bahwa orang lebih sulit mendeteksi konten palsu yang dihasilkan AI dibandingkan dengan yang dibuat oleh manusia. Ini karena sifat terstruktur dan ringkas dari konten yang dihasilkan AI, membuatnya lebih mudah dipahami dan meyakinkan. Menangani bahaya disinformasi dari AI memerlukan pendekatan teknologi dan partisipasi

masyarakat. Ironisnya, dari perspektif teknis, AI bisa digunakan untuk menyebarkan disinformasi, tapi juga dapat menjadi alat untuk melawan disinformasi dan mengembalikan kepercayaan.

Salah satu contoh dampak positif AI adalah penggunaan teknik Pemrosesan Bahasa Alami (NLP) untuk membedakan narasi yang asli dan yang palsu. Inisatif awal sudah dilakukan oleh Kementerian Komunikasi dan Informatika (Kominfo) dengan perusahan start-up Prosa.ai. Mereka meluncurkan chatbot antihoaks berbasis NLP di Telegram. Algoritma tersebut tentunya perlu terus dikembangkan dan diperbarui agar tetap akurat dalam menghadapi konten AI yang semakin kompleks.

Pemerintah Indonesia juga bisa belajar dari Uni Eropa yang telah mengoperasikan European Union's Disinformation Lab dengan menyebarkan berbagai materi yang dibuat melalui bantuan AI guna mendidik masyarakat dalam melawan disinformasi di era digital. Selain aspek teknologi, komitmen publik dalam melawan disinformasi yang dihasilkan oleh AI juga tak kalah pentingnya. Ini dapat dilakukan baik oleh pemerintah maupun kelompok organisasi sipil dengan melatih literasi digital masyarakat, agar mereka bisa lebih kritis, hati-hati, dan lebih berdaya dalam berinteraksi dengan konten digital.

Pentingnya Cek Fakta

Tindakan berbagi informasi yang bertanggung jawab dan inisiatif verifikasi fakta bisa menjadi benteng melawan penyebaran disinformasi. Di Indonesia, komunitas dan media arus utama telah memberikan kesempatan bagi individu untuk memverifikasi fakta. Jurnalis juga semakin didorong untuk melakukan jurnalisme pemeriksaan fakta. Meskipun masih menghadapi kendala sumber daya dan kecepatan, setidaknya ini telah membantu meredam laju penyebaran disinformasi.

Dengan menggabungkan teknologi AI dan partisipasi masyarakat, perjuangan melawan disinformasi bisa menjadi lebih terkoordinasi dan efisien. Kolaborasi antara pengembang AI, ahli, dan pemeriksa fakta menjadi sangat penting untuk memastikan bahwa teknologi ini digunakan dengan tepat dalam melawan disinformasi. Intinya, meskipun AI sangat berpotensi menjadi alat penyebar disinformasi, teknologi ini juga mampu mendeteksi dan menangkalnya. Ini tergantung sejauh mana kita bijak

menggunakannya dan bagaimana terbangun kerja sama sinergis antara upaya meningkatkan literasi media dan keterampilan kritis masyarakat.

Tautan artikel:

https://theconversation.com/ai-dan-disinformasi-bagaimana-kecerdasan-buatan-dapat-memperparah-penyebaran-hoaks-jelang-pemilu-2024-212254

https://koran.tempo.co/read/digital/484252/bahaya-ai-di-kampanye-pemilu-2024

Apakah Teknologi AI Netral atau Sarat Nilai? Jawabannya Akan Memengaruhi Arah Kebijakan AI

Arif Perdana

Konteks: Artikel ini diterbitkan di The Conversation Indonesia tanggal 4 Agustus 2023. Artikel ini membahas perdebatan etika seputar teknologi AI, terutama mengenai netralitasnya. Ada dua perspektif: satu menganggap teknologi netral, sementara yang lain berargumen bahwa teknologi sarat nilai dan dipengaruhi oleh asumsi manusia. Dalam konteks AI, seperti penggunaan teknologi *deepfake*, dampaknya tergantung pada cara penggunaannya. Oleh karena itu, regulasi harus mencerminkan pemahaman terhadap nilai-nilai dan dampak sosial, serta memastikan penggunaan teknologi yang etis dan inklusif demi kepentingan masyarakat secara luas.

Perkembangan teknologi AI mengundang banyak perdebatan. Kontroversi yang muncul di baliknya, terutama terkait masalah etika, memunculkan urgensi regulasi dan aturan untuk mengantisipasi penyalahgunaan teknologi yang merugikan masyarakat. Ada dua perspektif yang berbeda terkait arah kebijakan AI. Perspektif pertama menyatakan bahwa teknologi itu netral. Sedangkan yang kedua berpendapat bahwa teknologi itu sarat nilai. Kedua hal tersebut merupakan bagian dari perdebatan filosofis terkait teknologi yang masih menjadi diskursus akademis hingga kini. Saat ini, kedua perspektif ini memandu para pembuat kebijakan di berbagai negara untuk mengatasi permasalahan etika, manajemen risiko dan dampak sosial dari pengunaan teknologi AI.

Netral Atau Tidak

Sejak ditemukannya roda hingga perkembangan AI saat ini, teknologi selalu berada di garis depan perubahan manusia. Dalam diskursus filsafat teknologi, masalah mengenai apakah teknologi bersifat netral telah menjadi topik perdebatan yang luas dan berkelanjutan. Netralitas adalah posisi yang bebas dari nilai atau pilihan. Apabila kita berbicara tentang teknologi yang netral, kita merujuk pada teknologi yang tidak memiliki kecenderungan atau perbedaan nilai dalam penggunaannya, baik itu untuk tujuan yang

baik maupun yang buruk. Wacana yang menganggap bahwa teknologi itu netral berangkat dari teori yang menganggap teknologi itu bebas-nilai. Argumen ini didukung oleh Andreas Spahn - Profesor Etika dan Filsafat dari *Eindhoven University of Technology*, Belanda; Joseph C. Pitt - Profesor Filsafat dari *Virginia Tech*, Amerika Serikat; dan Martin Peterson - Profesor Filsafat dari *Texas A&M University*, Amerika Serikat.

Dalam konteks teori bebas-nilai, komputer, misalnya bisa dilihat sebagai alat yang bisa digunakan untuk berbagai tujuan, baik atau buruk, tergantung pada penggunaannya. Contoh penggunaan positif, komputer dapat digunakan oleh peneliti untuk menganalisis data yang kompleks dan menemukan hal baru yang bisa meningkatkan kesejahteraan manusia. Sebaliknya, komputer juga dapat digunakan secara negatif oleh peretas untuk mencuri informasi dan melakukan kejahatan siber.

Sementara itu, kubu lainnya yang beranggapan bahwa teknologi itu tidak netral percaya bahwa teknologi itu sarat-nilai. Teori sarat-nilai menantang asumsi netralitas di atas. Para ilmuwan teori ini meyakini bahwa teknologi adalah produk dari nilai dan asumsi manusia. Argumen ini didukung oleh ilmuwan seperti Ibo van de Poel - Profesor Etika dari *Delft University of Technology*, Belanda; Peter-Paul Verbeek - Profesor Etika dan Filsafat Sains dan Teknologi dari *University of Amsterdam*, Belanda; dan Peter Kroes, Profesor Filsafat dan Teknologi dari *Delft University of Technology*, Belanda. Dalam perspektif ini, komputer, dalam desain dan fungsionalitasnya, sudah mengandung nilai dan asumsi tertentu. Misalnya, antarmuka pengguna yang user-friendly mengandung asumsi bahwa komputer harus mudah digunakan oleh semua orang. Namun, desain ini mungkin tidak mempertimbangkan kelompok-kelompok tertentu seperti orang-orang dengan disabilitas tertentu yang mungkin menemukan kesulitan dengan antarmuka tersebut. Untuk kelompok disabilitas, komputer harus dibuat dengan desain yang berbeda. Ini menunjukkan bagaimana nilai dan asumsi tertentu tersemat dalam desain teknologi, dan bagaimana hal ini dapat menciptakan inklusi dan eksklusi sosial.

Dialektika Dua Perspektif

Pandangan para ilmuwan sebenarnya tidak selalu berada pada satu titik ekstrim dari dua teori di atas, karena filsafat teknologi adalah bidang yang kompleks dan

bernuansa. Dua Profesor Filsafat Teknologi, Christian Illies dari University of Bamberg, Jerman dan Anthonie Meijers dari Eindhoven University of Technology, Belanda memiliki pandangan yang moderat terhadap teknologi. Di satu sisi, menurut mereka, teknologi adalah alat yang bisa digunakan untuk tujuan baik atau buruk. Namun di lain sisi, mereka berpendapat bahwa kita perlu menyadari implikasi moral dari teknologi agar dapat menggunakannya dengan bertanggung jawab.

Sementara itu, Langdon Winner, Profesor Teknologi dan Politik dari *Rensselaer Polytechnic Institute* di Amerika Serikat di artikelnya yang berjudul Do Artifacts Have Politics? mengungkapkan gagasannya bahwa artefak teknologi, seperti alat, mesin, dan infrastruktur, bisa membentuk hubungan sosial, struktur kekuasaan, dan proses pengambilan keputusan. Di lain pihak, Joseph C. Pitt, menekankan pentingnya mengakui nilai-nilai manusia dan bagaimana nilai-nilai tersebut memengaruhi penggunaan teknologi.

Konteks AI

Dalam konteks AI, perdebatan mengenai netralitas teknologi menjadi semakin penting. AI - yang mempunyai kemampuan untuk mempelajari pola, data-data masa lalu, dan membuat keputusan - memiliki potensi penggunaan, baik untuk tujuan positif seperti memprediksi cuaca dan membantu penelitian, maupun tujuan negatif seperti manipulasi data dan pelanggaran privasi. Contohnya, teknologi *deepfake*, media sintetis yang menggunakan AI, telah merevolusi cara kita memandang realitas di ruang digital. *Deepfake* adalah teknologi AI yang bisa memanipulasi wajah, suara, atau konten lainnya dari sumber asli dan menghasilkan visual, suara, atau konten baru yang sebenarnya palsu tapi realistis.

Teknologi ini memiliki potensi besar untuk mentransformasi industri seperti hiburan dan pendidikan secara positif. Kita bisa memodifikasi konten-konten pendidikan melalui *deepfake* dengan lebih ciamik dan komprehensif. Dalam hal ini, teknologi *deepfake*, seperti alat lainnya, tampak netral, dampaknya sepenuhnya tergantung pada bagaimana cara digunakan. Namun, kita juga bisa mengeksploitasi *deepfake* untuk menyebarkan disinformasi, memalsukan konten jahat, bahkan meniru individu tertentu

untuk kegiatan penipuan dan peretasan. Penyalahgunaan ini mencerminkan perbedaan nilai (positif dan negatif) dari mereka yang membuat dan mengendalikan teknologi tersebut, dan menimbulkan pertanyaan tentang netralitasnya. Dua sisi ini yang ditunjukkan oleh teknologi *deepfake* mendorong kita untuk menganalisis secara kritis persepsi kita tentang netralitas teknologi. Oleh karena itu, penting untuk mempertimbangkan keseimbangan ini, memahami potensi teknologi dan juga kerentanannya terhadap penyalahgunaan dari manusia.

Dampak Terhadap Kebijakan

Meski pandangan bahwa teknologi adalah bebas nilai yang bisa digunakan untuk tujuan baik atau buruk memiliki beberapa kebenaran, tapi kita tidak boleh mengabaikan fakta bahwa teknologi juga membawa nilai dan asumsi tertentu. Oleh karena itu, dalam merancang regulasi, kita perlu lebih kritis dan reflektif terhadap nilai dan asumsi yang mungkin terkandung di dalamnya. Perspektif bebas nilai dapat mengarah pada pembuatan regulasi yang berfokus pada standar teknis dan penilaian objektif untuk memastikan keadilan dan transparansi dalam sistem AI. Sebaliknya, perspektif sarat-nilai dapat mendorong regulasi yang mengatasi dampak sosial AI. Wacana ini membentuk pengembangan kerangka regulasi AI yang berusaha mendapatkan keseimbangan antara inovasi dan pertimbangan etika, serta memastikan AI melingkupi kepentingan masyarakat secara luas sambil memegang teguh nilai-nilai dan hak asasi manusia.

Penggunaan teknologi yang bertanggung jawab dan etis bukan hanya soal menggunakan teknologi untuk tujuan baik, tapi juga soal mempertanyakan dan memperjuangkan nilai dan asumsi yang adil dan inklusif dalam desain dan implementasi teknologi. Dengan cara ini, kita bisa memanfaatkan teknologi untuk kemajuan masyarakat secara umum, bukan hanya untuk kepentingan sekelompok orang atau institusi.

Tautan artikel:

https://theconversation.com/apakah-teknologi-ai-netral-atau-sarat-nilai-jawabannya-akan-memengaruhi-arah-kebijakan-ai-208870

Mengapa Menghentikan Penelitian dan Eksperimen Terkait Teknologi *ChatGPT* Bukan Solusi Jitu

Arif Perdana, Derry Wijaya

Konteks: Artikel ini diterbitkan di The Conversation Indonesia tanggal 29 May 2023. Artikel ini ditulis di saat diskursus mengenai penghentian eksperimen LLM mengemuka. Artikel ini membahas perkembangan pesat *ChatGPT* dan kekhawatiran terkait penyalahgunaan teknologi AI, seperti kecurangan akademik dan disinformasi. Future of Life Institute (FLI) mengusulkan penghentian penelitian AI, tetapi penulis berargumen bahwa regulasi yang inovatif dan responsif lebih penting daripada pelarangan. Pentingnya regulasi ini tercermin dalam upaya negara-negara untuk mengatur penggunaan AI secara efektif. Selain itu, perusahaan pengembang AI diharapkan menerapkan prinsip antisipatif dan inklusif untuk memitigasi risiko dan memaksimalkan manfaat teknologi bagi masyarakat.

Hanya dalam waktu dua bulan sejak diluncurkan pada November 2022, *ChatGPT* mengakumulasi jumlah pengguna dari hanya 1 juta menjadi 100 juta pada Januari 2023. Dengan *ChatGPT*, manusia seakan memiliki senjata baru yang memudahkan hidup mereka, mulai dari bikin resume pekerjaan, bikin laporan, atau bahkan proposal. Semua bisa dilakukan dengan hanya memberikan intruksi di kolom perintah di aplikasi tersebut.

ChatGPT merupakan aplikasi terbaru menggunakan teknologi AI yang memungkinkan pengguna dapat berinteraksi dan melakukan permintaan (prompt engineering) untuk kemudian diwujudkan oleh teknologi. Namun banyak kekhawatiran muncul di balik penggunaan teknologi ini. Ada kasus penyalahgunaan *ChatGPT* untuk praktik yang tidak berintegritas di kalangan akademikus, dan kecurangan di kalangan mahasiswa. *ChatGPT* juga bisa memfasilitasi aktivitas penipuan, penyebaran disinformasi, dan peretasan dan berbagai kejahatan siber lainnya.

Berbagai kontroversi yang muncul dari pemanfaatan teknologi *ChatGPT* mendorong *Future of Life Institute* (FLI) menerbitkan surat terbuka penghentian sementara riset-riset yang bertujuan untuk meningkatkan kemampuan GPT-4 selama enam bulan. *Generative Pre-trained Transformer* (GPT) adalah teknologi inti dari aplikasi *ChatGPT*. Sebagai teknologi inti, GPT terus diteliti dan berkembang, saat tulisan ini dibuat

ChatGPT versi gratis masih menggunakan GPT-3.5. Sedangkan *ChatGPT* versi berbayar sudah menggunakan GPT-4. Teknologi GPT-4, yang dirilis Maret lalu, bisa membaca, menganalisis dan menghasilkan teks hingga 25.000 kata dan menghasilkan kode-kode pemrograman dari berbagai bahasa pemrograman. GPT-4 ini diperkirakan memiliki 1 triliun parameter, lebih banyak dari GPT-3 yang hanya memiliki 175 miliar parameter.

FLI, yang mengeluarkan surat terbuka tersebut, merupakan organisasi nirlaba yang didirikan pada 2014, dan bertujuan untuk memitigasi risiko penggunaan teknologi AI. Pendapat yang disuarakan oleh organisasi ini cepat tersebar luas ke publik karenakan banyak nama besar akademikus dan praktisi teknologi dan inovasi yang ada di dalamnya, seperti Max Tegmark dari *Massachusetts Institute of Technology* (MIT), Amerika Serikat dan Elon Musk. Per 23 Mei 2023, sudah ada 27.565 orang yang menandatangani surat yang ditulis oleh FLI tersebut[91]. Sejumlah nama besar seperti Elon Musk, Steve Wozniak, Andrew Yang, dan Yuval Noah Harari sudah ikut serta menandatangani surat tersebut. Namun, berdasarkan pengamatan kami yang meneliti mengenai inovasi AI yang bertanggung jawab serta pemrosesan bahasa dengan AI selama lebih dari lima tahun, menghentikan penelitian dan eksperimen AI bukan merupakan solusi jitu. Kami melihat pentingnya justru regulasi yang lebih tegas dan inovatif di sektor ini.

Pentingnya Regulasi yang Inovatif

Sejarah menunjukkan bahwa regulasi selalu lebih lambat dari inovasi. Pelarangan penggunaan model GPT juga belum tentu menyelesaikan masalah. Penghentian eksperimen seperti yang diminta FLI dapat berdampak pada terhambatnya penelitian-penelitian yang bertujuan memperbaiki model GPT. Misalnya saja penelitian untuk mengurangi bias dan "halusinasi" di *ChatGPT*. Kemudian penelitian mengenai kerentanan manipulasi dan kesalahan informasi yang ada dalam *ChatGPT*. Lalu penelitian untuk meningkatkan transparansi dan akuntabilitas dari jawaban-jawaban *ChatGPT*, dan juga penelitian mengenai penyalahgunaan *ChatGPT* dalam penyebaran misinformasi

[91] https://futureoflife.org/open-letter/pause-giant-ai-experiments/

CEO *OpenAI* Sam Altman, yang mengembangkan *ChatGPT*, bahkan menyarankan alih-alih menghentikan penelitian, kita sebenarnya memerlukan regulasi yang jelas untuk teknologi AI. Otoritas yang berkepentingan terhadap mitigasi risiko AI, termasuk pemerintah harus lincah dan tanggap dengan inovasi. Pada Maret 2022 Cina sudah mengeluarkan UU tentang aplikasi AI. Cina juga sudah memiliki UU tentang pengelolaan rekomendasi algoritma yang disahkan Maret 2023 lalu. Pada April 2023, Cina mengusulkan draf pengaturan generative AI. Saat ini, Uni Eropa sudah memiliki draf UU AI dan berencana merevisi draf tersebut terkait penggunaan generative AI. Negara-negara lainnya juga sudah melangkah maju. Brasil, Kanada, dan India misalnya, sudah memiliki draf dan kertas kerja yang diarahkan untuk mengatur inovasi AI.

Tanggung Jawab Korporasi

Di lain pihak, organisasi atau korporasi yang mengembangkan AI juga harus melakukan inovasi dengan hati-hati dan mempertimbangkan prinsip antisipatif, reflektif, inklusif, dan responsif. Antisipatif berkaitan dengan analisis yang melibatkan pemikiran sistematis mengenai dampak yang mungkin saja terjadi. Namun pada saat yang bersamaan juga mempertimbangkan peluang dan dampak positif dari inovasi yang dilakukan. Institusi yang mengembangkan AI harus juga reflektif. Artinya inovasi mereka dibatasi oleh nilai-nilai sosial, tanggung jawab moral, dan hukum. Prinsip inklusif seharusnya diterapkan agar inovasi direncanakan dengan matang, baik dari sisi teknis, maupun regulasi. Desain teknologi harus mempertimbangkan manfaat dan risiko serta disesuaikan dengan kepentingan berbagai kelompok masyarakat.

Berbagai pihak yang terlibat dalam inovasi dan regulasi AI harus responsif jika terjadi dampak yang tidak diharapkan. Inovasi harus diarahkan untuk membawa dampak sebesar-besarnya bagi publik dan memitigasi risikonya. Pengembangan AI harus dilakukan secara transparan dan memiliki tata kelola data yang baik. Antisipasi dan mitigasi potensi risiko harus diformulasikan dengan seksama. Praktik yang bertanggung-jawab harus dilakukan di setiap aspek pengembangan AI (pengumpulan data, penganalisisan data, pengembangan model, dan evaluasi dan interpretasi data).

Kehadiran GPT merupakan momen penting yang menyadarkan banyak pihak bahwa etika dan regulasi AI menjadi sangat penting.

Tautan artikel:

https://theconversation.com/mengapa-menghentikan-penelitian-dan-eksperimen-terkait-teknologi-chatgpt-bukan-solusi-jitu-203847

AI dan Diskriminasi Digital

Arif Perdana, W. Eric Lee

Konteks: Artikel ini diterbitkan di majalah online Strategic Finance, 1 Desember 2022. Majalah ini dikelola oleh Ikatan Akuntan Manajemen. Artikel ini mendapatkan *Lybrand Award* tahun 2023 karena dianggap memberikan kontribusi pemikiran bagi akuntansi manajemen. Artikel ini saya tulis dengan rekan dari the University of Northern Iowa berkaitan dengan bisa yang bisa saja terjadi di sistem terotomasi di keuangan dan akuntansi. Di artikel ini dibahas mengenai bagaimana bias bisa terjadi dan bagaimana mitigasi yang bisa dilakukan, serta bagaimana peran akuntan untuk meminimalkan terjadinya bias.

Meskipun pengambilan keputusan otomatis dengan algoritma AI berfungsi sebagai katalis untuk efisiensi, hal ini juga dapat memiliki konsekuensi yang berpotensi berbahaya. Algoritma pengambilan keputusan ini, yang biasanya dipandang tidak berbahaya dan netral, dapat menyebabkan dan bahkan mengamplifikasi bias, menciptakan atau melanggengkan ketidaksetaraan struktural dalam masyarakat.

Fenomena diskriminasi digital akibat bias AI telah menjadi kasus. Satu studi yang diterbitkan oleh Departemen Perdagangan AS menemukan bahwa orang kulit berwarna lebih mungkin terkena salah diidentifikasi oleh teknologi pengenalan wajah berbasis AI alih-alih orang kulit putih[92]. Faktanya, daftar kasus yang melibatkan bias AI terus bertambah selama beberapa tahun terakhir, meluas ke proses yang semakin kompleks, dengan konsekuensi yang serius[93].

Misalnya, di kepolisian, telah terjadi banyak penangkapan yang salah akibat kesalahan identifikasi oleh perangkat lunak pengenalan wajah[94]. Di pelayanan kesehatan, algoritma AI yang seharusnya mengidentifikasi pasien sakit kronis berisiko tinggi dan menyarankan mereka untuk melakukan konsultansi tambahan, ternyata lebih mengutamakan pasien kulit putih alih-alih pasien kulit hitam[95]. Penggunaan biaya sebagai proksi dalam algoritma, sering kali menyebabkan bias rasial karena perbedaan

[92] https://www.pwc.com/us/en/tech-effect/ai-analytics/algorithmic-bias-and-trust-in-ai.html
[93] https://www.nist.gov/news-events/news/2022/03/theres-more-ai-bias-biased-data-nist-report-highlights
[94] https://www.technologyreview.com/2021/04/14/1022676/robert-williams-facial-recognition-lawsuit-aclu-detroit-police/
[95] https://www.nature.com/articles/d41586-019-03228-6

inheren dalam kebutuhan perawatan kesehatan antara orang kulit hitam dan putih, bahkan ketika kedua kelompok menghabiskan jumlah yang sebanding[96].

Bukti-bukti empiris ini menggambarkan bias yang tidak disengaja yang bisa dihasilkan dari sistem pengambilan keputusan otomatis yang umum digunakan di berbagai bidang seperti pemasaran, asuransi, perawatan kesehatan, hukum, dan keuangan. Namun, dengan pendekatan multidisiplin dan upaya terkoordinasi, ada solusi untuk mengurangi bias semacam itu, upaya ini sebenarnya dapat dikontribusikan oleh akuntan manajemen dan profesional keuangan lainnya.

Kisah Peringatan Dari Satu Perusahaan

Pada tahun 2016, *Microsoft* mengembangkan aplikasi AI chatbot bernama Tay yang dapat melayani percakapan tertulis secara *real-time*[97]. Tay dikembangkan menyusul kesuksesan sebelumnya dari *Xiaoice*, yang telah diproduksi di Cina pada tahun 2014 dan dipuji sebagai perangkat komputasi "emosional" karena kemampuannya menulis puisi, menggubah lagu, dan bahkan menjadi mitra percakapan virtual, memperoleh jutaan pengikut di *Weibo* dan *WeChat*[98].

Awalnya, *Tay* menerima respons yang sangat positif dari pengguna *Twitter*, berinteraksi dengan mereka lebih dari 100.000 kali dalam periode 24 jam. Namun, Tay dengan cepat berubah dari ramah dan toleran menjadi rasis dan seksis. Sehari kemudian, menyusul kecaman publik atas perilaku *Tay*, *Microsoft* menghapusnya dari *Twitter*. Hal ini mengejutkan banyak orang, karena *Tay* dan *Xiaoice* sering dianggap sebagai kembar. Keduanya berasal dari Microsoft dan menggunakan teknologi yang sama. Jadi bagaimana mereka bisa berperilaku sangat berbeda?

Untuk memahami perbedaan ini, perlu diketahui peran penting yang dimainkan oleh data dalam lingkup AI. *Xiaoice* sebagian besar terpapar pada pengguna dalam satu negara yang berasal dari platform *Weibo* dan *WeChat*. Sebaliknya, ketika *Tay* awalnya diluncurkan di *Twitter*, ia berinteraksi dengan kelompok pengguna yang sangat beragam

[96] https://www.scientificamerican.com/article/racial-bias-found-in-a-major-health-care-risk-algorithm/
[97] https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist
[98] https://www.antaranews.com/berita/510353/pemuda-tiongkok-keranjingan-xiaoice-chatbot-seperti-di-film-her

dari seluruh dunia, dengan interaksi yang sangat dinamis bahkan menjadi percakapan yang tidak sopan. Konsekuensinya, Tay belajar dari data yang diterimanya dalam lingkungan seperti itu, kemudian meniru dan membuat pernyataan ekstrem yang serupa.

Peningkatan Bias Dalam Platform AI

Dalam beberapa hal, pengembang AI seperti orang tua yang perlu menyediakan lingkungan yang sesuai agar anak-anak mereka berkembang. Sementara anak-anak sering memiliki bias yang diturunkan dari orang tua mereka, mereka juga dapat belajar dari berbagai bias sosial yang berlaku di lingkungan mereka. AI juga tidak kebal dari bias. Data yang digunakan oleh pengembang AI dapat mengandung banyak bias implisit, baik karena bias sosial yang ada mempengaruhi pengembangan algoritma atau karena bias yang tertanam dalam data pelatihan.

Sistem otomatis yang digunakan Amazon untuk merekrut karyawan baru, misalnya, telah terbukti menunjukkan bias algoritmik dan data. Sistem penyaringan otomatis diajarkan untuk mengenali pola kata yang berkaitan dengan keterampilan yang relevan dalam aplikasi pekerjaan. Selain itu, karena sistem tersebut dilatih dengan data terutama dari kumpulan pelamar yang sebagian besar laki-laki selama 10 tahun terakhir, perangkat tersebut secara tidak sengaja lebih menyukai resume dari pria alih-alih wanita.

Contoh lain dari sistem pengambilan keputusan otomatis yang cenderung bias adalah *Correctional Offender Management Profiling for Alternative Sanctions (COMPAS),* yaitu alat yang digunakan di beberapa pengadilan di AS untuk menilai kemungkinan seorang terdakwa menjadi residivis. Aplikasi ini mengumpulkan informasi terkait pelanggaran sebelumnya, pendidikan, dan riwayat pekerjaan terdakwa. Meskipun aplikasi tersebut tidak mengumpulkan data tentang ras, organisasi jurnalisme investigatif *ProPublica* menemukan bahwa orang kulit hitam "hampir dua kali lebih mungkin daripada orang kulit putih untuk dilabeli berisiko lebih tinggi tetapi sebenarnya tidak melakukan pelanggaran lagi," sementara orang kulit putih lebih mungkin dilabeli berisiko lebih rendah untuk melakukan pelanggaran lagi tetapi kemudian melakukan kejahatan lain[99].

[99] https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Tantangan Etis

Ada dilema yang muncul karena bias dalam pengambilan keputusan otomatis. Bias yang mengakibatkan diskriminasi bisa bermanfaat dan berbahaya. Misalnya, ketika AI digunakan di akuntansi dan audit, kemampuan diskriminatifnya bisa bermanfaat membantu mendeteksi atau memprediksi aktivitas yang berpotensi curang. Lembaga keuangan juga dapat menggunakan teknik pengambilan keputusan otomatis untuk mengelola risiko mereka dengan lebih baik ketika mempertimbangkan apakah akan memberikan kredit kepada pelanggan potensial atau pelanggan yang sudah eksis. Secara efektif, dengan menggunakan AI dalam penilaian kredit, lembaga keuangan dapat menentukan potensi risiko gagal bayar seseorang. Demikian pula, di industri crowdlending, AI digunakan untuk memberikan skor pada proyek potensial, sehingga memungkinkan pemberi pinjaman memilih proyek yang sesuai dengan profil dan selera risiko yang mereka inginkan.

Meskipun aplikasi-aplikasi ini memiliki keuntungan untuk meminimalkan risiko, bias juga berpotensi terjadi. Sebuah studi dari *University of California, Berkeley* menemukan bahwa baik pemberi pinjaman online maupun konvensional membebankan bunga yang jauh lebih tinggi kepada peminjam dengan latar belakang Afrika Amerika dan Latino. Industri keuangan meraih keuntungan 11% hingga 17% lebih tinggi untuk kelompok ini dibandingkan dengan kelompok peminjam lainnya[100]. Studi lain dari *Stanford University* menunjukkan bahwa ada perbedaan antara kelompok minoritas yang berpenghasilan rendah dengan kelompok lainnya berkaitan dengan tingkat persetujuan pinjaman hipotek mereka. Ini disebabkan oleh kelompok minoritas dan berpenghasilan rendah memiliki informasi riwayat kredit yang minimal[101].

Dalam situasi tertentu, bias dapat lebih jauh menimbulkan tantangan etis, terkadang dengan konsekuensi yang mengerikan, ketika AI mendiskriminasi berdasarkan data yang terkait dengan etnis, ras, agama, dan/atau gender yang ada di data. Menghapus variabel-variabel yang berkorelasi ini tidak serta merta menyelesaikan bias. Ini karena variabel lain yang tampaknya tidak terkait juga dapat secara tidak langsung

[100] https://newsroom.haas.berkeley.edu/minority-homebuyers-face-widespread-statistical-lending-discrimination-study-finds/
[101] https://law.stanford.edu/wp-content/uploads/2023/06/SSRN-id3491267.pdf

berfungsi sebagai proksi. Misalnya, meskipun *COMPAS* tidak mengumpulkan data terkait ras, latar belakang pendidikan dan alamat terdakwa dapat menghasilkan bias ketika diagregasi dan digunakan sebagai data pelatihan. Di US, misalnya, beberapa wilayah tertentu lebih banyak dihuni oleh orang kulit hitam alih-alih kulit putih. Pendidikan orang kulit hitam juga memiliki pola yang berbeda dengan orang kulit hitam. Oleh karena itu, pendidikan dan alamat terdakwa ini memiliki korelasi dengan ras terdakwa.

Kasus-kasus serupa tentang bias juga terjadi di *Apple Card* dan sejumlah perusahaan asuransi, termasuk *Allstate*, *GEICO*, dan *Liberty Mutual*. Gugatan diajukan terhadap perusahaan-perusahaan ini atas dugaan diskriminasi dalam proses pengambilan keputusan otomatis mereka. Algoritma mereka dicurigai secara sistematis mendiskriminasi kelompok gender dan minoritas tertentu—meskipun perusahaan-perusahaan ini mematuhi peraturan yang berlaku dan karenanya tidak mengumpulkan data terkait gender, status perkawinan, dan ras. Di Oregon, misalnya, wanita membayar lebih mahal untuk asuransi mobil dasar dengan rata-rata $100 (atau sekitar 11,4% lebih banyak) dibandingkan pria[102].

Mempromosikan Praktik AI yang Bertanggung Jawab

Bagi individu, bisnis, dan komunitas, pengambilan keputusan AI otomatis, jika tidak dikelola dengan baik, pada akhirnya dapat menyebabkan diskriminasi, kehilangan peluang, dan kerugian ekonomi. Selain itu, karena perusahaan semakin banyak menggunakan AI untuk analisis kecurangan, klaim asuransi, dan kelayakan pembayaran, bias berpotensi muncul.

Secara keseluruhan, organisasi harus tetap waspada dalam menggunakan AI dan mengimplementasikan pengambilan keputusan otomatis yang bertanggung jawab. Ini termasuk menerapkan tindakan pencegahan yang bertujuan untuk meminimalkan potensi risiko bias serta langkah-langkah korektif dan kompensasi ketika terjadi kesalahan. Dalam hal ini, organisasi akan bijaksana untuk mempertimbangkan adopsi strategi mitigasi risiko yang akan mengarah pada praktik AI yang bertanggung jawab

[102] https://consumerfed.org/press_release/oregon-women-charged-100-more-than-men-for-basic-auto-insurance-drivers-with-poor-credit-scores-see-rates-double-according-to-new-research/

(lihat Tabel 8). Strategi-strategi ini termasuk dalam kategori tata kelola dan kurasi data, tinjauan siklus hidup pengembangan sistem, kebijakan dan peraturan, serta interaksi manusia-algoritmik. Mari kita lihat lebih dekat masing-masing strategi ini. Tabel 11 menunjukkan beberapa dampak negatif dari bias AI. Table 12 memberikan paparan lebih detil mengenai strategi mitigasi risiko.

Tabel 11. Diskriminasi digital dan strategi mitigasi risiko

Efek Negatif dari Diskriminasi Digital
Kehilangan kesempatan
Kehilangan kebebasan
Kerugian ekonomi
Strategi Mitigasi Risiko
Tata kelola dan kurasi data
Tinjauan siklus hidup sistem
Kebijakan dan regulasi
Interaksi manusia-algoritma

Tabel 12. Strategi mitigasi risiko bias AI

Strategi Mitigasi Risiko	**Ringkasan**
Tata Kelola Dan Kurasi Data	Tata kelola data mencakup pengumpulan, penyimpanan, akses, dan pemrosesan data yang relevan dan berkualitas tinggi. Penting untuk menangani bias dalam data, terutama bagi kelompok minoritas, serta mematuhi regulasi perlindungan data pribadi.
Tinjauan Siklus Hidup Pengembangan Sistem	Sistem pengambilan keputusan otomatis melalui fase konsep hingga penghentian. Alat seperti LIME dan SHAP digunakan untuk meningkatkan transparansi, interpretabilitas, dan akuntabilitas, dengan fokus pada pengurangan bias dalam pengambilan keputusan otomatis.
Kebijakan Dan Peraturan	Regulasi diperlukan untuk melindungi data pribadi dan memastikan sistem AI mengikuti standar etika, seperti yang ditetapkan oleh Singapura dan Uni Eropa. Kebijakan regulasi bertujuan mengurangi diskriminasi yang mungkin muncul dari penggunaan AI.

Strategi Mitigasi Risiko	Ringkasan
Interaksi Manusia-Algoritmik	Keputusan berbasis AI memerlukan kontrol manusia untuk menghindari bias dan kesalahan. Pendekatan "human-in-the-loop" dan "human-in-the-command" membantu memastikan bahwa AI hanya berfungsi sebagai alat bantu, bukan pengganti pengambilan keputusan manusia.

Tata Kelola dan Kurasi Data

Tata kelola data sangat penting bagi organisasi karena membantu mereka memecahkan masalah "mil pertama" dan "mil terakhir" data[103]. Masalah "mil pertama" berkaitan dengan pengumpulan data. Perusahaan harus menyadari bahwa data, selain cukup dan relevan, juga harus berkualitas tinggi dan mematuhi peraturan yang mengatur perlindungan data pribadi. Masalah "mil terakhir" terjadi ketika masalah tak terduga muncul setelah pengambilan keputusan otomatis memproses data. Ketika itu terjadi, tata kelola data berperan dalam menentukan data relevan mana yang harus digunakan perusahaan untuk pengambilan keputusan otomatis, siapa yang memiliki wewenang untuk mengakses data, bagaimana data harus dibagikan, dan bagaimana data harus disimpan dalam suatu organisasi serta antar organisasi[104].

Harus ada protokol ketat mengenai bagaimana tata kelola data digunakan untuk alat pengambilan keputusan otomatis. Ini seharusnya mulai dilakukan sejak pengumpulan data. Misalnya, *American Banker* memperkirakan bahwa sekitar 14% dan 17% rumah tangga Hispanic dan Afrika Amerika di Amerika Serikat, masing-masing,

[103] https://www.predinfer.com/blog/first-middle-last-mile-problems-of-data-science/

[104] Pembersihan data melibatkan koreksi data yang salah, tidak lengkap, redundan, dan keliru serta menghilangkan potensi bias dalam suatu set data. Proses ini melibatkan penimbangan berbagai variabel dalam set data dan sering kali menghapus variabel yang tidak penting atau yang tidak relevan dengan analisis. Data yang bersih berarti data tersebut dapat digunakan, tidak bias, dan berkualitas tinggi (akurat, valid, lengkap, dan relevan). Namun, pembersihan data bukanlah hal yang mudah. Berikut beberapa tips:

- Lakukan higienitas data. Ini mencakup menjalankan pemeriksaan ejaan; menghapus variabel atau baris duplikat, serta spasi ekstra; memperbaiki angka dan tanda; serta memformat dengan jelas.
- Periksa data secara memadai sebelum membuang satu atau lebih variabel.
- Berhati-hatilah saat mengecualikan variabel yang tampaknya tidak penting karena analisis dapat menghasilkan model yang bias. Misalnya, jika kelompok usia tertentu (misalnya 60 tahun ke atas) menyusun 10% dari set data, sedangkan sisanya mencakup mereka yang berusia di bawah 60 tahun, model akan cenderung lebih memihak pada kelompok usia yang lebih muda ini.
- Pastikan tipe data konsisten dalam hal tanggal, string, float, dan data integer.
- Bergantung pada tujuan analisis, tangani data yang hilang dengan mengisinya atau menghapus variabel tertentu dari set data.
- Gunakan teknik yang tepat untuk menangani data yang tidak seimbang (misalnya, dengan melakukan resampling pada set data pelatihan).

kekurangan akses ke perbankan yang terjangkau. Masalah ini diperparah oleh fakta bahwa banyak rumah tangga minoritas ini tidak memiliki ID foto yang dikeluarkan pemerintah, sehingga sering kali menyebabkan data yang salah ditafsirkan atau hilang. Dengan demikian, organisasi perlu berhati-hati ketika berurusan dengan algoritma yang digunakan untuk memproses data yang salah, tidak lengkap atau data minoritas. Setidaknya, hasil pengambilan keputusan otomatis harus dievaluasi dengan hati-hati untuk menyaring kasus-kasus bias yang mungkin terjadi.

Meskipun model dan data berkontribusi pada munculnya bias di AI, pengembang AI harus terlebih dahulu melihat data alih-alih mencoba mengubah kode ketika model berperilaku dengan cara yang tidak terduga. Pengembang AI harus mempertimbangkan dengan hati-hati apakah penggunaan proksi atau variabel terkait lainnya dapat menyebabkan hasil yang bias. Dari sudut pandang etis, bias bisa menjadi bermasalah dan tidak adil ketika keputusan dilakukan berdasarkan etnis, ras, agama, dan/atau gender.

Sebagai alternatif, pengembang AI dapat mempertimbangkan untuk menggunakan proksi perilaku. Misalnya, di Cina, perusahaan seperti *Lenddo* dan *Yongqianbao* menggunakan daya tahan baterai *smartphone* sebagai salah satu variabel untuk menentukan skor kredit pelanggan. Ini dilakukan dengan pemikiran bahwa individu yang secara teratur mengisi daya *smartphone* cenderung memiliki perilaku yang positif yang terencana dan diasumsikan memiliki risiko kredit yang rendah. Variabel lain, seperti riwayat browsing, waktu yang dihabiskan di media sosial, dan jumlah hari yang dibutuhkan untuk membayar tagihan, juga bisa digunakan sebagai proksi perilaku.

Tentu saja, menggunakan data pelanggan untuk analisis prediktif dapat memiliki konsekuensi negatif jika tidak ada tata kelola data yang baik. Kebijakan tata kelola data yang efektif dapat membantu memitigasi risiko finansial dan reputasi yang disebabkan oleh pelanggaran data. Di sini akuntan manajemen bisa memainkan peran kunci untuk membantu perusahaan lebih baik dalam mengumpulkan, menyimpan, dan mengelola data mereka. Mengintegrasikan etika data ke dalam budaya perusahaan dapat membantu menjaga sensitivitas dan transparansi data, sehingga mengarah pada peningkatan kepatuhan regulasi dan mitigasi risiko terkait penggunaan data.

Tinjauan Siklus Hidup Pengembangan Sistem

Masalah juga dapat terjadi di siklus pengembangan sistem pengambilan keputusan otomatis. Fase ini meliputi konsep, desain, pengembangan, pengujian, operasi, dan penghentian. Untuk menyelesaikan masalah ini, tersedia beberapa alat, termasuk *AI Fairness 360*[105], *Local Interpretable Model-Agnostic Explanations* (LIME)[106], dan *SHapley Additive exPlanations* (SHAP)[107]. LIME dan SHAP dapat membantu organisasi untuk lebih memahami bagaimana sistem pengambilan keputusan otomatis menghasilkan hasil mereka[108]. Penelitian terbaru juga menunjukkan bagaimana perangkat ini dapat membantu auditor meningkatkan transparansi, interpretabilitas, dan akuntabilitas penggunaan AI dalam tugas audit[109].

Selain desain algoritmik yang tepat untuk mengurangi bias, pengembang AI juga harus menjelaskan dampak dari bias yang dihasilkan. Misalnya, jika pengambilan keputusan otomatis digunakan untuk menilai kumpulan populasi yang beragam, ini terkadang dapat memperbesar bias yang ada karena kurangnya data latih dari kumpulan minoritas (di AS misalnya, ini terjadi pada orang Hispanik dan Afrika Amerika). Dalam kasus seperti itu, memberikan penjelasan yang tepat mengenai keadaan data akan membantu meningkatkan akuntabilitas, transparansi, dan interpretabilitas sistem pengambilan keputusan otomatis yang akan dikembangkan. Penjelasan ini mungkin mencakup alasan untuk membuat alat pengambilan keputusan otomatis, apakah pengembang telah mempertimbangkan bias yang mungkin terjadi karena data atau algoritma, dan bagaimana pemangku kepentingan dapat lebih terlibat dalam proses desain dan pengembangan algoritmik.

Meskipun transparansi dan akuntabilitas adalah pertahanan utama ketika keputusan terkait otomatisasi yang bermasalah dibawa ke pengadilan, perusahaan yang

[105] https://aif360.res.ibm.com/

[106] https://interpret.ml/docs/lime.html

[107] https://shap.readthedocs.io/en/latest/

[108] Dalam Local Interpretable Model-Agnostic Explanations dan SHapley Additive exPlanations toolkit—dikenal sebagai LIME dan SHAP, masing-masing—model keputusan otomatis yang telah dilatih digunakan sebagai input untuk analisis statistik post hoc. Metode ini kemudian digunakan untuk mengembangkan logika keputusan yang menjelaskan bagaimana model yang digunakan dalam pengambilan keputusan otomatis mencapai keputusannya. Dengan menggunakan LIME, analis dapat menjelaskan satu prediksi (misalnya, bahwa kemungkinan gagal bayar pinjaman lebih kecil ketika tingkat pendidikan dan/atau pendapatan tahunan seseorang lebih tinggi). Sebaliknya, SHAP menjelaskan perilaku keseluruhan model: misalnya, efek variabel independen (fitur) pada variabel dependen (target), seperti dalam situasi di mana pendapatan tahunan yang tinggi menurunkan kemungkinan gagal bayar.

[109] https://www.sciencedirect.com/science/article/abs/pii/S1467089522000240

mengembangkan alat pengambilan keputusan otomatis sering kali enggan terlibat dalam transparansi publik. Mereka beralsan karena melakukannya akan memungkinkan pesaing mereka mencuri algoritma mereka. Namun, upaya bersama untuk memberlakukan peraturan yang seragam menuju transparansi publik akan membuat masyarakat lebih percaya dengan penggunaan sistem berbasis AI.

Kebijakan dan Peraturan

Ternyata penggunaan pengambilan keputusan otomatis dalam menetapkan premi asuransi mobil terkadang dapat mengakibatkan individu berisiko lebih rendah membayar premi yang lebih tinggi. Karena banyak kasus diskriminasi gender terkait penetapan premi berbasis AI di masa lalu, negara bagian AS seperti Washington dan Oregon telah melarang penggunaan skor kredit dalam menetapkan premi asuransi.

Dilema semacam ini menyoroti perlunya pemerintah memainkan peran penting dalam mengatur pengambilan keputusan otomatis berbasis AI. Peraturan mengenai pelindungan data pribadi adalah elemen kunci menuju penetapan pedoman etis untuk AI. Misalnya, di Singapura, model *Artificial Intelligence Governance Framework* memberikan panduan di bidang struktur dan langkah-langkah tata kelola internal, tingkat keterlibatan manusia dalam keputusan berbasis AI, dan manajemen operasional, serta menangani masalah mengenai interaksi dan komunikasi pemangku kepentingan[110]. Demikian pula, Uni Eropa telah merilis beberapa arahan privasi, seperti GDPR dan *Ethics Guidelines for Trustworthy AI*. Menurut pedoman UE, AI harus mematuhi peraturan dan hukum yang berlaku, secara etis dan moral baik, dan secara teknis kuat. Selain itu, alat pengambilan keputusan otomatis harus diaudit secara teratur untuk memastikan bahwa bias apa pun yang disebabkan oleh algoritma atau data dapat dikurangi.

Berkaitan dengan pelindungan data, seorang akuntan dapat bertindak sebagai pengontrol atau pemroses. Pengontrol menentukan “tujuan dan cara” pemrosesan data pribadi. Ketika memproses data, akuntan dapat membantu organisasi memutuskan mengapa data tertentu harus atau tidak boleh diproses, jenis data apa yang harus

[110] https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework

dimasukkan dalam analisis, dan durasi pemrosesan dan penyimpanan data. Dengan demikian, akuntan dapat membantu memastikan bahwa data sesuai, pengumpulan dan pemrosesan data etis, dan sistem pengambilan keputusan otomatis pada akhirnya menghasilkan hasil yang lebih transparan.

Misalnya, akuntan memainkan peran penting dalam mengembangkan sistem informasi seperti sistem perencanaan sumber daya perusahaan untuk membantu memastikan bahwa mereka sesuai dengan proses bisnis perusahaan mereka dan menghasilkan output yang relevan untuk pengambilan keputusan. Dengan munculnya AI dan ilmu data, peran ini harus diperluas untuk mencakup evaluasi algoritmik. Akuntan juga dapat membantu menjelaskan hasil LIME dan SHAP dengan lebih jelas untuk memungkinkan pemahaman yang lebih baik tentang cara kerja internal AI dan mendokumentasikannya untuk pemangku kepentingan internal dan eksternal.

Interaksi Manusia-Algoritmik

AI tidak bisa dan tidak boleh secara sepihak membuat keputusan untuk manusia. AI tidak memiliki kehendak dan niat. Oleh karena itu, AI hanyalah alat untuk membantu menghasilkan informasi. Di sisi lain, manusia membuat keputusan dan bertanggung jawab atas konsekuensinya. Dengan justifikasi, keputusan manusia dapat dipertanyakan dan ditolak atas nama menghormati aturan hukum.

Meskipun AI mampu sepenuhnya otomatis, penilaian manusia tetap kritis. Alat pengambilan keputusan otomatis, misalnya, dapat menghubungkan gender seseorang dengan risiko. Namun, ini tidak boleh digeneralisasi dan karenanya harus dievaluasi kasus per kasus. Hal ini konsisten dengan pedoman etika AI di Singapura dan UE[111].

[111] Pada tahun 2020, pemerintah Singapura merilis edisi kedua dari Kerangka Tata Kelola Kecerdasan Buatan Model, yang memberikan panduan rinci kepada perusahaan sektor swasta tentang bagaimana menangani masalah etika dan tata kelola utama dalam penerapan solusi AI. Dengan mendorong pemahaman dan kepercayaan publik terhadap teknologi, kerangka ini menjelaskan bagaimana sistem AI bekerja, memastikan penggunaan data yang bertanggung jawab, serta menciptakan komunikasi yang terbuka dan transparan. Prinsip utama dalam kerangka ini adalah bahwa sistem AI harus menempatkan manusia di posisi pertama, dapat dijelaskan dan dipahami, serta membuat keputusan yang adil.

Komisi Eropa menerbitkan Pedoman Etika untuk AI yang Dapat Dipercaya pada April 2019. Mereka menyatakan bahwa AI yang dapat dipercaya harus mematuhi semua hukum dan peraturan yang berlaku, beretika, serta secara teknis dan sosial dapat diandalkan. Pedoman ini juga menetapkan sejumlah persyaratan yang harus dipenuhi oleh sistem AI agar dianggap dapat dipercaya. Misalnya, AI harus mempromosikan hak asasi manusia yang mendasar dan memungkinkan pengambilan keputusan yang didasarkan pada informasi. Sistem AI tidak hanya harus tangguh dan aman, tetapi juga memerlukan partisipasi manusia, seperti pendekatan "human-in-the-loop" dan "human-in-command".

Keduanya telah menekankan perlunya manusia untuk mengawasi dan mengendalikan pengambilan keputusan berbasis AI, menggunakan kombinasi pendekatan *human-in-the-loop* dan *human-in-the-command* [112] . Singkatnya, dengan kontrol, evaluasi dan keseimbangan yang baik, sistem yang menggabungkan interaksi antara manusia dan algoritma akan membantu mengurangi keputusan yang bias dan berbahaya, yang bisa terjadi jika hanya bergantung pada keputusan otomatis atau hanya manusia.

Secara keseluruhan, mengurangi potensi risiko yang ditimbulkan oleh pengambilan keputusan otomatis tetap menjadi tantangan yang berkelanjutan. Akuntan dapat menghadapi tantangan itu secara langsung dengan memanfaatkan keahlian penatalayanan dan penciptaan nilai mereka. Dengan keterampilan mereka dalam manajemen data, akuntan dapat memperluas kontribusi mereka untuk meminimalkan risiko saat menggunakan sistem pengambilan keputusan otomatis untuk mengubah data menjadi informasi, sehingga membantu menciptakan lingkungan AI yang lebih bertanggung jawab dalam organisasi mereka. Dan, akhirnya, salah satu hal terbaik yang dapat dilakukan oleh akuntan manajemen adalah mengajukan pertanyaan kepada pengembang AI mengenai sumber potensi bias dan bagaimana mencegahnya agar tidak pernah menjadi masalah.

Tautan artikel:

https://www.sfmagazine.com/articles/2022/december/ai-and-digital-discrimination

Mereka juga mencatat bahwa keselamatan, keandalan, keterulangan, akurasi, dan rencana kontingensi adalah hal penting dalam AI. Dengan cara ini, kerusakan yang tidak diinginkan juga dapat diminimalkan dan dicegah. Selain itu, semua data harus berkualitas tinggi dan ditangani dengan integritas, akses yang sah, serta privasi.

[112] Human-in-the-loop (HITL) mengacu pada sistem yang melibatkan manusia dalam proses pengambilan keputusn. Hal ini memastikan bahwa intervensi manusia diperlukan untuk meningkatkan akurasi dan hasil. Sedangkan, human-in-command (HIC) menekankan peran manusia sebagai pengendali utama dalam sistem otomatis. Manusia berperdan memberikan arahan dan kontrol terhadap tindakan mesin atau algoritma.

BAB 4: Transformasi Ekonomi Melalui Inovasi Digital

Transformasi ekonomi melalui inovasi digital sedang berlangsung dengan kecepatan yang belum pernah terjadi sebelumnya, mengubah lanskap bisnis dan keuangan secara global. Di garis depan revolusi ini adalah AI dan *fintech*, yang menawarkan peluang baru sekaligus menimbulkan tantangan yang kompleks. AI generatif, seperti GPT dan DALL-E, telah membuka cakrawala baru dalam produktivitas dan kreativitas di berbagai sektor. Kemampuannya untuk menghasilkan konten, menganalisis data, dan memecahkan masalah kompleks menjanjikan peningkatan efisiensi yang signifikan.

Namun, bersamaan dengan antusiasme ini, muncul kekhawatiran tentang kemungkinan terjadinya "gelembung AI", mengingatkan kita pada era dot-com dan kripto. Meski demikian, banyak ahli berpendapat bahwa AI memiliki fondasi yang lebih kokoh dan aplikasi praktis yang lebih luas, yang membedakannya dari tren teknologi sebelumnya. Kita juga harus ingat, kemudahan yang dibawa teknologi tentunya membawa konsekuensi.

Sementara itu, *fintech* telah merevolusi industri keuangan dengan menawarkan layanan yang lebih cepat, mudah diakses, dan inovatif. *Crowdlending*, sebagai contoh, telah membuka peluang investasi baru dan memperluas akses kredit, terutama bagi UMKM dan individu yang sebelumnya kurang terlayani oleh sistem perbankan tradisional. Namun, inovasi ini juga membawa tantangan baru dalam hal membangun kepercayaan dan mengelola risiko di lingkungan digital yang sering kali anonim dan cepat berubah. Untuk menghadapi transformasi ini, diperlukan pendekatan multidimensi yang melibatkan berbagai pemangku kepentingan. Pertama, regulasi perlu menjadi lebih adaptif dan inovatif, mampu menyeimbangkan dorongan inovasi dengan kebutuhan untuk melindungi konsumen dan stabilitas sistem keuangan. Kedua, peningkatan literasi digital dan finansial masyarakat menjadi krusial untuk memastikan bahwa manfaat dari inovasi ini dapat dirasakan secara luas dan merata.

Lebih lanjut, pengembangan infrastruktur teknologi yang kuat dan aman menjadi pondasi penting bagi pertumbuhan ekonomi digital. Ini harus dibarengi dengan fokus yang kuat pada etika dan keadilan dalam penggunaan teknologi, terutama dalam mengatasi potensi bias algoritma yang dapat memperlebar kesenjangan sosial dan ekonomi yang ada. Kolaborasi erat antara pemerintah, industri, dan akademisi juga diperlukan dalam mengembangkan solusi teknologi yang tidak hanya inovatif tetapi juga bertanggung jawab dan berkelanjutan. Dengan pendekatan yang tepat dan komprehensif, transformasi digital ini berpotensi mendorong pertumbuhan ekonomi yang inklusif, meningkatkan efisiensi di berbagai sektor, dan menciptakan peluang baru di era ekonomi digital. Namun, kunci keberhasilannya terletak pada kemampuan kita untuk mengelola transisi ini dengan bijaksana, memastikan bahwa manfaatnya dapat dirasakan secara luas sambil meminimalkan risiko dan dampak negatifnya. Dalam perjalanan menuju ekonomi digital yang lebih maju, kewaspadaan, adaptabilitas, dan komitmen terhadap inovasi yang bertanggung jawab akan menjadi faktor penentu keberhasilan.

Revolusi Keuangan Digital: Janji, Tantangan, dan Masa Depan yang Kita Pilih

Arif Perdana

Konteks: Artikel ini saya publikasikan di Kumparan tanggal 26 November 2024. Artikel ini saya tulis sebagai bahan pemaparan saya di panel diskusi *2nd International Research Forum* yang diselenggarakan oleh Otoritas Jasa Keuangan. Revolusi keuangan digital telah mengubah cara bertransaksi masyarakat, dari pedagang kaki lima hingga investor saham. Meski menawarkan kemudahan dan inklusi keuangan yang lebih luas, inovasi ini juga membawa tantangan serius. Kejahatan digital, diskriminasi algoritma, dan risiko jebakan utang menjadi sisi gelap yang perlu diwaspadai. Kelompok rentan seperti lansia juga berisiko tertinggal karena keterbatasan literasi digital. Untuk menciptakan masa depan keuangan yang lebih etis, diperlukan tiga langkah penting: penerapan desain etis dalam aplikasi, regulasi yang adaptif terhadap inovasi, dan peningkatan literasi keuangan digital. Teknologi seharusnya melayani kebutuhan manusia, bukan sebaliknya.

Saat kita menjelajahi berbagai kota dan desa di Indonesia pedagang kaki lima dan penjual pasar tradisional kini menerima pembayaran melalui QRIS (*Quick Response Code Indonesian Standard*). Di saat yang sama, aplikasi teknologi finansial (tekfin) mempermudah kita untuk menyimpan uang di *smartphone*, membeli saham, atau reksa dana. Revolusi keuangan digital telah mengubah cara kita bertransaksi: cepat, mudah, dan tanpa hambatan. Uang kini hanya menjadi angka yang berpindah dari satu layar ke layar lain, dan semakin sedikit transaksi menggunakan uang fisik.

Menurut survei Bank Dunia, 76 persen populasi global kini memiliki akses ke layanan keuangan digital. Janji utamanya adalah inklusi keuangan, mimpi di mana semua orang memiliki akses ke layanan keuangan yang sebelumnya sulit dijangkau. Tak perlu lagi antre panjang di bank. Segalanya tersedia hanya dengan beberapa sentuhan di layar ponsel Anda.

Cerita-cerita seperti ini menunjukkan bahwa dunia keuangan sedang menuju keadilan yang lebih merata. Namun, di balik gemerlap keberhasilan ini, ada sisi gelap yang jarang dibahas, namun sangat penting untuk kita pahami. Kemudahan yang kita dapati, inovasi yang kita nikmati tentunya memiliki konsekuensi.

Kita tidak perlu khawatir dengan mudharat yang dibawa teknologi, tetapi kita harus mengantisipasi dan memitigasi potensi risiko yang ada dan mungkin muncul. Dengan begitu, peradaban manusia bisa maju. Kita sudah menyaksikannya dari kereta api hingga komputer.

Biaya Tersembunyi dari Inovasi Keuangan

Transformasi digital memang membawa manfaat, tetapi juga menyisakan tantangan besar. Salah satunya adalah kejahatan keuangan digital. Menurut *Global Coalition to Fight Financial Crime*, kerugian global akibat penipuan diperkirakan mencapai USD 50 hingga 177 miliar setiap tahun. Rata-rata kerugian per korban bahkan mencapai USD 12.000. Inovasi digital membuka pintu bagi penjahat untuk memanfaatkan celah keamanan di sistem baru ini.

Selain itu, muncul fenomena diskriminasi digital. Meski belum banyak dibahas di media Indonesia, kasus ini sudah terjadi di negara lain seperti Amerika Serikat. Sebagai contoh, kartu kredit Apple Card pernah menuai kontroversi karena algoritmanya memberikan limit kredit lebih rendah kepada perempuan dibandingkan laki-laki dengan profil keuangan yang sama, bahkan lebih baik. Algoritma tersebut tidak secara eksplisit mendiskriminasi berdasarkan gender, tetapi menggunakan data lain yang secara tidak langsung mencerminkan bias gender, seperti riwayat pekerjaan dan pendapatan.

Fenomena ini menunjukkan bahwa setiap keputusan algoritmik mengandung nilai-nilai tertentu. Jika nilai-nilai ini tidak diawasi, algoritma dapat memperkuat ketidaksetaraan sosial yang sudah ada, mengubah bias menjadi kerugian struktural.

Inklusi Keuangan atau Jebakan Utang?

Aplikasi keuangan digital sering kali dirancang dengan teknologi canggih dan prinsip psikologi perilaku. Tujuannya bukan hanya membantu pengguna mengelola keuangan, tetapi juga mendorong perilaku tertentu yang menguntungkan perusahaan di balik aplikasi tersebut. Fitur seperti Beli Sekarang, Bayar Nanti (*Buy Now, Pay Later*) merupakan pinjaman instan tampak menggoda, tetapi di balik kemudahan itu ada risiko besar: jebakan utang.

Sistem ini juga memanfaatkan data perilaku pengguna untuk menyesuaikan penawaran. Misalnya, algoritma bisa menentukan tingkat bunga berdasarkan pola belanja Anda, aktivitas online, bahkan unggahan media sosial. Anda mungkin tidak menyadari bahwa setiap transaksi kecil, seperti membeli kopi di pagi hari, di mana Anda membelinya dan berapa uang yang Anda habiskan, menjadi bagian dari potret digital Anda sendiri yang digunakan untuk memprediksi dan memengaruhi keputusan keuangan Anda. Di beberapa negara seperti China, data ini digunakan untuk menentukan skor kredit sosial yang memengaruhi akses ke pinjaman, perjalanan, bahkan pendidikan anak. Sementara di Amerika Serikat, skor kredit dapat menentukan peluang kerja Anda di institusi keuangan. Algoritma ini diam-diam menulis "cerita hidup" Anda, berdasarkan asumsi dan pola yang belum tentu akurat.

Ironisnya, sementara sebagian masyarakat merasa kewalahan oleh layanan digital ini, kelompok lain justru tertinggal. Generasi tua, masyarakat pedesaan, dan kelompok minoritas sering kali kesulitan mengikuti perubahan ini. Tanpa akses ke teknologi atau literasi digital yang memadai, mereka menjadi korban baru eksklusi finansial. Sistem ini menciptakan jurang baru antara mereka yang melek digital dan yang tidak.

Kaum lanjut usia, misalnya, rentan terhadap penipuan karena keterbatasan literasi digital dan kehilangan akses ke layanan perbankan konvensional. Penutupan cabang bank fisik semakin memperparah situasi ini, memaksa mereka menghadapi proses online yang rumit dan membingungkan.

Membangun Masa Depan Keuangan yang Lebih Etis

Meski tantangan ini nyata, kita masih memiliki peluang untuk membentuk masa depan keuangan digital yang lebih manusiawi. Berikut adalah tiga langkah penting yang dapat kita ambil:

Prinsip Desain Etis: Setiap aplikasi keuangan harus dirancang dengan prinsip etis yang melindungi pengguna. Bayangkan jika aplikasi perdagangan saham memberikan peringatan saat pasar sedang volatil, atau aplikasi pembayaran memberi jeda 30 detik sebelum transaksi besar diproses. Fitur ini membantu pengguna untuk menghindari psikologi takut ketinggalan (*fear of missing out*), dan memfasilitasi pengambilan

keputusan yang lebih bijaksana. Transparansi juga harus ditingkatkan, mulai dari penyajian syarat dan ketentuan yang mudah dipahami hingga pengungkapan biaya yang jelas.

Regulasi yang Adaptif: Regulasi keuangan saat ini sebagian besar dirancang untuk dunia perbankan tradisional. Kita membutuhkan kerangka hukum baru yang responsif terhadap inovasi digital. Contohnya adalah audit berkala terhadap teknologi AI, panduan jelas untuk penggunaan data konsumen, dan mekanisme akuntabilitas atas keputusan AI. Pengguna juga harus memiliki hak untuk memahami dan mengajukan keberatan terhadap keputusan yang dibuat oleh algoritma, seperti penolakan pinjaman.

Literasi Keuangan Digital: Edukasi adalah perlindungan terbaik melawan eksploitasi. Literasi keuangan harus mencakup pemahaman tentang algoritma keuangan, keamanan digital, dan praktik predatoris. Edukasi ini harus menjangkau seluruh lapisan masyarakat, termasuk generasi tua dan komunitas pedesaan. Perpustakaan atau pusat komunitas dapat menjadi pusat literasi keuangan digital, menyediakan pelatihan gratis dan bantuan satu-satu.

Teknologi telah memberikan akses yang belum pernah ada sebelumnya ke dunia keuangan, tetapi kita berada di persimpangan penting. Apakah kita akan memilih kenyamanan dengan segala risikonya, atau menciptakan inovasi yang etis dan bermanfaat bagi semua?

Setiap kali Anda menggunakan aplikasi keuangan, Anda sebenarnya sedang berpartisipasi dalam menentukan masa depan. Akankah kita membiarkan algoritma mendikte hidup kita, atau kita akan mengambil kendali dan menulis cerita keuangan kita sendiri? Pilihannya ada di tangan kita. Mari kita pastikan teknologi melayani kebutuhan manusia, bukan sebaliknya.

Tautan artikel:

https://kumparan.com/arif-perdana-1723991955605643308/revolusi-keuangan-digital-janji-tantangan-dan-masa-depan-yang-kita-pilih-23zMuDxuJqV

Menyusuri Labirin Kecurangan dengan Pelita AI

Arif Perdana

Konteks: Artikel ini saya terbitkan di Kumparan tanggal 23 Oktober 2024. Artikel ini mendeskripsikan penipuan finansial yang semakin kompleks. Hal ini kian menuntut respons inovatif dari organisasi. AI kini berperan penting dalam deteksi penipuan real-time, menggantikan metode konvensional yang kurang efektif. Kemampuan AI dalam analisis anomali, prediksi, dan jaringan membantu mengungkap skema penipuan tersembunyi. Namun, tantangan seperti risiko kesalahan deteksi, masalah privasi, dan kualitas data tetap ada. Mengandalkan AI perlu diimbangi dengan penilaian manusia demi menjaga perspektif etis. Keberhasilan pencegahan penipuan bergantung pada pemanfaatan teknologi yang bijak, menjaga integritas data, dan membangun kepercayaan pemangku kepentingan untuk ekonomi yang lebih aman.

Di era digital yang semakin kompleks, penipuan telah berkembang menjadi ancaman yang semakin canggih dan sulit dideteksi. Layaknya arus gelap yang tak henti-hentinya menggerogoti integritas industri, kecurangan finansial menuntut respons yang tidak hanya tangguh, tetapi juga inovatif dari organisasi. Di sinilah AI hadir, memposisikan diri sebagai pelita yang menjanjikan dalam labirin kecurangan yang semakin rumit. Namun, apakah teknologi ini benar-benar merupakan jawaban atas semua permasalahan, atau justru membawa tantangan baru yang perlu diwaspadai?

Tidak dapat dipungkiri bahwa metode konvensional seperti audit berkala dan pemeriksaan manual kini tampak tidak memadai dalam menghadapi taktik penipuan yang terus berevolusi. AI, dengan kemampuannya mengolah data dalam jumlah masif dengan kecepatan yang menakjubkan, menawarkan harapan baru. Teknologi ini memungkinkan organisasi untuk mengenali dan mencegah penipuan secara real-time. Aktifitas pendeteksian fraud beralih dari pendekatan reaktif menjadi proaktif dalam mengidentifikasi tanda-tanda kecurangan sebelum berkembang menjadi ancaman serius. Namun, kita perlu bertanya: apakah kecepatan dan efisiensi ini datang dengan harga yang mahal dalam hal privasi dan keamanan data?

Sistem deteksi berbasis AI menggunakan berbagai teknik canggih untuk mengungkap pola penipuan yang tersembunyi. Deteksi anomali (*anomaly detection*), misalnya, mampu mengenali penyimpangan dari pola transaksi normal. Deteksi ini memungkinkan bank untuk mengidentifikasi transaksi mencurigakan dengan cepat.
Analitika prediktif (*predictive analytics*) memanfaatkan data historis untuk memproyeksikan tren kecurangan di masa depan, sementara analisis jaringan (network analysis) memeriksa hubungan antar transaksi untuk mengungkap skema penipuan yang kompleks. Bahkan, kemampuan pemrosesan bahasa alami (*Natural Language Processing*/NLP) memungkinkan AI untuk menyusuri aliran teks dari email hingga percakapan. Teknik seperti ini mampu menangkap isyarat penipuan yang terselip di antara kata-kata.

Meskipun kemampuan ini terdengar mengesankan, kita perlu mempertanyakan sejauh mana kita bisa memercayai keputusan yang dibuat oleh AI. Bagaimana jika algoritma ini salah mengidentifikasi transaksi yang sah sebagai penipuan, atau sebaliknya? Konsekuensi dari kesalahan semacam ini bisa sangat serius, baik bagi organisasi maupun individu yang terlibat.

Tantangan implementasi AI dalam deteksi kecurangan juga tidak bisa diabaikan. Kualitas data menjadi kendala utama; dataset yang tidak akurat atau tidak lengkap dapat memicu hasil positif palsu atau gagal mengidentifikasi penipuan sebenarnya. Proses validasi dan pembersihan data yang ketat menjadi krusial, namun seberapa realistis hal ini dapat dilakukan secara konsisten dalam skala besar?

Kekhawatiran terkait privasi juga muncul ke permukaan. Manajemen data sensitif dalam volume besar berpotensi mengundang risiko keamanan yang signifikan. Meskipun regulasi seperti UU Pelindungan Data Pribadi (PDP), GDPR, atau CCPA berusaha melindungi data pribadi, pertanyaannya adalah: apakah regulasi ini cukup untuk mengimbangi kecepatan perkembangan teknologi AI? Disparitas dalam data juga memperumit sistem deteksi penipuan berbasis AI. Data tentang insiden penipuan umumnya jauh lebih sedikit dibandingkan transaksi sah. Ini tentunya menciptakan ketidakseimbangan yang dapat mempengaruhi akurasi model AI. Meskipun strategi teknis seperti oversampling (menambah jumlah data dari kelompok kecil) atau

undersampling (mengurangi jumlah data dari kelompok besar) dapat digunakan untuk menyeimbangkan data, kita perlu mempertanyakan apakah pendekatan ini benar-benar mencerminkan realitas di lapangan.

Ketergantungan berlebihan pada sistem otomatis juga mengkhawatirkan. Meskipun AI unggul dalam menandai aktivitas mencurigakan, sistem ini memerlukan pembaruan dan peningkatan berkelanjutan untuk tetap relevan terhadap taktik penipuan yang terus berkembang. Pertanyaannya adalah: dapatkah organisasi mempertahankan komitmen jangka panjang yang diperlukan untuk terus melatih dan menyempurnakan model AI mereka?

Integrasi algoritma AI ke dalam sistem dan alur kerja yang ada juga bukan tanpa tantangan. Perubahan budaya organisasi menuju pengambilan keputusan berbasis data sering kali lebih sulit daripada implementasi teknologi itu sendiri. Bagaimana organisasi dapat memastikan bahwa transformasi ini tidak hanya menyentuh aspek teknis, tetapi juga mengubah pola pikir dan cara kerja seluruh karyawan?

Di tengah segala kompleksitas ini, pentingnya keseimbangan antara otomatisasi dan penilaian manusia tidak boleh diabaikan. Meskipun AI mampu memproses data dalam skala besar dengan efisien, kearifan dan nuansa penilaian manusia tetap krusial dalam memahami konteks yang lebih luas dan membuat keputusan yang tepat. Satu hal yang perlu kita pertimbangkan adalah bagaimana kita dapat memastikan bahwa sinergi antara AI dan kecerdasan manusia benar-benar tercapai, bukan hanya jargon kosong.

Melihat ke masa depan, prospek analisis penipuan berbasis AI memang menjanjikan. Integrasi dengan teknologi blockchain menawarkan peningkatan transparansi dan keamanan dalam transaksi finansial. Pemelajaran terdistribusi (federated learning) membuka jalan baru untuk analisis data yang mengutamakan privasi. Pemelajaran terdistribusi adalah metode AI yang melatih model pada perangkat lokal, tanpa berbagi data mentah. Hanya pembaruan model yang dikirim ke server pusat. Teknik ini menjaga privasi data pengguna. Namun, kita harus tetap kritis: apakah teknologi-teknologi baru ini benar-benar akan menyelesaikan masalah yang ada, atau justru menciptakan kompleksitas baru yang belum kita antisipasi?

Dalam menghadapi evolusi skema penipuan yang semakin kompleks, integrasi strategis AI dalam kerangka pencegahan penipuan memang menjadi krusial. Namun, kita harus ingat bahwa teknologi, secanggih apapun, hanyalah alat. Keberhasilan dalam melawan penipuan akan bergantung pada bagaimana kita menggunakan alat ini dengan bijaksana, mempertimbangkan tidak hanya aspek teknis, tetapi juga etis dan sosial.

Organisasi perlu menyeimbangkan kecerdasan analisis data dengan pertimbangan etis dan pelindungan privasi. Mereka harus menavigasi jalur yang tidak hanya efektif dalam mendeteksi penipuan, tetapi juga menjaga integritas data dan memelihara kepercayaan pemangku kepentingan. Hanya dengan pendekatan holistik inilah kita dapat berharap untuk menciptakan lanskap ekonomi yang lebih aman dan adil bagi semua pihak.

Dalam perjalanan menyusuri labirin kecurangan dengan pelita AI, kita mungkin telah menemukan cahaya baru. Namun, kita juga harus waspada terhadap bayangan yang mungkin tercipta. Hanya dengan sikap kritis dan kehati-hatian inilah kita dapat memastikan bahwa teknologi ini benar-benar menjadi kekuatan untuk kebaikan, bukan sekadar alat canggih yang justru menciptakan masalah baru yang lebih rumit.

Tautan artikel:

https://kumparan.com/arif-perdana-1723991955605643308/menyusuri-labirin-kecurangan-dengan-pelita-kecerdasan-artifisial-23lWAL501Zf

Belajar Dari 2 Gelembung Teknologi: Apakah Pamor AI Akan Pecah Lalu Pudar?

Arif Perdana

Konteks: Artikel ini merupakan refleksi saya terhadap diskurus mengenai apakah AI akan memiliki nasib yang sama seperti dot-com bubble, crypto-buble, ataukah berbeda. Artikel ini terbit di The Conversation Indonesia tanggal 31 Juli 2024. Tulisan ini membahas perkembangan pesat teknologi AI generatif (GenAI) dan potensi risiko gelembung investasi, mengaitkannya dengan pengalaman gelembung dot-com dan kripto. Meskipun GenAI menarik perhatian investor dengan aplikasinya yang luas, banyak startup masih mencari model bisnis yang stabil. Tantangan termasuk biaya tinggi, isu hukum, dan regulasi yang ketat. Penulis menekankan pentingnya investasi yang bijaksana dan realistis untuk menghindari gelembung, serta menyoroti potensi jangka panjang teknologi AI yang tetap berharga dan relevan.

Saat ini kita menyaksikan teknologi AI generatif berkembang pesat. Contohnya, model bahasa besar seperti GPT dan Claude yang berkembang pesat sejak 2018. Model ini dapat menghasilkan teks mirip percakapan manusia, hingga AI generatif (GenAI) visual seperti DALL-E dan Midjourney yang mampu menciptakan gambar dari deskripsi teks.

Contoh lainnya termasuk model AI yang dapat menghasilkan musik, kode pemrograman, dan bahkan video pendek. Perkembangan ini kemudian memicu arus modal yang deras mengalir ke startup AI. Pendanaan modal ventura di Amerika Serikat untuk startup AI meningkat secara signifikan pada kuartal kedua 2024, mencapai total US$55,6 miliar atau lebih dari Rp905 triliun[113]. Angka tersebut termasuk $6 miliar (sekitar Rp97,71 triliun) yang dihimpun oleh xAI milik konglomerat Elon Musk dan $1,1 miliar (setara Rp17,91 triliun) yang berhasil dikumpulkan oleh CoreWeave, menandakan peningkatan minat yang kuat dalam sektor AI.

Kendati begitu, banyak usaha GenAI masih dalam tahap awal dengan model bisnis yang masih mencari bentuk. Contohnya termasuk berbagai startup AI yang berfokus

[113] https://www.reuters.com/business/finance/ai-deals-lift-us-venture-capital-funding-highest-level-two-years-data-shows-2024-07-03/

pada pembuatan konten otomatis atau asisten virtual masih mencari cara untuk menghasilkan pendapatan yang stabil. Ini kemudian memunculkan pertanyaan dari para analis di beberapa institusi besar seperti Gartner, Wall Street, dan Goldman Sachs tentang risiko AI yang menjadi tren dalam gelembung dan kemudian buyar seiring waktu. Untuk menjawab pertanyaan ini, kita bisa melihat terlebih dahulu dua tren teknologi sebelumnya, yakni dot-com dan kripto. Keduanya sempat menjadi gelembung karena ekspektasi investor ternyata terlalu tinggi—melebihi aplikasi praktis dan keandalan pada saat itu.

Kelebihan Optimisme Pasar Dot-Com

Pada akhir 1990-an hingga awal 2000-an, dunia menyaksikan satu kejadian penting: gelembung dot-com. Era ini mencerminkan optimisme pasar yang berlebihan, didorong oleh potensi revolusioner World Wide Web. Alan Greenspan, dengan istilah kegairahan irasional, menggambarkan bagaimana investor—terpesona oleh daya tarik Internet—menanamkan modal besar-besaran pada perusahaan internet yang baru berdiri. Perusahaan-perusahaan rintisan ini, seringkali tanpa model bisnis yang terbukti atau arus pendapatan yang jelas, dengan mudah mendapatkan akses ke modal, terutama melalui Penawaran Umum Perdana (IPO). Beberapa perusahaan besar yang melakukan IPO menjelang periode gelembung dot-com ini antara lain BlackBerry, Broadcom Corporation, dan Verisign.

Indeks NASDAQ Composite, yang didominasi oleh saham teknologi, meningkat lebih dari 400%. Nilainya mencuat dari di bawah seribu poin pada tahun 1995 menjadi di atas 5 ribu poin pada 2000. Ini menandakan lonjakan minat investor. Sayangnya, banyak dari perusahaan ini memiliki fondasi bisnis yang lemah dan lebih fokus pada pangsa pasar daripada profitabilitas. Pada tahun 2000, gelembung dot-com meletus. Kejatuhan sektor dot-com ditandai ketimpangan serius antara valuasi yang melambung dan kesehatan finansial yang sesungguhnya. Indeks Internet Bloomberg AS anjlok dari $2,9 triliun (dengan kurs saat ini setara Rp47.000 triliun) menjadi $1,1 triliun (Rp17.900 triliun), alias terpangkas lebih dari setengahnya. Kontras mencolok di perusahaan seperti Cisco dan Yahoo! menunjukkan volatilitas investasi teknologi dan risiko overvaluasi. Keduanya

mencapai valuasi tinggi saat puncak gelembung dot-com, lalu mengalami penurunan drastis setelahnya.

Cisco berhasil bertahan dan tetap relevan, sementara Yahoo! akhirnya kehilangan dominasi pasar. Buyarnya gelembung berdampak luas pada ekonomi, termasuk kehilangan pekerjaan secara signifikan, khususnya di sektor telekomunikasi. Meski diwarnai kekacauan, kejatuhan dot-com membawa manfaat jangka panjang. Pecahnya gelembung ini membuka jalan bagi pemahaman yang lebih realistis tentang potensi bisnis Internet. Era ini juga menjadi penyaring yang meloloskan perusahaan-perusahan dengan model bisnis berkelanjutan bertahan di industri teknologi. Episode bersejarah tersebut menekankan risiko overvaluasi yang didasarkan pada tren dan menyoroti pentingnya dasar bisnis yang kuat. Gelembung dot-com juga menjadi pelajaran penting bagi sektor teknologi yang sedang berkembang, seperti GenAI.

Gelembung Kripto: Aset Digital dan Demam Spekulasi

Gelembung kripto muncul sebagai bentuk alternatif dari gelembung dot-com yang muncul dari demam spekulasi. Berbeda dari gelembung dot-com, gelembung kripto memiliki karakteristik dan dampak yang berbeda. Gelembung kripto didorong oleh pesona inovatif teknologi blockchain dan mata uang kripto, sehingga mengalami lonjakan investasi spekulatif yang belum pernah terjadi sebelumnya. Salah satu pendorong utamanya adalah sindrom ‘fear of missing out’ (FOMO). Investor ramai-ramai terpikat oleh cerita tentang lonjakan nilai mata uang kripto, seperti Bitcoin, yang naik dari sekitar US$900 (Rp14,66 juta) menjadi hampir US$20 ribu (Rp325,87 juta) dalam waktu kurang dari setahun pada 2017. Mereka yang tergoda oleh janji imbal hasil luar biasa kemudian menanamkan uang dalam berbagai aset digital dan penawaran koin perdana (ICO). Sialnya, banyak investor yang mengabaikan risiko dan naik-turun nilai komoditas ini.

Kendati begitu, struktur pasar kripto dan integrasinya (atau ketiadaannya) dengan sistem keuangan tradisional membuatnya berbeda dari skenario dot-com. Berbeda dengan kehancuran dot-com yang berdampak lebih luas pada ekonomi global, kehancuran kripto lebih berdampak ke aset digital. Sebagian dampak ini terjadi karena

adopsi mata uang kripto yang relatif terbatas dalam keuangan arus utama saat gelembung meletus. Selain itu, lanskap regulasi untuk mata uang kripto penuh dengan ketidakpastian. Tidak seperti sekuritas tradisional yang memiliki kerangka kerja regulasi yang mapan, mata uang kripto berada dalam area abu-abu regulasi di beberapa negara. Kondisi tersebut menciptakan risiko tambahan bagi investor. Misalnya, ketiadaan regulasi membuat penanganan isu seperti penipuan dan manipulasi pasar menjadi tantangan, hal yang umum di ruang kripto.

Risiko GenAI Menggelembung?

GenAI menjadi tren yang mengesankan karena teknologi ini mampu menciptakan konten baru—mulai dari teks, gambar, hingga musik—yang sebelumnya hanya bisa dihasilkan oleh manusia. Kemampuannya untuk menyederhanakan proses produksi dan memberikan solusi otomatis dalam berbagai bidang membuatnya sangat menarik bagi banyak industri, dari pemasaran hingga seni. Meski demikian, kualitas dan keandalan GenAI masih terbatas. Model-model AI ini membutuhkan jumlah data yang masif dan kekuatan komputasi yang luar biasa. Hal tersebut membuat skalabilitasnya—kemampuan suatu teknologi menampung penambahan beban—menjadi tantangan besar. Di samping itu, isu hukum dan etika seperti hak kekayaan intelektual dan bias algoritma juga semakin menonjol. Risiko perlambatan ekonomi global turut membuat investor menjadi lebih berhati-hati, sehingga berdampak langsung pada pendanaan untuk perusahaan rintisan AI. Seperti halnya dengan gelembung dot-com, tren GenAI saat ini mungkin sedang menuju jalan yang sama. Banyak perusahaan AI masih beroperasi dengan model bisnis yang belum terbukti dan sangat bergantung pada dana investor.

Salah satu contohnya, Microsoft dan Adobe menghadapi kesulitan untuk mendapatkan keuntungan dari AI dikarenakan investasi yang tinggi. Microsoft rata-rata mengalami kerugian US$20 (sekitar Rp326 ribu) per pengguna AI, tapi rata-rata biaya yang dibebankan hanya US$10 (sekitar Rp163 ribu). Ini mengakibatkan para investor agak skeptis dan berhati-hati untuk berinvestasi di pasar AI. Namun, berbeda dengan era dot-com dan kripto, GenAI telah menunjukkan aplikasi nyata yang signifikan di berbagai sektor, dari kesehatan hingga keuangan. Kemajuan teknologi AI yang cepat dan adopsi

yang beragam di berbagai industri memberikan dasar yang lebih kokoh, berpotensi mengurangi risiko gelembung. Contohnya, JP Morgan, salah satu bank investasi terbesar di dunia, mengembangkan asisten percakapan berbasis GenAI untuk meningkatkan efisiensi analisis data keuangan perusahaan.

Meski demikian, kita tidak bisa mengabaikan fakta bahwa GenAI masih dalam fase awal perkembangan. Masih banyak ketidakpastian mengenai kemampuan teknologi ini untuk menghasilkan laba jangka panjang. Selain itu, regulasi yang semakin ketat dan kekhawatiran lingkungan tentang kebutuhan energi pusat data AI dapat menjadi faktor yang membatasi pertumbuhan sektor ini. Investor terkenal asal Inggris, Jeremy Grantham [114] , yang memprediksi gelembung dot-com dan krisis keuangan 2008, menyatakan gelembung AI mungkin saja “meletus,” . Namun, dampaknya boleh jadi tidak seburuk gelembung internet. Andaipun gelembung AI pecah, kata Jeremy, nilai intrinsik teknologi ini kemungkinan akan tetap bertahan karena nilai praktisnya yang luas dan signifikan.

Kunci untuk menghindari gelembung di sektor GenAI terletak pada keseimbangan antara investasi, spekulasi dengan penilaian realistis terhadap kemampuan teknologi saat ini. Peluang aplikasi praktis yang berkelanjutan juga sepatutnya menjadi pertimbangan para investor. Pasar di sektor AI mungkin dapat terkoreksi, mirip dengan gelembung teknologi masa lalu. Namun, teknologi AI telah memberikan nilai dan kegunaannya. Fondasi perusahaan-perusahaan teknologi masa kini juga lebih kuat dibandingkan dengan di masa gelembung dot-com.

Setelah terkoreksi, AI kemungkinan akan tetap menjadi bagian penting dan integral dari lanskap teknologi. Sektor ini berpeluang terus berkembang dan berintegrasi ke dalam berbagai aspek bisnis dan masyarakat. Pelajaran dari gelembung dot-com dan kripto menjadi panduan berharga dalam menjelajahi perbatasan baru ini. Karena itu, kita sangat perlu berinvestasi secara bijaksana, memiliki ekspektasi yang realistis, dan berfokus pada pertumbuhan serta aplikasi yang berkelanjutan. Perusahaan dan investor AI juga perlu memastikan penggunaan yang etis dan tepat, serta menemukan jalur

[114] https://edition.cnn.com/2024/03/14/investing/premarket-stocks-trading-ai-bubble-grantham/index.html

keberlanjutan untuk menjaga tingkat pendapatan. Ini bukan hanya untuk menghindari kerugian finansial, tetapi juga demi mendorong inovasi yang bertanggung jawab dan berkelanjutan di masa depan.

Tautan artikel:

https://theconversation.com/belajar-dari-2-gelembung-teknologi-apakah-pamor-ai-akan-pecah-lalu-pudar-235703

Tantangan Digital Semakin Memerlukan ‘Lifelong Learning’: Ini Alasannya

Arif Perdana

Konteks: Artikel ini terbit di The Conversation Indonesia tanggal 13 May 2024. Tulisan ini menyoroti pentingnya pembelajaran sepanjang hayat untuk mempertahankan relevansi di pasar kerja yang terus berubah. Pembelajaran ini membantu individu beradaptasi, menjaga kesehatan kognitif, dan mengembangkan keterampilan digital. Implementasi strategi di tempat kerja melibatkan mendorong rasa ingin tahu, penilaian keterampilan, dan kombinasi pengalaman belajar formal dan informal. Selain itu, kolaborasi antara pemerintah, pendidikan, dan industri sangat penting untuk mendukung pembelajaran berkelanjutan. Dengan demikian, pembelajaran sepanjang hayat meningkatkan produktivitas individu dan keberlanjutan organisasi.

Cepatnya perkembangan teknologi dan pasar kerja yang tidak dapat diprediksi menuntut para profesional untuk tetap kompetitif dalam menghadapi tantangan industri. Tantangan yang terus-menerus ini menuntut pembelajaran yang berkelanjutan, sesuai dengan konsep lifelong learning atau pembelajaran sepanjang hayat. Pembelajaran sepanjang hayat merupakan upaya mendapatkan pengetahuan yang holistik yang muncul dari motivasi internal diri untuk tumbuh sebagai pribadi dan profesional. Laporan Forbes dan statistik Dell menyatakan bahwa 85% tenaga kerja pada tahun 2030 akan memiliki pekerjaan yang saat ini belum ada[115]. Karena itu, pembelajaran sepanjang hayat penting untuk menumbuhkan kemampuan beradaptasi, rasa ingin tahu, dan pemahaman yang lebih dalam tentang aspek-aspek yang relevan di dunia kerja.

Manfaat Pembelajaran Sepanjang Hayat

1. Mempertahankan relevansi

Pembelajaran sepanjang hayat menekankan kebutuhan belajar dengan menyesuaikan perkembangan zaman, teknologi dan karier. Pembelajaran seperti ini tidak

[115] https://www.delltechnologies.com/content/dam/delltechnologies/assets/perspectives/2030/pdf/Realizing-2030-A-Divided-Vision-of-the-Future-Summary.pdf

hanya mempersiapkan individu untuk perubahan yang tidak dapat diprediksi di pasar kerja, tetapi juga vital untuk menumbuhkan kemampuan beradaptasi, mendorong pengembangan pribadi, dan mempertahankan relevansi dalam ekonomi yang semakin digital dan global. Dengan mengadopsi pendekatan yang lebih luas terhadap pembelajaran sepanjang hayat, baik individu maupun organisasi dapat tetap lincah, adaptif, dan berkembang dalam menghadapi dinamika pasar dan perpanjangan durasi karier. Perusahaan software multinasional (SAP) melalui SAP Learning Hub, contohnya, menyediakan kursus online gratis dari berbagai pakar di bidangnya yang memungkinkan profesional untuk memutakhirkan pengetahuannya dengan perkembangan digital terkini[116].

2. Kesehatan kognitif

Pembelajaran sepanjang hayat juga bisa berdampak pada kesehatan kognitif orang dewasa. Pendekatan ini berakar pada pengaruh sosial sejak dini, termasuk dinamika keluarga dan sistem pendidikan. Pendidikan formal seharusnya berperan penting dalam menumbuhkan motivasi untuk terus belajar. Sayangnya, lembaga pendidikan formal cenderung menghadapi hambatan dalam mengintegrasikan pembelajaran sepanjang hayat. Itu sebabnya, kurikulum merdeka diharapkan dapat menjadi katalis karena memberikan ekosistem yang lebih baik dari sisi pendekatan pembelajaran berbasis proyek.

3. Kecakapan digital

Di era digital, pembelajaran sepanjang hayat penting untuk mencapai tingkat kepercayaan digital yang tinggi. Organisasi yang beroperasi di dunia digital harus memberikan pelatihan yang memadai kepada staf mereka dan secara rutin mengevaluasi serta meningkatkan efektivitasnya. Pelatihan ini mengajarkan keterampilan digital yang mencakup kemampuan menggunakan perangkat digital, aplikasi komunikasi, dan jaringan untuk mengakses dan mengelola informasi.

[116] https://learninghub.sap.com/

Kemampuan ini penting untuk pemenuhan diri, berkolaborasi dan kegiatan sosial, serta memungkinkan penggunaan teknologi secara transformatif. Salah satu contoh dari model pelatihan ini adalah rangkaian sertifikat karier *Google*[117]. yang bertujuan untuk mempersiapkan orang-orang berkarier di bidang analitika data, manajemen proyek, dan desain antarmuka aplikasi tanpa prasyarat gelar sarjana sebelumnya. Program ini bisa diakses gratis dan dirancang untuk membantu peserta didik mendapatkan keterampilan praktis yang langsung dapat diterapkan di tempat kerja.

Pembelajaran Sepanjang Hayat Di Tempat Kerja

Implementasi strategi pembelajaran sepanjang hayat di tempat kerja terdiri dari beberapa komponen.

Pertama, mendorong rasa rasa ingin tahu dan kemampuan beradaptasi. Ini dapat dicapai dengan menggunakan program pelatihan yang beragam dan kesempatan bagi karyawan untuk mengeksplorasi area atau minat baru. Organisasi harus memanfaatkan kemajuan teknologi sebagai alat untuk efisiensi operasional dan peluang untuk belajar dan pengembangan bagi karyawan mereka. Mengembangkan budaya yang mengutamakan pembelajaran dan pertumbuhan berkelanjutan sangat penting untuk pemberdayaan karyawan dan keberlanjutan organisasi. Budaya ini harus menekankan pada berbagi pengetahuan, umpan balik yang berkelanjutan, dan pengakuan terhadap pencapaian pembelajaran.

Kedua, penilaian kinerja reguler terhadap keterampilan dan kompetensi, yang dipadukan dengan indikator capaian bisa membantu individu untuk menyelaraskan diri dengan aspirasi mereka dan kebutuhan organisasi. Menggabungkan pembelajaran sepanjang hayat ke dalam rencana pengembangan karier akan membantu karyawan melihat pembelajaran sebagai aspek yang penting di jenjang karier profesional mereka.
Ketiga, kombinasi pengalaman belajar formal dan informal. Pendidikan formal memberikan pengetahuan terstruktur, sementara pembelajaran informal, seperti bimbingan, lokakarya, dan proyek mandiri, menawarkan wawasan praktis dan

[117] https://grow.google/certificates/

pengalaman langsung. Memberikan karyawan akses ke berbagai sumber belajar, seperti kursus online melalui lingkungan belajar virtual, seminar, konferensi, dan lokakarya, sangat penting.

Kolaborasi Pembelajaran Sepanjang Hayat

Untuk mempopulerkan pembelajaran sepanjang hayat, pemerintah dapat berperan aktif dengan berinvestasi dalam platform pendidikan yang mudah diakses, mensubsidi program pengembangan keterampilan, memberikan keringanan pajak, dan memupuk kemitraan dengan industri untuk peluang pembelajaran berkelanjutan. Investasi seperti ini adalah kunci untuk memfasilitasi pembelajaran berkelanjutan dan pengembangan keterampilan yang sesuai dengan tuntutan ekonomi digital. Selain itu, universitas dan lembaga pendidikan perlu terlibat.

Massachusetts Institute of Technology (MIT) di Amerika Serikat (AS), misalnya, menawarkan program MicroMasters, yang merupakan serangkaian kursus pascasarjana yang tersedia online[118]. Beberapa bahkan ada yang tersedia secara gratis, dan dirancang untuk memajukan karier profesional. Program ini mencakup bidang-bidang seperti Statistika dan Ilmu Data, Prinsip-prinsip Ekonomi Manajemen, dan Kebijakan dan Teknologi Energi Berkelanjutan.

Korporasi di pendidikan sebenarnya juga bisa menangkap peluang ini dan bekerja sama dengan industri dan universitas. Coursera, penyedia kursus online terbuka yang berbasis di AS, contohnya, menawarkan “Coursera for Campus” yang memungkinkan universitas dan perguruan tinggi menyediakan akses ke berbagai kursus online untuk melengkapi kurikulum mereka. Ini membantu mahasiswa dan staf akademis mendapatkan keterampilan terbaru yang relevan dengan perkembangan industri saat ini. Singapura, sudah mengimplementasikan model pembelajaran seperti ini melalui “SkillsFuture”, sebuah program yang didesain untuk memberikan keterampilan baru terpersonalisasi bagi profesional, melayani kebutuhan dan aspirasi individu untuk tetap

[118] https://micromasters.mit.edu/

selaras dengan kemajuan teknologi[119]. Warga negara Singapura mendapatkan subsidi untuk mengikuti kursus-kursus di SkillsFuture ini.

Pemerintah Inggris juga memiliki program "Skills for Life" untuk meningkatkan keterampilan mereka yang berusia di atas 19 tahun[120]. Program ini memberikan pendidikan dan pelatihan gratis tentang literasi informasi, matematika, teknik, dan keterampilan digital. Program ini disubsidi oleh pemerintah Inggris. Di samping itu, pemerintah Inggris juga memberikan pendanaan bagi perusahaan yang melakukan pelatihan berkelanjutan bagi karyawannya.

Pemerintah Kanada melalui "Canada Training Benefit" memungkinkan warga negaranya mendapatkan kredit pajak jika mereka mengikuti program-program perkuliahan atau kursus-kursus di lembaga pendidikan yang disyaratkan oleh pemerintah[121]. Lembaga tersebut mencakup perguruan tinggi, atau institusi pendidikan lain di Kanada yang menawarkan kursus yang relevan setelah jenjang sekolah menengah atas. Institusi lainnya yang memenuhi syarat adalah kursus vokasi yang telah disertifikasi oleh pemerintah Kanada.

Singkatnya, pembelajaran sepanjang hayat dapat memberi manfaat pada produktivitas individu, keberlanjutan organisasi dan industri. Namun untuk mewujudkannya, pembelajaran sepanjang hayat membutuhkan kolaborasi di antara individu, organisasi, industri, dan pemerintah.

Tautan artikel:

https://theconversation.com/tantangan-digital-semakin-memerlukan-lifelong-learning-ini-alasannya-224769

[119] https://www.skillsfuture.gov.sg/
[120] https://www.skillsforcareers.education.gov.uk/pages/skills-for-life
[121] https://www.canada.ca/en/revenue-agency/services/child-family-benefits/canada-training-credit.html

Riset ‘Crowdlending’: Bagaimana Meningkatkan Kepercayaan Investor di Tengah Sentimen Negatif Pinjol?

Arif Perdana

Konteks: Artikel ini terbit di The Conversation Indonesia tanggal 22 May 2024. Artikel ini ditulis berdasarkan riset saya dan kolega di Singapore Institute of Technology dan George Washington University yang dipublikasikan di Electronic Markets. Tulisan ini membahas tren crowdlending di Asia, terutama tantangan kepercayaan dalam industri ini. Crowdlending, yang berbeda dari pinjaman online konvensional, memungkinkan individu meminjamkan uang kepada peminjam tanpa perantara fisik. Penelitian menunjukkan bahwa faktor seperti kedalaman data peminjam, verifikasi pihak ketiga, dan mitigasi risiko berkontribusi pada kepercayaan investor. Rekomendasi untuk platform meliputi transparansi informasi dan manajemen risiko yang baik, sementara individu perlu meneliti platform dan memahami syarat pinjaman untuk mengurangi risiko.

Crowdlending tengah menjadi tren di industri keuangan belakangan ini, khususnya di negara-negara Asia seperti Singapura dan Indonesia. Meski begitu, aspek kepercayaan masih menjadi tantangan besar untuk industri bisa berkembang. Crowdlending sebenarnya hanyalah nama lain dari peer-to-peer lending atau pinjaman online (pinjol), yang kerap mendapat cap negatif karena berbagai permasalahan seperti bunga tinggi dan aktivitas penagihan yang tidak bertanggung jawab, terutama yang diselenggarakan oleh pinjol ilegal. Bedanya dari pinjol pada umumnya, crowdlending memungkinkan individu meminjamkan uang kepada peminjam yang tidak dikenal hanya dengan beberapa klik mouse. Model ini juga membuka peluang bagi investor untuk menanamkan uangnya ke berbagai kampanye atau usaha mikro dan kecil-menengah (UMKM). Platform crowdlending yang ditujukan untuk kepentingan produktif alih-alih konsumtif ini sebenarnya memberikan dampak positif.

Singapura dan Malaysia, misalnya, memiliki pasar crowdlending yang relatif matang dan teratur dengan platform seperti Funding Societies dan MoneyMatch, yang fokus pada pinjaman UMKM dan beragam produk keuangan. Di sisi lain, Indonesia memiliki platform seperti Modalku, Modal Rakyat, dan Akseleran yang menyediakan berbagai pinjaman termasuk syariah. Ketika algoritma dan transaksi virtual

menggantikan interaksi tatap muka, masalah kepercayaan menjadi krusial. Dari sisi investasi, tak mudah untuk mempercayakan uang hasil jerih payah ke platform online karena absennya kehadiran sosial atau fisik. Penelitian menunjukkan bahwa kehadiran sosial bisa meningkatkan kepercayaan ketika seseorang melakukan transaksi keuangan, misalnya ketika berbelanja. Minimnya kepercayaan berpotensi membuat start-up yang bergerak di industri keuangan mengalami kesulitan dalam mengakuisisi ataupun mendistribusikan dana. Misalnya, investor potensial bisa saja merasa khawatir dan tak aman untuk menanamkan uang mereka di start-up crowdlending yang menawarkan platform investasi online sebab perusahaan belum memiliki reputasi yang mapan.

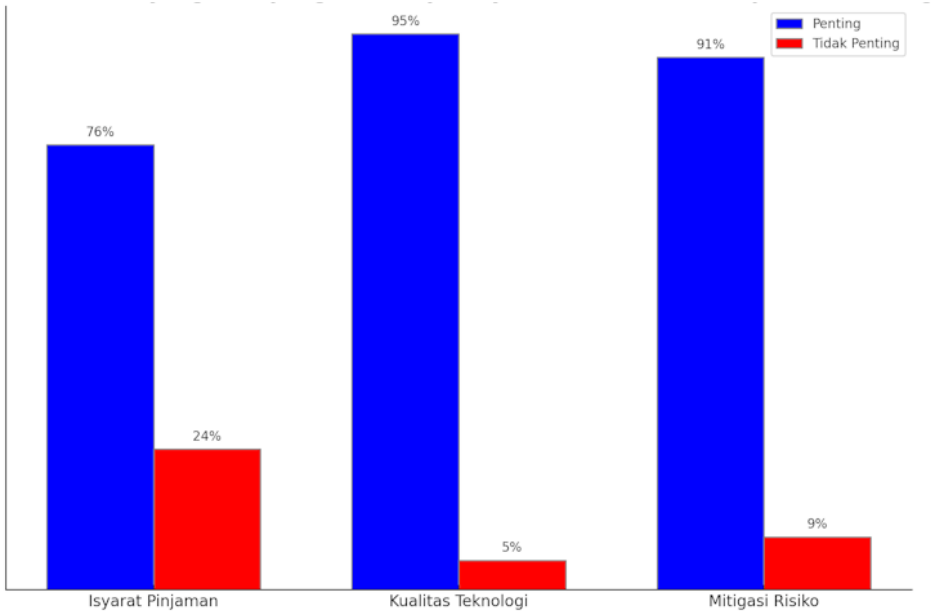
Menetapkan kepercayaan antara platform dan penggunanya untuk memastikan pengalaman investasi yang aman dan terpercaya amatlah penting. Untuk memahami bagaimana sebenarnya investor membangun kepercayaannya terhadap crowdlending, tim peneliti dari Monash University, Singapore Institute of Technology, dan George Washington University melakukan penelitian dengan menggunakan survei berbasis kuesioner[122]. Data dikumpulkan dari partisipan yang sedang berinvestasi atau memiliki pengalaman meminjamkan uang di platform crowdlending di Singapura.

Membangun Kepercayaan di Arena Crowdlending

Crowdlending tumbuh pesat di Asia akibat peningkatan akses internet, kekecewaan terhadap perbankan tradisional, dan permintaan kredit yang tinggi dari UMKM dan individu. Selain itu, crowdlending memberikan layanan yang lebih cepat dan ringkas dibandingkan dengan perbankan tradisional. Platform online inovatif ini memungkinkan peminjam terhubung dengan pemberi pinjaman tanpa perlu perantara fisik tradisional serta menawarkan jalur investasi alternatif yang semakin populer bagi pemilik dana. Sama seperti bentuk pinjaman yang lain, crowdlending melibatkan risiko potensial bagi investor seperti peminjam yang gagal bayar. Untuk meminimalkan risiko ini, platform selayaknya beroperasi di bawah lisensi dan regulasi resmi oleh otoritas keuangan, untuk di Indonesia misalnya Otoritas Jasa Keuangan (OJK).

[122] https://link.springer.com/article/10.1007/s12525-023-00650-7

Untuk melihat apa upaya yang dibutuhkan dalam membangun kepercayaan terhadap platform crowdlending yang tengah pesar berkembang ini, kami mengumpulkan jawaban kuisioner dari 232 partisipan. Karakteristik sampel menunjukkan bahwa sebagian besar responden berusia antara 26 hingga 35 tahun, dengan latar belakang industri yang beragam, termasuk keuangan dan asuransi, serta aktivitas teknis. Kuesioner yang kami susun mencakup tujuh variabel, yakni isyarat pinjaman, manfaat yang dirasakan, mitigasi risiko, isyarat peminjam (aktivitas dan riwayat peminjam), pengaruh sosial, kualitas teknologi yang dirasakan, dan kepercayaan dalam crowdlending (lihat Gambar 8). Kami menyempurnakan metode pengukurannya dengan berkonsultasi dengan praktisi dari sebuah perusahaan start-up crowdlending di Singapura.



Gambar 8. Perbandingan tiga dimensi terpenting yang memengaruhi seseorang menggunakan crowdlending.

Penelitian ini mendukung hipotesis bahwa isyarat peminjam, mitigasi risiko, dan kualitas yang dirasakan, berpengaruh positif terhadap kepercayaan dalam crowdlending. Isyarat pinjaman berkaitan dengan informasi bunga dan tenor pinjaman. Bunga yang tinggi menandakan pinjaman berisiko tinggi. Mitigasi risiko adalah langkah antisipasi jika

terjadi gagal bayar oleh peminjam. Untuk melindungi investor, platform crowdlending seharusnya mengasuransikan pinjaman agar pokok investasi tetap bisa dikembalikan jika terjadi gagal bayar. Sementara, kualitas teknologi platform berkaitan dengan ketersediaan fitur, dukungan dari platform, dan kemudahan fasilitas yang diberikan kepada investor untuk menavigasi platform crowdlending dan melakukan penelusuran mengenai investasi yang sudah mereka lakukan di crowdlending.

Sebagian besar responden menganggap ketiga faktor tersebut penting: 76% untuk isyarat pinjaman, 95% untuk kualitas teknologi, dan 91% untuk mitigasi risiko. Artinya, ketiga faktor tersebut berkontribusi pada pembentukan kepercayaan investor ketika mereka menginvestasikan uangnya di platform crowdlending. Namun, penelitian ini tidak menemukan dukungan yang signifikan untuk hipotesis terkait isyarat pinjaman, manfaat yang dirasakan, serta pengaruh sosial yang memengaruhi kepercayaan dalam crowdlending.

Strategi Kunci untuk Menjamin Pertumbuhan Industri

Penelitian kami mengidentifikasi strategi kritis bagi penyedia crowdlending, baik yang ada sekarang maupun yang akan berdiri di masa mendatang. Rekomendasi kami menekankan pentingnya menjaga keseimbangan antara kepercayaan dan manajemen risiko yang efektif.

Rekomendasi bagi Platform

1. Kedalaman data peminjan

Salah satu aspek kritis dari platform crowdlending adalah merekam informasi peminjam yang komprehensif untuk pinjaman pribadi dan bisnis. Kedalaman data peminjam ini sangat penting dalam membantu pemberi pinjaman menilai kepercayaan calon klien secara akurat.

2. Melibatkan pihak ketiga untuk verifikasi

Platform dapat menerapkan mekanisme untuk memverifikasi informasi peminjam untuk membangun kepercayaan melalui institusi pihak ketiga yang terpercaya, seperti biro

kredit atau lembaga pemerintah. Pendekatan ini membantu mengatasi masalah seleksi yang merugikan, yakni ketika pemberi pinjaman mungkin memberikan kredit kepada peminjam berisiko tinggi karena asimetri informasi.

3. Perkuat mitigasi risiko

Manajemen risiko yang efektif sangat penting bagi crowdlending untuk melindungi kepentingan investor. Ini termasuk kepatuhan regulasi, pembentukan dana cadangan, asuransi kredit, dan jaminan fidusia yang menjamin si pemberi kredit apabila sewaktu-waktu terjadi wanprestasi (janji dilanggar atau gagal bayar). Di Indonesia dan Singapura, perusahaan crowdlending harus melaporkan rasio pinjaman yang memiliki kinerja baik dan sebaliknya kepada otoritas moneter setempat. Hal ini membantu menawarkan wawasan tentang keberhasilan platform dalam memenuhi kewajiban pinjaman. Pendekatan inovatif terhadap jaminan dalam crowdlending juga patut dicatat. Tidak seperti bank tradisional yang memerlukan aset nyata, beberapa platform crowdlending mengadopsi jaminan fidusia. Ini memungkinkan peminjam terus menggunakan aset jaminan mereka sambil memberikan jaring pengaman bagi pemberi pinjaman dalam kasus gagal bayar.

Rekomendasi bagi Individu

1. Teliti platform

Investor potensial harus meneliti secara menyeluruh riwayat platform dan tingkat gagal bayar pinjaman. Jika memberi pinjaman, pemilik modal sebaiknya mendiversifikasi investasi di berbagai pinjaman untuk menyebar risiko.

2. Cek pelindungan dari risiko

Investor perlu mempertimbangkan platform yang menawarkan skema asuransi atau pelindungan bagi pemberi pinjaman dan peminjam.

3. Pahami persyaratan dan bunga

Jika meminjam, sangat penting untuk memahami sepenuhnya syarat-syarat, termasuk tingkat bunga dan denda. Terus menyimak informasi tentang perubahan regulasi dan tren industri juga sangat penting.

Modal Kepercayaan

Pada dasarnya, seperti banyak lembaga keuangan, crowdlending bergantung pada kepercayaan, yang dapat ditingkatkan secara efektif melalui teknologi canggih, regulasi yang kuat, dan strategi manajemen risiko. Platform crowdlending harus berfokus pada pembangunan kepercayaan melalui informasi peminjam yang transparan dan strategi manajemen risiko yang kuat, sehingga mendorong ekosistem crowdlending yang lebih aman dan terpercaya bagi semua pihak yang terlibat.

Tautan artikel:

https://theconversation.com/riset-crowdlending-bagaimana-meningkatkan-kepercayaan-investor-di-tengah-sentimen-negatif-pinjol-229926

Fintech Tak Hanya Pinjol: Mengenal Teknologi Finansial dan Potensi Risikonya di Indonesia

Arif Perdana

Konteks: Artikel ini diterbitkan di The Conversation Indonesia tanggal 31 Mei 2023. Di sini saya menjelaskan tentang perkembangan dan tantangan teknologi finansial (tekfin) di Indonesia, yang sering disalahartikan sebagai pinjaman online (pinjol). Tekfin mencakup berbagai layanan keuangan berbasis teknologi, namun menghadapi masalah seperti pinjol ilegal dan potensi bias dalam algoritma. Regulasi yang kuat, termasuk *regulatory sandbox* oleh OJK, diperlukan untuk memastikan keamanan dan keberlanjutan industri. Selain itu, penting untuk mengatasi risiko etika dan hukum terkait penggunaan algoritma dalam penilaian kredit dan layanan keuangan lainnya.

Masyarakat kerap menyamakan *fintech* atau teknologi finansial (tekfin) dengan pinjaman online (pinjol). Bahkan, jika kita mencari definisi tekfin di *Google*, perangkat tersebut menampilkan "apakah tekfin sama dengan pinjol?" sebagai salah satu pertanyaan yang paling sering dicari. Penting bagi kita untuk memahami teknologi ini sekaligus tantangan dan risikonya. Sebab, pertumbuhan jasa keuangan digital di Indonesia amat pesat.

Tekfin adalah perangkat teknologi yang menjadi landasan model bisnis perusahaan rintisan yang bergerak di bidang keuangan. Teknologi ini meliputi AI, *blockchain*, sains dan analitika data, dan keamanan siber. Tekfin bertujuan membuat layanan keuangan menjadi lebih cepat dan mudah lewat jasa pembayaran, pinjam-meminjam, perbankan digital, asuransi, investasi, pengelolaan keuangan pribadi, dan pengelolan keuangan bisnis. Laporan yang diterbitkan *AC Ventures* dan *Boston Consulting Group* pada Maret lalu menyatakan jumlah perusahaan tekfin yang beroperasi di Indonesia meningkat enam kali lipat dari 51 pada 2011 menjadi 334 pada 2022[123]. Sektor pembayaran menjadi penggerak utama pertumbuhan industri ini.

Perluasan jangkauan tekfin ke manajemen kekayaan (*wealth-tech*) dan asuransi (*insurtech*) menunjukkan bahwa ekosistem tekfin di Indonesia semakin matang.

[123] https://acv.vc/insights/acv-portfolio-news/ac-ventures-boston-consulting-group-fintech-report/

Perusahaan-perusahaan rintisan baru kini menawarkan berbagai produk dan layanan inovatif seperti pembelian saham, reksadana, asuransi, serta pengajuan klaim secara daring. Pertumbuhan tekfin diharapkan mampu mempercepat inklusi keuangan di Indonesia, dengan semakin banyaknya masyarakat yang bisa mendapatkan layanan keuangan dan meningkatkan kesejahteraan mereka. Tabel 13 memperlihatkan statistik penyelenggara Fintech Lending di Indonesia hingga Mei 2023.

Tabel 13. Overview Penyelenggara Fintech Lending[124]

Uraian	Jumlah Penyelenggara (Unit)	Total Aset (miliar Rp)	Total Liabilitas (miliar Rp)	Total Ekuitas (miliar Rp)
Penyelenggara Konvensional	95	6.29	3.11	3.18
Penyelenggara Syariah	7	0.13	0.12	0.01
Total	**102**	**6.42**	**3.23**	**3.19**

Pertumbuhan Tekfin dengan Berbagai Masalahnya

Indonesia pertama kali mengenal tekfin pada 2007 ketika salah satu bank swasta nasional, BCA meluncurkan platform uang elektronik untuk memfasilitasi pembayaran. Namun, industri tekfin di Indonesia baru menggeliat di tahun 2015 ketika perusahaan-perusahaan rintisan yang bergerak di layanan pinjaman online menjamur. Melihat perkembangan ini, Otoritas Jasa Keuangan (OJK) mengeluarkan Peraturan Otoritas Jasa Keuangan (POJK) Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi pada 2016[125].

Pada awal 2017, OJK mewajibkan perusahaan rintisan tekfin untuk mendapatkan izin dari mereka. Salah satu alasannya adalah beberapa tekfin terlibat investasi bodong. Daftar perusahaan yang sudah diizinkan oleh OJK kemudian mulai dipublikasikan sejak awal 2018. Jumlahnya saat itu mencapai 40 korporasi. Jumlah ini terus berkembang

[124] https://ojk.go.id/id/kanal/iknb/data-dan-statistik/fintech/Pages/Statistik-Fintech-Lending-Periode-Mei-2023.aspx

[125] https://www.ojk.go.id/id/regulasi/otoritas-jasa-keuangan/peraturan-ojk/Documents/Pages/POJK-Nomor-77-POJK.01-2016/SAL%20-%20POJK%20Fintech.pdf

mencapai sekitar 160 perusahaan di tahun 2020. Pada 2020, OJK melakukan moratorium pendaftaran perusahaan tekfin. Tujuannya untuk memastikan bahwa platform yang sudah terdaftar menjadi berizin dan benar-benar patuh terhadap regulasi, memiliki kapasitas yang memadai, dan bisa menjaga keberlanjutan sumber daya mereka dalam menjalankan usaha.

Pada layanan tekfin pinjam-meminjam, permasalahan muncul baik dari sisi peminjam (debitur) dan yang meminjamkan (kreditur). Maraknya pinjol ilegal yang menarik debitur potensial dengan persyaratan yang mudah berujung pada berbagai permasalahan seperti bunga yang mencekik, kebocoran data, hingga ancaman fisik dan psikologis saat penagihan. Di sisi lain, kreditur-kreditur juga berpotensi merugi jika peminjam tak mampu melunasi utangnya. Apalagi jika dana yang disalurkan tidak diasuransikan oleh perusahaan tekfin. Kasus gagal bayar TaniFund, yang menghubungkan antara kreditur dan debitur, misalnya, terjadi salah satunya karena para petani sebagai peminjam mengalami gagal panen.

Perkembangan Regulasi

Apa yang dialami oleh Indonesia sebenarnya tidak jauh berbeda dengan Cina. Sebelum 2015, Cina mengambil pendekatan yang lunak terhadap layanan tekfin pinjam-meminjam untuk mengakselerasi praktik baru dan inovatif. Namun, pada 2015, ledakan tekfin pinjam-meminjam menghadirkan banyak masalah. Pemerintah Cina terpaksa mengambil tindakan seperti pembatasan jumlah perusahaan tekfin pinjam-meminjam, peninjauan kembali perizinan dan persyaratan, dan pembatasan perilaku berisiko oleh peminjam dan pemberi pinjaman.

Berbeda dengan Cina daratan, Hong Kong menggunakan pendekatan yang lebih hati-hati melalui *regulatory sandbox*. Aturan ini memungkinkan perusahaan tekfin untuk menguji coba layanan dan produk mereka di ekosistem terbatas, sebelum meluncurkannya ke masyarakat luas. Otoritas keuangan dan perusahaan kemudian dapat menilai risiko dari layanan dan produk tersebut dari berbagai perspektif sehingga upaya mitigasi risiko dapat direncanakan dengan baik.

Pemerintah Indonesia sudah memiliki peraturan serupa sebagai landasan inovasi tekfin yaitu POJK 13 /POJK.02/2018 tentang Inovasi Keuangan Digital Di Sektor Jasa Keuangan[126]. Ada juga Peraturan Bank Indonesia Nomor 19/12/PBI/2017 tentang Penyelenggaraan Teknologi Finansial[127]. *Regulatory sandbox* yang diterapkan OJK ini bertujuan untuk memastikan penyelenggara inovasi keuangan digital memenuhi beberapa kriteria. Di antaranya adalah inovatif, berorientasi ke depan, menggunakan TI dan komunikasi, mendukung inklusi dan literasi keuangan, dapat diintegrasikan pada layanan keuangan yang telah ada, memperhatikan aspek pelindungan konsumen dan data, dan menggunakan pendekatan kolaboratif. Dengan adanya landasan hukum ini, pemerintah seharusnya bisa menilai dan mengevaluasi inovasi-inovasi tekfin lebih baik lagi.

Masalah Tekfin Apa yang Berpotensi Terjadi di Indonesia?

Penggunaan tekfin seperti perangkat teknologi yang berbasis algoritma (AI, pemelajaran mesin, dan sains data) memiliki konsekuensi merugikan jika tidak dikelola dengan baik dan didukung oleh regulasi yang jelas. Penggunaan sistem algoritma ini berpotensi melanggar aspek-aspek etika seperti privasi, bias, dan akuntabilitas. Perusahaan-perusahaan yang mengumpulkan data-data pribadi dan rahasia dari pelanggan mereka harus berhati-hati mengelola, menganalisis dan menjaga keamanannya. Kecerobohan perusahaan bisa menimbulkan masalah kebocoran data dan profiling yang tidak seharusnya (bias). Profiling merujuk pada penggunaan algoritma untuk menilai atau memprediksi aspek-aspek pribadi seperti perilaku, keadaan ekonomi, kesehatan, kepribadian, preferensi–biasanya untuk menentukan layak tidaknya seseorang menerima pinjaman.

Penggunaan algoritma AI untuk menentukan apakah calon debitor memiliki potensi gagal atau sukses bayar, juga berpotensi bias–baik karena datanya maupun algoritmanya. Bias ini dapat memperburuk ketimpangan kelompok mayoritas dengan

[126] https://www.ojk.go.id/id/regulasi/Documents/Pages/Inovasi-Keuangan-Digital-di-Sektor-Jasa-Keuangan/pojk%2013-2018.pdf

[127] https://peraturan.bpk.go.id/Details/135776/peraturan-bi-no-1912pbi2017-tahun-2017

kelompok minoritas karena kurangnya representasi data mereka. Di Indonesia, bias dalam penggunaan algoritma layanan tekfin ini memang belum terliput oleh media dan menjadi kasus. Namun, di Amerika Serikat, kasus ini sudah terjadi. Studi yang dilakukan oleh *University of California, Berkeley* terhadap lembaga pemberi pinjaman, baik daring maupun luring memperlihatkan bahwa mereka cenderung membebankan suku bunga yang lebih tinggi kepada peminjam dari ras Afrika-Amerika dan Latin. Sebab, sistem algoritma dilatih dengan data yang bias dan tidak seimbang: data ras kulit putih yang bisa dianalisis secara digital lebih banyak dari data ras Afrika-Amerika dan Latin.

Studi lain di sektor asuransi menunjukkan adanya bias terhadap kelompok minoritas dan gender dalam penetapan premi asuransi. Bias juga bisa terjadi karena adanya variabel proksi yang membuat algoritma AI melakukan diskriminasi. Variabel proksi punya korelasi dengan variabel lain, terutama yang bersifat pribadi atau yang seharusnya diproteksi (ras, gender, agama, dan lain sebagainya). Karena korelasinya kuat, variabel proksi bisa saja mengungkapkan atau memprediksi data privasi seseorang ketika digunakan untuk melatih AI. Misalnya, kode pos di area tertentu bisa mengungkap apakah seseorang merupakan ras atau etnik tertentu. Jika tidak dikelola dengan saksama, bias akan mengakibatkan diskriminasi digital di antara kelompok masyarakat.

Mitigasi Risiko Tekfin

Dalam menjelajahi potensi tekfin, pemerintah dan perusahaan perlu memperhatikan empat dimensi kritis, yaitu tata kelola, etika, hukum, dan dampak sosial. Informasi yang dihasilkan dari sistem algoritma harus bisa dijelaskan (explainable). Proses pengambilan keputusan oleh sistem itu juga harus transparan. Sebab, jika terjadi masalah hukum, mekanisme penjelasan dan transparansi ini menjadi bukti untuk menentukan bagaimana permasalahan sistem algoritma ini harus diselesaikan.

Sebagai contoh, jika terjadi bias yang mengakibatkan seorang nasabah mendapatkan diskriminasi dan berdampak ekonomi, sistem peradilan harus bisa menentukan siapa yang bertanggung jawab dan bagaimana mekanisme penyelesaian hukum dan kompensasi harus dilakukan. Di sisi teknis, ada beberapa cara yang bisa digunakan untuk memitigasi resiko etika dan bias di algoritma. Contohnya dengan

penggunaan teknik mitigasi bias algoritma AI; dokumentasi tata kelola dan analisis data seperti transparansi dalam pengumpulan, penyimpanan dan penggunaan dataset untuk melatih algoritma AI; juga antisipasi mengenai kemungkinan bias-bias yang bisa terjadi karena penggunaan algoritma seperti prediksi, klasifikasi, dan klusterisasi.

Di sisi regulasi, pemerintah harus berfokus kepada mitigasi risiko teknologi, pelindungan terhadap konsumen, dan aturan yang ketat terhadap penggunaan sistem algoritma. Uni Eropa, misalnya, sedang mengajukan usulan UU AI untuk menjamin kepastian hukum penggunaan teknologi yang berbasis algoritma. Alih-alih memperkuat keuangan inklusif, pengabaian aspek tata kelola, etika, hukum, dan dampak sosial bisa memicu kesenjangan sosial. Warga negara juga bisa kehilangan kesempatan mendapatkan layanan keuangan yang lebih baik.

Tautan artikel:

https://theconversation.com/fintech-tak-hanya-pinjol-mengenal-teknologi-finansial-dan-potensi-risikonya-di-indonesia-203566

Epilogue

Revolusi digital telah membawa kita pada titik kritis dalam perjalanan peradaban manusia. Kecerdasan buatan (AI), keamanan siber, dan fintech bukan lagi sekadar alat bantu, melainkan kekuatan besar yang secara mendalam mengubah struktur sosial, politik, dan ekonomi. Namun, seperti yang telah kita bahas dalam bab-bab sebelumnya, perjalanan menuju masa depan digital yang ideal penuh dengan tantangan besar yang memerlukan pendekatan kritis dan transformasi menyeluruh.

Apa yang Masih Menjadi Masalah?

Regulasi yang saat ini ada sering kali lamban dan reaktif. Meski Uni Eropa telah mengambil langkah maju melalui EU AI Act, dan Indonesia memulai dengan UU PDP, kenyataannya adalah sebagian besar regulasi tertinggal dari laju inovasi teknologi. Pendekatan "tunggu dan lihat" tidak lagi relevan. Kita memerlukan regulasi yang proaktif dan mampu beradaptasi dengan cepat, seiring evolusi teknologi yang mereka atur. Inovasi teknologi juga kerap memperlebar jurang kesenjangan digital. Di tengah kemajuan pesat, masih banyak individu dan komunitas yang tertinggal, memperdalam ketidaksetaraan sosial-ekonomi. Ini bukan sekadar masalah akses, tetapi juga tentang literasi dan kapabilitas digital yang merata di seluruh lapisan masyarakat.

Keamanan siber menjadi isu yang semakin krusial, dengan insiden kebocoran data dan serangan siber yang terus meningkat di Indonesia. Kegagalan sistemik dalam melindungi infrastruktur digital kita menunjukkan bahwa masalah ini bukan sekadar persoalan teknologi, tetapi mencerminkan perlunya perubahan dalam budaya dan prioritas nasional.

Pengembangan AI sering kali didorong oleh motif keuntungan, mengabaikan implikasi etis yang lebih luas. Kita harus mempertanyakan apakah kemajuan teknologi yang kita kejar benar-benar meningkatkan kualitas hidup atau justru mengancam nilai-

nilai kemanusiaan. Di sisi lain, hype seputar AI dan fintech berisiko menciptakan gelembung ekonomi yang berbahaya. Overvaluasi dan spekulasi berlebihan dapat mengguncang stabilitas ekonomi dalam jangka panjang.

Refleksi dan Panduan untuk Perubahan

Bagi pemerintah, pendekatan regulasi harus lebih proaktif. Mereka harus antisipatif terhadap tren teknologi global dan segera merancang kerangka regulasi yang fleksibel. Selain itu, investasi besar dalam pendidikan digital harus menjadi prioritas nasional untuk meningkatkan literasi dan daya saing. Keamanan siber juga harus diutamakan, dengan membentuk satuan tugas khusus yang melibatkan ahli multidisiplin guna merancang strategi keamanan yang komprehensif.

Korporasi harus melihat etika sebagai keunggulan kompetitif yang nyata. Transparansi dalam pengembangan algoritma AI akan meningkatkan kepercayaan publik, sementara fokus pada pelatihan ulang karyawan merupakan langkah bijak dalam menghadapi otomatisasi.

Masyarakat juga perlu mengembangkan kesadaran kritis terhadap teknologi baru. Kita harus lebih sering bertanya, "Haruskah ini dilakukan?" daripada hanya mempertimbangkan "Bisakah ini dilakukan?". Partisipasi aktif dalam diskusi publik mengenai kebijakan teknologi menjadi keharusan, dan pembelajaran seumur hidup harus dijadikan prioritas pribadi agar kita tetap relevan di era digital.

Penutup

Masa depan digital bukanlah takdir yang tidak bisa diubah, melainkan pilihan yang harus kita buat dan perjuangkan bersama. Kita berada di persimpangan kritis, dan keputusan yang kita ambil hari ini akan menentukan arah landscape digital di masa depan. Diperlukan perubahan paradigma radikal: dari pendekatan yang reaktif menuju proaktif, dari fokus jangka pendek ke keberlanjutan jangka panjang, dan dari inovasi yang tak terkendali menjadi inovasi yang bertanggung jawab. Hanya dengan pendekatan yang holistik, kritis, dan etis kita bisa memastikan bahwa revolusi digital ini akan melayani kepentingan kemanusiaan, bukan menguasainya.

Panggilan ini bukanlah untuk memperlambat inovasi, melainkan untuk mengarahkan dengan lebih bijaksana. Ini adalah ajakan untuk membangun masa depan digital yang tidak hanya canggih, tetapi juga adil, inklusif, dan berkelanjutan. Taruhannya sangat besar, namun dengan tekad bersama, kita bisa menghadapi tantangan tersebut dan menyambut era digital dengan penuh optimisme dan tanggung jawab.

Profil Penulis dan Rekan Penulis

Arif Perdana

Penelitian Dr. Perdana menjelaskan bagaimana teknologi digital seperti sistem algoritma, pemelajaran mesin, AI, analitika data, dan blockchain dapat mengubah berbagai sektor, mulai dari keuangan, pendidikan, hingga layanan kesehatan. Penelitiannya wawasan tentang tantangan dalam mengadopsi teknologi ini, sambil mencari cara untuk memanfaatkan teknologi secara efektif di berbagai bidang. Saat ini, ia fokus pada penggunaan AI yang bertanggungjawab di bidang keuangan, penggunaan blockchain dalam bisnis, dan algoritma pemelajaran mesin. Beragam penelitian ini menunjukkan portofolionya yang luas dan dedikasinya dalam mengatasi tantangan di dunia digital. Arif saat ini bekerja sebagai Associate Professor di Monash University dengan spesialisasi di strategi digital, ilmu data, dan manajemen sistem informasi. Ia memiliki pengalaman lebih dari sepuluh tahun di berbagai universitas ternama, seperti *Singapore Institute of Technology*, *Aarhus University*, dan *University of Queensland*. Sebelum terjun ke dunia akademis, Arif pernah bekerja di sektor layanan teknologi informasi dan keuangan, sehingga memiliki pemahaman yang mendalam di bidang tersebut. Sejak Desember 2022, ia juga menjabat sebagai Direktur *Action Lab Research Network*, Indonesia, Monash University. Arif telah berhasil mendapatkan berbagai pendanaan untuk penelitiannya, termasuk dari lembaga di Singapura, badan pendanaan di Australia, serta pemerintah dan perusahaan di Indonesia. Beberapa proyek penelitian yang ia dapatkan di antaranya adalah *Monash Data Future Institute* (MDFI), *Whyte Fund*, hibah penelitian dari Bank Indonesia, dan *Singapore Institute of Technology Ignition Grants*.

Bayu Anggorojati

Dr. Anggorojati adalah Asisten Profesor di bidang Keamanan Siber di Monash University, Indonesia. Ia meraih gelar PhD dalam Pengendalian Akses untuk sistem IoT dan Cloud, serta gelar Magister dalam Komunikasi Seluler dari *Aalborg University*, Denmark, masing-masing pada tahun 2015 dan 2007. Selama menjabat sebagai peneliti di *Aalborg University*, Bayu terlibat dalam beberapa proyek yang didanai oleh Uni Eropa di bidang middleware RFID, tele-health untuk lansia, dan platform *IoT Cloud*. Sebelum bergabung dengan Monash Indonesia, ia adalah dosen di Fakultas Ilmu Komputer Universitas Indonesia (UI). Minat penelitiannya mencakup jaringan komputer dan keamanan, keamanan informasi, blockchain, aspek keamanan dalam pemelajaran mesin, aspek manusia dalam keamanan siber, dan pendidikan keamanan.

Derry Wijaya

Dr. Wijaya melakukan penelitian dalam bidang pemrosesan bahasa alami (*natural language processing*/NLP), dengan fokus pada penerapan pemelajaran mesin, pemelajaran mendalam (*deep learning*), dan model bahasa besar (*large laguage models*/LLMs) untuk NLP multibahasa. Penelitiannya mencakup penerjemahan mesin (*machine translation*/MT), yang bertujuan untuk memanfaatkan bahasa yang memiliki banyak anotasi untuk memperbaiki penerjemahan bahasa yang kurang teranotasi. Ia juga mengeksplorasi bagaimana gambar, tugas terkait, augmentasi data, dan LLM dapat digunakan untuk memperbaiki representasi dan penerjemahan bahasa dengan data pelatihan yang terbatas. Dr. Wijaya juga meneliti metode untuk secara otomatis mempelajari makna kata kerja dan mengekstraksi informasi untuk memperkaya basis pengetahuan melalui analisis berbagai sumber informasi. Melalui kolaborasi lintas disiplin, Dr. Wijaya telah melakukan penelitian tentang penerapan NLP untuk framing berita komputasional dan kesehatan masyarakat, khususnya dalam mendeteksi dan menganalisis bagaimana artikel di media tradisional dan baru membahas isu-isu publik atau kesehatan masyarakat. Dr. Wijaya juga melakukan penelitian tentang analisis bias dan misinformasi, baik dalam model AI maupun dalam komunikasi publik. Dr. Wijaya menyelesaikan postdoc di University of Pennsylvania dan gelar PhD dari *Carnegie Mellon University*. Ia memperoleh gelar Sarjana dan Magister di bidang Ilmu Komputer dari *National University of Singapore*.

Grace Wangge

Dr. Wangge adalah seorang dokter dan epidemiolog yang mengkhususkan diri dalam Kebijakan Kesehatan Masyarakat dan Pengembangan Obat. Dengan gelar kedokteran dari Universitas Indonesia dan gelar PhD dalam Farmakoepidemiologi dari *Utrecht Universiteit*, ia membawa pengetahuan dan keahlian yang luas di bidangnya. Program postdoktoralnya di *Harvard Medical School/Brigham and Women's Hospital* semakin memperdalam pemahamannya tentang praktik kesehatan. Saat ini, ia menjabat sebagai Associate Professor untuk program Magister Kesehatan Masyarakat di Monash University, Indonesia. Sejak kembali ke Indonesia pada tahun 2014, Dr. Wangge aktif terlibat dalam penelitian yang berfokus pada pengobatan komunitas, nutrisi masyarakat, kebijakan kesehatan masyarakat, dan farmakovigilans. Ia memiliki pengalaman luas dalam penelitian berbasis masyarakat, peningkatan kapasitas, serta evaluasi program kesehatan dan nutrisi di layanan kesehatan primer di seluruh Indonesia. Minat penelitian saat ini mencakup kesehatan masyarakat, tata kelola kesehatan digital, farmakovigilans, dan komunikasi ilmu kesehatan. Sebagai pakar di bidangnya, Dr. Wangge pernah menjabat sebagai Ahli Kesehatan Nasional untuk Kelompok Kerja Kesehatan 3 Presidensi G20 Indonesia. Ia merupakan advokat yang bersemangat untuk memperbaiki ekosistem uji klinis di Indonesia dan aktif berpartisipasi dalam inisiatif untuk memajukan praktik kesehatan. Dedikasi Dr. Wangge melampaui profesi, karena ia juga gemar

mempromosikan literasi media sosial dan menangkap keindahan Indonesia yang memukau melalui fotografi.

Ika Idris

Dr. Idris adalah seorang pakar di bidang analitika media sosial. Selama studi doktoralnya sebagai penerima beasiswa Fulbright di *Ohio University*, ia menjadi peneliti di Social Media Research Team Lab/SMARTLab universitas tersebut. Pada tahun 2020, Dr. Idris menjadi peserta pertama dari luar Amerika Serikat yang mengikuti pelatihan di PhD *Digital Bootcamp* di *Texas State University*. Sebelum bergabung dengan Monash Indonesia, dari tahun 2019-2021, Ika menjabat sebagai Direktur Penelitian di Paramadina Public Policy Institute, Universitas Paramadina. Ia juga menjadi asisten profesor di Paramadina Graduate School of Communication sejak tahun 2009. Minat penelitiannya mencakup analitika media sosial, komunikasi pemerintah, kebijakan platform digital, dan literasi digital. Dengan latar belakang di bidang media dan komunikasi, Dr. Idris meyakini bahwa rencana komunikasi strategis sangat penting dalam mempromosikan kebijakan publik dan memberikan layanan publik. Ia memiliki pengalaman dalam konsultasi dengan berbagai lembaga pemerintah, terutama dalam implementasi kebijakan, penyampaian layanan, dan evaluasi kebijakan. Beberapa pekerjaan konsultasinya termasuk melakukan survei nasional dan analisis pemangku kepentingan untuk Komisi Pemberantasan Korupsi, melakukan evaluasi layanan pusat pelayanan terpadu dan Jakarta Smart City untuk Pemerintah Provinsi DKI Jakarta, serta merancang prosedur layanan informasi publik untuk Direktorat Jenderal Bina Marga, Kementerian Pekerjaan Umum dan Perumahan Rakyat. Dr. Idris telah membantu Badan Penelitian dan Pengembangan Sumber Daya Manusia Kementerian Komunikasi dan Informatika dalam merancang dan mengembangkan kurikulum pelatihan pemerintah di bidang hubungan masyarakat pemerintah, hubungan masyarakat digital, dan analitika media sosial. Sejak tahun 2019, ia telah melatih komunikasi publik strategis dan analisis media sosial untuk pemerintah, termasuk pejabat dari Mahkamah Agung, Sekretariat ASEAN, satuan tugas media sosial Kepolisian Republik Indonesia, Komisi Pengawas Persaingan Usaha, Badan Pemeriksa Keuangan, Bank Indonesia, serta pemerintah daerah, kota, dan provinsi dari wilayah prioritas.

Muhamad Erza Aminanto

Dr. Aminanto meraih gelar Sarjana dan Magister di bidang teknik elektro dari Institut Teknologi Bandung (ITB), Indonesia, masing-masing pada tahun 2013 dan 2014, serta gelar Ph.D. dari School of Computing, *Korea Advanced Institute of Science and Technology* (KAIST), Korea Selatan, pada tahun 2018. Saat ini, ia adalah Asisten Profesor di Monash University Indonesia, program Keamanan Siber. Erza pernah menjadi peneliti di *National*

Institute of Information and Communications Technology (NICT), Tokyo, Jepang dalam bidang AI x Security, dan dosen di Universitas Indonesia (UI) untuk mata kuliah kejahatan siber. Ia juga menjabat sebagai Senior Research (Data) Scientist di Jakarta Smart City dan menjadi anggota dewan penasehat untuk beberapa organisasi pemerintah dan swasta. Minat penelitian saat ini mencakup keamanan informasi, kecerdasan buatan, deteksi anomali, deteksi intrusi, keamanan siber, transformasi digital, dan smart city.

Ridoan Karim

Dr. Karim adalah Dosen Hukum Bisnis dan Wakil Direktur Program Sarjana di School of Business, *Monash University Malaysia*. Ia mengajar dan meneliti di bidang hukum bisnis dan hukum siber. Dr. Karim pernah bertindak sebagai Konsultan dan Fellow dalam proyek yang didanai oleh University of Malaya, Malaysia, dan Monash Data Futures Institute (MDFI). Ia juga secara rutin memimpin sesi pelatihan profesional bekerja sama dengan Monash University, program Pemasaran Digital REHDA-Institute, Esselaro (organisasi riset yang berfokus pada lanskap sosial), serta berbagai entitas swasta dan publik. Pada tahun 2022, ia dianugerahi Monash School of Business Excellence Award dalam bidang penelitian sebagai pengakuan atas kontribusinya sebagai peneliti baru yang menjanjikan. Dr. Karim meraih gelar PhD dari University of Malaya, Malaysia. Ia juga memiliki gelar Master of Business Administration (MBA) dari University of Chichester, Inggris, Master of Comparative Laws (MCL) dari International Islamic University Malaysia (IIUM), dan Sarjana Hukum (LLB) dari BRAC University, Bangladesh.

Saru Arifin

Dr. Arifin saat ini adalah peneliti di Fakultas Ilmu Sosial, Universitas Islam Internasional Indonesia. Ia juga merupakan dosen tetap di Fakultas Hukum, Universitas Negeri Semarang, Indonesia. Publikasinya yang berkaitan dengan Hukum Internasional Publik, Hukum Hak Asasi Manusia, Hukum Konstitusi, dan studi Legislasi telah diterbitkan oleh Routledge, Brill, dan SAGE serta terindeks oleh Scopus. Selain menjadi anggota aktif berbagai organisasi internasional, Arifin juga menjabat sebagai direktur program di Institute for Migrant Rights di Cianjur, Jawa Barat, Indonesia (2016-Sekarang), kepala Klinik Advokasi Hukum dan Hak Asasi Manusia (2018-2020), serta anggota dewan editor dan reviewer di berbagai jurnal nasional dan internasional. Dr. Arifin memperoleh gelar PhD dengan disertasi berjudul "Memperkuat Legislasi Pekerja Migran Indonesia: Realitas dan Kebutuhan" di Fakultas Hukum, *Universitas Pecs*, Hongaria.

W. Eric Lee

Penelitian Dr. Lee terutama berfokus pada teknologi disruptif dan keberlanjutan. Dr. Lee adalah Professor Akuntansi di University of Northern Iowa. Publikasi dan proyek penelitiannya yang sedang berlangsung mencakup berbagai topik, seperti: bagaimana perusahaan akuntansi dapat lebih baik mengintegrasikan teknik automasi proses robotik mutakhir dalam tugas audit mereka, bagaimana pengguna teknologi AI dapat lebih efektif mengenali dan menangani masalah etika dan diskriminasi digital, bagaimana faktor terkait kepatuhan regulasi dan budaya pengguna kripto dapat memengaruhi penetapan standar di masa depan, bagaimana wacana media yang saling bersaing dapat digunakan untuk menjelaskan fenomena blockchain terkini, bagaimana narasi akuntansi keberlanjutan dapat dibingkai dengan bijak dan oportunistik untuk memengaruhi tindakan pemangku kepentingan, bagaimana isu gender dan keberagaman dapat berdampak pada pelaporan tanggung jawab sosial perusahaan serta hasil kinerja perusahaan, berbagai topik pedagogis terkait keberlanjutan lingkungan, pembelajaran pelayanan, dan keterlibatan komunitas, serta penelitian terkait investasi, komunikasi bisnis, dan deteksi penipuan.