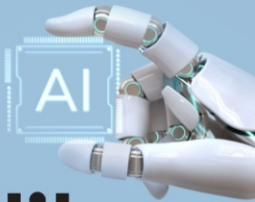


ATURAN PENGUNAAN Kecerdasan Buatan

di Sektor Swasta dan Publik



Dr. Ir. Agus Wibowo, M.Kom, M.Si, MM.

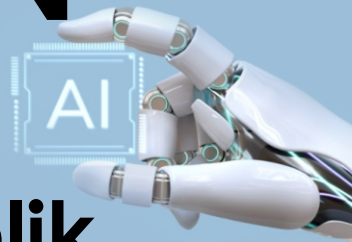


YAYASAN PRIMA AGUS TEKNIK



Dr. Ir. Agus Wibowo, M.Kom, M.Si, MM.

ATURAN PENGUNAAN Kecerdasan Buatan di Sektor Swasta dan Publik



YAYASAN PRIMA AGUS TEKNIK

PENERBIT :

YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

ISBN 978-634-7227-93-5 (PDF)



9

786347

227935

Aturan Penggunaan Kecerdasan Buatan (AI) di Sektor Swasta dan Publik

Penulis :

Dr. Ir. Agus Wibowo, M.Kom, M.Si, MM.

ISBN : 978-634-7227-93-5 (PDF)

Editor :

Dr. Joseph Teguh Santoso, S.Kom., M.Kom.

Penyunting :

Dr. Mars Caroline Wibowo. S.T., M.Mm.Tech

Desain Sampul dan Tata Letak :

Irdha Yuniarto, S.Ds., M.Kom

Penebit :

Yayasan Prima Agus Teknik Bekerja sama dengan
Universitas Sains & Teknologi Komputer (Universitas STEKOM)

Anggota IKAPI No: 279 / ALB / JTE / 2023

Redaksi :

Jl. Majapahit no 605 Semarang

Telp. 08122925000

Fax. 024-6710144

Email : penerbit_ypat@stekom.ac.id

Distributor Tunggal :

Universitas STEKOM

Jl. Majapahit no 605 Semarang

Telp. 08122925000

Fax. 024-6710144

Email : info@stekom.ac.id

Hak cipta dilindungi undang-undang

Dilarang memperbanyak karya tulis ini dalam bentuk dan dengan cara
apapun tanpa ijin dari penulis

KATA PENGANTAR

Dengan mengucapkan syukur yang mendalam kepada Tuhan Yang Maha Esa, kami dengan penuh sukacita mempersembahkan buku ini yang berjudul Aturan Penggunaan Kecerdasan Buatan (AI) di Sektor Swasta dan Publik. Lahir dari kebutuhan mendesak di tengah derasnya gelombang transformasi digital, buku ini hadir sebagai mercusuar bagi kita semua yang ingin memahami, mengatur, dan memanfaatkan AI secara bijak. Sebagai teknologi revolusioner yang mampu mengubah paradigma kerja, interaksi sosial, hingga pengambilan keputusan, AI bukan hanya peluang emas, tetapi juga tantangan etis yang menuntut kewaspadaan kolektif. Seperti kata Kai-Fu Lee, pakar AI terkemuka, "AI bukan masa depan yang jauh; ia sudah ada di sini, dan kita harus membentuknya agar melayani kemanusiaan."

Buku ini dirancang sebagai panduan komprehensif yang mudah dicerna, ditujukan bagi para profesional industri, akademisi pencari ilmu, pembuat kebijakan visioner, serta semua pemangku kepentingan yang ingin menerapkan AI dengan etis, bertanggung jawab, dan berkelanjutan. Dibagi menjadi sembilan bab yang saling terkait seperti benang merah, kami mengupas tuntas berbagai dimensi AI dari fondasi hingga aplikasi nyata, lengkap dengan studi kasus terkini, rekomendasi praktis, dan kerangka regulasi global.

Bab Pertama: Fondasi Konseptual membuka pintu dengan menjelaskan perbedaan mendasar antara AI, Data Science, dan Data Analytics. Di sini, pembaca akan memahami bagaimana AI bukan sekadar alat analisis data, melainkan sistem cerdas yang belajar dan beradaptasi seperti otak manusia, dilengkapi contoh sederhana seperti algoritma pengenalan gambar.

Bab Kedua: Geopolitik Kecerdasan Buatan menyelami lanskap global yang dinamis, termasuk perlombaan regulasi antarnegara besar seperti UE dengan AI Act-nya, AS dengan Executive Order Biden, dan China dengan kerangka etisnya sendiri. Kami bahas bagaimana ketegangan geopolitik memengaruhi akses teknologi dan standar internasional.

Bab Ketiga: Undang-Undang AI dan Pendekatan Berbasis Risiko menguraikan kerangka hukum utama, hak serta kewajiban penyedia layanan AI, dengan fokus pada klasifikasi risiko (rendah, tinggi, hingga terlarang) untuk memastikan transparansi, akuntabilitas, dan pencegahan bias.

Bab Keempat: Perlindungan Data dalam Ekosistem AI dan Bab Kelima: Hak Kekayaan Intelektual saling melengkapi, membahas GDPR, PDPA Indonesia, serta isu seperti kepemilikan data hasil generatif AI dan pelanggaran hak cipta akibat training model pada konten dilindungi.

Bab Keenam: Hukum Kontrak dan Teknologi Informasi mengeksplorasi klausul kontrak khusus AI, seperti tanggung jawab atas kesalahan algoritma dan force majeure digital, dengan template praktis untuk transaksi bisnis.

Bab Ketujuh: AI di Sektor Swasta menggali aplikasi di keuangan (fraud detection), manufaktur (prediksi maintenance), hingga pendidikan (personalisasi pembelajaran), disertai tantangan seperti pengangguran teknologi dan solusi adaptasi.

Bab Kedelapan: AI di Sektor Publik membahas peran AI dalam e-government, pengambilan keputusan publik yang adil, serta penguatan demokrasi melalui analisis sentimen pemilu, sambil waspada terhadap risiko pengawasan massal.

Bab Kesembilan: Panduan Etika AI yang Dapat Dipercaya menutup dengan prinsip-prinsip seperti fairness, robustness, dan human oversight, termasuk roadmap untuk membangun ekosistem AI nasional yang inklusif dan berkeadilan.

Kami berharap buku ini tak hanya menjadi rujukan berharga, melainkan pemicu diskusi mendalam, kolaborasi lintas sektor, dan aksi nyata. Mari bersama menjelajahi samudra kecerdasan buatan dengan kompas etika dan tangan terbuka, demi masa depan yang lebih cerah bagi generasi mendatang.

Akhir kata, kami ucapkan terima kasih yang sebesar-besarnya kepada para kontributor, reviewer, penerbit, dan keluarga yang telah mendukung perjalanan panjang ini. Semoga buku ini membawa manfaat abadi dan inspirasi tak terlupakan dalam menaklukkan era AI.

Selamat Membaca.....!!

Semarang, Februari 2026
Penulis

Dr. Ir. Agus Wibowo, M.Kom, M.Si, MM.

DAFTAR ISI

KATA PENGANTAR.....	ii
DAFTAR ISI.....	iv
BAB 1 AI, DATA SCIENCE, & DATA ANALYTICS: APA BEDANYA?	1
1.1 Pendahuluan.....	1
1.2 Landasan AI	1
1.3 Ilmu Data Dan Analisis Data	7
1.4 Pengembangan AI Di UKM	8
BAB 2 GEOPOLITIK KECERDASAN BUATAN.....	13
2.1 Pendahuluan.....	13
2.2 Lanskap Regulasi AI Yang Sedang Berkembang.....	13
2.3 Perlombaan Regulasi AI – Tiga Besar	17
BAB 3 HAK DAN KEWAJIBAN DALAM UU AI.....	24
3.1 Pengantar Undang-Undang AI.....	24
3.2 Pengantar Undang-Undang AI.....	25
3.3 Literasi AI Untuk Penyedia.....	36
3.4 Pendekatan Berbasis Risiko	47
3.5 Penilaian Dampak Hak Fundamental	76
3.6 Standar Yang Harmonis, Penilaian Kesesuaian, Sertifikat Dan Registrasi	89
3.7 Kewajiban Transparansi Dalam Undang-Undang AI.....	99
3.8 Kecerdasan Buatan Serbaguna (GPAI).....	105
3.9 Sandbox AI.....	112
3.10 Otoritas.....	119
3.11 Tata Kelola Dalam Undang-Undang AI	122
3.12 Sanksi Dan Hukuman.....	132
3.13 UKM Dan Perusahaan Rintisan Dalam Undang-Undang AI.....	134
BAB 4 PERLINDUNGAN DATA	143
4.1 Pendahuluan.....	143
4.2 Persyaratan Umum GDPR.....	144
4.3 Privasi Berdasarkan Desain.....	154
4.3 Persyaratan Untuk Data Pengujian	157
4.4 Pengambilan Keputusan Otomatis	158
4.5 Pedoman Otoritas Data: GDPR & AI	161
4.6 ChatGPT Dan Pengaduan Perlindungan Data Dari NOTB	169
BAB 5 HAK KEKAYAAN INTELEKTUAL	171
5.1 Pendahuluan.....	171
5.2 Perlindungan AI Dan Komponennya.....	172

5.3	Kepatuhan Hki Dalam Penggunaan AI.....	178
5.4	Daftar Periksa	183
5.5	Tabel Referensi Perundang-Undangan	183
BAB 6	HUKUM KONTRAK AI DAN TI	185
6.1	Pendahuluan.....	185
6.2	Lisensi Perangkat Lunak Standar	186
6.3	Pengembangan Perangkat Lunak	188
6.4	Pemeliharaan Perangkat Lunak	190
6.5	Perangkat Lunak Sumber Terbuka	191
6.6	Pembelian Dan Pemeliharaan Perangkat Keras.....	199
6.7	Informasi Umum Tentang Tanggung Jawab.....	199
BAB 7	SEKTOR SWASTA.....	203
7.1	AI – Dari Prasangka Ke Diskriminasi	203
7.2	AI Di Sektor Keuangan	217
7.3	AI Dalam Industri Asuransi	227
7.4	AI Dan Pelaporan Pelanggaran	230
7.5	Evolusi AI Dalam Hubungan Kerja	241
7.6	AI Dalam Pendidikan.....	246
7.7	AI Dalam Perawatan Kesehatan	253
7.8	AI Dalam Periklanan	258
7.9	Pariwisata	263
7.10	AI Dalam Pengemudian Otonom.....	277
BAB 8	SEKTOR PUBLIK	284
8.1	“Pengambilan Keputusan Publik” Dan AI	284
8.2	AI Dalam Penuntutan Pidana.....	287
8.3	AI Dalam Pemilu Dan Proses Demokrasi	290
8.4	AI Di Sektor NIS.....	302
BAB 9	ETIKA	309
9.1	Pedoman Etika Untuk AI Yang Dapat Dipercaya	309
9.2	Pedoman & Kebijakan AI Yang Relevan	316
DAFTAR PUSTAKA		329

BAB 1

AI, DATA SCIENCE, & DATA ANALYTICS: APA BEDANYA?

1.1 PENDAHULUAN

Kecerdasan buatan berada di pusat revolusi yang tidak hanya mengubah cara mesin berpikir dan belajar, tetapi juga menantang pemahaman kita tentang kecerdasan itu sendiri. Revolusi ini didorong oleh big data dan kekuatan komputasi luar biasa dari komputer modern, yang dapat melakukan perhitungan statistik kompleks dengan kecepatan dan presisi yang telah lama tak terbayangkan. AI memiliki banyak wajah. Dari program sederhana yang melakukan tugas-tugas individual dengan akurasi yang melampaui kemampuan manusia, hingga sistem kompleks yang belajar beradaptasi dan membuat keputusan yang mengingatkan kita pada pikiran manusia.

Peningkatan digitalisasi dapat membebaskan kita dari tugas-tugas yang berulang dan membosankan serta memberi kita kebebasan untuk bertindak lebih kreatif dan strategis. Jika Anda memiliki sedikit bakat atau pengalaman di satu bidang, Anda dapat mengimbangnya dengan asisten virtual. AI menawarkan peluang untuk memperluas keterampilan kita dan mendorong batasan kita. Namun, untuk memanfaatkannya sepenuhnya, kita perlu belajar bagaimana bekerja secara efektif dengan AI.

Tetapi apa sebenarnya yang membuat mesin "cerdas"? Apakah itu kemampuannya untuk mengenali dan merespons ucapan manusia? Efisiensinya dalam membuat keputusan dalam hitungan milidetik yang hanya dapat dilakukan manusia dengan susah payah dan setelah pertimbangan yang panjang? Atau apakah itu kemampuannya untuk belajar dari pengalaman dan berkembang seiring waktu? Faktanya, AI mencakup spektrum teknologi yang beragam seperti definisi yang berusaha untuk menangkapnya. Jadi mari kita mulai perjalanan kita ke dunia AI dengan melihat komponen dasar dan berbagai teknik yang dirangkum dalam istilah "kecerdasan buatan".

1.2 LANDASAN AI

Di bidang AI, nama dan istilah sering digunakan tanpa mengetahui definisi dan latar belakangnya yang tepat. Namun di dunia matematikawan, ilmuwan komputer, dan arsitek AI, ketelitian sangat penting. Definisi yang jelas dan tidak ambigu diperlukan untuk mendorong batas-batas kemungkinan dan mengembangkan generasi sistem cerdas berikutnya.

Saat mengembangkan sistem AI apa pun, ada komponen yang diperlukan terlepas dari teknologi atau kasus penggunaan spesifiknya. Landasan-landasan ini membentuk dasar di mana algoritma AI yang lebih kompleks dapat dibangun. Oleh karena itu, mari kita lihat komponen-komponen sistem AI ini dan definisikan detail terkaitnya:

Tabel 1.1 Gambaran Umum Komponen AI Penting

Komponen	Deskripsi	Pentingnya	Kompleksitas	Kemampuan Kustomisasi
Data	Informasi untuk pembelajaran dan pengambilan keputusan	Tinggi	Variabel	Tinggi
Algoritma	Prosedur atau metode untuk memproses data	Tinggi	Tinggi	Tinggi
Daya komputasi	Untuk memproses sejumlah besar data dan perhitungan kompleks	Tinggi	Sedang	Sedang
Penyimpanan	Diperlukan untuk menyimpan data, model, dan hasil	Sedang	Rendah	Sedang
Pengukuran dan optimasi model	Penting untuk mengevaluasi efektivitas model AI dan optimasinya	Tinggi	Tinggi	Tinggi
Antarmuka untuk interaksi	Memungkinkan interaksi antara manusia dan sistem AI	Sedang	Sedang	Tinggi
Keamanan dan perlindungan data	Melindungi data dari akses dan penyalahgunaan yang tidak sah, memastikan kepatuhan terhadap standar hukum	Tinggi	Tinggi	Sedang

1. Pentingnya: Peringkat “Tinggi” berarti komponen ini sangat penting dalam konteks pengoperasian sistem AI yang benar dan efisien. Sedang dan Rendah menunjukkan kriteria yang kurang penting.
2. Kompleksitas: Peringkat mengacu pada tingkat kesulitan dalam menghasilkan hasil yang benar atau berkinerja baik secara andal oleh AI.
3. Kemampuan Adaptasi: Peringkat menunjukkan seberapa fleksibel perusahaan dapat menyesuaikan komponen AI dengan kebutuhan dan tugasnya sendiri.

Mari kita sekarang menelaah lebih dekat masing-masing komponen. Penjelasan berikut hanya mewakili aspek-aspek terpenting dan tidak mengklaim sebagai penjelasan yang lengkap.

Data

Data adalah bahan bakar untuk model AI. Mirip dengan kendaraan, model AI tidak akan berguna tanpa data. Data menyediakan informasi yang dibutuhkan untuk mengenali pola, membuat keputusan, dan belajar dari pengalaman.

Data adalah sumber kehidupan AI. Tanpa data, AI tidak akan memiliki titik acuan untuk menganalisis, belajar, atau meningkatkan diri. Oleh karena itu, kualitas data yang digunakan sangat penting! Jika kualitasnya tidak cukup tinggi, tidak mungkin untuk mencapai hasil yang baik.

Dari Kumpulan Data Sederhana hingga Pendekatan Big Data Saat Ini

Ketersediaan dan kualitas data terus meningkat dalam beberapa tahun terakhir. Perkembangan internet dan teknologi digital telah menyebabkan peningkatan eksponensial dalam jumlah dan variasi data yang sekarang digunakan sistem AI untuk pembelajaran dan analisis.

Data harus selalu berada dalam konteks penggunaannya agar dapat memahami makna dan nilainya. Konteks memberikan wawasan tentang apa yang diwakili data, konteks di mana data tersebut dikumpulkan, dan bagaimana data tersebut harus diinterpretasikan. Misalnya, tergantung pada konteksnya, angka 9 dapat mewakili suhu [dalam derajat Celcius), panjang (dalam sentimeter), durasi (dalam menit), atau berbagai pengukuran lainnya.

Dalam analisis data dan kecerdasan buatan, konteks sangat penting untuk menarik kesimpulan yang benar dan membuat prediksi yang akurat. Model membutuhkan pelatihan dengan data yang tidak hanya akurat dan bersih, tetapi juga disajikan dalam kerangka kerja yang sesuai. Oleh karena itu, konteks secara langsung memengaruhi hasil model AI:

Tabel 1.2 Tujuan dan Tantangan untuk Konteks Generasi Hasil AI

Rentang	Tujuan	Tantangan	Contoh
Pemilihan data	Pemilihan data yang relevan dan representatif terhadap masalah.	Data yang tidak mencukupi atau terdistorsi dapat menyebabkan kinerja model yang buruk.	Pemilihan data pasien untuk model AI guna memprediksi diabetes.
Rekayasa fitur	Pengembangan dan transformasi fitur untuk meningkatkan penyajian informasi untuk model.	Overfitting pada data pelatihan dan mengabaikan generalisasi.	Pembuatan rentang waktu untuk perilaku pembelian pelanggan dalam model AI untuk memprediksi penjualan.
Interpretasi model	Analisis dan jelaskan hasil yang dihasilkan oleh model AI.	Penelusuran dan verifikasi proses pengambilan keputusan dari model kompleks seperti jaringan saraf dalam seringkali sulit dilakukan.	Interpretasi peringkat kredit dalam model keuangan.

Tergantung pada format data yang tersedia, konteks dapat dikenali dan diproses dengan lebih baik atau lebih buruk.

- **Data terstruktur** diorganisir dalam format yang telah ditentukan sebelumnya, biasanya dalam bentuk tabel, yang memudahkan analisis dan pemrosesannya. Contohnya adalah basis data dan tabel Excel.
- **Data tidak terstruktur**, di sisi lain, tidak memiliki format atau struktur yang telah ditentukan sebelumnya. Ini termasuk teks, buku, gambar, video, dan banyak lagi. Pemrosesan data ini membutuhkan metode yang lebih kompleks, karena penataan terlebih dahulu diperlukan.

Kumpulan data yang ekstensif dan dipersiapkan dengan baik diperlukan untuk pelatihan model AI. Kumpulan data ini dibagi menjadi tiga kategori utama:

1. **Data pelatihan** adalah data yang digunakan untuk melatih model. Data ini menjadi dasar untuk mempelajari pola dan korelasi.

2. **Data validasi** digunakan untuk mengevaluasi kinerja model selama pelatihan dan untuk menyesuaikan parameter.
3. **Data pengujian** digunakan untuk mengevaluasi kinerja akhir model. Data ini harus independen dari data pelatihan dan validasi untuk memastikan evaluasi yang objektif.

Kualitas data juga sangat penting untuk kinerja model AI. Data berkualitas tinggi akurat, lengkap, konsisten, dan mutakhir. Kualitas data yang buruk menyebabkan model yang tidak dapat diandalkan dan menghasilkan hasil yang terdistorsi atau salah. Seringkali baru setelah fase pelatihan Anda menyadari bahwa kualitas data tidak cukup untuk tujuan yang dimaksud dan kemudian harus mengolah kembali data tersebut.

Tantangan utama lainnya adalah pemrosesan data sensitif dan pribadi serta data dari kelompok minoritas yang sesuai dengan hukum. Solusi seperti anonimisasi data dan metode untuk mengurangi bias harus dibahas dan diimplementasikan dalam setiap proyek. Opsi dan kriteria untuk ini adalah subjek dari bab-bab berikut.

Algoritma

Algoritma adalah aturan atau serangkaian instruksi yang didefinisikan secara tepat untuk memecahkan masalah atau melakukan suatu tugas. Pada dasarnya, algoritma dapat dianggap seperti resep dalam buku masak: Algoritma memberikan instruksi langkah demi langkah tentang cara mencapai keadaan akhir yang diinginkan (kentang mentah) dari keadaan awal.

Dalam ilmu komputer, algoritma terdiri dari urutan langkah-langkah yang terdefinisi dengan baik dan dapat dieksekusi yang memecahkan suatu tugas atau masalah. Dalam AI, algoritma adalah proses atau metode yang digunakan untuk belajar dari data, memecahkan tugas, membuat prediksi dan keputusan, atau mengenali pola dalam data.

Area AI yang sangat populer saat ini adalah pembelajaran mesin. Tidak seperti programmer yang harus secara eksplisit merumuskan setiap instruksi dalam perangkat lunak berbasis aturan, sistem AI dalam pembelajaran mesin belajar dari data yang diberikan dan secara independen mengidentifikasi pola untuk mendapatkan aturan yang mendasarinya. Berikut beberapa konsep kunci yang sering digunakan dalam pembelajaran mesin:

- **Pembelajaran Terawasi**

Ini adalah salah satu kategori algoritma AI yang paling umum di mana model belajar dari kumpulan data yang sudah berisi jawaban yang benar (label). Tujuannya adalah untuk membuat prediksi untuk data baru yang tidak dikenal (misalnya, deteksi spam atau prediksi harga).

- **Pembelajaran Tak Terawasi**

Di sini, model belajar dari data tanpa label yang telah ditentukan sebelumnya untuk mengenali pola atau struktur secara independen. Aplikasi tipikal adalah pengelompokan titik data berdasarkan kesamaan (misalnya, segmentasi pelanggan).

- **Pembelajaran Semi-terawasi**

Bentuk campuran di mana model dilatih dengan kumpulan data yang berisi data berlabel dan tidak berlabel. Teknik ini berguna ketika data berlabel terbatas atau mahal untuk diperoleh.

- **Pembelajaran Penguatan**

Dalam pendekatan ini, agen belajar bagaimana bertindak dalam suatu lingkungan untuk memaksimalkan imbalan. Metode ini didasarkan pada prinsip coba-coba dan digunakan di berbagai bidang seperti permainan (misalnya catur) dan kendaraan otonom.

- **Pembelajaran Mendalam (Deep Learning)**

Sebuah sub-bidang pembelajaran mesin yang didasarkan pada jaringan saraf dalam. Jaringan ini mampu mengenali pola kompleks dalam jumlah data yang besar. Aplikasinya meliputi pengenalan gambar dan ucapan serta pemrosesan bahasa alami (NLP).

- **Pembelajaran Transfer (Transfer Learning)**

Ini melibatkan transfer pengetahuan dari satu bidang ke bidang lain, yang sangat berguna jika data pelatihan yang tersedia untuk aplikasi target tidak mencukupi. Konsep ini menjadi semakin penting dalam pembelajaran mendalam, khususnya dalam pemrosesan gambar dan bahasa.

Daya Komputasi

Teknik AI modern, terutama pembelajaran mendalam (deep learning), membutuhkan daya komputasi yang cukup besar. Daya ini diperlukan untuk memproses sejumlah besar data dan melakukan perhitungan kompleks dari metode matematika yang dibutuhkan untuk melatih model AI.

Daya komputasi telah meningkat secara eksponensial selama beberapa dekade terakhir, didorong oleh kemajuan dalam teknologi semikonduktor (dikenal sebagai Hukum Moore) dan inovasi dalam arsitektur komputer. Dari masa-masa awal komputer mainframe hingga GPU (unit pemrosesan grafis) berkinerja tinggi saat ini, peningkatan ketersediaan daya komputasi telah secara dramatis meningkatkan kompleksitas model AI yang dapat kita latih saat ini.

Teknologi cloud juga dapat digunakan untuk melatih model AI untuk menghindari keharusan membeli server sendiri. Dengan cara ini, teknologi ini memungkinkan penggunaan daya komputasi yang fleksibel sesuai dengan kebutuhan saat ini. Daya komputasi ini jauh lebih tinggi selama pelatihan daripada selama pengoperasian.

Penyimpanan

Penyimpanan digunakan di semua bidang kecerdasan buatan, mulai dari menyimpan kumpulan data pelatihan yang besar untuk pembelajaran mesin hingga menyimpan informasi status dalam aplikasi waktu nyata seperti kendaraan otonom.

Untuk menyimpan, mengakses, dan memproses data, sistem AI membutuhkan kapasitas penyimpanan yang memadai baik untuk penyimpanan jangka pendek (untuk pemrosesan data saat ini) maupun penyimpanan jangka panjang (untuk menyimpan model dan hasil). Oleh karena itu, perkembangan teknologi penyimpanan lebih lanjut telah secara signifikan memengaruhi kemungkinan sistem AI. Meskipun waktu akses sangat lambat dengan pita magnetik, solid-state drive (SSD) modern dan basis data dalam memori telah meningkatkan kapasitas penyimpanan dan mempercepat akses.

Pengukuran dan Optimasi Model

Pengukuran kinerja dan optimasi model AI merupakan langkah penting dalam proses pengembangan kecerdasan buatan. Hal ini memastikan bahwa model tidak hanya membuat prediksi yang akurat, tetapi juga efisien dan dapat digunakan dalam kondisi dunia nyata. Penting untuk mengevaluasi kinerja model AI untuk memastikan keakuratan, efisiensi, dan keadilannya. Melalui evaluasi, kelemahan dapat diidentifikasi dan perbaikan dapat dilakukan. Teknik optimasi diperlukan untuk meningkatkan model dan menyesuaikan kinerjanya dengan persyaratan spesifik.

Pengukuran dan optimasi berkelanjutan juga sangat penting untuk pengembangan model AI yang bertanggung jawab. Ini adalah satu-satunya cara untuk memastikan dan membuktikan bahwa sistem AI menjalankan tugasnya dengan cara yang adil dan mudah dipahami. Bukti ditentukan dan diarsipkan melalui tindakan kontrol yang telah ditentukan sebelumnya.

Antarmuka untuk Interaksi

Antarmuka pengguna (UI) dan antarmuka pemrograman aplikasi (API) diperlukan untuk memungkinkan orang berinteraksi dengan sistem AI. Antarmuka ini memfasilitasi input data, konfigurasi model, dan akses ke hasil pemrosesan data atau pengambilan keputusan oleh AI.

Antarmuka interaksi harus disesuaikan dengan aplikasi AI masing-masing dan kelompok pengguna individu. Dalam kasus asisten pribadi atau bot layanan pelanggan untuk kelompok pelanggan non-teknis, UI harus tetap intuitif, sedangkan dalam kasus sistem kontrol kompleks untuk robotika dan perangkat pintar untuk teknisi, pengetahuan sebelumnya yang lebih banyak dapat diharapkan. Contoh-contoh ini menggambarkan bagaimana antarmuka yang berbeda meningkatkan aksesibilitas dan keramahan pengguna sistem AI dan membantu menghindari kesalahan. Aspek-aspek berikut juga harus diperhatikan:

- **Aksesibilitas:** Memastikan bahwa antarmuka AI dapat diakses oleh semua pengguna, termasuk penyandang disabilitas dan kebutuhan khusus.
- **Interaksi alami:** pengembangan antarmuka yang memungkinkan komunikasi alami dan intuitif.
- **Perlindungan dan keamanan data:** Memastikan bahwa interaksi dengan sistem AI melindungi privasi pengguna.

Perkembangan di masa depan dapat mencakup teknologi imersif seperti realitas virtual (VR) dan realitas tertambah (AR), yang memungkinkan jenis interaksi baru. Kemajuan ini dapat menghasilkan antarmuka yang lebih personal dan adaptif yang menyesuaikan dengan preferensi dan kebutuhan pengguna individu.

Keamanan dan Perlindungan Data

Karena sistem AI sering bekerja dengan data sensitif atau pribadi, langkah-langkah keamanan dan perlindungan data yang kuat sangat penting. Langkah-langkah ini melindungi informasi dari akses dan penyalahgunaan yang tidak sah serta memastikan kepatuhan terhadap standar hukum dan etika.

Risiko mendasar dan persyaratan hukum adalah:

- **Perlindungan data:** Konsep seperti minimalisasi data, pembatasan tujuan, dan transparansi harus diimplementasikan untuk memastikan bahwa data pribadi dilindungi dan diperlakukan secara rahasia.
- **Hak cipta:** Bukti harus diberikan bahwa data dan karya yang digunakan tidak dilindungi hak cipta oleh orang lain dan bahwa organisasi memiliki hak untuk menggunakannya.
- **Risiko keamanan dalam sistem AI:** Langkah-langkah harus diambil untuk mendeteksi dan mencegah ancaman dan skenario serangan terhadap sistem AI. Salah satu contohnya adalah serangan adversarial, di mana data masukan dimanipulasi oleh pengguna untuk memicu prediksi atau keputusan yang salah. Risiko ini harus diminimalkan dengan menganalisis data masukan.
- **Enkripsi dan anonimisasi:** Teknik harus diterapkan untuk melindungi data, baik selama transmisi maupun penyimpanan. Anonimisasi harus diterapkan untuk data pribadi dan sensitif. atau pseudonimisasi dari data tersebut diperhitungkan.

Penting untuk mendokumentasikan langkah-langkah perlindungan yang telah diterapkan, untuk tujuan apa langkah-langkah tersebut diberlakukan, serta bagaimana perlindungan dijamin sepanjang seluruh siklus hidup kecerdasan buatan (AI). Untuk tujuan tersebut, tindakan pengendalian harus ditetapkan dan kepatuhan terhadapnya harus diarsipkan secara tertelusur.

Keamanan dan perlindungan data merupakan aspek penting yang membentuk keberhasilan dan penerimaan teknologi AI. Dengan terus beradaptasi dengan ancaman baru dan mematuhi standar perlindungan data yang ketat, sistem AI dapat digunakan dengan percaya diri dan bertanggung jawab.

1.3 ILMU DATA DAN ANALISIS DATA

Istilah seperti "Ilmu data" dan "Analisis data" sering digunakan secara bergantian, meskipun ada perbedaan. Ilmu data merupakan bidang yang lebih luas yang berkaitan dengan pembuatan model dan algoritma untuk menganalisis data, sedangkan analisis data lebih berfokus pada interpretasi data untuk menjawab pertanyaan-pertanyaan mendesak. Tabel berikut mengilustrasikan perbedaan berdasarkan kriteria dasar:

Tabel 1.3 Perbedaan antara Ilmu Data dan Analisis Data

Kriteria	Ilmu data	Analisis data
Tujuan utama	Menemukan pola dan memprediksi tren serta perilaku masa depan dengan menganalisis data.	Interpretasi data historis untuk menjawab pertanyaan spesifik atau memecahkan masalah.
Poin fokus	Persiapan data, eksplorasi, pemodelan, pembelajaran mesin, analitik prediktif.	Pengumpulan data, pembersihan data, analisis deskriptif, pelaporan.
Metode dan teknik	Pembelajaran mesin (pembelajaran mendalam), algoritma pembelajaran, model statistik, penambangan data.	Analisis statistik, analisis data eksploratif, alat visualisasi, penambangan proses.

Contoh aplikasi	Pengembangan ide produk baru, deteksi penipuan, manajemen risiko, sistem rekomendasi yang dipersonalisasi.	Analisis penjualan dan pasar, analisis perilaku pelanggan, efisiensi operasional, pengendalian mutu.
Keterampilan yang dibutuhkan	Statistik, pembelajaran mesin, pemrograman (misalnya Python, R), pengetahuan basis data, pemahaman bisnis.	Statistik, pemikiran analitis, pengetahuan tentang alat BI (misalnya Tableau, Power BI), pengetahuan dasar pemrograman.

Oleh karena itu, ilmu data berkaitan dengan pengumpulan, pembersihan, dan analisis data untuk mengenali pola, membuat prediksi, dan mengambil keputusan berdasarkan kumpulan data yang besar. Ilmuwan data menggunakan algoritma kompleks, pembelajaran mesin, dan metode statistik untuk mengolah data. Mereka mencari jawaban atas pertanyaan yang belum diajukan dan menciptakan cara baru untuk menggunakan data.

Analisis data lebih berfokus pada pemrosesan dan analisis data yang ada dari proses manufaktur suatu organisasi untuk menjawab pertanyaan spesifik yang berkaitan dengan bidang bisnis. Analisis data menggunakan alat dan teknik statistik untuk membantu organisasi mengambil keputusan operasional. Berbeda dengan ilmu data, yang seringkali lebih eksploratif dan berorientasi ke masa depan, analisis data biasanya lebih terfokus dan diarahkan untuk memecahkan masalah spesifik.

Namun, tidak ada definisi "tetap" untuk istilah-istilah ini, karena bidang ilmu data dan analitik berkembang pesat dan batasan antar disiplin ilmu seringkali kabur. Perusahaan harus menentukan area tanggung jawab dan area aplikasi yang tepat dalam iklan lowongan kerja dan deskripsi posisi untuk menghindari ekspektasi yang tidak terpenuhi atau mengecewakan.

1.4 PENGEMBANGAN AI DI UKM

Penggunaan kecerdasan buatan (AI) menawarkan sejumlah peluang bagi usaha kecil dan menengah (UKM) dan khususnya perusahaan rintisan. Dengan teknologi AI, mereka dapat mengotomatiskan proses, meningkatkan efisiensi, dan mengembangkan produk atau layanan inovatif yang dapat memberikan keunggulan kompetitif.

Bagi UKM, penggunaan AI membuka kemungkinan untuk menggunakan sumber daya secara lebih efisien dengan menyediakan asisten AI bagi tenaga kerja yang mengambil alih tugas-tugas yang memakan waktu dan mendukung proses pengambilan keputusan dengan wawasan berbasis data. Hal ini dapat menyebabkan pengurangan biaya yang signifikan dan peningkatan layanan pelanggan. Perusahaan rintisan yang bereksperimen dengan AI dapat mengembangkan solusi khusus yang disesuaikan dengan kebutuhan industri tertentu dan dengan demikian membuka pasar baru atau mengganggu pasar yang sudah ada.

Selain itu, penggunaan AI di kedua jenis perusahaan tersebut mendorong budaya fokus data dan inovasi. Hal ini penting untuk pertumbuhan jangka panjang dan kemampuan beradaptasi terhadap kondisi pasar yang berubah dengan cepat. Di dunia di mana data telah menjadi sumber daya terpenting yang baru, teknologi AI menyediakan UKM dan perusahaan rintisan dengan alat untuk memanfaatkan sumber daya berharga ini dan mengembangkan model bisnis yang tahan masa depan.

Oleh karena itu, penggunaan AI di UKM dan perusahaan rintisan memiliki potensi yang cukup besar, tetapi juga menghadirkan tantangan yang signifikan. Salah satu masalah utama adalah perekrutan dan retensi personel yang berkualitas yang terampil dalam pengembangan dan implementasi teknologi AI. Tantangan lainnya meliputi:

▪ **Perekrutan ahli**

- Kekurangan keterampilan: Ada kekurangan ahli di bidang AI dan pembelajaran mesin secara global. Hal ini membuat UKM dan perusahaan rintisan kesulitan untuk menarik para profesional berbakat yang familiar dengan teknologi dan metode terbaru.
- Bersaing dengan perusahaan besar: Perusahaan rintisan dan UKM bersaing dengan perusahaan besar yang sudah mapan untuk mendapatkan talenta AI. Perusahaan besar seringkali dapat menawarkan gaji, tunjangan, dan peluang pengembangan karier yang lebih menarik.

▪ **Sumber daya keuangan**

- Biaya tinggi: Pengembangan dan implementasi solusi AI bisa mahal, terutama dalam hal pembelian perangkat keras atau perangkat lunak yang diperlukan. Bagi perusahaan rintisan dan UKM dengan anggaran terbatas, ini bisa menjadi hambatan yang signifikan.
- Ketidakpastian ROI: Berinvestasi dalam AI membawa ketidakpastian mengenai pengembalian investasi (ROI), terutama jika perusahaan tersebut baru di bidang ini. Hal ini dapat menyebabkan keraguan dalam alokasi sumber daya.

▪ **Data dan perlindungan data**

- Kualitas dan ketersediaan data: Sistem AI yang efektif membutuhkan sejumlah besar data berkualitas tinggi. Namun, banyak UKM dan perusahaan rintisan kesulitan untuk mengakses data tersebut atau untuk mengumpulkan dan memprosesnya dengan cara yang bermakna.
- Peraturan perlindungan data: Kepatuhan terhadap undang-undang perlindungan data seperti GDPR dapat menjadi tantangan bagi perusahaan yang bekerja dengan data pribadi. Mengembangkan sistem AI yang memenuhi persyaratan ini membutuhkan pengetahuan dan sumber daya khusus.
- Keamanan TI: Menerapkan dan terus memastikan langkah-langkah keamanan TI dalam infrastruktur organisasi membutuhkan spesialis berpengalaman, perangkat lunak mahal, dan sumber daya waktu. Hal ini juga berlaku untuk integrasi fitur keamanan dalam perangkat lunak atau produk AI.

▪ **Integrasi Teknologi**

- Integrasi Proses: Mengintegrasikan solusi AI ke dalam proses dan sistem bisnis yang ada dapat menjadi kompleks dan menantang. Masalah kompatibilitas dan kebutuhan akan solusi yang disesuaikan dapat menunda atau meningkatkan biaya implementasi.
- Kontrol: Mendefinisikan langkah-langkah pengendalian internal dan tata kelola untuk layanan digital dapat menjadi tantangan bagi UKM atau perusahaan rintisan karena banyak aktivitas diimplementasikan dengan tenaga kerja yang kecil. Seringkali,

pengetahuan atau orang untuk menerapkan pemisahan fungsi atau prinsip pengendalian ganda tidak tersedia di perusahaan.

▪ **Pengetahuan dan Perubahan Budaya**

- Perusahaan kecil yang sudah mapan: Pengenalan AI seringkali membutuhkan perubahan budaya di dalam organisasi. Di UKM, hal ini dapat dengan cepat menyebabkan kecemasan dan penolakan jika tenaga kerja tidak dilatih dengan benar.
- Perusahaan rintisan: Di perusahaan baru yang digerakkan oleh teknologi, seringkali terdapat suasana inovasi dan awal yang baru, tanpa memperhatikan keberlanjutan penggunaan alat atau memastikan bahwa alat tersebut digunakan dengan aman (dalam hal rahasia dagang, perlindungan data, dan lain-lain.) dan sesuai dengan hukum (sesuai dengan hak cipta, hak penggunaan).
- Pengembangan pengetahuan: Siklus teknologi dan produk AI baru muncul dengan interval yang semakin pendek, dan sulit untuk selalu mengikuti perkembangan di samping pekerjaan sehari-hari. Terutama di perusahaan kecil, seringkali sulit untuk terus membangun pengetahuan para spesialis dan mentransfernya ke seluruh tenaga kerja.

Tantangan ini menyoroti kebutuhan bagi perusahaan rintisan dan UKM untuk mempertimbangkan kemitraan strategis, mencari nasihat dan dukungan eksternal, serta berinvestasi dalam pelatihan dan peningkatan keterampilan tenaga kerja mereka. Terlepas dari hambatan-hambatan ini, integrasi AI menawarkan peluang besar untuk mengoptimalkan proses bisnis, mengeksplorasi peluang pertumbuhan baru, dan tetap kompetitif dalam jangka panjang.

Komisi Uni Eropa akan menyusun pedoman untuk pelaksanaan praktis Peraturan Kecerdasan Buatan (AI), dengan memberikan perhatian khusus pada kebutuhan usaha kecil dan menengah (UKM), termasuk perusahaan rintisan (start-up) (Pasal 96 Undang-Undang Kecerdasan Buatan).

Daftar periksa berikut untuk penggunaan AI di perusahaan rintisan dan UKM dapat membantu mengambil pendekatan terstruktur dan memastikan bahwa semua aspek penting untuk perencanaan penggunaan AI dalam organisasi diperhitungkan:

▪ **Analisis kebutuhan dan tujuan untuk inisiatif AI**

- Tetapkan tujuan yang jelas untuk penggunaan AI di perusahaan Anda.
- Identifikasi masalah atau proses spesifik yang dapat ditingkatkan oleh AI.
- Evaluasi status teknologi dan tingkat kematangan perusahaan saat ini terkait dengan AI.
- Diskusikan bersama tim potensi risiko dan masalah etika yang terkait dengan penggunaan AI, termasuk perlindungan data dan dampaknya pada tempat kerja.

▪ **Riset pasar dan teknologi**

- Tren teknologi AI saat ini dan masa depan apa yang akan berdampak pada industri Anda?

- Teliti alat dan solusi AI yang tersedia yang sesuai atau dapat disesuaikan dengan kebutuhan Anda.
- Susun daftar teknologi dan platform AI yang relevan dengan model bisnis perusahaan.
- Evaluasi kesiapan pasar dan keandalan teknologi AI potensial.
- Teliti keandalan dan reputasi berbagai penyedia teknologi AI.
- Identifikasi bagaimana pesaing menggunakan teknologi AI dan evaluasi keberhasilan serta kegagalan mereka.
- Produk atau layanan berbasis AI mana yang diminati di segmen pasar Anda dan kebutuhan pelanggan mana yang dapat dipenuhi?
- **Perencanaan Sumber Daya**
 - Periksa apakah sumber daya keuangan dan manusia yang diperlukan tersedia untuk implementasi dan pemeliharaan solusi AI.
 - Rencanakan kursus pelatihan untuk tim Anda guna membangun pengetahuan yang diperlukan untuk berhasil menggunakan teknologi AI.
 - Nilai apakah infrastruktur TI perusahaan saat ini sesuai untuk mendukung solusi AI baru atau apakah diperlukan peningkatan.
- **Persiapan Data**
 - Pastikan Anda memiliki akses ke data berkualitas tinggi yang dapat digunakan untuk melatih model AI.
 - Periksa kelengkapan, keakuratan, ketepatan waktu, dan relevansi data terkait dengan kasus penggunaan AI.
 - Sejumlah besar data pelatihan seringkali diperlukan untuk melatih model AI yang andal. Pastikan data yang cukup tersedia untuk mengembangkan model yang tangguh dan pertimbangkan juga keragaman data.
 - Periksa persyaratan perlindungan data dan keamanan data yang ada untuk memastikan kepatuhan.
 - Siapkan data menggunakan teknik seperti normalisasi, penskalaan, dan pengkodean data kategorikal untuk mempersiapkan data untuk pelatihan model AI.
 - Atur penyimpanan data secara efisien untuk akses cepat dan pengelolaan yang mudah.
- **Pemilihan solusi AI**
 - Tentukan apakah Anda ingin mengembangkan solusi AI yang disesuaikan atau menggunakan perangkat lunak AI yang tersedia di pasaran.
 - Bandingkan berbagai penyedia dan produk dalam hal kinerja, biaya, dan dukungan.
 - Klarifikasi persyaratan hukum yang harus diperhatikan saat mengimplementasikan teknologi AI yang direncanakan.
 - Selidiki bagaimana solusi AI potensial dapat diintegrasikan ke dalam lanskap teknologi yang ada.
- **Proyek percontohan dan evaluasi**
 - Mulailah dengan proyek percontohan untuk menguji efektivitas dan integrasi solusi AI.

- Ukur hasil dan dampak solusi AI terhadap tujuan yang telah ditetapkan.
- Jangan lupa untuk memasukkan persyaratan hukum dan peraturan kontrak khusus dalam evaluasi.
- Evaluasi risiko dalam hal perlindungan data dan keamanan data untuk solusi AI tertentu.
- Mendokumentasikan efek pembelajaran dan praktik terbaik dari proyek percontohan dan mentransfer pengetahuan dari proyek tersebut.
- **Integrasi dan penskalaan**
 - Mengintegrasikan solusi AI ke dalam sistem dan alur kerja yang ada.
 - Melatih tenaga kerja agar mereka dapat menangani AI dan hasil yang dihasilkan dengan tepat.
 - Merencanakan penskalaan solusi AI untuk mencakup area lain di perusahaan Anda.
- **Pemantauan dan optimasi berkelanjutan**
 - Menetapkan proses untuk pemantauan kinerja AI secara berkelanjutan.
 - Menetapkan prosedur kontrol untuk memverifikasi bahwa implementasi sesuai dengan hukum.
 - Menggunakan umpan balik dan data kinerja untuk terus meningkatkan solusi AI.
- **Keamanan dan etika data**
 - Menerapkan langkah-langkah keamanan yang kuat untuk melindungi sistem dan data yang didukung AI.
 - Bekerja sama dengan spesialis dalam manajemen dan pemrosesan data.
 - Mengembangkan arsitektur data yang kuat yang secara efektif mendukung pertumbuhan dan skalabilitas data. Pertimbangkan juga persyaratan pengarsipan.
 - Mempertimbangkan aspek etika dan dampak penggunaan AI terhadap karyawan, pelanggan, dan masyarakat.
- **Umpan balik dan penyesuaian**
 - Kumpulkan umpan balik secara berkala tentang solusi AI dari pengguna dan pemangku kepentingan.
 - Jangan mulai mengumpulkan umpan balik dari pelanggan (potensial) terlalu lambat.
 - Bersiaplah untuk melakukan penyesuaian guna memaksimalkan efektivitas dan penerimaan AI.

Daftar periksa ini berfungsi sebagai kerangka kerja bagi perusahaan rintisan dan usaha kecil dan menengah (UKM) yang berencana mengintegrasikan teknologi kecerdasan artifisial (AI) ke dalam proses bisnis mereka. Kunci keberhasilan terletak pada perancangan yang cermat, pemilihan teknologi yang tepat, serta evaluasi berkelanjutan terhadap dampaknya terhadap kegiatan usaha.

BAB 2

GEPOLITIK KECERDASAN BUATAN

2.1 PENDAHULUAN

Definisi

- **Geopolitik menurut Encyclopædia Britannica:** “studi tentang bagaimana geografi dan ekonomi memengaruhi politik dan hubungan antar negara; bagian politik dan geografis dari sesuatu.”
- **Geopolitik menurut Cambridge Dictionary:** “studi tentang bagaimana ukuran, posisi, dan lain-lain. suatu negara memengaruhi kekuasaannya dan hubungannya dengan negara lain; aktivitas politik yang dipengaruhi oleh fitur fisik suatu negara atau wilayah di dunia.”
- **Definisi OECD tentang sistem AI (per Maret 2024):** “Sistem AI adalah sistem berbasis mesin yang, untuk tujuan eksplisit atau implisit, menyimpulkan, dari masukan yang diterimanya, bagaimana menghasilkan keluaran seperti prediksi, konten, rekomendasi, atau keputusan yang dapat memengaruhi lingkungan fisik atau virtual. Sistem AI yang berbeda bervariasi dalam tingkat otonomi dan adaptabilitasnya setelah diterapkan.”

Dengan mempertimbangkan definisi di atas, geopolitik AI dapat didefinisikan sebagai berikut:

Geopolitik AI oleh karena itu mengkaji bagaimana karakteristik, kemampuan, dan penerapan teknologi AI memengaruhi dinamika kekuatan global, memengaruhi posisi strategis negara, kerja sama internasional, dan persaingan. Hal ini mencakup peran AI dalam meningkatkan atau menantang status ekonomi dan militer suatu negara, dalam membentuk keputusan politik, dan dalam mendefinisikan kembali lanskap geopolitik di dunia di mana dominasi teknologi semakin menentukan kedaulatan nasional dan hubungan internasional. Hal ini mencerminkan kemampuan suatu negara untuk memimpin atau berinovasi dalam teknologi, khususnya di bidang-bidang seperti kecerdasan buatan (AI), keamanan siber, dan infrastruktur digital, yang menyoroti kekuatan, pengaruh, dan otoritasnya, serta otonomi strategisnya di panggung global.

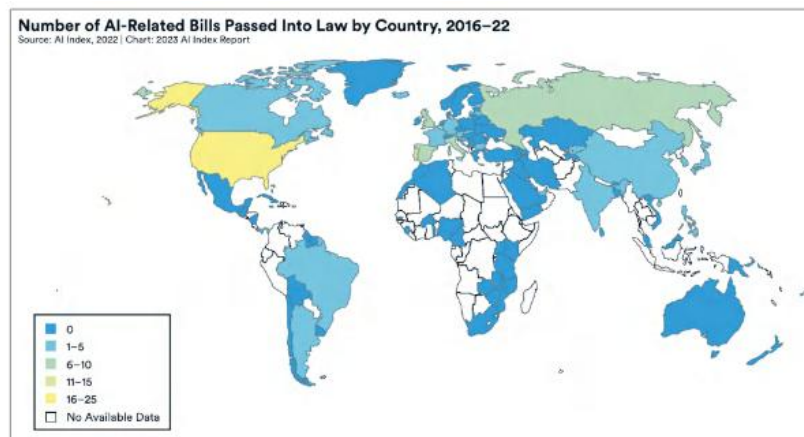
2.2 LANSKAP REGULASI AI YANG SEDANG BERKEMBANG

Dalam beberapa tahun terakhir, dunia telah memasuki perlombaan untuk AI, didorong oleh berbagai harapan akan manfaat ekonomi, peningkatan keselamatan, terobosan teknologi, kemajuan etika, dan masyarakat yang lebih baik.

Pemerintah di seluruh dunia telah menyadari bahwa kepemimpinan dalam AI dapat memberi mereka keunggulan strategis yang menentukan dan berinvestasi besar-besaran untuk mengamankan posisi mereka di garis depan revolusi teknologi transformatif ini. Namun, lanskap AI tetap sangat beragam, mencerminkan berbagai tingkat kematangan pendekatan

dan strategi pemerintah di seluruh dunia - dari pemerintah dengan strategi AI yang kuat dan berwawasan ke depan hingga pemerintah yang belum sepenuhnya menyadari potensi AI.

Laporan Kecerdasan Buatan Stanford 2023, sebuah studi dokumen legislatif dari 127 negara, menunjukkan peningkatan signifikan dalam adopsi undang-undang yang menyebutkan “kecerdasan buatan”, meningkat dari satu RUU pada tahun 2016 menjadi 37 pada tahun 2022. Demikian pula, sebuah studi diskusi parlemen tentang AI di 81 negara menunjukkan bahwa referensi terhadap AI dalam undang-undang telah meningkat 6,5 kali lipat sejak tahun 2016.



Gambar 2.1 Jumlah Regulasi Terkait AI per Negara

Dari hasil penelitian Indeks AI menunjukkan bahwa tren legislatif tahun 2022 mengikuti tren global menuju integrasi AI yang bertanggung jawab dan etis ke dalam masyarakat. Negara-negara mengembangkan undang-undang yang tidak hanya mendorong kemajuan kecerdasan buatan, tetapi juga bertujuan untuk mengurangi risikonya, memastikan keamanan, dan mempromosikan distribusi manfaat yang adil bagi masyarakat secara keseluruhan.

- Pentingnya dan dampak AI pada berbagai bidang masyarakat – dari industri kreatif hingga keamanan nasional – jelas diakui. Negara-negara secara aktif berupaya menciptakan kerangka peraturan yang tidak hanya mendorong pengembangan AI, tetapi juga mengatasi potensi risiko dan dampaknya. Legislasi dan peraturan sedang diberlakukan untuk mengatasi tantangan dan peluang revolusi AI yang berkembang pesat.
- Negara-negara melakukan upaya signifikan untuk memodernisasi kerangka hukum mereka sebagai respons terhadap perkembangan AI yang pesat dan dampaknya terhadap masyarakat.
- Legislasi mencerminkan berbagai aplikasi AI, mulai dari mempromosikan industri kreatif dan pendidikan hingga memastikan keamanan nasional dan mempromosikan pengambilan keputusan yang adil dan tidak diskriminatif dalam administrasi publik.
- Beberapa negara sedang dalam proses memperkenalkan peraturan untuk melindungi dari penyalahgunaan AI, dengan fokus pada keselamatan, etika, dan meminimalkan bias.

- Pengenalan program pelatihan menjawab kebutuhan untuk mempersiapkan dan melatih pekerja untuk masa depan yang digerakkan oleh AI.

Indeks AI Global adalah metrik komprehensif lain yang menilai keadaan kecerdasan buatan di 62 negara. Indeks ini terdiri dari 111 indikator yang diambil dari 28 sumber data publik dan swasta serta informasi dari 62 pemerintah, yang mencakup tujuh sub-pilar: bakat atau keterampilan, infrastruktur, lingkungan operasi, penelitian, pengembangan, strategi pemerintah, dan sektor komersial.

	Overall	Talent	Infrastructure	Operating Environment	Research	Development	Government Strategy	Commercial	Scale	Intensity
United States	100.0	100.0	100.0	82.8	100.0	100.0	90.3	100.0	10.0	80.3
China	61.5	39.0	92.1	99.7	54.7	80.6	93.5	43.1	67.8	39.5
Singapore	49.7	56.9	82.9	85.7	45.8	24.4	81.8	26.2	28.1	10.0
United Kingdom	41.6	53.8	61.8	79.5	36.1	19.5	89.2	20.9	34.6	52.8
Canada	40.9	48.0	62.1	93.1	34.0	18.9	93.4	18.9	31.9	55.9
South Korea	40.9	35.1	74.4	91.4	24.5	60.9	91.0	8.3	31.5	57.3
Israel	40.0	45.5	60.5	85.1	24.8	22.2	31.8	40.5	23.5	70.1
Germany	39.2	57.0	68.2	90.7	29.3	19.5	93.9	10.3	31.7	45.4
Switzerland	37.7	44.5	68.0	81.9	41.3	24.9	9.0	13.3	23.5	71.6
Finland	34.0	34.5	73.0	97.7	27.4	19.1	82.7	9.5	24.2	62.0
Netherlands	34.5	45.2	65.7	90.3	27.1	15.7	71.8	7.9	25.5	55.5
Japan	33.9	38.0	80.8	92.4	16.6	22.2	80.3	6.8	32.2	36.4
France	32.0	41.5	68.9	84.2	21.4	8.3	87.3	10.8	29.5	39.7
India	31.4	86.2	34.7	81.1	12.0	7.8	58.0	8.9	33.7	20.0
Australia	30.9	34.2	54.3	53.8	34.4	11.7	83.3	7.0	23.6	47.5
Denmark	30.5	39.5	67.5	100.0	19.4	8.9	75.0	8.2	23.3	50.9
Sweden	30.3	33.7	62.2	99.9	22.4	11.4	47.0	8.6	22.5	50.1
Luxembourg	29.2	24.0	74.9	90.4	19.4	7.5	65.8	8.8	19.0	53.1
Ireland	28.8	31.8	60.8	88.0	13.6	19.2	71.7	8.6	20.1	49.6
Spain	27.7	31.5	65.2	90.2	14.5	4.3	93.4	4.7	24.6	34.5
Austria	27.7	27.6	57.0	94.7	21.3	7.4	83.1	5.8	21.7	44.0
Belgium	26.0	27.4	55.3	94.8	21.9	5.1	57.0	6.6	21.6	41.4

Gambar 2.2 Negara-negara dengan Poin Terbanyak dalam Indeks AI Global

Data dari indeks ini dengan jelas menunjukkan hal-hal berikut:

- Amerika Serikat memimpin lanskap AI global dengan skor optimal dalam keterampilan/bakat dan pengembangan, yang mencerminkan ekosistem AI yang kuat yang didukung oleh universitas dan perusahaan teknologi terkemuka.
- Tiongkok menunjukkan kinerja yang kuat secara keseluruhan, terutama di bidang infrastruktur dan strategi pemerintah, karena investasi pemerintah yang signifikan dan prioritas strategis AI.
- Meskipun merupakan negara kecil, Singapura berada di peringkat teratas dengan hasil yang baik dalam infrastruktur dan lingkungan operasional, menunjukkan kondisi yang menguntungkan untuk pertumbuhan AI.
- Negara-negara Eropa memiliki kekuatan yang berbeda. Negara-negara seperti Finlandia dicirikan oleh infrastruktur yang sangat baik, yang menunjukkan fondasi yang kokoh untuk teknologi AI, sementara negara lain seperti Jerman memiliki strategi pemerintah yang kuat yang dapat mendorong agenda AI nasional mereka.

- India menonjol dibandingkan dengan peringkat keseluruhannya dengan skor keterampilan dan bakat yang sangat tinggi.
- Terdapat perbedaan yang mencolok dalam pilar perdagangan: beberapa negara, seperti Amerika Serikat, berkinerja sangat baik, sementara negara lain tertinggal meskipun memiliki dukungan dan kemampuan pemerintah yang kuat, mungkin karena strategi industri atau kondisi pasar yang berbeda.
- Indeks ini membedakan antara “cakupan” dan “intensitas” aktivitas AI, dengan beberapa negara mencetak skor tinggi pada intensitas (seperti Israel), meskipun cakupannya tidak sebesar itu, menunjukkan kemampuan AI yang terkonsentrasi dan kuat.
- Austria menunjukkan kinerja yang solid di bidang “Lingkungan Operasional”. Namun, skor Austria di bidang kemampuan dan strategi pemerintah relatif rendah dibandingkan dengan lingkungan operasional.

Indeks Kesiapan AI Pemerintah 2023 menunjukkan bahwa kolaborasi internasional tentang tata kelola dan etika AI mengalami pertumbuhan yang signifikan pada tahun 2023. Tahun tersebut juga ditandai dengan meningkatnya jumlah pertemuan puncak dan inisiatif AI, yang menunjukkan meningkatnya kesadaran global dan tindakan bersama untuk memahami dampak sosial AI.

Peristiwa penting termasuk peluncuran proses AI Hiroshima pada KTT G7 pada bulan Mei dan *KTT Keamanan AI Inggris* pada bulan November 2023. Pertemuan-pertemuan ini dan pertemuan lainnya menggarisbawahi komitmen global untuk membentuk tata kelola AI di masa depan.

Sejumlah proposal untuk pedoman dan prinsip untuk AI telah dibuat, termasuk Prinsip Panduan *Internasional G7 untuk Sistem AI Tingkat Lanjut* dan Deklarasi Bletchley dari *KTT Keamanan AI Inggris*. Proposal-proposal baru ini bergabung dengan sejumlah kerangka kerja dan rekomendasi yang telah mapan yang bertujuan untuk pengembangan AI yang etis, seperti *Prinsip AI OECD 2019*, Rekomendasi UNESCO 2021 tentang Etika Kecerdasan Buatan. Peran UNESCO dalam mempromosikan etika AI melalui metodologi seperti *Metodologi Penilaian Kesiapan (RAM)* dan *penilaian dampak etis* telah menjadi pusat perhatian. UNESCO telah mendukung kelompok awal yang terdiri dari 50 negara, terutama negara berkembang, dalam menerapkan metodologi ini. Inisiatif ini, yang berpotensi memprioritaskan etika daripada pengembangan strategi AI nasional yang komprehensif, dapat merevolusi cara pemerintah di seluruh dunia mendekati AI, khususnya yang berkaitan dengan layanan publik.

Upaya regional di bidang kecerdasan buatan juga semakin intensif. Di Amerika Latin dan Karibia, *Deklarasi Santiago* ditandatangani oleh dua puluh negara pada tahun 2023, sementara negara-negara Afrika Selatan berkumpul di Namibia pada tahun 2022 untuk menyepakati *Deklarasi Windhoek*, yang menekankan tindakan regional tentang AI di bidang data, pendidikan, dan tata kelola.

Awal tahun 2024 ditandai dengan dua perkembangan penting di bidang tata kelola AI:

- Pada tanggal 13 Maret 2024, Parlemen Eropa menyetujui Peraturan Kecerdasan Buatan (“UU AI”), kerangka peraturan pertama untuk AI yang membahas risiko AI dan memungkinkan Eropa untuk mengambil peran utama secara global.
- *Konvensi Kerangka Kerja tentang Kecerdasan Buatan, Hak Asasi Manusia, Demokrasi dan Aturan Hukum* diselesaikan oleh Komite Dewan Eropa tentang Kecerdasan Buatan pada tanggal 14 Maret 2024. Draf teks akan diajukan kepada Komite Menteri untuk diadopsi dan dibuka untuk penandatanganan pada tanggal yang akan datang.

Meskipun posisi Uni Eropa ditantang oleh dominasi teknologi AS dan Tiongkok dengan peraturan AI, hal itu sangat penting karena pengaruh regulasinya.

2.3 PERLOMBAAN REGULASI AI – TIGA BESAR

Uni Eropa, Amerika Serikat, dan Tiongkok saat ini sedang berlomba untuk mengatur AI, dengan masing-masing negara mengejar tujuan yang berbeda.

- Regulasi AI Uni Eropa mengejar strategi komprehensif berbasis risiko yang berfokus pada meminimalkan dampak negatif sosial, seperti diskriminasi dalam proses perekrutan yang didorong oleh AI. Pendekatan ini bertujuan untuk mengurangi risiko yang terkait dengan teknologi AI melalui regulasi yang terperinci, dengan fokus pada perlindungan nilai-nilai sosial dan hak asasi manusia.
- Pendekatan Tiongkok dalam mengatur AI berfokus pada penguatan kendali negara atas informasi. Regulasi tersebut dirancang untuk menegaskan otoritas negara dan memastikan bahwa pengembangan AI sejalan dengan kepentingan negara dan masalah keamanan, daripada terutama mempromosikan inovasi di sektor AI.
- Amerika Serikat masih dalam proses mendefinisikan posisinya tentang tata kelola AI. Meskipun perintah eksekutif AI pemerintahan Biden merupakan langkah pertama yang penting, regulasi komprehensif membutuhkan tindakan legislatif. AS berupaya menciptakan kerangka kerja regulasi yang menyeimbangkan kebutuhan akan ekosistem AI yang terbuka dan kompetitif, keamanan dan pengendalian teknologi AI yang berbahaya, sambil mempertahankan kepemimpinan teknologi dan mengatasi tantangan strategis yang ditimbulkan oleh Tiongkok.

Tabel 2.1 Gambaran Umum Kerangka Regulasi AI di Uni Eropa, AS, dan Tiongkok

Pemimpin global dalam tata kelola AI	Pendekatan terhadap tata kelola AI
Uni Eropa (UE)	Pendekatan Uni Eropa terhadap tata kelola AI bersifat komprehensif, bijaksana, dan berbasis multi-pemangku kepentingan. Pendekatan ini bertujuan untuk menyeimbangkan kemajuan teknologi dengan pertimbangan etis dan kepercayaan publik. Pendekatan Uni Eropa mencakup konsultasi dan keterlibatan berbagai pemangku kepentingan, termasuk pengembang AI, pengguna, otoritas publik, akademisi, dan masyarakat sipil, untuk memastikan bahwa Undang-Undang AI dan langkah-langkah AI lainnya komprehensif dan mengatasi kekhawatiran semua pemangku kepentingan. Pendekatan

	kolaboratif ini mencerminkan beragam kepentingan dan nilai-nilai warga Eropa. Uni Eropa bertekad untuk menetapkan tolok ukur global dengan Undang-Undang AI, yang mencerminkan potensinya untuk memimpin penciptaan standar internasional. Namun, dalam persaingan untuk kepemimpinan teknologi, Eropa menghadapi persaingan ketat dari raksasa teknologi dari AS dan Tiongkok. Oleh karena itu, komitmen Uni Eropa terhadap kedaulatan teknologi dipertanyakan oleh kebutuhan akan investasi yang lebih besar dan kurangnya mitra Eropa untuk "Silicon Valley", yang merupakan rumah bagi perusahaan teknologi besar. "Upaya Uni Eropa untuk mengejar inovasi AI dalam negeri menggarisbawahi pentingnya AI dalam memperkuat kedaulatan teknologi Eropa dan mengurangi ketergantungan strategis." (Carnegie Europe, Maret 2024) Ketentuan penting dari Undang-Undang AI: Tujuan dari Peraturan AI adalah untuk "meningkatkan fungsi pasar internal dengan menetapkan kerangka hukum tunggal, khususnya untuk pengembangan, penempatan di pasar, penerapan, dan penggunaan sistem kecerdasan buatan di Uni Eropa, sesuai dengan nilai-nilai Uni Eropa, untuk mempromosikan penerapan kecerdasan buatan yang berpusat pada manusia dan dapat dipercaya sambil memastikan tingkat perlindungan yang tinggi terhadap kesehatan, keselamatan, dan hak-hak mendasar yang diabadikan dalam Piagam, termasuk demokrasi dan supremasi hukum, perlindungan lingkungan, terhadap dampak buruk sistem kecerdasan buatan di Uni Eropa dan untuk mempromosikan inovasi. Peraturan ini memastikan pergerakan bebas barang dan jasa berbasis AI lintas batas dan mencegah Negara Anggota untuk membatasi pengembangan, pemasaran, dan penggunaan sistem kecerdasan buatan (AI), kecuali sebagaimana secara tegas diizinkan oleh Peraturan ini." "Kecerdasan buatan harus menjadi teknologi yang menempatkan manusia sebagai pusatnya. Teknologi ini harus berfungsi sebagai alat bagi manusia yang pada akhirnya bertujuan untuk meningkatkan kesejahteraan manusia." Undang-Undang AI mengusulkan kerangka peraturan yang mengklasifikasikan sistem AI menurut tingkat risikonya: ▪ Risiko yang tidak dapat diterima dilarang (misalnya, sistem peringkat sosial dan AI manipulatif). ▪ Sebagian besar teks membahas regulasi sistem AI berisiko tinggi. ▪ Bagian yang lebih kecil membahas sistem AI dengan risiko terbatas, yang tunduk pada kewajiban transparansi: Pengembang dan penyebar harus memastikan bahwa pengguna akhir menyadari bahwa mereka berinteraksi dengan AI (chatbot dan deepfake).

	▪ Risiko terendah tidak diatur (termasuk sebagian besar aplikasi AI yang saat ini tersedia di pasar tunggal Uni Eropa, seperti filter spam). Sebagian besar kewajiban berlaku untuk penyedia (yaitu, khususnya pengembang) sistem AI berisiko tinggi. Pengguna adalah orang perseorangan atau badan hukum yang menggunakan sistem AI secara profesional, tetapi bukan pengguna akhir yang terdampak. Penyedia model AI untuk tujuan umum harus mematuhi standar dokumentasi dan transparansi tertentu, terutama jika sistem AI mereka diklasifikasikan sebagai sistem dengan risiko sistemik. Pasal 5 Undang-Undang AI melarang jenis-jenis sistem AI tertentu: ▪ AI yang memanipulasi perilaku melalui teknik subliminal atau mengeksploitasi kerentanan, menyebabkan kerusakan yang signifikan. ▪ Sistem yang mengklasifikasikan individu berdasarkan atribut sensitif tanpa konteks yang tepat atau kategorisasi penegakan hukum. ▪ Praktik penilaian sosial yang memiliki konsekuensi negatif bagi individu (“penilaian sosial”). ▪ AI yang memprediksi perilaku kriminal hanya berdasarkan profil, tanpa hubungan konkret dan faktual dengan aktivitas kriminal yang sebenarnya. ▪ Pengumpulan data pengenalan wajah tanpa target untuk basis data. ▪ AI yang menghasilkan emosi di lingkungan kerja atau pendidikan, kecuali untuk aplikasi medis atau keamanan. ▪ Identifikasi biometrik jarak jauh secara real-time (“RBI”) oleh lembaga penegak hukum di ruang publik, dengan pengecualian terbatas untuk hal-hal mendesak seperti pencarian orang hilang atau pencegahan ancaman yang akan segera terjadi, termasuk kejahatan serius. Undang-undang menetapkan prosedur ketat untuk penilaian dan persetujuan aplikasi AI berisiko tinggi, khususnya yang digunakan dalam penegakan hukum dan pengawasan publik. Sistem ini harus menjalani penilaian dampak hak asasi manusia dan menerima persetujuan yang diperlukan sebelum digunakan untuk memastikan bahwa penggunaannya sah dan etis. Regulasi ini sangat menekankan perlindungan hak-hak mendasar individu dan memastikan transparansi dalam penggunaan sistem AI. Ini termasuk komunikasi yang jelas dengan publik tentang penggunaan teknologi yang berpotensi mengganggu, seperti identifikasi biometrik secara real-time, dan memastikan bahwa sistem AI tidak melanggar bias atau melanggar privasi serta hak dan kebebasan mendasar lainnya.

Amerika Serikat	Amerika Serikat mengambil sikap dengan memiliki total investasi swasta tertinggi di bidang ini di dunia. Pada tahun 2022, AS akan menyediakan investasi AI sebesar \$47,4 miliar, sekitar 3,5 kali lebih banyak daripada China, yang merupakan investor tertinggi berikutnya. Amerika Serikat juga memiliki jumlah perusahaan rintisan AI tertinggi, hampir dua kali lipat dari total jumlah perusahaan di Uni Eropa dan Inggris dan 3,4 kali lebih banyak di China. Pada Oktober 2023, Presiden Biden mengeluarkan perintah eksekutif yang bertujuan menjadikan Amerika Serikat sebagai pemimpin dalam kecerdasan buatan (AI) sambil mengelola risikonya. Perintah eksekutif ini menetapkan standar baru untuk keamanan AI, menekankan perlindungan privasi, promosi kesetaraan dan hak-hak sipil, perlindungan konsumen dan pekerja, promosi inovasi dan persaingan, dan penguatan kepemimpinan Amerika di tingkat global. Tujuan utama dari Perintah Eksekutif tersebut meliputi: ▪ Para pengembang sistem AI yang paling canggih harus diwajibkan untuk membagikan hasil uji keamanan mereka dan informasi penting lainnya kepada pemerintah AS. ▪ Institut Standar dan Teknologi Nasional (NIST) akan menetapkan standar ketat untuk pengujian ekstensif guna memastikan keamanan sebelum dirilis ke publik. ▪ Melindungi dari risiko penggunaan AI dalam pengembangan bahan biologis berbahaya dengan mengembangkan standar baru yang ketat untuk penyaringan sintesis biologis. ▪ Melindungi warga Amerika dari penipuan dan tipu daya yang didukung AI dengan menetapkan standar dan praktik terbaik untuk mengenali konten yang dihasilkan AI dan mengautentikasi konten resmi. ▪ Mengatasi potensi diskriminasi dan bias AI di berbagai sektor dan memberikan panduan yang jelas untuk mengurangi risiko ini. ▪ Memastikan bahwa AI bermanfaat bagi konsumen tanpa menimbulkan kerugian dan mempromosikan perubahan positif dalam perawatan kesehatan dan pendidikan melalui AI. ▪ Melihat dampak AI pada angkatan kerja, mempromosikan pelatihan kejuruan, dan mengembangkan praktik terbaik untuk memaksimalkan manfaat AI bagi pekerja. ▪ Bertujuan untuk mempertahankan kepemimpinan Amerika dalam inovasi AI dengan mendukung penelitian dan memastikan ekosistem AI yang kompetitif. ▪ Memperluas kerja sama internasional untuk mempromosikan penggunaan AI yang aman dan bertanggung jawab di seluruh dunia guna memastikan bahwa penggunaan AI sesuai dengan standar keselamatan dan pertimbangan etika.

	▪ Memberikan panduan kepada lembaga federal tentang pengadaan dan penggunaan AI untuk memastikan bahwa penggunaan AI oleh pemerintah aman, etis, dan efektif. Perintah Eksekutif ini mewakili pendekatan komprehensif terhadap AI yang menyeimbangkan kebutuhan akan inovasi dengan kebutuhan untuk mengatasi tantangan etika dan keselamatan yang ditimbulkan oleh teknologi AI.
Cina	China melaporkan investasi sebesar 13,4 miliar dolar dalam AI untuk tahun 2022. Berdasarkan makalah tentang tata kelola AI di China: Pendekatan China terhadap tata kelola AI ditanda dengan upaya mencari keseimbangan antara mendukung pengembangan AI dan pengendalian regulasi untuk mengurangi ancaman sosial dan ekonomi. Pemerintah China secara bertahap meningkatkan perhatian regulasinya terhadap AI, mengambil pendekatan yang ditargetkan untuk menghindari terhambatnya inovasi. Pendekatan ini mencakup persyaratan keamanan siber dan perlindungan data yang tinggi, dengan sebagian besar dokumen regulasi pada tahap ini bersifat tidak mengikat dan eksperimental. Diharapkan bahwa persyaratan yang lebih spesifik akan dimasukkan dalam undang-undang dan peraturan AI provinsi di masa mendatang dari waktu ke waktu untuk memperjelas legislasi untuk semua sektor. Makalah ini menyoroti fase-fase terpenting regulasi AI di China: ▪ Tahun 2017–2020: Awalnya, China berfokus pada pengaturan mandiri industri dan peluang strategis untuk AI dengan memperkenalkan kebijakan dasar tanpa memberlakukan hambatan regulasi yang ketat. ▪ Tahun 2020–2022: Selama periode ini, standar nasional untuk teknologi AI dan aplikasi pembelajaran mesin dirumuskan, yang mencerminkan pergeseran menuju keterlibatan langsung pemerintah dalam tata kelola AI. ▪ Dari tahun 2022 hingga saat ini: Baru-baru ini, fokus telah bergeser ke pemberlakuan peraturan khusus dan mengikat untuk masing-masing industri dan teknologi, yang dipimpin oleh Administrasi Ruang Siber Tiongkok (CAC). Tren menuju peraturan yang lebih terarah dan spesifik sektor ini kemungkinan akan berlanjut dengan terciptanya kerangka hukum untuk AI. Kota-kota percontohan seperti Shenzhen dan Shanghai telah mengambil peran pelopor dalam memberlakukan peraturan untuk mempromosikan pengembangan AI dan telah melakukan eksperimen administratif di tingkat lokal untuk menarik investasi AI dan persetujuan kebijakan dari pemerintah pusat. Pilar utama tata kelola AI Tiongkok:

	▪ Moderasi konten: Pengelolaan konten daring dengan fokus pada keterlacakan, keaslian, dan pembatasan informasi yang melanggar peraturan yang berlaku. ▪ Perlindungan data: dibahas secara singkat dalam konteks tata kelola AI, dengan mengacu pada ketentuan undang-undang perlindungan data yang ada untuk mencakup pemrosesan data pribadi dalam layanan AI. ▪ “Tata kelola algoritma”: Memastikan keamanan, etika, dan kejelasan algoritma, dengan fokus khusus pada penilaian keamanan, standar etika, dan penyediaan layanan yang transparan. Dengan kerangka kerja yang terus berkembang yang bertujuan untuk mendukung inovasi AI sekaligus mengelola potensi risikonya, model tata kelola Tiongkok mencerminkan pengawasan pemerintah dan pertumbuhan industri dalam konteks tata kelola digital dan data yang lebih luas.
Perbandingan Uni Eropa vs. AS vs. Tiongkok	Cakupan: ▪ Undang-Undang AI Uni Eropa adalah kerangka hukum komprehensif yang mengklasifikasikan sistem AI berdasarkan tingkat risikonya dan menyediakan serangkaian persyaratan untuk berbagai kategori aplikasi AI. Tujuannya adalah untuk mengurangi risiko dengan memberlakukan kewajiban ketat pada sistem AI berisiko tinggi, dengan fokus pada perlindungan hak-hak fundamental dan memastikan keamanan. ▪ Perintah Eksekutif Presiden Biden adalah arahan administratif yang menguraikan pendekatan pemerintah AS untuk mempromosikan inovasi AI sambil mengelola risikonya. Perintah ini menekankan keamanan nasional, daya saing ekonomi, privasi, kesetaraan, dan penggunaan AI yang etis, serta mengarahkan tindakan spesifik di seluruh lembaga federal. ▪ China mempromosikan pengawasan negara, dengan fokus pada menjaga ketertiban sosial, pembangunan ekonomi, dan meningkatkan kontrol negara atas informasi. Pendekatan Regulasi: ▪ Uni Eropa menekankan pendekatan regulasi preventif berbasis risiko yang berupaya secara proaktif mengatasi potensi bahaya yang terkait dengan teknologi AI, khususnya berfokus pada risiko sosial seperti diskriminasi. ▪ Strategi AS yang diuraikan dalam perintah eksekutif bertujuan untuk mendorong inovasi dan daya saing di sektor AI, sekaligus mengatasi masalah keamanan dan etika. Strategi ini mengusulkan kerangka kerja yang lebih fleksibel dan mudah beradaptasi yang akan berkembang seiring dengan teknologi AI.

	▪ Pendekatan Tiongkok mencakup langkah-langkah dukungan untuk pengembangan AI dan regulasi kehati-hatian untuk mengurangi risiko, dengan fokus pada moderasi konten, perlindungan data, dan tata kelola algoritma. Implementasi dan penegakan: ▪ Undang-Undang AI Uni Eropa dirancang untuk berlaku langsung di semua Negara Anggota Uni Eropa dan menetapkan aturan dan kewajiban yang seragam untuk sistem AI yang ditegakkan oleh otoritas pengawas nasional. ▪ Perintah Eksekutif AS mengarahkan lembaga federal untuk mengembangkan dan menerapkan standar, kebijakan, dan langkah-langkah untuk memastikan pengembangan dan penerapan AI yang bertanggung jawab. Perintah tersebut menyerukan kolaborasi dengan Kongres untuk menciptakan kerangka peraturan yang lebih kuat yang menekankan pendekatan yang lebih terdesentralisasi dan spesifik sektor. ▪ Tiongkok menggunakan campuran peraturan wajib dan standar yang tidak mengikat, dengan pemerintah provinsi dan pengaturan mandiri industri memainkan peran penting pada tahap awal dan beralih ke peraturan yang lebih spesifik dan terarah seiring waktu. Kualitas kepemimpinan: ▪ Meskipun Uni Eropa dan AS sama-sama mengakui sifat global dari tantangan AI dan kebutuhan akan kerja sama internasional, Undang-Undang AI Uni Eropa memposisikan Uni Eropa sebagai penentu standar dalam tata kelola AI global dan berupaya memengaruhi norma dan praktik internasional. ▪ Pendekatan AS, menurut Perintah Eksekutif, berfokus pada mempertahankan kepemimpinan AS dalam inovasi AI dan memastikan penggunaan AI yang aman dan etis baik di dalam negeri maupun internasional. Hal ini menekankan peran AS dalam membentuk kerangka kerja dan standar global melalui komitmen bilateral dan multilateral. ▪ China menekankan kontrol domestik dan penggunaan strategis AI untuk pembangunan nasional dan manajemen sosial, berfokus pada penetapan aturannya sendiri untuk dunia maya sambil terlibat dalam kerja sama internasional untuk memengaruhi standar dan norma global.

BAB 3

HAK DAN KEWAJIBAN DALAM UU AI

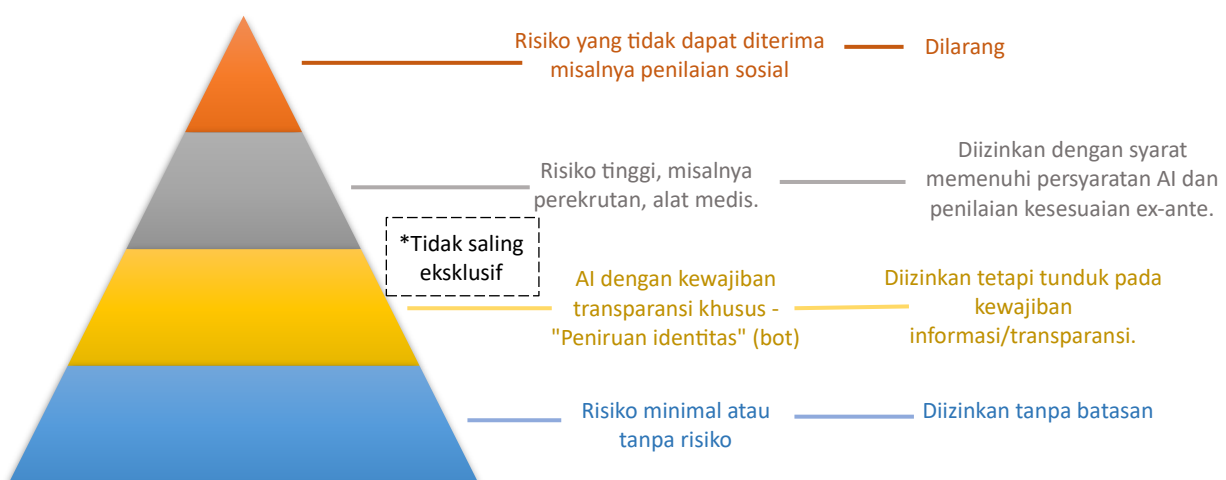
3.1 PENGANTAR UNDANG-UNDANG AI

Di era revolusi digital, kecerdasan buatan telah mengambil tempatnya sebagai kekuatan pendorong di balik inovasi dan peningkatan yang tak terhitung jumlahnya di berbagai bidang kehidupan. Dari optimalisasi proses industri hingga personalisasi pengalaman pengguna di media digital dan dukungan dalam diagnostik medis – kemampuan sistem AI tampaknya tak terbatas. Namun, perkembangan pesat ini juga disertai dengan tantangan etika dan hukum yang signifikan, khususnya terkait dengan perlindungan hak-hak fundamental.

UU AI pada dasarnya didasarkan pada gagasan melindungi hak-hak fundamental, memastikan keamanan, dan melindungi demokrasi, supremasi hukum, dan lingkungan. Undang-undang ini merupakan undang-undang AI komprehensif pertama di dunia (lihat bab 2 “Geopolitik”) dan bertujuan untuk memanfaatkan potensi manfaat AI bagi masyarakat sekaligus mengurangi risiko yang terkait dengan sistem AI tertentu.

Pendekatan berbasis risiko untuk mengklasifikasikan sistem AI ke dalam berbagai kategori memastikan bahwa upaya regulasi difokuskan pada aplikasi AI yang memiliki dampak signifikan terhadap keselamatan dan hak-hak dasar individu sebagaimana dilindungi oleh Piagam Hak-Hak Dasar Uni Eropa. Regulasi tersebut mencantumkan sistem AI berisiko tinggi, merinci kewajiban bagi penyedia sistem tersebut, termasuk perlunya penilaian kesesuaian sebelum sistem ini dapat dipasarkan atau dioperasikan.

Selain itu, regulasi tersebut melarang praktik AI tertentu yang dianggap tidak dapat diterima karena bertentangan dengan nilai-nilai Uni Eropa dengan melanggar hak-hak dasar. Contohnya termasuk sistem peringkat sosial, eksploitasi kerentanan melalui teknik subliminal, dan penggunaan tertentu dari pengenalan biometrik jarak jauh secara real-time.



Gambar 3.1 Pendekatan Berbasis Risiko terhadap Regulasi

Persyaratan kerja sama dengan otoritas, pembentukan kembali otoritas (terutama kantor AI), dan sanksi berat melengkapi gambaran tersebut.

3.2 PENGANTAR UNDANG-UNDANG AI

Informasi dasar tentang Undang-Undang AI

Peraturan Uni Eropa tentang regulasi kecerdasan buatan, yang dikenal sebagai Undang-Undang AI atau Peraturan AI, memiliki judul resmi lengkap “Peraturan (UE) 2024/1689 Parlemen Eropa dan Dewan tanggal 13 Juni 2024 yang menetapkan aturan harmonisasi tentang kecerdasan buatan” dan diterbitkan dalam Jurnal Resmi Uni Eropa pada tanggal 12 Juli 2024. Undang-Undang AI berlaku mulai 2 Agustus 2024 sesuai dengan Pasal 113 Undang-Undang AI, tetapi ketentuan tertentu tidak akan berlaku sampai nanti.

Parlemen Eropa mengadopsi Undang-Undang AI pada tanggal 13 Maret 2024. Persetujuan Dewan Uni Eropa berlangsung pada Mei 2024. Pada tanggal 12 Juli 2024, Peraturan tersebut diterbitkan dalam Jurnal Resmi Uni Eropa dan mulai berlaku 20 hari kemudian, pada tanggal 2 Agustus 2024, untuk diterapkan pada prinsipnya dua tahun kemudian (Pasal 113 Undang-Undang AI dan Pertimbangan 179 Undang-Undang AI). Namun, beberapa bidang mulai berlaku pada waktu lain.

Sebagai peraturan, ketentuan Undang-Undang AI langsung berlaku di semua Negara Anggota Uni Eropa di semua wilayahnya tanpa perlu transposisi ke dalam hukum nasional (Pasal 113 Undang-Undang AI).



Awal Penerapan UU AI

Pertimbangan 179 UU AI lebih lanjut menyatakan bahwa “Meningkatkan risiko yang tidak dapat diterima yang terkait dengan penggunaan AI dengan cara tertentu,” beberapa ketentuan

harus diterapkan lebih awal, seperti aturan tentang sistem yang dilarang. Sebaliknya, diperkirakan bahwa ketentuan untuk sistem berisiko tinggi yang tercantum dalam Pasal 6 ayat 1 UU AI hanya akan berlaku tiga tahun setelah mulai berlaku.

Gambaran umum ini mengilustrasikan jadwal bertahap untuk pemberlakuan berbagai bagian peraturan tersebut. Pendekatan bertahap ini memberi semua pemangku kepentingan, mulai dari pengembang dan penyedia AI hingga pengguna, kesempatan untuk mempersiapkan diri menghadapi persyaratan baru dan memastikan bahwa sistem dan proses mereka memenuhi persyaratan baru tersebut.

Kerangka waktu yang berbeda untuk pemberlakuan masing-masing bab mencerminkan keinginan untuk mencapai keseimbangan antara melindungi warga negara secara langsung dan memberikan perusahaan periode implementasi yang wajar.

Tujuan Undang-Undang AI

Peraturan Kecerdasan Buatan Uni Eropa adalah seperangkat aturan komprehensif yang bertujuan untuk membentuk pengembangan dan penggunaan sistem AI di Eropa. Ini merupakan langkah penting untuk mendorong inovasi dan kepercayaan pada teknologi dengan mencapai keseimbangan antara melindungi kepentingan publik, keamanan, dan hak-hak fundamental, serta mendukung kemajuan teknologi.

Keberfungsian Pasar Uni Eropa	AI yang Berpusat pada Manusia dan Dapat Dipercaya	Tingkat Perlindungan yang Tinggi terhadap Dampak Berbahaya	Untuk Mendukung Inovasi
•Kerangka hukum yang seragam di seluruh Negara Anggota •Harmonisasi pasar Uni Eropa •Pergerakan barang lintas batas secara bebas	•Perlindungan data pribadi •Menjamin keselamatan •Menjamin kesehatan •Perlindungan hak-hak fundamental •Pembangunan kompetensi	•Perlindungan demokrasi •Perlindungan supremasi hukum •Hak-hak sipil •Perlindungan lingkungan •Mendorong kesempatan kerja	•Pengembangan •Penempatan di pasar •Pengoperasian •Penggunaan sistem AI •Dukungan bagi usaha kecil dan menengah (UKM) serta perusahaan rintisan

Gambar 3.2 Tujuan Regulasi AI Uni Eropa

Salah satu tujuan utama Undang-Undang AI adalah untuk memastikan kelancaran fungsi pasar internal. Hal ini dicapai dengan memperkenalkan aturan seragam untuk pengembangan, pemasaran, dan penggunaan sistem AI di Uni Eropa. Pendekatan yang harmonis ini mencegah fragmentasi pasar melalui berbagai hukum nasional dan mendorong penerapan dan kepatuhan yang koheren di seluruh perbatasan nasional.

Elemen kunci lain dari regulasi ini adalah promosi AI yang berpusat pada manusia dan dapat dipercaya. Ini berarti bahwa pengembangan dan penggunaan teknologi AI harus sejalan dengan nilai-nilai dan hak-hak mendasar yang dijunjung tinggi di Uni Eropa. Ini termasuk melindungi data pribadi, memastikan keselamatan dan kesehatan warga negara, serta melindungi demokrasi dan supremasi hukum.

Pasal 1 ayat 1 UU AI

Tujuan Peraturan ini adalah untuk meningkatkan fungsi pasar internal dan mendorong penerapan kecerdasan buatan (AI) yang berpusat pada manusia dan dapat dipercaya, sekaligus memastikan tingkat perlindungan yang tinggi terhadap kesehatan, keselamatan, dan hak-hak mendasar yang diabadikan dalam Piagam Hak-Hak Dasar, termasuk demokrasi, supremasi hukum, dan perlindungan lingkungan, dari dampak buruk sistem kecerdasan buatan (AI) di Uni Eropa dan mendukung inovasi.

Pertimbangan ke-6 UU AI juga mensyaratkan “bahwa AI adalah teknologi yang berpusat pada manusia. AI harus berfungsi sebagai alat bagi manusia dan pada akhirnya meningkatkan kesejahteraan manusia”. Oleh karena itu, seruan Uni Eropa yang jelas adalah untuk menggunakan kecerdasan buatan sebagai alat untuk meningkatkan kualitas hidup manusia, baik dengan memfasilitasi proses kerja, meningkatkan perawatan kesehatan, meningkatkan efisiensi di berbagai sektor, atau membantu mengatasi tantangan global seperti perubahan iklim atau efisiensi sumber daya dan energi (Pertimbangan ke-4 UU AI).

Lingkup Penerapan UU AI

Pasal 2 UU AI mendefinisikan lingkup penerapan Peraturan dan pada dasarnya mencakup semua sistem AI yang dibuat, didistribusikan, dan dioperasikan di Uni Eropa atau diterapkan pada orang-orang yang berada di dalam Uni Eropa (Pasal 2 ayat 1 huruf l UU AI).

Gambaran umum berikut mengilustrasikan area penerapan peraturan dan area yang tidak tercakup oleh peraturan tersebut:

Tabel 3.1 Lingkup Penerapan Undang-Undang AI Uni Eropa

Ruang Lingkup Penerapan Undang-Undang AI	Tidak termasuk dalam Area Aplikasi
- Penyedia yang memasarkan model AI untuk tujuan umum (Pasal 2 ayat 1 huruf a UU AI) - Penyedia dan penyebar sistem AI, terlepas dari apakah mereka berbasis di Uni Eropa atau di negara ketiga, asalkan sistem tersebut digunakan di Uni Eropa atau hasilnya digunakan di Uni Eropa (Pasal 2 ayat 1 huruf a sampai c UU AI) - Produsen produk yang memasarkan sistem AI atau mengoperasikannya bersama dengan produk mereka dengan nama atau merek dagang mereka sendiri (Pasal 2 ayat 1 huruf e UU AI) - Sistem AI yang dipasarkan, dioperasikan, atau digunakan di Uni Eropa. Ini berlaku untuk penyedia, penyebar, importir, dan distributor sistem AI (Pasal 2 ayat 1 UU AI) - Perwakilan resmi penyedia yang tidak berkedudukan di Uni Eropa (Pasal 2 ayat 1 huruf f UU AI)	- Sistem AI yang dapat digunakan untuk aktivitas pribadi dan non-komersial individu (Pasal 2 ayat 10 UU AI) - Sistem AI yang digunakan di bidang yang tidak tercakup oleh hukum Uni Eropa (misalnya, keamanan nasional) dan sistem AI yang digunakan secara eksklusif untuk tujuan militer atau keamanan nasional (Pasal 2 ayat 3 UU AI) - Sistem AI yang digunakan semata-mata untuk tujuan penelitian dan pengembangan dikembangkan dan dioperasikan (Pasal 2 ayat 6 UU AI) - Sistem AI untuk kegiatan penelitian, pengujian, dan pengembangan sebelum dipasarkan atau dioperasikan, kecuali untuk pengujian di dunia nyata (Pasal 2 ayat 8 UU AI) - Otoritas di negara ketiga dan organisasi internasional, dengan ketentuan bahwa terdapat perlindungan yang memadai terkait perlindungan individu (Pasal 2 ayat 4 GDPR)

Sistem AI yang menimbulkan risiko tertentu terhadap kesehatan, keselamatan, atau hak-hak dasar warga negara disebut sistem AI berisiko tinggi.

Pasal 2 ayat 2 Undang-Undang AI menetapkan area penerapan dan pengecualian untuk sistem AI berisiko tinggi yang terkait dengan produk yang tercakup dalam undang-undang harmonisasi Uni Eropa tertentu sebagaimana tercantum dalam Lampiran I Bagian B Undang-Undang AI. Paragraf ini mengklarifikasi bahwa hanya Pasal 112 Undang-Undang AI (Penilaian dan verifikasi) yang berlaku untuk sistem AI berisiko tinggi tertentu ini. Pasal 57 Undang-Undang AI (Sandbox AI) berlaku, tetapi hanya sejauh persyaratan untuk sistem AI berisiko tinggi telah diintegrasikan ke dalam undang-undang harmonisasi Uni Eropa yang disebutkan di atas.

Peraturan ini mencerminkan upaya untuk menghindari tumpang tindih atau konflik antara Undang-Undang AI dan undang-undang Uni Eropa yang sudah ada dan telah diharmonisasikan. Diakui bahwa produk-produk tertentu yang menggabungkan atau dianggap menggabungkan teknologi AI mungkin sudah diatur oleh arahan Uni Eropa atau peraturan Uni Eropa lainnya. Referensi khusus pada Pasal 112 Undang-Undang AI dan penerapan bersyarat Pasal 57 Undang-Undang AI (Sandbox AI) berlaku, tetapi hanya sejauh persyaratan untuk sistem AI berisiko tinggi telah diintegrasikan ke dalam undang-undang harmonisasi Uni Eropa yang disebutkan di atas. Pasal 57 UU AI dimaksudkan untuk memastikan bahwa kepatuhan terhadap persyaratan untuk sistem AI berisiko tinggi sejalan dengan kerangka hukum harmonis yang sudah ada, tanpa menciptakan peraturan yang berlebihan atau bertentangan.

Pertimbangan 9 UU AI menyebutkan peraturan Uni Eropa harmonis lainnya yang tetap tidak terpengaruh. Ini secara eksplisit adalah “bidang perlindungan data, perlindungan konsumen, hak-hak dasar, ketenagakerjaan, perlindungan karyawan, dan keamanan produk”, “termasuk kesehatan dan keselamatan kerja serta hubungan antara pengusaha dan karyawan”.

Pasal 2 ayat 11 UU AI memperkuat kekhawatiran ini dengan mensyaratkan “pemeliharaan atau pengenalan undang-undang, peraturan, atau ketentuan administratif yang lebih menguntungkan karyawan sehubungan dengan perlindungan hak-hak mereka ketika pengusaha menggunakan sistem AI”.

Pasal 2 ayat 11 UU AI Pasal 12 UU AI menyatakan bahwa sistem AI yang tersedia secara bebas untuk semua orang dan kode sumbernya dapat diakses dan digunakan secara terbuka (open source) tidak tunduk pada aturan UU AI, kecuali dalam kasus-kasus berikut:

- Sistem AI open source diklasifikasikan sebagai berisiko tinggi: Sistem AI berisiko tinggi berpotensi berdampak serius pada keselamatan, kesehatan, atau hak-hak dasar masyarakat. Jika sistem tersebut, meskipun open source, dipasarkan atau digunakan di Uni Eropa, sistem tersebut harus mematuhi persyaratan ketat UU AI.
- Sistem AI termasuk dalam Pasal 5 UU AI atau Pasal 50 UU AI: Kedua pasal tersebut membahas jenis-jenis sistem AI tertentu dan penggunaannya, yang secara khusus diatur karena potensi dampaknya. Pasal 5 membahas praktik-praktik terlarang di bidang AI dan Pasal 50 membahas kewajiban transparansi bagi penyedia dan

pengembang sistem AI tertentu. Jika sistem AI open source termasuk dalam kategori ini, sistem tersebut juga tunduk pada ketentuan hukum.

*Pada prinsipnya, penggunaan lisensi sumber terbuka (*open source license*) tidak mengecualikan berlakunya AI Act. Faktor penentu adalah jenis sistem serta konteks penggunaannya, khususnya apabila sistem tersebut menimbulkan risiko bagi individu atau termasuk dalam ketentuan khusus sebagaimana diatur dalam Pasal 5 AI Act atau Pasal 50 AI Act.*

Definisi Sistem AI

Definisi sistem AI dalam Undang-Undang AI sengaja dibuat luas untuk mencakup berbagai macam teknologi dan bentuk aplikasi serta untuk mengikuti perkembangan teknologi regulasi yang pesat. Hal ini untuk memastikan bahwa regulasi tetap berlaku meskipun teknologi terus berkembang.

*Menurut AI Act, istilah ****sistem AI**** mencakup sistem berbasis mesin yang dirancang untuk beroperasi dengan tingkat otonomi yang bervariasi, yang dapat bersifat adaptif setelah dioperasikan, serta yang—berdasarkan masukan yang diterimanya untuk tujuan yang bersifat eksplisit maupun implisit—menentukan cara menghasilkan keluaran seperti prediksi, konten, rekomendasi, atau keputusan yang dapat memengaruhi lingkungan fisik maupun virtual (Pasal 3 angka 1 AI Act).*

Definisi ini secara konseptual komprehensif dan mencakup perkembangan teknologi AI saat ini dan di masa mendatang. Fokusnya adalah pada sistem yang dapat memproses dan menginterpretasikan data untuk melakukan tugas, membuat keputusan, atau menghasilkan konten yang mensimulasikan atau menggantikan pekerjaan manusia.

Model AI tujuan umum didefinisikan dalam Pasal 3 ayat 63 UU AI sebagai model AI yang dirancang untuk melakukan berbagai tugas, bukan terbatas pada fungsi tertentu. Model-model ini sangat fleksibel dan dapat digunakan di berbagai bidang. Beberapa karakteristik utamanya adalah:

- **Kegunaan umum yang signifikan:** Model ini tidak terbatas pada aplikasi atau tugas tertentu, tetapi dapat digunakan untuk berbagai tugas. Fleksibilitas ini membedakannya dari sistem AI yang dikembangkan untuk tujuan tertentu.
- **Kemampuan untuk melakukan tugas secara kompeten:** Model ini dapat melakukan berbagai tugas secara efektif. Ini berarti bahwa model ini dapat berguna dan efektif di banyak bidang atau konteks yang berbeda.
- **Integrasi ke dalam sistem atau aplikasi hilir:** Model ini dapat disematkan dalam berbagai sistem atau aplikasi yang berbeda. Hal ini menjadikannya komponen serbaguna yang dapat digunakan dalam berbagai produk atau layanan.
- **Pelatihan dengan sejumlah besar data di bawah pengawasan mandiri yang ekstensif:** Seringkali model-model ini dikembangkan dengan pelatihan menggunakan sejumlah besar data, di mana teknik-teknik canggih seperti pengawasan mandiri dapat

digunakan. Hal ini memungkinkan model untuk belajar dari berbagai macam informasi dan meningkatkan kemampuannya untuk melakukan tugas di berbagai domain.

- **Pengecualian untuk penelitian dan pengembangan:** Model AI yang digunakan secara eksklusif untuk tujuan penelitian dan pengembangan atau untuk pembuatan prototipe sebelum peluncuran pasar tidak termasuk dalam kategori ini. Ini berarti bahwa model-model tertentu yang masih dalam tahap pengembangan dan digunakan untuk tujuan eksperimental atau penelitian tidak dianggap sebagai model AI tujuan umum.

Sistem AI tujuan umum adalah sistem AI yang didasarkan pada model AI tujuan umum dan mampu melayani berbagai tujuan baik untuk penggunaan langsung maupun untuk integrasi ke dalam sistem AI lainnya (Pasal 3 no. 66 UU AI).

Peran Orang Perseorangan atau Badan Hukum

UU AI mendefinisikan berbagai sebutan untuk peran yang dapat diemban oleh orang perseorangan atau badan hukum, otoritas, lembaga, atau badan lainnya. Semua ini dirangkum dalam istilah “**operator**”. Peran-peran individual dalam UU AI dijelaskan sebagai berikut:

Peran	Deskripsi	Tugas
Penyedia (Pasal 3 ayat 3 UU AI)	Pengembang atau yang telah mengembangkan sistem AI atau model AI dengan tujuan umum yang memasarkannya atau mengoperasikannya dengan nama atau merek dagangnya, baik berbayar maupun gratis.	Bertanggung jawab atas kesesuaian sistem AI dengan persyaratan Peraturan AI, termasuk melakukan penilaian kesesuaian, menyediakan dokumentasi yang diperlukan, dan mendaftarkan sistem AI berisiko tinggi.
Penyebarnya (Pasal 3 ayat 4 UU AI)	Pengguna sistem AI atas tanggung jawab mereka sendiri, kecuali untuk penggunaan pribadi dan non-profesional.	Memastikan kepatuhan terhadap peraturan operasional sistem AI, khususnya terkait dengan transparansi dan kewajiban informasi terhadap subjek data dan kepatuhan terhadap peraturan perlindungan data.
Perwakilan resmi (Pasal 3 ayat 5 UU AI)	Seseorang yang ditunjuk secara tertulis oleh penyedia yang berbasis di Uni Eropa dan yang memikul kewajiban penyedia sehubungan dengan kepatuhan terhadap Undang-Undang AI.	Mengemban kewajiban yang ditetapkan dalam Peraturan atas nama penyedia, termasuk memastikan kepatuhan dan melakukan prosedur yang diperlukan.
Importir (Pasal 3 ayat 6 UU AI)	Memasarkan sistem AI di Uni Eropa dengan nama atau merek dagang seseorang yang berkedudukan di luar Uni Eropa.	Memastikan bahwa sistem AI yang diimpor ke Uni Eropa mematuhi persyaratan Undang-Undang AI sebelum dipasarkan, termasuk penilaian kesesuaian dan penyediaan dokumentasi yang diperlukan.
Distributor (Pasal 3 ayat 7 UU AI)	Setiap orang dalam rantai pasokan yang menyediakan sistem AI di pasar Uni Eropa, kecuali pemasok atau importir.	Harus memeriksa bahwa sistem AI memiliki penandaan yang benar, bahwa dokumen yang diperlukan tersedia, dan bahwa penyedia sistem AI telah memenuhi persyaratan Uni Eropa.
Produsen produk (Pasal 2 ayat 1 huruf e UU AI)	Membawa sistem AI bersama dengan produknya ke pasar atau mengoperasikannya dengan nama atau merek dagangnya sendiri.	Bertanggung jawab untuk memastikan bahwa produk, termasuk sistem AI terintegrasi, mematuhi persyaratan keselamatan dan

kesesuaian Uni Eropa yang berlaku sebelum dipasarkan.

Selain itu, istilah “penyedia hilir” berarti penyedia sistem AI, termasuk sistem AI tujuan umum, yang mengintegrasikan model AI, terlepas dari apakah model tersebut disediakan dan diintegrasikan secara vertikal oleh dirinya sendiri atau disediakan oleh entitas lain berdasarkan hubungan kontraktual (Pasal 3 No. 68 UU AI).

Fase Peluncuran Pasar

Berbagai fase dalam siklus hidup sistem AI mencakup tidak hanya pengembangan dan penggunaan sistem AI, tetapi yang terpenting adalah peluncurannya ke pasar. Dari perspektif hukum, fase-fase berikut adalah definisi untuk fase penyebaran AI dari Pasal 3 UU AI:

Nama Tahapan	Penjelasan
Penempatan di pasar (Pasal 3 ayat 9 UU AI)	Mengacu pada pertama kalinya sistem AI atau model AI tujuan umum tersedia di pasar Uni Eropa. Ini menandai titik waktu ketika produk baru pertama kali tersedia secara komersial.
Penyediaan di pasar (Pasal 3 ayat 10 UU AI)	Mengacu pada penyediaan sistem AI atau model AI dengan tujuan umum untuk didistribusikan atau digunakan di pasar Uni Eropa dalam konteks kegiatan bisnis, baik dengan imbalan pembayaran atau gratis. Fase ini mencakup distribusi komersial dan ketersediaan produk.
Pengoperasian (Pasal 3 ayat 11 UU AI)	Penyediaan sistem AI oleh penyedia di Uni Eropa untuk penggunaan pertama langsung kepada pengguna atau untuk penggunaan sendiri sesuai dengan tujuan yang dimaksudkan. Ini adalah saat sistem AI benar-benar diaktifkan dan digunakan untuk tujuan yang dimaksudkan.
Penarikan kembali sistem AI (Pasal 3 ayat 16 UU AI)	Segala tindakan yang bertujuan untuk mengembalikan sistem AI yang telah disediakan kepada penyedia kepada pengguna atau menonaktifkan atau mematikannya.
Penghentian penggunaan sistem AI (Pasal 3 ayat 17 UU AI)	Segala tindakan yang dimaksudkan untuk mencegah sistem AI dalam rantai pasokan agar tidak tersedia di pasar.

Definisi hukum dari berbagai fase sebagian besar didasarkan pada penerapannya dalam penggunaan AI secara produktif, karena fase pengembangan dan pengujian bukanlah bagian dari peraturan dalam Undang-Undang AI. Waktu transisi dari satu fase ke fase lainnya sangat penting, karena hal ini berdampak pada tanggung jawab dan tugas pengawasan.

Pengecualian untuk ini adalah **pengujian dalam kondisi nyata**, yang memungkinkan pengembang untuk mendapatkan wawasan berharga tentang penerapan praktis dan efektivitas sistem AI mereka dan membantu memastikan bahwa sistem tersebut sesuai dengan persyaratan hukum sebelum secara resmi dipasarkan atau dioperasikan. Proses pengujian ini bertujuan untuk mengumpulkan data dan wawasan tentang fungsi sistem AI dalam kondisi nyata (Pasal 3 ayat 57 Undang-Undang AI).

Istilah untuk Penggunaan Sistem AI

Istilah-istilah kunci yang menjadi pusat pemahaman, penggunaan, dan proses yang berlaku untuk pengembangan, penilaian, dan pemantauan sistem AI berdasarkan Peraturan AI

tercantum dan dijelaskan di bawah ini. Istilah-istilah ini membentuk dasar untuk manajemen keselamatan dan kualitas yang kuat:

Penetapan Penggunaan	Deskripsi
Tujuan penggunaan (Pasal 3 ayat 12 UU AI)	Ini merujuk pada penggunaan atau fungsi sistem AI sebagaimana ditentukan oleh penyedia, seperti yang tertera dalam dokumentasi, instruksi, atau materi promosi yang menyertainya. Tujuan yang dimaksud menentukan tugas-tugas atau kondisi di mana sistem AI dirancang.
Penyalahgunaan yang dapat diperkirakan secara wajar (Pasal 3 ayat 13 UU AI)	Istilah yang menggambarkan situasi di mana sistem AI digunakan dengan cara yang tidak dimaksudkan oleh penyedia, tetapi yang mungkin muncul karena perilaku pengguna akhir atau interaksi yang dapat diperkirakan secara wajar dengan sistem lain. Oleh karena itu, pengembang harus menyadari baik risiko yang mereka sadari maupun risiko yang dapat diperkirakan secara wajar. Ini termasuk penyalahgunaan sistem AI berdasarkan bagaimana manusia biasanya bertindak. Ini termasuk penyalahgunaan atau penggunaan sistem yang tidak tepat yang dapat menyebabkan risiko atau bahaya.
Penilaian kesesuaian (Pasal 3 ayat 20 UU AI)	Suatu prosedur yang memastikan bahwa sistem AI memenuhi persyaratan yang ditetapkan dalam peraturan. Ini termasuk peninjauan dokumentasi teknis, peninjauan proses manajemen keselamatan dan risiko, dan, jika perlu, pengujian atau inspeksi lebih lanjut. Penilaian kesesuaian dapat dilakukan secara internal atau eksternal.
Sistem manajemen risiko (Pasal 9 ayat 2 UU AI)	Suatu proses berkelanjutan yang ditetapkan oleh penyedia sistem AI untuk terus mengidentifikasi, menilai, mengurangi, dan memantau risiko yang terkait dengan penggunaan sistem AI. Ini termasuk langkah-langkah untuk mencegah dan mengurangi risiko terhadap kesehatan, keselamatan, dan hak-hak dasar individu. "Risiko" adalah kombinasi dari kemungkinan terjadinya bahaya dan tingkat keparahan bahaya tersebut (Pasal 3 ayat 2 UU AI).
Risiko sistemik (Pasal 3 ayat 65 UU AI)	Mengacu pada risiko spesifik yang terkait dengan kemampuan luas model AI tujuan umum. Risiko ini muncul dari potensi atau dampak negatif yang dapat diperkirakan terhadap kesehatan masyarakat, keselamatan, hak-hak dasar, atau masyarakat dan dapat berdampak signifikan pada pasar Uni Eropa dengan menyebar luas di sepanjang rantai nilai.
Kinerja sistem AI (Pasal 3 ayat 18 UU AI)	Mengacu pada kemampuan sistem AI untuk melakukan tugas-tugas yang telah ditentukan dan diharapkan dalam kondisi operasi yang dimaksudkan. Kinerja dapat diukur menggunakan berbagai kriteria seperti akurasi, keandalan, ketahanan, dan efisiensi. Evaluasi kinerja sangat penting untuk memastikan bahwa sistem AI memenuhi tujuan yang dimaksudkan dan tidak menimbulkan risiko yang tidak diinginkan.
Perubahan signifikan (Pasal 3 ayat 23 UU AI)	Perubahan substansial adalah setiap modifikasi pada sistem AI setelah dipasarkan atau dioperasikan yang dapat memengaruhi kesesuaiannya dengan persyaratan penting dalam Pasal 8 dan seterusnya dari UU AI, persyaratan untuk sistem AI berisiko tinggi. Ini termasuk perubahan pada fungsionalitas, lingkungan operasi, atau komponen sistem yang berpotensi mengubah profil keselamatan, kinerja, atau risikonya. Perubahan signifikan memerlukan penilaian ulang kesesuaian sistem AI.
Penandaan CE (Pasal 3 ayat 24 UU AI)	Tanda CE adalah tanda yang menunjukkan bahwa suatu produk, termasuk sistem AI, mematuhi peraturan UE yang berlaku dan dapat dipasarkan secara bebas di Wilayah Ekonomi Eropa (EEA). Pemasangan tanda CE merupakan hasil dari

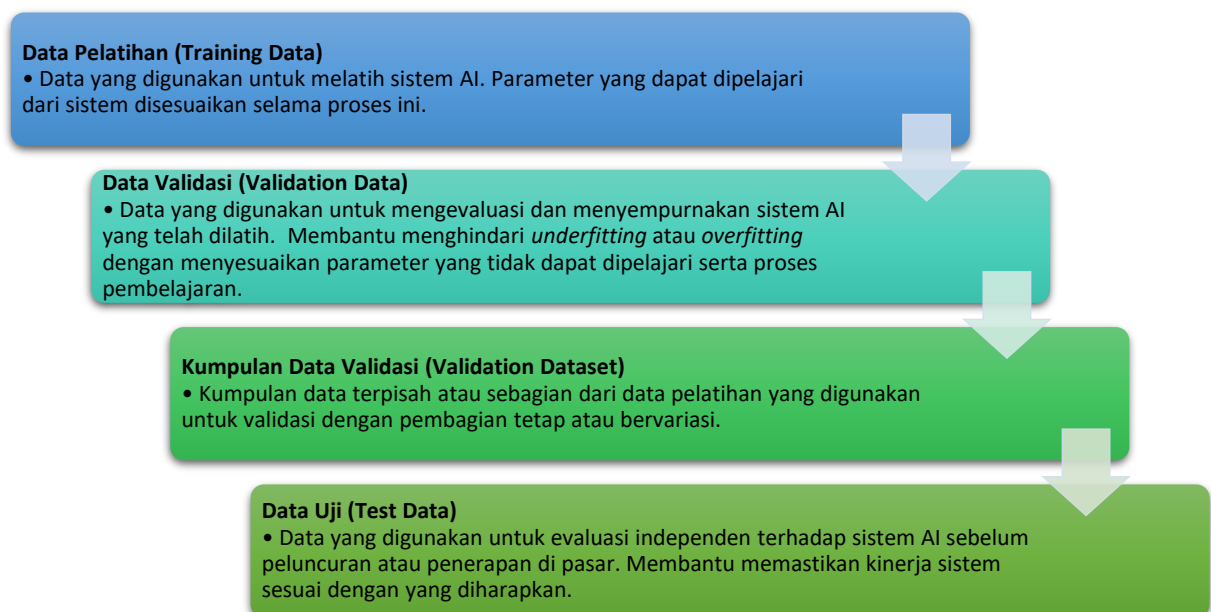
	prosedur penilaian kesesuaian yang menegaskan bahwa produk tersebut mematuhi persyaratan keselamatan, kesehatan, dan perlindungan lingkungan UE.
Sistem pemantauan pasca-pemasaran (Pasal 3 ayat 25 UU AI)	Proses atau aktivitas yang ditetapkan oleh penyedia sistem AI untuk terus memantau kinerja dan keselamatan sistem AI setelah diperkenalkan ke pasar. Ini termasuk mengumpulkan dan menganalisis umpan balik pengguna, memantau insiden, mengidentifikasi potensi masalah keselamatan, dan menerapkan tindakan korektif yang diperlukan. Tujuannya adalah untuk meminimalkan risiko dan memastikan bahwa sistem AI tetap aman dan efektif sepanjang siklus hidupnya.

Penamaan Terkait Data

UU AI menekankan pentingnya transparansi dan ketertelusuran sistem AI. Informasi rinci tentang data yang digunakan membantu memahami dan mengerti keputusan dan tindakan sistem AI. Hal ini sangat penting untuk akuntabilitas dan kepercayaan pada teknologi AI.

Oleh karena itu, sangat penting bahwa penamaan data harus tepat agar selalu berbicara tentang informasi yang benar. Penamaan berikut ini digunakan untuk fase pelatihan AI sesuai dengan Pasal 3 ayat 29-32 UU AI:

Akses ke data berkualitas tinggi sangat penting untuk memastikan fungsionalitas dan keamanan sistem AI tingkat lanjut, terutama ketika model dilatih dengan data. Hal ini diperlukan untuk menjamin bahwa sistem AI berisiko tinggi memenuhi tujuan yang dimaksudkan, beroperasi dengan aman, dan tidak menyebabkan diskriminasi yang melanggar hukum Uni Eropa.



Gambar 3.3 Penunjukan Data untuk Fase Pelatihan dan Pengujian

Hal ini membutuhkan kumpulan data pelatihan, validasi, dan pengujian berkualitas tinggi yang pada gilirannya membutuhkan praktik tata kelola dan manajemen data yang efektif.

Kumpulan data ini tidak hanya harus relevan dan representatif dalam kaitannya dengan tujuan sistem, tetapi juga seakurat dan selengkap mungkin, termasuk pelabelan yang akurat (Pertimbangan 67 Undang-Undang AI).

Prosedur tata kelola data dan manajemen data spesifik yang disesuaikan secara tepat dengan tujuan sistem sangat penting untuk kumpulan data pelatihan, validasi, dan pengujian sistem AI berisiko tinggi. Menurut Pasal 10 ayat 1. 2 Undang-Undang AI, ini mencakup sejumlah langkah penting (seleksi):

- pemilihan dan justifikasi keputusan konseptual yang mendasarinya
- metode pengumpulan dan asal data, termasuk pertimbangan tujuan awal pengumpulan data pribadi
- Proses persiapan data penting seperti anotasi, pelabelan, pembersihan, pembaruan, perluasan, dan penggabungan
- Definisi asumsi, khususnya terkait informasi yang akan dikumpulkan dan disajikan oleh data
- Implementasi langkah-langkah untuk mengidentifikasi, mencegah, dan mengurangi distorsi yang diakui
- Identifikasi kesenjangan atau kekurangan data yang relevan yang menghambat kepatuhan dan strategi untuk mengatasinya

Data juga dibedakan berdasarkan isi dan komposisinya. Tabel berikut berisi definisi dalam hal ini:

Istilah	Deskripsi
Data masukan (Pasal 3 ayat 33 UU AI)	Data yang dimasukkan ke dalam sistem AI atau dikumpulkan langsung oleh sistem tersebut dan berdasarkan data tersebut sistem menghasilkan suatu hasil.
Data biometrik (Pasal 3 ayat 34 UU AI)	Data pribadi yang mencatat karakteristik fisik, fisiologis, atau perilaku seseorang dan diperoleh menggunakan prosedur teknis khusus, misalnya gambar wajah atau sidik jari.
Kategori khusus data pribadi (Pasal 3 ayat 37 UU AI)	Kategori data pribadi yang mengandung informasi yang sangat sensitif, sebagaimana didefinisikan dalam GDPR.
Data pribadi (Pasal 3 ayat 50 UU AI)	Menurut Pasal 4 ayat 1 GDPR, ini adalah setiap informasi yang berkaitan dengan orang perseorangan yang teridentifikasi atau dapat diidentifikasi ("subjek data").
Data non-pribadi (Pasal 3 ayat 51 UU AI)	Data yang bukan data pribadi dalam arti GDPR. Data ini tidak berkaitan dengan orang perseorangan yang teridentifikasi atau dapat diidentifikasi atau telah dianonimkan sedemikian rupa sehingga subjek data tidak dapat atau tidak lagi dapat diidentifikasi. Data non-pribadi dapat diproses dan digunakan secara bebas selama proses ini tidak melanggar hukum lain atau menghilangkan anonimisasi dan membuat orang dapat diidentifikasi.
Data operasional sensitif (Pasal 3 ayat 38 UU AI)	Data operasional yang berkaitan dengan pencegahan, deteksi, investigasi, atau penuntutan tindak pidana, yang pengungkapannya dapat membahayakan integritas proses pidana.

Perlindungan data sensitif dan pribadi sangat penting untuk menjaga privasi, keamanan, dan hak-hak mendasar subjek data. Di dunia di mana data dianggap sebagai minyak baru, konsekuensi dari perlindungan data yang tidak memadai dapat sangat berat bagi individu yang bersangkutan. Mulai dari pencurian identitas dan penipuan keuangan hingga pengawasan yang tidak diinginkan dan diskriminasi, potensi kerugian yang dapat timbul dari penyalahgunaan informasi ini dapat beragam.

Selain itu, penggunaan tanpa izin atau hilangnya data pribadi dapat secara signifikan merusak kepercayaan terhadap teknologi, perusahaan, dan bahkan lembaga pemerintah.

Pasal 3 angka 60 AI Act

*Istilah **deepfake** merujuk pada konten—baik dalam bentuk gambar, rekaman suara, maupun video—yang dibuat atau dimanipulasi menggunakan kecerdasan artifisial (AI). Konten tersebut meniru orang, objek, tempat, atau peristiwa nyata secara begitu meyakinkan sehingga dapat tampak autentik dan benar bagi seseorang yang tidak memiliki kesiapan atau pengetahuan untuk mengidentifikasinya.*

Literasi AI

Sangat penting bagi pengembang (“penyedia”) dan pengguna (“penyebar”) sistem AI untuk memastikan bahwa tim mereka dan semua orang yang berinteraksi dengan sistem ini atas nama mereka memiliki kompetensi dan pengetahuan yang dibutuhkan di bidang kecerdasan buatan (Pasal 4 UU AI). Ini termasuk pemahaman teknis, pengalaman praktis, pendidikan formal, dan pelatihan. Aspek-aspek kunci berikut harus dipertimbangkan:

- **Pengetahuan dan pengalaman teknis:** Penting agar staf tidak hanya memiliki pengetahuan dasar tentang AI, tetapi juga dapat memperoleh pengalaman khusus dengan sistem AI masing-masing.
- **Pendidikan dan pelatihan:** Karyawan harus selalu mengikuti perkembangan teknologi terbaru melalui pendidikan dan pelatihan berkelanjutan. Hal ini membantu memastikan bahwa mereka dapat menggunakan sistem AI secara efektif dan aman.
- **Konteks penggunaan:** Kondisi dan kerangka kerja spesifik di mana sistem AI akan digunakan harus diperhitungkan saat mengembangkan keterampilan. Berbagai bidang aplikasi dapat menimbulkan persyaratan dan tantangan yang berbeda.
- **Kelompok sasaran:** Penting juga untuk mempertimbangkan orang atau kelompok untuk siapa atau kepada siapa sistem AI akan digunakan. Memahami kebutuhan dan potensi risiko bagi kelompok sasaran ini dapat membantu merancang dan mengadaptasi penggunaan sistem AI dengan lebih baik.

Diperlukan penanganan sistem AI yang kompeten oleh personel yang terlatih dengan baik untuk memastikan penggunaannya yang aman dan efektif. Hal ini juga menekankan bahwa pelatihan dan pengalaman yang memadai sangat penting untuk memanfaatkan sepenuhnya potensi manfaat teknologi AI sambil meminimalkan risiko.

Menurut Pasal 3 angka 56 AI Act, “literasi AI” mencakup keterampilan, pengetahuan, dan pemahaman yang memungkinkan penyedia, pengguna (deployer), serta subjek data—

dengan mempertimbangkan hak dan kewajiban masing-masing berdasarkan Peraturan ini—untuk menggunakan sistem AI secara kompeten serta memahami peluang dan risiko AI, termasuk potensi kerugian yang dapat ditimbulkannya.

3.3 LITERASI AI UNTUK PENYEDIA

Bagian ini memberikan pendekatan terstruktur untuk literasi AI dan menekankan perlunya pembelajaran berkelanjutan dan adaptasi terhadap lanskap AI yang terus berkembang. Dengan mengikuti kerangka kerja yang disarankan, penyedia dapat memastikan bahwa karyawan mereka memiliki bekal yang cukup untuk menangani teknologi AI secara bertanggung jawab dan efektif. Selain itu, mereka akan mampu menumbuhkan budaya penggunaan AI yang etis, mempromosikan transparansi dan akuntabilitas, serta mendorong inovasi dalam organisasi mereka.

Kerangka kerja ini menguraikan rekomendasi utama untuk meningkatkan kesiapan digital lembaga, meningkatkan keterampilan digital staf, mempromosikan literasi data, menyediakan pelatihan khusus AI, mempromosikan pembelajaran berkelanjutan, berinvestasi dalam pengembangan bakat, menerapkan strategi manajemen perubahan, dan membangun komunitas praktik. Langkah-langkah ini akan membantu penyedia AI memenuhi persyaratan Undang-Undang AI, memastikan kompetensi AI yang kuat dan penggunaan AI yang bertanggung jawab, dan pada akhirnya berkontribusi pada pengembangan tenaga kerja yang lebih berpengetahuan dan beretika.

Pendahuluan

Transformasi digital, khususnya melalui penggunaan kecerdasan buatan (AI), telah menjadi prioritas bagi organisasi swasta dan publik.

Pemerintah menggunakan teknologi untuk lebih memahami dan memenuhi kebutuhan warga negara. Agar transformasi ini berhasil, diperlukan pendekatan yang komprehensif dan inklusif. Hal ini membutuhkan perubahan dalam model tata kelola, struktur, dan organisasi untuk mengatasi tantangan dan peluang baru yang dihadirkan oleh teknologi digital. Pemerintah dihadapkan pada tantangan yang kompleks dan tidak terduga yang memberikan tekanan pada sektor publik untuk meningkatkan kemampuan.

Sebuah laporan oleh Kelompok Kerja tentang Peningkatan Kapasitas AI menunjukkan kesenjangan yang signifikan dalam **keterampilan digital** pemerintah, khususnya di Global South. Kegagalan proyek transformasi digital seringkali disebabkan oleh infrastruktur TI dan kerangka kebijakan yang tidak memadai, serta keterampilan digital yang tidak mencukupi dan kesulitan dalam menerapkannya secara efektif.

Oleh karena itu, pemerintah di seluruh dunia berfokus pada kompetensi penting – di luar pengetahuan, keterampilan, dan sikap – yang dibutuhkan pegawai negeri untuk menggunakan alat digital, mengembangkan dan menerapkan proyek transformasi digital, serta secara efektif mengatasi masalah tata kelola yang kompleks. Banyak organisasi publik kekurangan keahlian internal dalam AI dan analitik data, sehingga mereka sangat bergantung pada konsultan dan organisasi eksternal untuk proyek AI. Ketergantungan ini sebagian

disebabkan oleh gaji yang lebih rendah di sektor publik, sehingga sulit untuk menarik dan mempertahankan talenta terbaik.

Selain itu, sektor publik harus **mempertimbangkan aspek etika dan hukum yang kompleks** ketika menggunakan AI. Isu-isu seperti privasi, bias, dan akuntabilitas sangat penting, yang merupakan kesulitan lebih lanjut dibandingkan dengan sektor swasta di mana kendala tersebut kurang menonjol. Terlepas dari tantangan ini, ada pengakuan yang semakin meningkat di sektor publik bahwa kemampuan AI perlu dikembangkan. Pemerintah di seluruh dunia semakin fokus pada pembangunan keterampilan digital yang diperlukan di antara pegawai negeri sipil agar dapat menggunakan AI secara efektif. Ini tidak hanya melibatkan perolehan keterampilan teknis, tetapi juga menumbuhkan budaya yang mendukung transformasi digital.

Sebaliknya, **sektor** swasta mendapat manfaat dari gaji yang lebih tinggi dan sumber daya yang lebih baik, yang menarik talenta AI terbaik. Perusahaan swasta memiliki akses ke infrastruktur canggih, termasuk sumber daya komputasi berkinerja tinggi yang dibutuhkan untuk pengembangan AI. Budaya di perusahaan swasta seringkali berfokus pada inovasi cepat dan pengambilan risiko, memungkinkan mereka untuk dengan cepat menerapkan dan mengadaptasi teknologi AI baru. Karyawan di perusahaan-perusahaan ini biasanya memiliki keterampilan yang luas yang memungkinkan mereka untuk secara efektif mengembangkan, memelihara, dan mengoperasikan sistem AI yang canggih. Meskipun demikian, sektor swasta menghadapi kesenjangan keterampilan AI yang signifikan yang sama seperti sektor publik. Berdasarkan data dari survei yang dilakukan pada tahun 2023 oleh Access Partnership dan Amazon Web Services (AWS) dengan 3297 karyawan dan 1340 perusahaan di AS, 73% pemberi kerja memprioritaskan perekrutan profesional AI, dan 75% kesulitan menemukan talenta yang mereka butuhkan.

Permintaan tidak terbatas pada keterampilan teknis; pemikiran kritis dan kreatif juga sangat dihargai. Sayangnya, sebagian besar pemberi kerja dan karyawan tidak yakin keterampilan AI spesifik mana yang harus ditargetkan dan tidak menyadari program pelatihan yang tersedia. Survei yang sama menunjukkan bahwa pada tahun 2028, lebih dari 90% perusahaan AS berencana untuk mengintegrasikan solusi berbasis AI ke dalam operasi mereka. Berbagai departemen diharapkan mendapat manfaat dari perubahan ini, dengan departemen TI memimpin, diikuti oleh penjualan, pemasaran, dan sumber daya manusia. Manfaat utama AI meliputi otomatisasi tugas, peningkatan alur kerja, peningkatan komunikasi, dan membantu karyawan mempelajari keterampilan baru.

Permintaan akan keterampilan AI juga menyebabkan perubahan di pasar tenaga kerja. Perusahaan bersedia menawarkan gaji yang jauh lebih tinggi kepada karyawan dengan keterampilan AI, dengan staf IT berpotensi mendapatkan 47% lebih banyak, menurut laporan AWS. Tren ini juga meluas ke departemen lain, mencerminkan penerapan keterampilan AI yang luas. Hampir 80% pekerja tertarik untuk mengembangkan keterampilan AI, termasuk sebagian besar pekerja yang lebih tua yang melihat nilai dalam peningkatan keterampilan. Diprediksi bahwa AI akan secara fundamental meningkatkan produktivitas. 88% karyawan berharap akan menggunakan AI setiap hari pada tahun 2028. Pemberi kerja percaya bahwa AI dapat

meningkatkan produktivitas secara keseluruhan hingga 49% – peningkatan yang luar biasa dibandingkan dengan tingkat pertumbuhan produktivitas baru-baru ini.

Penelitian dari tahun 2023 oleh Coursera, yang melibatkan 650 manajer dari bidang L&D (**Learning & Development**) dan HR (Human Resources) dari delapan negara, menunjukkan pergeseran yang jelas menuju investasi yang lebih besar dalam pengembangan bakat. Lebih dari 95% eksekutif ini menyatakan bahwa anggaran untuk L&D telah meningkat, dengan 51% eksekutif mengakui L&D sebagai fungsi bisnis strategis.

Temuan utama survei menunjukkan bahwa L&D mengalami dukungan yang belum pernah terjadi sebelumnya dari manajemen senior. Pergeseran ini menggarisbawahi peran penting yang dimainkan oleh para pemimpin L&D dan SDM dalam mencapai tujuan organisasi. Mayoritas eksekutif menunjukkan bahwa peningkatan anggaran didorong oleh kebutuhan untuk meningkatkan keterlibatan karyawan dan mengembangkan keterampilan penting yang sangat penting untuk tetap kompetitif. Secara khusus, 75% eksekutif menunjukkan bahwa manajemen memprioritaskan investasi dalam L&D untuk memastikan keberhasilan ambisi teknologi mereka.

Urgensi pelatihan ulang dan peningkatan keterampilan ditentukan oleh beberapa faktor. Meningkatkan produktivitas, mempertahankan daya saing, mendorong keterlibatan karyawan, beradaptasi dengan perubahan teknologi, dan mempertahankan karyawan adalah prioritas utama. Para pemimpin L&D dan SDM berfokus pada keterampilan bisnis dan keterampilan interpersonal seperti manajemen proyek, kepemimpinan, kemampuan beradaptasi, dan ketangkasan karena hal-hal ini sangat penting untuk tempat kerja yang berubah. Keterampilan digital dan data juga menjadi prioritas utama, mencerminkan transformasi digital yang sedang berlangsung.

Menariknya, keterampilan AI dinilai sebagai prioritas yang lebih rendah: Hanya 19% eksekutif yang menganggapnya sebagai fokus utama, dan hanya 20% yang memiliki metrik efektif untuk keterampilan AI. Hal ini kemungkinan disebabkan oleh fakta bahwa banyak organisasi masih dalam tahap awal dalam hal bagaimana mengintegrasikan dan memanfaatkan AI. Meskipun demikian, potensi dampak AI generatif pada berbagai peran pekerjaan menghadirkan peluang bagi para pemimpin SDM untuk mendorong perubahan dengan bekerja sama dengan para pemimpin bisnis dan teknologi.

Salah satu tantangan terbesar bagi para pemimpin L&D adalah menciptakan pengalaman belajar yang bermakna di tengah banyaknya konten yang tersedia, sebuah fenomena yang disebut sebagai "kekacauan konten". Hampir setengah dari eksekutif menyebutkan ini sebagai tantangan terbesar mereka, dengan alasan bahwa terlalu banyak inisiatif pembelajaran untuk diukur menyisakan terlalu sedikit waktu untuk perencanaan strategis.

Meskipun demikian, peningkatan kinerja dan produktivitas, bersama dengan pengembangan keterampilan, dipandang sebagai indikator utama keberhasilan program. Yang perlu diperhatikan, 46% manajer melaporkan bahwa karyawan mereka menggunakan keterampilan yang diperoleh melalui program L&D lebih banyak dalam pekerjaan sehari-hari mereka dibandingkan tahun sebelumnya. Temuan dari laporan ini berfungsi sebagai katalis

untuk ide-ide baru yang akan memungkinkan organisasi untuk membangun tenaga kerja yang lebih terlibat dan fleksibel yang siap menghadapi tantangan di masa depan.

Secara keseluruhan, penting untuk disebutkan bahwa penelitian tentang literasi AI masih dalam tahap awal dan hanya sedikit literatur tentang topik ini. Meskipun demikian, wawasan tentang literasi AI yang diperoleh dari temuan-temuan baru ini dan lainnya sangat penting untuk selaras dengan Undang-Undang AI, yang bertujuan untuk mengatur pengembangan dan penerapan AI di seluruh Uni Eropa. Undang-undang tersebut menekankan standar transparansi, akuntabilitas, dan pertimbangan etis yang tinggi dan menyoroti perlunya kompetensi AI yang kuat. Mengatasi kesenjangan signifikan dalam keterampilan digital yang diidentifikasi dalam laporan ini sangat penting untuk kepatuhan terhadap Undang-Undang AI. Baik sektor publik maupun swasta harus berinvestasi dalam pendidikan dan pelatihan untuk memastikan tenaga kerja mereka siap menghadapi persyaratan yang ketat ini.

Lebih lanjut, fokus undang-undang pada pertimbangan etis dan hukum selaras dengan tantangan yang dihadapi oleh sektor publik, menyoroti perlunya inisiatif pembangunan kapasitas yang ditargetkan. Peningkatan investasi dalam L&D, yang didorong oleh kebutuhan akan ketangkasan organisasi, mencerminkan pendekatan proaktif untuk memenuhi persyaratan Undang-Undang AI dan memastikan penerapan AI yang bertanggung jawab dan efektif.

Definisi Literasi AI

Pertama-tama, penting untuk mendefinisikan **literasi**. Menurut UNESCO, perolehan keterampilan membaca dan menulis bukanlah tindakan sekali saja. Di luar konsep tradisional literasi dan numerasi, literasi sekarang dipahami sebagai cara untuk mengidentifikasi, memahami, menafsirkan, menciptakan, dan berkomunikasi di dunia yang semakin digital, berbasis teks, kaya informasi, dan berubah dengan cepat. Literasi adalah kontinum pembelajaran dan penguasaan membaca, menulis, dan numerasi sepanjang hidup dan merupakan bagian dari seperangkat keterampilan yang lebih luas yang mencakup literasi digital, literasi media, pendidikan untuk pembangunan berkelanjutan dan kewarganegaraan global, serta keterampilan khusus pekerjaan. Keterampilan literasi itu sendiri berkembang dan meluas seiring semakin banyaknya orang yang terpapar informasi dan belajar melalui teknologi digital.

Literasi, hak asasi manusia fundamental, mencakup keterampilan kognitif, linguistik, sosial, afektif, relasional, dan budaya. Literasi melampaui sekadar penguraian dan pemahaman teks dan mendorong pemikiran kritis serta pemahaman informasi yang lebih dalam. Keterampilan AI, seperti pengetahuan umum, sangat penting untuk menavigasi dunia modern, terutama karena AI semakin terintegrasi ke dalam berbagai bidang kehidupan.

Sama seperti literasi tradisional merupakan hak asasi manusia, literasi AI dapat dilihat sebagai hak yang sangat penting di era digital. Literasi AI memungkinkan individu untuk memahami, berinteraksi dengan, dan mengevaluasi secara kritis teknologi AI untuk memastikan mereka tidak tertinggal di dunia yang semakin digerakkan oleh AI. Literasi AI memberdayakan orang untuk memahami dampak AI yang luas terhadap masyarakat dan mendorong pemikiran kritis tentang implikasi dan aplikasinya.

Literasi AI mencakup kemampuan untuk **memahami, menerapkan, memantau, dan merefleksikan secara kritis aplikasi AI tanpa harus mengembangkan model AI**. Literasi AI memiliki kesamaan dengan bentuk literasi teknologi lainnya, seperti literasi digital, literasi media, dan literasi data.

Istilah “Literasi AI” pertama kali digunakan dalam sebuah artikel daring pada tahun 2015 dan muncul tak lama kemudian dalam sebuah artikel empiris. Literasi AI didefinisikan sebagai *“seperangkat kompetensi yang memungkinkan individu untuk mengevaluasi teknologi AI secara kritis, berkomunikasi dan berkolaborasi secara efektif dengan AI, dan menggunakan AI sebagai alat secara daring, di rumah, dan di tempat kerja”*.

Literasi AI terutama ditujukan untuk pelajar tanpa latar belakang ilmu komputer dan menekankan perlunya masyarakat umum untuk melek AI. Karena AI merambah berbagai bidang seperti pendidikan, perawatan kesehatan, transportasi, layanan sosial, pemasaran, dan lainnya, pemahaman tentang AI menjadi sangat penting bagi interaksi pribadi dan profesional dengan teknologi tersebut.

Sumber lain menunjukkan bahwa literasi AI mencakup seperangkat kompetensi holistik yang memungkinkan individu tidak hanya untuk menggunakan alat AI, tetapi juga untuk mengevaluasi dan memahami konteks yang lebih luas di mana AI beroperasi secara kritis. Dengan mengembangkan keterampilan teknis, pemikiran kritis, dan pemahaman kontekstual, individu dapat secara efektif terlibat dengan teknologi AI, membuat keputusan yang tepat, dan berkontribusi pada pengembangan dan penggunaan AI yang bertanggung jawab di masyarakat.

Singkatnya, memupuk literasi AI membantu orang untuk lebih baik menavigasi dunia yang semakin didorong oleh AI dan meningkatkan kemampuan mereka untuk terlibat secara kritis dengan teknologi AI serta menggunakannya secara efektif di berbagai bidang.

Literasi AI dan Ketentuan UU AI

Memberikan pengetahuan tentang kecerdasan buatan (AI) merupakan faktor penentu untuk penggunaan dan pengoperasian sistem AI yang bertanggung jawab.

Pasal 4 UU AI menyatakan: *“Penyedia dan pengimplementasikan sistem AI wajib mengambil langkah-langkah untuk memastikan, sebisa mungkin, bahwa personel mereka dan orang lain yang terlibat dalam pengoperasian dan penggunaan sistem AI atas nama mereka memiliki tingkat literasi AI yang memadai, dengan mempertimbangkan pengetahuan teknis, pengalaman, pendidikan dan pelatihan mereka serta konteks di mana sistem AI dimaksudkan untuk digunakan dan orang atau kelompok orang yang akan menggunakan sistem AI tersebut.”*

Ketentuan lebih lanjut tentang literasi AI dalam Undang-Undang AI:

- **Pertimbangan 20 Undang-Undang AI:** *“Untuk memaksimalkan manfaat sistem AI sambil melindungi hak-hak fundamental, kesehatan dan keselamatan serta memungkinkan pengawasan demokratis, literasi AI harus membekali penyedia, penyebar, dan subjek data dengan konsep-konsep yang diperlukan untuk membuat keputusan yang tepat tentang sistem AI. Konsep-konsep ini dapat bervariasi tergantung pada konteksnya dan dapat mencakup pemahaman tentang penerapan*

yang benar dari elemen-elemen teknis dalam fase pengembangan sistem AI, langkah-langkah yang harus diterapkan dalam penggunaannya dan interpretasi yang tepat dari keluaran sistem AI dan, dalam hal subjek data, pengetahuan yang diperlukan untuk memahami bagaimana keputusan yang dibuat menggunakan AI akan memengaruhi mereka. Dalam konteks penerapan Peraturan ini, literasi AI harus memberikan semua operator yang relevan dalam rantai nilai AI dengan pengetahuan yang diperlukan untuk memastikan kepatuhan yang tepat dan penegakan Peraturan yang benar. Selain itu, implementasi penuh langkah-langkah literasi AI dan pengenalan langkah-langkah tindak lanjut yang tepat dapat membantu meningkatkan kondisi kerja dan pada akhirnya mendukung konsolidasi dan jalur inovasi AI yang dapat dipercaya di Uni Eropa. Panel Eropa tentang Kecerdasan Buatan ('the Panel AI harus mendukung Komisi dalam mempromosikan alat literasi AI dan kesadaran serta pendidikan publik tentang manfaat, risiko, perlindungan, hak, dan kewajiban yang terkait dengan penggunaan sistem AI. Dalam kerja sama dengan para pemangku kepentingan terkait, Komisi dan Negara-negara Anggota harus memfasilitasi pengembangan kode etik sukarela untuk mempromosikan literasi AI di antara orang-orang yang terlibat dalam pengembangan, pengoperasian, dan penggunaan AI."

- **Pasal 3 ayat 56 Undang-Undang AI:** *"...istilah 'literasi AI' berarti keterampilan, pengetahuan, dan pemahaman yang memungkinkan penyedia, penyebar, dan subjek data, dengan mempertimbangkan hak dan kewajiban masing-masing berdasarkan Peraturan ini, untuk menggunakan sistem AI secara terinformasi dan menyadari peluang dan risiko AI serta potensi bahaya yang dapat ditimbulkannya."*
- **Pertimbangan 91 Undang-Undang AI:** *"Mengingat sifat sistem AI dan risiko terhadap keselamatan dan hak-hak mendasar yang mungkin terkait dengan penggunaannya, sudah sepatutnya menetapkan tanggung jawab khusus bagi para pengembang, termasuk terkait dengan kebutuhan untuk memastikan pemantauan yang memadai terhadap kinerja sistem AI dalam kondisi nyata. Secara khusus, para pengembang harus mengambil langkah-langkah teknis dan organisasi yang tepat untuk memastikan bahwa mereka menggunakan sistem AI berisiko tinggi sesuai dengan petunjuk penggunaan dan kewajiban lain tertentu harus ditetapkan terkait dengan pemantauan fungsi sistem AI dan, jika sesuai, kewajiban pencatatan. Selain itu, para pengembang harus memastikan bahwa orang-orang yang dipercayakan dengan implementasi petunjuk penggunaan dan pengawasan manusia sesuai dengan Peraturan ini memiliki kompetensi yang diperlukan, khususnya tingkat literasi AI, pelatihan, dan wewenang yang sesuai, untuk melaksanakan tugas-tugas tersebut dengan benar. Kewajiban-kewajiban tersebut tidak boleh mengurangi kewajiban lain dari pengembang terkait dengan sistem AI berisiko tinggi berdasarkan peraturan Uni Eropa atau nasional. hukum."*
- **Pertimbangan 165 Undang-Undang AI:** *"Pengembangan sistem AI selain sistem AI berisiko tinggi sesuai dengan persyaratan Peraturan ini dapat menyebabkan peningkatan penggunaan AI yang etis dan tepercaya di Uni Eropa. Penyedia sistem AI*

non-berisiko tinggi harus didorong untuk menetapkan kode etik, termasuk mekanisme tata kelola terkait, untuk mempromosikan penerapan sukarela sebagian atau seluruh persyaratan yang berlaku untuk sistem AI berisiko tinggi, yang disesuaikan dengan tujuan sistem dan risiko yang lebih rendah, dan dengan mempertimbangkan solusi teknis yang tersedia dan praktik terbaik industri seperti kartu model dan data. Selain itu, penyedia dan, jika sesuai, pengembang semua sistem AI, baik berisiko tinggi maupun tidak, dan semua model AI juga harus didorong untuk secara sukarela menerapkan persyaratan tambahan, misalnya terkait dengan elemen Pedoman Etika Uni Eropa untuk AI Tepercaya, keberlanjutan lingkungan, langkah-langkah untuk literasi AI, desain dan pengembangan sistem AI yang inklusif dan beragam, termasuk dengan fokus pada orang-orang rentan dan aksesibilitas bagi individu. dengan disabilitas, partisipasi pemangku kepentingan, yang melibatkan, jika sesuai, pemangku kepentingan yang relevan seperti asosiasi bisnis dan organisasi masyarakat sipil, akademisi, organisasi penelitian, serikat pekerja dan organisasi perlindungan konsumen dalam desain dan pengembangan sistem AI, dan keragaman tim pengembang, termasuk keseimbangan gender. (...)”

- **Pasal 66 huruf f UU AI:** “... mendukung Komisi dalam **mempromosikan literasi AI**, meningkatkan kesadaran dan mendidik masyarakat tentang manfaat, risiko, perlindungan, hak dan kewajiban yang terkait dengan penggunaan sistem AI”.

Usulan Kerangka Kematangan untuk Penyedia AI

Salah satu titik awal untuk mendefinisikan kerangka tingkat kematangan untuk literasi AI adalah Rekomendasi tentang kompetensi kunci untuk pembelajaran sepanjang hayat dari Dewan Uni Eropa, yang diadopsi pada Mei 2018. Rekomendasi tersebut mengidentifikasi delapan kompetensi kunci yang penting bagi warga negara dalam hal pemenuhan pribadi, gaya hidup sehat dan berkelanjutan, kemampuan kerja, kewarganegaraan aktif, dan inklusi sosial.

Kompetensi digital, salah satu dari delapan kompetensi tersebut, mencakup penggunaan dan keterlibatan yang percaya diri, kritis, dan bertanggung jawab dengan teknologi digital untuk pembelajaran, pekerjaan, dan partisipasi dalam masyarakat. Ini termasuk literasi informasi dan data, komunikasi dan kolaborasi, literasi media, pembuatan konten digital (termasuk pemrograman), keamanan (termasuk kesejahteraan digital dan keterampilan keamanan siber), masalah kekayaan intelektual, pemecahan masalah, dan berpikir kritis.

Pengetahuan, keterampilan, dan sikap penting yang terkait dengan kompetensi ini: Individu harus memahami bagaimana teknologi digital dapat mendukung komunikasi, kreativitas, dan inovasi serta menyadari kemungkinan, keterbatasan, dampak, dan risikonya. Mereka harus memahami prinsip-prinsip umum, mekanisme, dan logika yang mendasari teknologi digital yang berkembang dan mengetahui fungsi dasar serta penggunaan berbagai perangkat, perangkat lunak, dan jaringan. Individu harus secara kritis mempertimbangkan validitas, keandalan, dan dampak informasi dan data yang disediakan melalui sarana digital dan menyadari prinsip-prinsip hukum dan etika yang terkait dengan penggunaan teknologi digital.

Sebagai titik awal untuk membangun kapasitas digital, banyak pemerintah, organisasi internasional, lembaga pemikir, dan universitas telah mengembangkan kerangka kerja kompetensi, kursus, dan kurikulum untuk meletakkan dasar bagi pelatihan pejabat sektor publik tentang transformasi digital. Analisis UNESCO mengidentifikasi kompetensi umum berikut dalam kerangka kerja yang dipelajari: *Kepemimpinan digital; identifikasi masalah; literasi digital; data terbuka; pendekatan berbasis data; kecerdasan buatan; berpusat pada manusia; peningkatan berbasis iterasi dalam pengembangan produk dan layanan.*

Untuk tujuan bagian ini, kerangka kerja kematangan berikut untuk literasi AI diusulkan. Kerangka kerja ini dapat dengan mudah diadaptasi dan diperluas. Dengan mengikuti kerangka kerja ini, penyedia AI dapat memastikan bahwa karyawan mereka dan individu terkait lainnya memiliki pengetahuan, keterampilan, dan sikap yang diperlukan untuk mengembangkan, menerapkan, dan mengelola sistem AI secara efektif dan etis. Hal ini memenuhi persyaratan Pasal 4 UU AI dan membantu mempromosikan budaya penggunaan AI yang bertanggung jawab.

Tabel 3.2 Kerangka kerja kematangan untuk literasi AI

Tingkat kematangan	Pengetahuan	Keterampilan	Sikap	Implikasi bagi penyedia AI
Tingkat dasar	Pemahaman dasar tentang prinsip, terminologi, dan konsep AI.	Pengetahuan dasar tentang alat digital dan pemahaman tentang aplikasi AI sederhana.	Keterbukaan untuk mempelajari tentang AI dan implikasi etisnya.	Implementasi program pengenalan AI untuk seluruh karyawan.
	Pengetahuan tentang Undang-Undang AI dan dampaknya terhadap pengembangan dan penggunaan AI.	Keterampilan data dasar, termasuk praktik pengumpulan, penyimpanan, dan keamanan data dasar.	Kesadaran akan pentingnya perlindungan data, keamanan, dan pertimbangan etis di bidang AI.	Mendorong budaya pembelajaran berkelanjutan dan rasa ingin tahu tentang AI. Memastikan bahwa semua karyawan mengetahui dan memahami prinsip-prinsip dasar Undang-Undang AI.
Tingkat menengah	Pemahaman mendalam tentang algoritma AI, teknik pemrosesan data, dan pedoman etika.	Pengetahuan tentang alat dan platform AI untuk analisis data dan pengambilan keputusan.	Pendekatan kritis dalam mengevaluasi hasil AI dalam hal akurasi dan bias.	Memberikan pelatihan yang terarah tentang konsep dan alat AI tingkat lanjut.
	Keakraban dengan persyaratan khusus Undang-Undang AI yang relevan dengan peran mereka.	Kemampuan untuk menangani dan menganalisis sejumlah besar data dan memahami dampaknya pada sistem AI.	Komitmen terhadap praktik AI yang etis dan kepatuhan terhadap standar hukum dan peraturan.	Mendorong pemikiran kritis dan pengambilan keputusan etis dalam tugas-tugas terkait AI.
	Pemahaman dasar tentang prinsip-prinsip pemikiran desain ¹ dan desain	Pemahaman tentang peran AI dalam meningkatkan proses operasional. Menerapkan prinsip-prinsip pemikiran desain pada proyek AI untuk meningkatkan	Menekankan peran sentral manusia dalam pengembangan dan penggunaan AI.	Memastikan bahwa karyawan mampu menafsirkan dan menerapkan Undang-

	AI yang berpusat pada manusia 2.	pengalaman pengguna dan kemudahan penggunaan.		Undang AI serta mengadopsi pendekatan yang berpusat pada manusia dalam pekerjaan sehari-hari mereka.
Tingkat Lanjutan	Pemahaman komprehensif tentang teknologi AI, termasuk pembelajaran mesin dan jaringan saraf. Pengetahuan mendalam tentang Undang-Undang AI, termasuk persyaratan kepatuhan khusus. Pemahaman tingkat lanjut tentang prinsip-prinsip pemikiran desain dan penerapannya dalam pengembangan AI.	Kemampuan untuk mengembangkan dan mengimplementasikan solusi AI yang canggih. Keterampilan analisis data dan pemecahan masalah tingkat lanjut. Keterampilan kepemimpinan dalam mengelola proyek dan inisiatif AI yang berfokus pada pengalaman pengguna dan desain yang berpusat pada manusia.	Mendukung penggunaan AI yang etis dan penggunaan sistem AI yang bertanggung jawab. Mempromosikan transparansi dan akuntabilitas dalam proses dan keputusan AI. Komitmen terhadap pengembangan sistem AI yang memprioritaskan kebutuhan manusia dan pertimbangan etis.	Pengembangan program pelatihan AI tingkat lanjut dengan fokus pada kepemimpinan dan inovasi. Mendorong budaya penggunaan AI yang etis dan transparansi. Memastikan bahwa karyawan mampu melaksanakan proyek AI sesuai dengan Undang-Undang AI dan prinsip-prinsip pemikiran desain.
Tingkat Pakar	Penguasaan teknologi dan inovasi AI terkini. Pengetahuan ahli tentang standar, regulasi, dan pertimbangan etika AI global, termasuk Regulasi AI. Pemahaman tentang lingkungan berbagai pemangku kepentingan, termasuk perspektif pemerintah, industri, akademisi, dan masyarakat sipil. Pengetahuan ahli tentang prinsip-prinsip pemikiran desain dan AI yang berpusat pada manusia 3 dan penerapannya secara strategis dalam AI.	Memimpin inisiatif penelitian dan pengembangan AI. Pengembangan dan implementasi kebijakan dan strategi AI. Membimbing organisasi tentang praktik AI yang etis dan sesuai. Memfasilitasi kolaborasi dan dialog antara berbagai pemangku kepentingan untuk membentuk kebijakan dan standar AI dengan pendekatan yang berpusat pada manusia.	Memberikan kepemimpinan dalam mempromosikan penggunaan AI yang bertanggung jawab dan memengaruhi kebijakan serta standar AI. Berkomitmen pada pembelajaran dan inovasi berkelanjutan di bidang AI. Menganjurkan pendekatan integratif dan partisipatif dalam tata kelola AI. Menganjurkan pendekatan inklusif, partisipatif, dan berpusat pada manusia dalam tata kelola AI. Memprioritaskan dampak AI terhadap	Mendukung pengembangan profesional berkelanjutan bagi karyawan senior dan manajer di bidang AI. Mendorong partisipasi dalam diskusi kebijakan AI global dan kegiatan penetapan standar. Membina hubungan antar berbagai pemangku kepentingan untuk memastikan bahwa berbagai perspektif dipertimbangkan dalam pengembangan dan penerapan AI. Memastikan bahwa organisasi berada di garis depan pengembangan dan penggunaan AI dari

	kesejahteraan manusia dan kesejahteraan masyarakat.	perspektif etis dan manusiawi dengan melibatkan berbagai pemangku kepentingan.
1.	Pemikiran desain berbeda dari proses inovasi dan pembangkitan ide lainnya karena berorientasi pada solusi dan berpusat pada pengguna, bukan berorientasi pada masalah. Ini berarti bahwa ia berfokus pada solusi untuk suatu masalah dan bukan pada masalah itu sendiri.	
2.	Jika Anda benar-benar berfokus pada peningkatan kemampuan manusia, itu adalah AI yang berpusat pada manusia	
3.	Tujuh prinsip untuk AI yang berpusat pada manusia	

Rekomendasi Utama bagi Penyedia AI untuk Mengembangkan dan Mempromosikan Literasi AI Berkelanjutan di dalam Perusahaan



Gambar 3.4 Rekomendasi Utama untuk Literasi AI

Terus meningkatkan kesiapan digital institusional dalam organisasi: Melakukan penilaian kesiapan digital yang komprehensif untuk mengidentifikasi kesenjangan dalam infrastruktur teknologi, kebijakan digital, dan kerangka kerja tata kelola. Mengembangkan rencana strategis untuk meningkatkan kesiapan digital, termasuk memodernisasi sistem TI, menetapkan kebijakan digital yang jelas, dan menumbuhkan budaya yang mendukung transformasi digital.

Peningkatan berkelanjutan keterampilan digital karyawan: Menetapkan program pelatihan keterampilan digital untuk semua karyawan untuk memastikan mereka menguasai alat digital dan memahami proses digital. Mengembangkan dan menerapkan pelatihan

keterampilan digital komprehensif yang mencakup alat dan platform digital terpenting. Menawarkan modul pelatihan khusus yang disesuaikan dengan tugas dan tanggung jawab karyawan. Mendorong partisipasi dalam kursus daring, webinar, dan lokakarya tentang tren digital baru.

Mempromosikan literasi data: Mempromosikan literasi data di seluruh organisasi untuk memastikan karyawan dapat secara efektif mengumpulkan, menganalisis, dan menafsirkan data serta membuat keputusan berdasarkan data. Mengintegrasikan pelatihan literasi data ke dalam proses orientasi dan program pengembangan profesional berkelanjutan. Menyediakan akses ke alat dan sumber daya analisis data. Buat lokakarya dan seminar berorientasi data untuk meningkatkan keterampilan analitis karyawan.

Berikan pelatihan khusus AI: Kembangkan program pelatihan khusus AI yang ditargetkan untuk membangun keahlian dalam teknologi AI, aplikasinya, dan pertimbangan etis. Bermitra dengan universitas dan platform online untuk menawarkan program sertifikasi AI. Lakukan lokakarya dan pelatihan AI internal yang dipimpin oleh pakar industri. Kembangkan keahlian internal tentang AI. Pastikan pelatihan mencakup etika AI, kepatuhan peraturan, dan aplikasi praktis AI.

Mendorong pembelajaran berkelanjutan: Menciptakan budaya pembelajaran berkelanjutan untuk menjaga karyawan tetap terdepan dalam teknologi AI dan digital. Berikan insentif bagi karyawan untuk melanjutkan pendidikan dan pengembangan profesional mereka di bidang AI dan bidang terkait. Bangun platform berbagi pengetahuan internal di mana karyawan memiliki akses ke penelitian, artikel, dan materi pelatihan terbaru. Dorong partisipasi dalam konferensi, seminar, dan acara jejaring yang terkait dengan AI dan inovasi digital.

Berinvestasi dalam pengembangan bakat: Fokus pada pengembangan bakat di dalam organisasi dengan mengidentifikasi karyawan dengan potensi tinggi dan memberi mereka kesempatan untuk memperluas keahlian AI mereka. Terapkan program pendampingan dan pembinaan untuk mendorong pengembangan profesional di bidang AI. Membangun jalur pengembangan talenta untuk peran-peran yang penting bagi inisiatif AI. Menyediakan program rotasi dan pengalaman belajar berbasis proyek untuk memperkenalkan karyawan pada berbagai aspek AI.

Implementasi strategi manajemen perubahan: pengembangan dan implementasi strategi manajemen perubahan yang efektif untuk memfasilitasi pengenalan teknologi dan proses AI. Melibatkan karyawan dalam proses perubahan melalui sesi umpan balik dan partisipasi dalam proyek percontohan. Memberikan dukungan dan sumber daya untuk mengatasi resistensi dan memastikan transisi yang lancar ke alur kerja yang didukung AI.

Membangun komunitas praktik (CoP): Buat komunitas praktik di dalam organisasi untuk mendorong kolaborasi, berbagi pengetahuan, dan inovasi di bidang AI. Bentuk kelompok atau forum minat AI internal tempat karyawan dapat mendiskusikan tren, tantangan, dan praktik terbaik AI. Dorong kolaborasi lintas departemen dalam proyek AI untuk memanfaatkan berbagai perspektif dan keahlian. Selenggarakan pertemuan rutin, hackathon,

dan tantangan inovasi untuk mendorong keterlibatan aktif dan peningkatan berkelanjutan keterampilan AI.

3.4 PENDEKATAN BERBASIS RISIKO

Undang-Undang AI membagi sistem AI ke dalam berbagai kategori, tergantung pada tingkat risiko yang ditimbulkannya terhadap kesehatan, keselamatan, atau hak-hak dasar individu. Klasifikasi sistem AI ke dalam kategori risiko sebagaimana didefinisikan oleh Undang-Undang AI tampaknya merupakan langkah terpenting bagi penyedia potensial yang ingin memasarkan sistem mereka atau mengoperasikannya di Uni Eropa.

Sistem AI yang Dilarang

Bab II UU AI dikhususkan untuk “Praktik Terlarang di bidang kecerdasan buatan”. Menurut UU AI, penggunaan AI tertentu dilarang untuk melindungi kesehatan, keselamatan, dan hak-hak dasar individu. Aplikasi AI yang dilarang ini meliputi:

a) Praktik manipulasi:

Menempatkan di pasar, mengoperasikan, atau menggunakan sistem AI untuk membujuk orang agar terlibat dalam perilaku yang dapat menyebabkan kerugian signifikan bagi mereka atau orang lain melalui teknik subliminal atau dengan mengeksploitasi kerentanan mereka dilarang. Ini termasuk aplikasi AI yang bertujuan untuk memengaruhi perilaku manusia dengan cara yang merusak kemampuan orang untuk membuat keputusan independen (Pasal 5 ayat 1 huruf a UU AI).

b) Eksploitasi kelemahan:

Pemasaran, pengoperasian, atau penggunaan sistem AI yang dirancang khusus untuk mengeksploitasi kerentanan kelompok orang tertentu berdasarkan usia, kondisi fisik atau mental mereka guna mendorong mereka untuk melakukan perilaku yang kemungkinan besar akan menyebabkan, atau secara wajar mungkin akan menyebabkan, kerugian bagi mereka atau orang lain juga dilarang (Pasal 5 ayat 1 huruf b UU AI).

c) Sistem peringkat sosial:

Penempatan di pasar, pengoperasian, atau penggunaan AI untuk tujuan menilai atau mengklasifikasikan kepercayaan seseorang berdasarkan perilaku sosial mereka atau karakteristik pribadi yang diketahui, disimpulkan, atau diprediksi selama periode waktu tertentu, yang mengakibatkan orang atau kelompok tertentu dirugikan atau dikecualikan, dilarang. Hal ini berlaku khususnya jika penilaian tersebut menyebabkan perlakuan tidak adil atau tidak menguntungkan di berbagai bidang kehidupan (Pasal 5 ayat 1 huruf c UU AI).

Dilarang melakukan diskriminasi atau merugikan orang tertentu atau seluruh kelompok orang

- I. dalam konteks sosial yang tidak terkait dengan keadaan di mana data tersebut awalnya dihasilkan atau dikumpulkan (Pasal 5 ayat 1 huruf c sub-ayat i UU AI),

- II. dengan cara yang tidak dapat dibenarkan atau tidak proporsional sehubungan dengan perilaku sosial mereka atau ruang lingkungannya (Pasal 5 ayat 1 huruf c sub-ayat i UU AI).

d) Pembatasan untuk penilaian berbasis risiko oleh AI:

Tidak diperbolehkan memasarkan, memesan, atau menggunakan sistem AI yang bertujuan untuk menentukan kemungkinan seseorang melakukan kejahatan hanya berdasarkan profil atau penilaian karakteristik pribadi mereka. Larangan ini tidak berlaku untuk sistem AI yang mendukung penilaian manusia, asalkan penilaian tersebut didasarkan pada fakta objektif dan terverifikasi yang secara langsung terkait dengan tindak pidana (Pasal 5 ayat 1 huruf d UU AI).

e) Larangan pembuatan basis data pengenalan wajah:

Dilarang memasarkan sistem AI, mengoperasikannya, atau menggunakannya yang membuat basis data pengenalan wajah melalui pembacaan gambar wajah secara tidak spesifik dari internet atau video pengawasan, untuk membuat atau memperluas basis data pengenalan wajah (Pasal 5 ayat 1 huruf e UU AI).

f) Batasan dalam pengenalan emosi:

Penempatan di pasar, pengoperasian, atau penggunaan sistem AI untuk mendeteksi atau menyimpulkan emosi seseorang di tempat kerja atau di lembaga pendidikan dilarang, kecuali sistem ini diperkenalkan atau ditempatkan di pasar karena alasan medis atau keselamatan (Pasal 5 ayat 1 huruf f UU AI).

g) Larangan kategorisasi biometrik:

Penempatan di pasar, pemesanan, atau penggunaan sistem AI yang mengidentifikasi seseorang berdasarkan data biometrik untuk menarik kesimpulan tentang ras, pandangan politik, keanggotaan serikat pekerja, keyakinan agama atau filosofis, kehidupan seks, atau orientasi seksual dilarang. Pengecualian berlaku untuk pelabelan atau penyaringan data biometrik yang diizinkan secara hukum, seperti pengurutan gambar berdasarkan karakteristik biometrik, atau untuk digunakan dalam penegakan hukum dalam kondisi tertentu (Pasal 5 ayat 1 g UU AI).

h) Biometrik jarak jauh waktu nyata di ruang publik:

Pemasangan, pengoperasian, atau penggunaan sistem AI untuk identifikasi biometrik jarak jauh waktu nyata terhadap orang di area yang dapat diakses publik untuk tujuan penegakan hukum hanya diizinkan dalam kondisi yang ditentukan secara ketat dan pada umumnya dilarang. Pengecualian hanya berlaku dalam situasi yang ditentukan secara tepat dan terbatas yang melibatkan ancaman signifikan terhadap keamanan atau kejahatan serius (Pasal 5 ayat 1 huruf h UU AI), seperti:

- I. Pencarian terarah untuk korban penculikan, perdagangan manusia, atau eksploitasi seksual tertentu dan pencarian orang hilang (Pasal 5 ayat 1 huruf h sub-ayat i UU AI)
- II. Mencegah bahaya spesifik, substansial, dan mendesak terhadap kehidupan atau integritas fisik orang atau bahaya nyata dan saat ini atau nyata dan dapat diperkirakan dari serangan teroris (Pasal 5 ayat 1 huruf h sub-ayat ii UU AI)

- III. Melacak atau mengidentifikasi seseorang yang diduga telah melakukan tindak pidana untuk tujuan melakukan penyelidikan kriminal, penuntutan, atau pelaksanaan hukuman atas tindak pidana yang tercantum dalam Lampiran II, yang dapat dihukum berdasarkan hukum Negara Anggota yang bersangkutan dengan hukuman penjara atau perintah penahanan untuk jangka waktu maksimal setidaknya empat tahun (Pasal 5 ayat 1 huruf h sub-ayat iii UU AI).

Penggunaan sistem identifikasi biometrik jarak jauh secara waktu nyata (real-time biometric remote identification systems) di area yang dapat diakses publik untuk tujuan penegakan hukum pada prinsipnya dilarang sesuai dengan Pasal 5 ayat (1) huruf h AI Act, kecuali dalam keadaan tertentu yang bersifat spesifik dan mendesak.

AI memiliki kemampuan untuk mengenali orang berdasarkan penampilan dan pergerakan mereka. Dalam kasus penculikan anak atau orang hilang dari panti jompo, polisi dapat menggunakan sistem pengenalan biometrik untuk dengan cepat menemukan orang-orang ini di ruang publik seperti stasiun kereta api atau pusat perbelanjaan. Atau jika ada ancaman khusus terhadap keselamatan publik, seperti ancaman serangan teroris yang akan segera terjadi, sistem tersebut dapat digunakan untuk mengidentifikasi tersangka sebelum mereka dapat menimbulkan bahaya.

Namun, kriteria ketat harus dipatuhi saat menggunakan teknologi ini sesuai dengan Pasal 5 ayat 2) UU AI:

- a) Penilaian situasi: Penggunaan teknologi harus diperlukan untuk mencegah kerusakan yang signifikan.
Contoh: Penggunaan identifikasi biometrik dapat dipertimbangkan jika buronan berbahaya yang dikenal dicurigai berada di suatu acara besar dan ada risiko tinggi terhadap keselamatan publik.
- b) Penilaian dampak: Dampak terhadap hak dan kebebasan masyarakat harus dipertimbangkan dengan cermat. Penting untuk melindungi privasi dan data orang yang berada di sekitar lokasi kejadian dan untuk memastikan bahwa teknologi tersebut tidak digunakan secara berlebihan atau invasif.

Langkah-langkah perlindungan tambahan juga harus diperhatikan:

- Penerapannya harus dibatasi secara ketat dalam hal waktu, geografi, dan orang-orang yang bersangkutan.
- Penilaian awal tentang dampak terhadap hak-hak fundamental (penilaian dampak hak-hak fundamental) sesuai dengan Pasal 27 UU AI diperlukan (lihat bagian 3.4).
- Teknologi tersebut harus didaftarkan dalam basis data Uni Eropa sesuai dengan Pasal 49 UU AI untuk memastikan transparansi dan pemantauan. Dalam kasus mendesak, pendaftaran ini dapat dilakukan secara retrospektif.

Aturan-aturan ini dimaksudkan untuk memastikan bahwa penggunaan teknologi invasif tersebut hanya terjadi dalam kasus yang benar-benar diperlukan dan dibenarkan untuk memastikan keselamatan publik dan untuk melindungi privasi dan kebebasan warga negara.

Oleh karena itu, Pasal 5 ayat 3 UU AI mensyaratkan otorisasi terlebih dahulu untuk penggunaan identifikasi jarak jauh biometrik waktu nyata:

- Setiap kali departemen kepolisian berencana untuk menggunakan teknologi identifikasi jarak jauh biometrik waktu nyata di area yang dapat diakses publik, mereka harus terlebih dahulu memperoleh otorisasi. Otorisasi ini harus diberikan oleh otoritas yudisial atau otoritas administratif independen di negara masing-masing, berdasarkan peninjauan menyeluruh terhadap permohonan tersebut. Otoritas tersebut kemudian membuat keputusan yang mengikat tentang apakah akan menyetujui atau tidak penggunaan teknologi tersebut.
- Dalam situasi yang sangat mendesak di mana tidak ada waktu untuk mendapatkan otorisasi sebelum penerapan, polisi dapat menggunakan teknologi tersebut secara sementara. Namun, mereka harus mengajukan permohonan otorisasi dalam waktu 24 jam sejak dimulainya operasi. Jika persetujuan ini ditolak, penggunaan harus segera dihentikan dan semua data dan hasil yang dikumpulkan harus dihapus.
- Otorisasi hanya akan diberikan jika ada bukti yang meyakinkan atau indikasi yang jelas bahwa penggunaan teknologi tersebut diperlukan untuk salah satu tujuan yang diizinkan. Otoritas juga harus memastikan bahwa penggunaan tersebut dibatasi secara ketat dalam hal waktu, geografi, dan orang yang terpengaruh dan tidak melampaui apa yang benar-benar diperlukan.
- Harus diperhatikan bahwa tidak ada keputusan yang dapat menimbulkan konsekuensi hukum negatif bagi seseorang yang dibuat semata-mata berdasarkan hasil identifikasi biometrik. Ini berarti bahwa hasil teknologi ini hanya boleh dianggap sebagai bagian dari bukti.

Oleh karena itu, otorisasi dan penggunaan identifikasi biometrik jarak jauh secara real-time di area publik untuk penegakan hukum diatur secara ketat untuk memastikan perlindungan privasi dan hak-hak sipil. Pihak berwenang hanya dapat menggunakan teknologi ini dalam kasus-kasus yang jelas dan mendesak, dan bahkan dalam kasus tersebut, pedoman yang ketat harus dipatuhi.

Terlepas dari pengecualian tertentu, setiap penggunaan sistem pengenalan biometrik jarak jauh secara real-time di area publik untuk keperluan kepolisian harus diberitahukan kepada otoritas yang berwenang untuk pengawasan pasar dan perlindungan data nasional sesuai dengan peraturan nasional tertentu. Pemberitahuan ini harus berisi informasi tertentu yang diperlukan, tetapi tidak boleh mencakup detail penggunaan yang bersifat rahasia (Pasal 5 ayat 4 UU AI).

Menurut Pasal 5 ayat 5 UU AI, setiap Negara Anggota Uni Eropa memiliki pilihan untuk mengizinkan penggunaan sistem identifikasi jarak jauh biometrik waktu nyata dalam batas dan ketentuan yang ditetapkan oleh hukum. Ini berarti bahwa penggunaan sistem tersebut tidak secara otomatis diizinkan di setiap negara Uni Eropa, tetapi bergantung pada peraturan khusus masing-masing negara. Untuk tujuan ini, Negara Anggota harus mengambil tindakan berikut:

1. **Legislasi:** Negara-negara harus menetapkan peraturan terperinci untuk seluruh proses dalam undang-undang nasional mereka, mulai dari aplikasi hingga persetujuan dan

penggunaan sistem tersebut. Ini juga termasuk peraturan tentang pemantauan dan pelaporan penggunaan teknologi ini.

2. **Tujuan otorisasi:** Undang-undang nasional harus menjelaskan untuk tujuan spesifik apa dan dalam keadaan apa otoritas penegak hukum dapat diizinkan untuk menggunakan teknologi ini. Ini termasuk, misalnya, pencarian orang hilang, pencegahan ancaman terhadap keselamatan publik, atau penuntutan kejahatan serius tertentu.
3. **Pemberitahuan kepada Komisi Uni Eropa:** Negara Anggota wajib memberi tahu Komisi Uni Eropa tentang peraturan nasional mereka selambat-lambatnya 30 hari setelah peraturan tersebut mulai berlaku.
4. **Regulasi nasional yang lebih ketat:** Selain itu, negara-negara juga dapat mengadopsi aturan yang lebih ketat daripada yang ditetapkan di tingkat Uni Eropa, selama aturan tersebut sejalan dengan hukum Uni Eropa. Hal ini memungkinkan Negara Anggota untuk memberikan perlindungan tambahan bagi privasi dan hak-hak fundamental warga negara di tingkat nasional.

Contoh

Misalkan suatu negara memutuskan bahwa sistem identifikasi biometrik jarak jauh secara waktu nyata hanya boleh digunakan untuk mencari anak yang hilang dan mencegah serangan teroris. Undang-undang nasional kemudian akan mengatur secara rinci bagaimana suatu otoritas mengajukan permohonan izin untuk penggunaan tersebut, kriteria apa saja yang harus dipenuhi, serta bagaimana penggunaan tersebut diawasi dan didokumentasikan. Negara tersebut juga wajib memberitahukan peraturan tersebut kepada Komisi Eropa dan dapat memutuskan untuk tidak mengizinkan penggunaan teknologi ini untuk memantau demonstrasi dalam keadaan apa pun, meskipun pada tingkat Uni Eropa hal tersebut dimungkinkan dalam kondisi tertentu.

Pasal 5 ayat 6 UU AI mengacu pada pemantauan dan pelaporan penggunaan sistem identifikasi jarak jauh biometrik waktu nyata di ruang publik untuk tujuan penegakan hukum oleh Negara-negara Anggota Uni Eropa.

- Otoritas pengawasan pasar nasional dan otoritas perlindungan data nasional Negara-negara Anggota Uni Eropa wajib menyampaikan laporan tahunan kepada Komisi Eropa.
- Laporan-laporan ini berkaitan dengan penggunaan sistem identifikasi jarak jauh biometrik waktu nyata di area publik untuk tujuan penegakan hukum.
- Laporan tersebut berisi informasi tentang jumlah kasus di mana otoritas peradilan atau otoritas administratif independen telah memutuskan permohonan otorisasi untuk menggunakan teknologi ini.
- Laporan tersebut juga mencatat hasil keputusan ini, yaitu apakah permohonan tersebut disetujui atau ditolak.
- Untuk memastikan bahwa laporan tersebut seragam dan berisi semua informasi yang diperlukan, Komisi Eropa menyediakan Negara-negara Anggota dan otoritas pengawasan pasar dan perlindungan data dengan templat pelaporan standar.

- Laporan tahunan ini memberikan gambaran umum tentang seberapa sering dan dalam keadaan apa sistem identifikasi jarak jauh biometrik waktu nyata digunakan untuk tujuan penegakan hukum di Uni Eropa.
- Laporan ini bertujuan untuk menciptakan transparansi dan pemantauan guna memastikan bahwa penggunaan teknologi tersebut sesuai dengan persyaratan hukum dan hak-hak dasar warga negara.

Komisi Uni Eropa bertanggung jawab untuk menerbitkan laporan tahunan tentang penggunaan sistem identifikasi jarak jauh biometrik waktu nyata di area yang dapat diakses publik untuk tujuan penegakan hukum sesuai dengan Pasal 5 ayat 7 UU AI. Laporan ini didasarkan pada data yang dirangkum (diagregasi) dari laporan tahunan masing-masing Negara Anggota Uni Eropa. Laporan nasional ini berisi informasi tentang otorisasi dan penggunaan sistem tersebut.

Penting untuk dicatat bahwa laporan tahunan yang diterbitkan ini tidak boleh memuat informasi operasional yang sensitif. Ini berarti bahwa detail yang dapat membahayakan langkah-langkah keamanan atau investigasi yang sedang berlangsung tidak diungkapkan.

Tujuan dari laporan ini adalah untuk menciptakan transparansi dan memberikan gambaran umum kepada publik, pembuat kebijakan, dan pemangku kepentingan lainnya tentang penggunaan teknologi ini di Uni Eropa. Tujuannya adalah untuk menciptakan pemahaman tentang seberapa sering dan dalam kondisi apa identifikasi biometrik digunakan dalam praktik tanpa mengganggu pekerjaan aparat penegak hukum.

Contoh

Misalkan sistem identifikasi biometrik jarak jauh waktu nyata digunakan dengan cara yang memenuhi persyaratan khusus artikel ini tetapi melanggar Peraturan Perlindungan Data Umum (GDPR) karena tidak mengikuti prinsip minimalisasi data atau pembatasan tujuan. Dalam hal ini, penggunaan sistem tersebut, meskipun sesuai dengan persyaratan penggunaan untuk tujuan penegakan hukum, akan melanggar GDPR dan oleh karena itu tidak dapat diterima.

Tujuan dari ketentuan ini adalah untuk mengklarifikasi bahwa kepatuhan terhadap persyaratan khusus Pasal ini tidak membebaskan dari kewajiban untuk mematuhi semua peraturan perundang-undangan Uni Eropa lainnya yang relevan. Hal ini menggarisbawahi perlunya mempertimbangkan berbagai dasar dan prinsip hukum ketika menerapkan sistem AI, terutama yang berpotensi berdampak signifikan pada hak-hak fundamental.

Sistem AI Berisiko Tinggi

Peraturan tentang Kecerdasan Buatan (selanjutnya disebut: UU AI) membagi sistem AI ke dalam berbagai kategori, tergantung pada tingkat risiko yang ditimbulkannya terhadap kesehatan, keselamatan, atau hak-hak fundamental individu.

Klasifikasi sistem AI ke dalam kategori risiko sebagaimana didefinisikan oleh UU AI tampaknya merupakan langkah terpenting bagi penyedia potensial yang ingin memasarkan sistem mereka atau mengoperasikannya di Uni Eropa. Klasifikasi sebagai sistem AI berisiko

tinggi berarti bahwa sistem tersebut harus memenuhi persyaratan tertentu dan penyedia tersebut tunduk pada kewajiban tertentu.

Klasifikasi AI sebagai Sistem AI Berisiko Tinggi

Jadi bagaimana penyedia sistem AI dapat menentukan apakah sistem tersebut harus diklasifikasikan sebagai berisiko tinggi atau tidak? Usulan awal Komisi Uni Eropa, selain membedakan antara sistem AI yang mengandung komponen keselamatan dari produk yang tercakup dalam undang-undang harmonisasi Uni Eropa yang tercantum dalam Lampiran I UU AI atau merupakan produk tersebut, dan sistem AI mandiri yang termasuk dalam Lampiran III UU AI, tidak ada indikasi lebih lanjut untuk klasifikasi tersebut.

Namun, hal ini berubah selama negosiasi hingga diakui bahwa ketentuan yang awalnya direncanakan tentang klasifikasi sistem AI mandiri yang tercakup dalam Lampiran III UU AI tidak memberikan panduan yang cukup bagi penyedia, karena tampaknya dirumuskan terlalu umum. Oleh karena itu, diputuskan untuk memasukkan kriteria yang lebih rinci dalam Pasal 6 UU AI, yang mendefinisikan kasus-kasus di mana sistem AI tidak diklasifikasikan sebagai berisiko tinggi sesuai dengan Pasal 6 ayat 2 (lihat Pertimbangan 52 UU AI). Pasal 6 ayat 3. UU AI menetapkan bahwa “sebagai pengecualian dari paragraf 2, sistem AI yang tercantum dalam Lampiran III tidak akan dianggap berisiko tinggi jika tidak menimbulkan risiko bahaya yang signifikan terhadap kesehatan, keselamatan, atau hak-hak dasar manusia, termasuk dengan tidak secara signifikan memengaruhi hasil pengambilan keputusan.

Subparagraf pertama berlaku jika salah satu dari kondisi berikut terpenuhi:

- a) sistem AI dimaksudkan untuk melakukan tugas prosedural yang didefinisikan secara sempit;
- b) sistem AI dirancang untuk meningkatkan hasil dari aktivitas manusia yang telah diselesaikan sebelumnya;
- c) sistem AI dimaksudkan untuk mengenali pola pengambilan keputusan atau penyimpangan dari pola pengambilan keputusan sebelumnya dan tidak dimaksudkan untuk menggantikan atau memengaruhi penilaian manusia yang telah diselesaikan sebelumnya tanpa tinjauan manusia yang sesuai; atau
- d) sistem AI dimaksudkan untuk melakukan tugas persiapan untuk penilaian yang relevan untuk tujuan kasus penggunaan yang tercantum dalam Lampiran III.

Pertimbangan 53 UU AI menjelaskan secara lebih rinci apa yang dimaksud dengan frasa “tidak memiliki dampak signifikan pada hasil dari proses pengambilan keputusan”, yaitu bahwa hal itu “tidak memiliki dampak signifikan pada isi dan oleh karena itu hasil dari proses pengambilan keputusan, terlepas dari apakah keputusan tersebut dibuat oleh manusia atau otomatis”. Lebih lanjut, pertimbangan ini juga menguraikan contoh-contoh kriteria di atas dan menjelaskannya secara lebih rinci untuk memberikan panduan lebih lanjut kepada penyedia untuk klasifikasi sistem AI mereka.

Menurut Pertimbangan 53, sistem AI yang dimaksud dalam Pasal 6 ayat 3 huruf a UU AI untuk melakukan tugas prosedural yang didefinisikan secara sempit akan mencakup, misalnya, sistem AI “yang mengubah data tidak terstruktur menjadi data terstruktur, sistem AI

yang mengklasifikasikan dokumen yang masuk ke dalam kategori atau sistem AI yang digunakan untuk mendeteksi duplikat di antara sejumlah besar aplikasi”.

Menurut Pertimbangan 53, sistem AI yang dimaksud dalam Pasal 6 ayat 3 huruf b UU AI untuk peningkatan aktivitas manusia yang telah diselesaikan sebelumnya akan mencakup, misalnya, sistem AI yang “dimaksudkan untuk meningkatkan bahasa yang digunakan dalam dokumen yang telah ditulis sebelumnya, seperti nada profesional, gaya bahasa ilmiah atau untuk menyesuaikan teks dengan gaya tertentu yang terkait dengan merek dagang”.

Menurut Pertimbangan 53, sistem AI yang dimaksud dalam Pasal 6 ayat 3 huruf c UU AI untuk mendeteksi pola pengambilan keputusan atau penyimpangan dari pola pengambilan keputusan sebelumnya akan mencakup, misalnya, sistem AI “yang dapat digunakan dalam kaitannya dengan pola penilaian tertentu dari seorang guru untuk memeriksa secara retrospektif apakah guru tersebut mungkin telah menyimpang dari pola penilaian tersebut untuk menarik perhatian pada kemungkinan ketidakkonsistenan atau penyimpangan”.

Menurut Pertimbangan 53, sistem AI yang dimaksud dalam Pasal 6 ayat 3 huruf d UU AI untuk melakukan tugas persiapan untuk tujuan kasus penggunaan yang tercantum dalam Lampiran III akan mencakup, misalnya, “solusi cerdas untuk memproses berkas, termasuk berbagai fungsi seperti pengindeksan, pencarian, pemrosesan teks dan bahasa atau menghubungkan data dengan sumber data lain, atau sistem AI untuk menerjemahkan dokumen”.

Karena pembuatan profil orang dianggap sebagai gangguan signifikan terhadap hak-hak fundamental mereka, Pasal 6 ayat 3 UU AI menetapkan bahwa sistem AI tersebut harus selalu diklasifikasikan sebagai berisiko tinggi, bahkan jika mereka memenuhi kriteria yang tercantum di atas.

Jika penyedia menentukan bahwa sistem AI mereka memenuhi satu atau lebih kriteria yang ditetapkan dalam Pasal 6 ayat 3, mereka wajib berdasarkan Pasal 6 ayat 4 UU AI untuk mendokumentasikan penilaian ini sebelum memasarkannya atau menggunakannya dan untuk mendaftarkan sistem AI tersebut dalam basis data Uni Eropa untuk sistem AI berisiko tinggi sesuai dengan Pasal 49 ayat 4 UU AI. 2 Undang-Undang AI. Dokumentasi ini juga harus diserahkan atas permintaan otoritas nasional yang berwenang.

Komisi Uni Eropa telah merancang Undang-Undang AI sebagai undang-undang yang memungkinkan penyesuaian ketentuan tertentu terhadap perkembangan teknologi baru secepat mungkin. Dalam kebanyakan kasus, peraturan pelaksana disediakan untuk tujuan ini, yang dapat diproses lebih cepat secara prosedural daripada dalam prosedur legislatif biasa. Dalam hal kriteria yang disebutkan di atas pada Pasal 6 ayat 3, oleh karena itu Komisi Uni Eropa dapat mengadopsi peraturan pelaksana sesuai dengan Pasal 6 ayat 6 Undang-Undang AI yang memperluas, mengubah, atau menghapus daftar kriteria ini – namun, hal ini tunduk pada kondisi ketat, yang dijelaskan lebih rinci dalam paragraf ini.

Sebagai dukungan tambahan bagi penyedia, Pasal 6 ayat 5 Undang-Undang AI menetapkan bahwa Komisi Uni Eropa – setelah berkonsultasi dengan Dewan Kecerdasan Buatan Eropa – harus memberikan pedoman tentang implementasi praktis pasal ini dan daftar

komprehensif contoh praktis kasus penggunaan untuk sistem AI berisiko tinggi dan tidak berisiko tinggi paling lambat 18 bulan setelah Peraturan tersebut berlaku.

Selain itu, pertimbangan-pertimbangan yang menjelaskan ketentuan-ketentuan individual dari UU AI secara lebih rinci, juga dapat memberikan bantuan tambahan untuk interpretasi Pasal 6 UU AI dalam kasus ini agar dapat mengklasifikasikan sistem AI sebagai sistem berisiko tinggi yang dapat termasuk dalam Pasal 6 ayat 1 atau 2 dengan lebih baik. Pertimbangan 46-63 menjelaskan secara lebih rinci apa yang dipikirkan oleh pembuat undang-undang Uni Eropa ketika merumuskan ketentuan tentang sistem AI berisiko tinggi (Pasal 6 bersamaan dengan Lampiran I dan Lampiran III).

Seperti yang disebutkan di atas, Pasal 6 UU AI membedakan antara dua jenis sistem AI berisiko tinggi yang berbeda:

Pasal 6 ayat 1 UU AI menyangkut sistem AI yang dianggap sebagai komponen keselamatan untuk suatu produk yang telah diatur berdasarkan salah satu undang-undang Uni Eropa yang tercantum dalam Lampiran I, atau yang merupakan produk itu sendiri dan tunduk pada prosedur penilaian kesesuaian sesuai dengan undang-undang Uni Eropa yang relevan yang tercantum dalam Lampiran I oleh badan penilaian kesesuaian yang bertindak sebagai pihak ketiga (disebut sebagai "badan yang diberi pemberitahuan").

Ketentuan harmonisasi yang tercantum dalam Lampiran I Bagian A UU AI, yang didasarkan pada Kerangka Legislatif Baru, menyangkut produk-produk seperti mesin, mainan, lift, peralatan dan sistem pelindung yang dimaksudkan untuk digunakan di atmosfer yang berpotensi meledak, peralatan radio, peralatan bertekanan, peralatan kapal rekreasi, kereta gantung, peralatan untuk pembakaran bahan bakar gas, perangkat medis, dan perangkat medis diagnostik in vitro.

Tujuan legislator Uni Eropa dengan ketentuan ini, yaitu Pasal 6 ayat 1 UU AI, adalah untuk fokus pada aplikasi AI yang memiliki dampak nyata pada keselamatan (dan khususnya pada keselamatan produk). Tujuannya adalah untuk mempertimbangkan undang-undang yang sudah mapan dan komprehensif yang mengatur banyak produk berisiko (contoh yang diberikan pada paragraf sebelumnya) dan untuk memastikan bahwa UU AI sepenuhnya terintegrasi ke dalam undang-undang sektoral yang relevan. Hal ini dilakukan dengan memastikan bahwa definisi yang relevan (misalnya, "komponen keselamatan") diharmonisasikan, tetapi juga fakta bahwa penilaian kesesuaian produk dalam undang-undang sektoral sebagai kriteria untuk tingkat risiko yang tinggi dan dengan menggunakan instrumen penegakan hukum dari undang-undang sektoral.

Apa artinya ini secara konkret bagi penyedia yang sistem AI-nya merupakan komponen keamanan suatu produk atau produk itu sendiri termasuk dalam salah satu undang-undang yang tercantum dalam Lampiran I Bagian A UU AI dan yang prosedur penilaian kesesuaiannya harus dilakukan oleh badan penilaian kesesuaian yang bertindak sebagai pihak ketiga sesuai dengan salah satu undang-undang Uni Eropa yang tercantum? Sistem AI tersebut diklasifikasikan sebagai berisiko tinggi dalam arti Pasal 6 ayat 1 UU AI. Oleh karena itu, dalam hal ini juga, penyedia harus mematuhi kewajiban yang tercantum dalam Pasal 16 dan seterusnya UU AI. Jika sistem AI yang dimaksud juga berinteraksi dengan manusia atau

menghasilkan konten audio, gambar, video, atau teks sintetis, penyedia juga harus mematuhi kewajiban transparansi sesuai dengan Pasal 50 UU AI.

Jika komponen keamanan sistem AI atau sistem AI sebagai produk itu sendiri terkait dengan undang-undang Uni Eropa yang tercantum dalam Lampiran I Bagian B UU AI, hanya Pasal 6 ayat 1 UU AI yang berlaku untuk sistem AI yang memiliki Pasal 112 UU AI (peninjauan UU AI, amandemen Lampiran, laporan tentang UU AI) berlaku sesuai dengan Pasal 2 ayat 2 UU AI. Tidak berlakunya bagian lain dari Peraturan AI dalam kasus ini disebabkan oleh perbedaan logika regulasi untuk AI dan peraturan perundang-undangan tersebut secara signifikan. Contoh bidang yang tercakup dalam Lampiran I Bagian B UU AI meliputi penerbangan sipil, kendaraan pertanian dan kehutanan, kendaraan bermotor dan trailernya, peralatan kelautan, dan lain-lain.

Pasal 6 ayat 2 UU AI menetapkan bahwa semua sistem AI yang termasuk dalam salah satu bidang yang tercantum dalam Lampiran III UU AI harus diklasifikasikan sebagai berisiko tinggi. Selain risiko tinggi membahayakan kesehatan dan keselamatan atau hak-hak dasar seseorang, Pertimbangan 52 UU AI mengharuskan penyedia untuk “mempertimbangkan baik keseriusan potensi bahaya maupun kemungkinan terjadinya.”

Menurut Pertimbangan 52, metodologi dan kriteria untuk menentukan sistem tersebut sama dengan yang ditetapkan untuk amandemen di masa mendatang terhadap daftar sistem AI berisiko tinggi dalam Lampiran III sesuai dengan Pasal 7 UU AI untuk mempertimbangkan laju perkembangan teknologi yang cepat dan kemungkinan perubahan dalam penggunaan sistem AI. Pasal 7 UU AI menetapkan kriteria ketat untuk penerapan tindakan delegasi oleh Komisi Uni Eropa mengenai penambahan, modifikasi, atau penghapusan kasus penggunaan dalam Lampiran III UU AI.

Sebagaimana dijelaskan pada paragraf sebelumnya, suatu sistem AI diklasifikasikan sebagai berisiko tinggi jika, antara lain, menimbulkan risiko signifikan terhadap hak-hak fundamental individu. Pertimbangan ke-48 UU AI menekankan bahwa besarnya dampak buruk terhadap hak-hak fundamental yang dilindungi oleh Piagam Hak Fundamental Eropa sangat penting untuk klasifikasi suatu sistem AI sebagai berisiko tinggi. Hal-hal tersebut kemudian dicantumkan dalam pertimbangan yang relevan, termasuk martabat manusia, penghormatan terhadap kehidupan pribadi dan keluarga, perlindungan data pribadi dan banyak lagi (lihat bagian 3.4).

Area dan kasus penggunaan yang tercakup dalam Lampiran III UU AI diuraikan di bawah ini. Selanjutnya, beberapa contoh kasus penggunaan tersebut diberikan untuk mengilustrasikan kepada penyedia sistem AI mana yang sebenarnya dapat termasuk dalam salah satu area yang tercantum dalam Lampiran III dalam praktiknya di masa mendatang. Pada titik ini – seperti yang telah disebutkan – sekali lagi merujuk pada Pasal 6 ayat 5 UU AI, yang mengatur kewajiban Komisi Uni Eropa untuk memberikan pedoman implementasi praktis dalam konteks ini, termasuk daftar contoh praktis kasus penggunaan berisiko tinggi dan tidak berisiko tinggi, paling lambat 18 bulan setelah UU AI mulai berlaku.

1. Biometrik, sejauh penggunaannya diizinkan berdasarkan hukum Uni Eropa atau hukum nasional yang relevan:

- a) sistem identifikasi jarak jauh biometrik. Ini tidak termasuk sistem AI yang dimaksudkan untuk digunakan untuk verifikasi biometrik yang tujuan utamanya adalah untuk memastikan bahwa orang tertentu adalah orang yang diklaimnya;
- b) Sistem AI yang dimaksudkan untuk digunakan untuk kategorisasi biometrik, menurut atribut atau karakteristik sensitif atau terlindungi berdasarkan inferensi dari atribut atau karakteristik tersebut;
- c) Sistem AI yang dimaksudkan untuk digunakan untuk pengenalan emosi.

Apa yang dimaksud dengan sistem identifikasi biometrik jarak jauh? Pasal 3 ayat 41 UU AI mendefinisikan ini sebagai sistem AI “yang berfungsi untuk mengidentifikasi orang tanpa keterlibatan aktif mereka dan, biasanya, dari jarak jauh dengan mencocokkan data biometrik seseorang dengan data biometrik yang tersimpan dalam basis data referensi”.

Pertimbangan 54 UU AI menjelaskan lebih rinci mengapa klasifikasi sistem identifikasi biometrik jarak jauh sebagai berisiko tinggi tampak sangat penting: “Ketidakakuratan teknis sistem AI yang ditujukan untuk identifikasi biometrik jarak jauh orang dapat menyebabkan hasil yang bias dan memiliki efek diskriminatif. Risiko hasil yang bias dan efek diskriminatif tersebut sangat penting terutama jika menyangkut usia, etnis, ras, jenis kelamin, atau disabilitas.”

Usulan asli Komisi Uni Eropa tidak menyediakan kasus penggunaan yang tercantum dalam Lampiran III/1b) dan c), sistem AI untuk kategorisasi biometrik dan sistem untuk pengenalan emosi hanya tunduk pada kewajiban transparansi. Dalam teks akhir Peraturan, kasus penggunaan ini dimasukkan sehingga sistem AI yang digunakan untuk kategorisasi biometrik menurut atribut atau karakteristik sensitif yang dilindungi berdasarkan data biometrik sesuai dengan Pasal 9 ayat 1 GDPR dan sistem AI untuk pengenalan emosi diklasifikasikan sebagai berisiko tinggi.

2. Infrastruktur kritis

Sistem AI yang dimaksudkan untuk digunakan sebagai komponen keselamatan dalam pengelolaan dan pengoperasian infrastruktur digital kritis, lalu lintas jalan raya, atau pasokan Air, gas, pemanas, atau listrik.

Mengapa sistem-sistem ini diklasifikasikan sebagai berisiko tinggi? Pasal 55 UU AI menyatakan bahwa “komponen keamanan infrastruktur kritis, termasuk infrastruktur digital kritis, digunakan untuk melindungi integritas fisik infrastruktur kritis atau kesehatan dan keselamatan orang dan properti, tetapi tidak diperlukan agar sistem tersebut berfungsi. Kegagalan atau malfungsi komponen tersebut dapat secara langsung menyebabkan risiko terhadap integritas fisik infrastruktur kritis dan dengan demikian menimbulkan risiko terhadap kesehatan dan keselamatan orang dan properti.” Sebagai contoh sistem tersebut, pasal ini

menyebutkan sistem untuk memantau tekanan Air atau sistem kontrol alarm kebakaran di pusat komputasi awan.

3. Pendidikan dan pelatihan kejuruan

- a) Sistem AI yang dimaksudkan untuk digunakan untuk menentukan akses atau penerimaan atau untuk menugaskan individu ke lembaga pendidikan dan pelatihan kejuruan di semua tingkatan;
- b) Sistem AI yang dimaksudkan untuk digunakan untuk mengevaluasi hasil pembelajaran, termasuk ketika hasil tersebut digunakan untuk mengarahkan proses pembelajaran individu di lembaga pendidikan dan pelatihan kejuruan di semua tingkatan;
- c) Sistem AI yang dimaksudkan untuk digunakan untuk tujuan menilai tingkat pendidikan yang sesuai yang akan diterima atau dapat diakses oleh individu, dalam konteks atau di dalam lembaga pendidikan dan pelatihan kejuruan di semua tingkatan;
- d) Sistem AI yang dimaksudkan untuk digunakan untuk memantau dan mendeteksi perilaku terlarang siswa selama ujian dalam konteks atau di dalam lembaga pendidikan dan pelatihan kejuruan di semua tingkatan.

Pertimbangan ke-56 UU AI menjelaskan secara lebih rinci mengapa kasus penggunaan yang tercantum di sektor pendidikan diklasifikasikan sebagai berisiko tinggi, meskipun penggunaan AI untuk mempromosikan pendidikan dan perolehan keterampilan digital pada prinsipnya harus disambut baik. Kasus penggunaan yang tercantum dalam Lampiran III/3a-d UU AI akan “menentukan jalannya pendidikan dan kehidupan profesional seseorang dan oleh karena itu dapat memengaruhi kemampuan mereka untuk mencari nafkah. Jika dirancang dan digunakan secara tidak tepat, sistem tersebut dapat sangat mengganggu dan melanggar hak atas pendidikan dan hak untuk tidak diskriminasi serta melanggar pola diskriminasi historis, misalnya terhadap perempuan, kelompok usia tertentu, dan penyandang disabilitas atau orang dengan asal ras atau etnis tertentu atau orientasi seksual tertentu”.

4. Ketenagakerjaan, manajemen pekerja, dan akses ke wirausaha

- a) Sistem AI yang dimaksudkan untuk digunakan dalam perekrutan atau seleksi individu, khususnya untuk menempatkan iklan lowongan kerja yang ditargetkan, untuk menganalisis dan menyaring lamaran kerja, dan untuk mengevaluasi kandidat;
- b) Sistem AI yang dimaksudkan untuk digunakan dalam pengambilan keputusan yang memengaruhi ketentuan hubungan kerja, promosi atau pengakhiran hubungan kontraktual terkait pekerjaan, untuk mengalokasikan tugas berdasarkan perilaku individu atau sifat atau karakteristik pribadi, atau untuk memantau dan mengevaluasi kinerja dan perilaku individu dalam hubungan tersebut.

Pertimbangan ke-57 UU AI menjelaskan klasifikasi kasus penggunaan yang tercantum dalam Lampiran III/4a dan b UU AI sebagai berisiko tinggi dengan menyatakan bahwa “sistem-sistem ini dapat berdampak signifikan pada prospek karir dan mata pencaharian individu-individu tersebut di masa depan serta pada hak-hak pekerja”. Kasus penggunaan ini juga menimbulkan risiko melanggengkan pola diskriminasi historis, serupa dengan kasus penggunaan yang tercantum dalam Lampiran III/3 UU AI. Sistem AI yang digunakan untuk memantau kinerja dan perilaku individu-individu tersebut juga dapat memengaruhi hak-hak mendasar mereka atas perlindungan data dan privasi.

5. Akses dan pemanfaatan layanan dan manfaat penting swasta dan publik:

- a) Sistem AI yang dimaksudkan untuk digunakan oleh otoritas publik atau atas nama otoritas publik untuk mengevaluasi kelayakan individu untuk mendapatkan manfaat dan layanan bantuan publik penting, termasuk layanan kesehatan, serta untuk memberikan, mengurangi, mencabut, atau menuntut kembali manfaat dan layanan tersebut;
- b) Sistem AI yang dimaksudkan untuk digunakan untuk mengevaluasi kelayakan kredit individu atau menetapkan skor kredit mereka, kecuali sistem AI yang digunakan untuk tujuan mendeteksi penipuan keuangan;
- c) Sistem AI yang dimaksudkan untuk digunakan untuk penilaian risiko dan penetapan harga terkait dengan individu dalam kasus asuransi jiwa dan kesehatan;
- d) Sistem AI yang dimaksudkan untuk mengevaluasi dan mengklasifikasikan panggilan darurat oleh individu atau untuk digunakan untuk mengirimkan, atau untuk menetapkan prioritas dalam pengiriman, layanan tanggap darurat pertama, termasuk oleh polisi, petugas pemadam kebakaran, dan bantuan medis, serta sistem triase pasien perawatan kesehatan darurat.

Pertimbangan 58 UU AI menjelaskan secara rinci mengapa klasifikasi sistem AI sebagai berisiko tinggi di bidang ini sangat penting dan mengapa kasus penggunaan tertentu yang tercantum dapat secara khusus mengganggu beberapa hak mendasar individu.

Sistem AI berdasarkan Lampiran III/5a UU AI, yang menilai kelayakan orang perseorangan untuk mendapatkan manfaat dukungan negara dasar seperti manfaat kesehatan, manfaat jaminan sosial atau layanan sosial dalam kasus-kasus seperti persalinan, sakit, kecelakaan kerja, ketergantungan atau usia lanjut dan kehilangan pekerjaan, serta dukungan sosial dan perumahan, “dapat berdampak signifikan pada mata pencaharian individu dan melanggar hak-hak mendasar mereka, seperti hak atas perlindungan sosial, non-diskriminasi, martabat manusia atau upaya hukum yang efektif” (Pertimbangan 58 UU AI).

Sistem AI sesuai dengan Lampiran III/5b diklasifikasikan sebagai berisiko tinggi “karena menentukan akses orang-orang ini ke sumber daya keuangan atau layanan penting seperti perumahan, listrik, dan layanan telekomunikasi” (Pertimbangan 58 UU AI). Lebih jauh lagi, ada juga risiko diskriminasi dan pelanggaran pola diskriminasi historis, seperti berdasarkan asal ras atau etnis, jenis kelamin, disabilitas, usia atau orientasi seksual, atau risiko bentuk

diskriminasi baru. Namun, sistem AI “yang digunakan berdasarkan hukum Uni Eropa untuk mendeteksi penipuan dalam penyediaan layanan keuangan atau untuk tujuan kehati-hatian untuk perhitungan persyaratan modal lembaga kredit dan perusahaan asuransi” dikecualikan di sini (Pertimbangan 58 UU AI).

Kasus penggunaan menurut Lampiran III/5c UU AI tidak termasuk dalam usulan awal. Namun, hal itu dimasukkan dalam Lampiran III selama negosiasi, karena keputusan untuk menggunakan sistem AI semacam itu “juga dapat berdampak signifikan pada mata pencaharian masyarakat dan, jika tidak dirancang, dikembangkan, dan digunakan dengan benar, dapat menimbulkan konsekuensi serius bagi kehidupan dan kesehatan masyarakat, termasuk pengucilan finansial dan diskriminasi” (Pertimbangan 58 UU AI).

Sistem AI sesuai dengan Lampiran III/5d UU AI diklasifikasikan sebagai berisiko tinggi “karena mereka mengambil keputusan dalam situasi yang sangat kritis bagi kehidupan dan kesehatan seseorang dan bagi harta benda mereka” (Pertimbangan 58 UU AI).

6. Penegakan hukum, sejauh penggunaannya diizinkan dan sesuai dengan hukum Uni Eropa atau hukum nasional yang berlaku:

- a) Sistem AI yang dimaksudkan untuk digunakan oleh atau atas nama otoritas penegak hukum, atau oleh lembaga, badan, kantor, atau badan Uni Eropa untuk mendukung otoritas penegak hukum atau atas nama mereka untuk menilai risiko seseorang menjadi korban tindak pidana;
- b) Sistem AI yang dimaksudkan untuk digunakan oleh atau atas nama otoritas penegak hukum atau oleh lembaga, badan, kantor, atau badan Uni Eropa untuk mendukung otoritas penegak hukum sebagai poligraf atau alat serupa;
- c) Sistem AI yang dimaksudkan untuk digunakan oleh atau atas nama otoritas penegak hukum, atau oleh lembaga, badan, kantor, atau badan Uni Eropa, untuk mendukung otoritas penegak hukum dalam mengevaluasi keandalan bukti selama penyelidikan atau penuntutan tindak pidana;
- d) Sistem AI yang dimaksudkan untuk digunakan oleh otoritas penegak hukum atau atas nama mereka atau oleh lembaga, badan, kantor, atau badan Uni Eropa untuk mendukung otoritas penegak hukum dalam menilai risiko seseorang melakukan pelanggaran atau mengulangi pelanggaran bukan semata-mata berdasarkan profil orang perseorangan sebagaimana dimaksud dalam Pasal 3(4) Direktif (EU) 2016/680, atau untuk menilai sifat dan karakteristik kepribadian atau perilaku kriminal masa lalu dari orang perseorangan atau kelompok;
- e) Sistem AI yang dimaksudkan untuk digunakan oleh atau atas nama otoritas penegak hukum atau oleh lembaga, badan, kantor, atau badan Uni Eropa untuk mendukung otoritas penegak hukum dalam pembuatan profil orang perseorangan sebagaimana dimaksud dalam Pasal 3(4) Direktif (EU) 2016/680 dalam rangka pendeteksian, penyelidikan, atau penuntutan tindak pidana.

Pertimbangan 59 UU AI menjelaskan secara lebih rinci mengapa kasus penggunaan tertentu harus diklasifikasikan sebagai berisiko tinggi, khususnya di bidang penuntutan pidana.

Sistem AI yang digunakan oleh aparat penegak hukum ditanda dengan ketidakseimbangan kekuasaan yang signifikan dan dapat berdampak negatif besar pada hak-hak mendasar yang diabadikan dalam Piagam bagi individu yang bersangkutan. Di bidang ini, tampaknya sangat penting jika sistem AI tidak memenuhi persyaratan UU AI mengenai kualitas data untuk pelatihan sistem AI, tidak memenuhi persyaratan untuk kinerja, akurasi atau ketahanannya, atau jika tidak dirancang dan diuji dengan benar, karena hal ini dapat menyebabkan diskriminasi terhadap subjek data. Kurangnya transparansi, penjelasan, dan dokumentasi dapat menghambat pelaksanaan hak-hak prosedural mendasar yang penting, seperti hak atas upaya hukum yang efektif dan pengadilan yang tidak memihak, serta hak pembelaan dan praduga tidak bersalah.

Karena alasan-alasan ini, kasus penggunaan yang tercantum dalam Lampiran III/6a-e UU AI diklasifikasikan sebagai berisiko tinggi.

7. Migrasi, suaka, dan kontrol perbatasan, sejauh penggunaannya diizinkan berdasarkan hukum Uni Eropa atau hukum nasional yang relevan:

- a) Sistem AI yang dimaksudkan untuk digunakan oleh atau atas nama otoritas publik yang berwenang atau oleh lembaga, badan, kantor, atau badan Uni Eropa sebagai poligraf atau alat serupa;
- b) Sistem AI yang dimaksudkan untuk digunakan oleh atau atas nama otoritas publik yang berwenang atau oleh lembaga, badan, kantor, atau badan Uni Eropa untuk menilai risiko, termasuk risiko keamanan, risiko migrasi ilegal, atau risiko kesehatan, yang ditimbulkan oleh orang perseorangan yang bermaksud memasuki atau telah memasuki wilayah Negara Anggota;
- c) Sistem AI yang dimaksudkan untuk digunakan oleh atau atas nama otoritas publik yang berwenang atau oleh lembaga, badan, kantor, atau badan Uni Eropa untuk membantu otoritas publik yang berwenang dalam pemeriksaan permohonan suaka, visa, atau izin tinggal dan untuk pengaduan terkait mengenai kelayakan orang perseorangan yang mengajukan permohonan status, termasuk penilaian terkait keandalan bukti;
- d) Sistem AI yang dimaksudkan untuk digunakan oleh atau atas nama otoritas publik yang berwenang, atau oleh lembaga, badan, kantor, atau badan Uni Eropa, dalam konteks migrasi, suaka, atau manajemen kontrol perbatasan, untuk tujuan mendeteksi, mengenali, atau mengidentifikasi orang perseorangan, dengan pengecualian verifikasi dokumen perjalanan.

Pertimbangan 60 UU AI membenarkan klasifikasi kasus penggunaan yang tercantum dalam Lampiran III/7a-d UU AI sebagai berisiko tinggi karena sistem AI yang digunakan di bidang ini akan memengaruhi orang-orang dalam situasi rentan yang bergantung pada hasil tindakan yang diambil oleh otoritas yang berwenang. Oleh karena itu, akurasi, sifat non-

diskriminatif, dan transparansi sistem AI ini penting untuk melindungi hak-hak mendasar orang yang bersangkutan (khususnya hak atas kebebasan bergerak, non-diskriminasi, perlindungan kehidupan pribadi dan data pribadi, perlindungan internasional, dan tata kelola yang baik).

Sistem AI di bidang migrasi, suaka, dan kontrol perbatasan yang termasuk dalam salah satu kasus penggunaan yang tercantum dalam Lampiran III/7a-d UU AI harus mematuhi peraturan prosedural Uni Eropa yang relevan dan tidak boleh digunakan untuk menghindari kewajiban internasional, seperti yang timbul dari Konvensi Jenewa tentang Pengungsi. Lebih lanjut, prinsip non-refoulement dan hak atas perlindungan internasional harus dipatuhi (Pertimbangan 60 UU AI).

8. Administrasi peradilan dan proses demokrasi

- a) Sistem AI yang dimaksudkan untuk digunakan oleh otoritas peradilan atau atas nama mereka untuk membantu otoritas peradilan dalam meneliti dan menafsirkan fakta dan hukum serta dalam menerapkan hukum pada serangkaian fakta konkret, atau untuk digunakan dengan cara serupa dalam Penyelesaian sengketa alternatif;
- b) Sistem AI yang dimaksudkan untuk digunakan untuk memengaruhi hasil pemilihan atau referendum atau perilaku pemungutan suara orang perseorangan dalam menggunakan hak pilih mereka dalam pemilihan atau referendum. Ini tidak termasuk sistem AI yang keluarannya tidak secara langsung memengaruhi orang perseorangan, seperti alat yang digunakan untuk mengatur, mengoptimalkan, atau menyusun kampanye politik dari sudut pandang administratif atau logistik.

Sistem AI di bidang ini diklasifikasikan sebagai berisiko tinggi menurut Pasal 61 UU AI, karena sistem ini dapat berdampak signifikan pada demokrasi, supremasi hukum, kebebasan individu, dan hak atas upaya hukum yang efektif dan pengadilan yang tidak memihak. Sehubungan dengan kasus penggunaan dalam Lampiran III/8a UU AI, Pasal 61 UU AI menekankan bahwa sistem AI di bidang peradilan hanya dapat mendukung kewenangan pengambilan keputusan hakim atau independensi peradilan, tetapi tidak pernah menggantikannya. Proses pengambilan keputusan akhir harus tetap menjadi aktivitas yang dikendalikan manusia. Sistem AI untuk kegiatan administratif tambahan semata, seperti anonimisasi atau pseudonimisasi putusan pengadilan, dokumen, atau data yang tidak memengaruhi administrasi peradilan yang sebenarnya dalam kasus-kasus individual, tidak boleh diklasifikasikan sebagai berisiko tinggi.

Kasus penggunaan yang tercantum dalam Lampiran III/8b UU AI tidak termasuk dalam proposal asli. Namun, hal itu dimasukkan dalam Lampiran III untuk menanggulangi “risiko campur tangan eksternal yang tidak semestinya terhadap hak pilih yang diabadikan dalam Pasal 39 Piagam dan dampak buruk terhadap demokrasi dan supremasi hukum” (Pertimbangan 62 UU AI).

Persyaratan untuk Sistem AI Berisiko Tinggi

Klasifikasi sistem AI berisiko tinggi telah dijelaskan pada bagian sebelumnya, setelah klasifikasi ditentukan, sistem AI berisiko tinggi harus memenuhi persyaratan tertentu. Persyaratan ini diatur dalam Pasal 8 dan seterusnya UU AI.

Pasal 8 UU AI sendiri hanya merujuk pada paragraf 1 pada fakta bahwa keadaan teknologi terkini harus diperhitungkan dan bahwa sistem manajemen risiko sebagaimana dijelaskan dalam Pasal 9 UU AI harus diterapkan. Paragraf 2 secara eksplisit menyatakan bahwa, sesuai dengan Lampiran 1 Bagian A UU AI, penyedia harus memastikan bahwa produk tersebut pertama-tama harus memenuhi persyaratan standar khusus ini dan bahwa persyaratan UU AI mengenai AI berisiko tinggi ditambahkan "di atasnya". Misalnya, alat kesehatan yang komponen keamanannya adalah sistem AI berisiko tinggi pertama-tama harus memenuhi persyaratan Peraturan Alat Kesehatan dan kemudian persyaratan Pasal 8 dan seterusnya UU AI. Untuk menghindari duplikasi pekerjaan, penyedia dapat mengintegrasikan kepatuhan terhadap persyaratan Undang-Undang AI ke dalam dokumentasi produk mereka sesuai dengan kerangka hukum Lampiran I yang berlaku.

Untuk melanjutkan contoh yang diberikan, penyedia karenanya tidak perlu menyimpan dua set dokumentasi, satu sesuai dengan Peraturan Perangkat Medis dan satu sesuai dengan Undang-Undang AI, tetapi dapat mengintegrasikan dokumentasi Undang-Undang AI ke dalam dokumentasi Peraturan Perangkat Medis.

Sistem Manajemen Risiko

Setiap sistem AI berisiko tinggi harus memiliki sistem manajemen risiko sesuai dengan Pasal 9 Undang-Undang AI, yang direncanakan, diimplementasikan, dipelihara, dan ditinjau secara berkala selama seluruh siklus hidup sistem AI.

Hanya risiko yang dapat dikurangi atau dihilangkan secara tepat melalui pengembangan atau desain sistem AI berisiko tinggi atau dengan menyediakan informasi teknis yang memadai yang perlu dipertimbangkan. Risiko yang sama sekali tidak dapat diprediksi (juga disebut sebagai "angsa hitam" dalam manajemen risiko) tidak perlu dipertimbangkan.

Undang-Undang AI mengharapkan pihak yang menerapkan memiliki keahlian teknis yang diperlukan untuk menghilangkan atau mengurangi risiko yang terkait dengan penggunaan AI berisiko tinggi.

Daftar Periksa: Langkah-langkah dalam manajemen risiko

1. Identifikasi dan analisis risiko yang diketahui dan dapat diprediksi
 - *Pertanyaan penilaian: Risiko apa yang ditimbulkan oleh sistem AI berisiko tinggi terhadap kesehatan, keselamatan, atau hak-hak dasar jika digunakan sesuai dengan tujuan yang dimaksudkan?*
2. Penilaian dan evaluasi risiko

- *Pertanyaan penilaian: Risiko apa yang dapat timbul jika sistem AI berisiko tinggi digunakan sesuai dengan tujuan yang dimaksudkan atau dalam konteks penyalahgunaan yang dapat diprediksi secara wajar?*
- 3. Penilaian risiko lain yang mungkin timbul
 - *Pertanyaan penilaian: Bagaimana risiko yang timbul setelah produk dipasarkan dapat dikurangi dengan mengevaluasi data dari sistem pemantauan sesuai dengan Pasal 72 Undang-Undang AI?*
- 4. Mengambil langkah-langkah manajemen risiko yang tepat dan terarah
 - *Pertanyaan penilaian: Langkah-langkah apa yang dapat diambil untuk mengatasi risiko yang diidentifikasi pada pertanyaan pertama?*
 - *Pertanyaan penilaian: Apakah dampak dan kemungkinan interaksi telah diperhitungkan dengan semestinya?*
 - *Pertanyaan penilaian: Apakah langkah-langkah telah diambil untuk memastikan bahwa risiko residual yang terkait dengan bahaya tertentu dan risiko residual keseluruhan dapat diklasifikasikan sebagai dapat diterima?*
 - *Sub-pertanyaan: Apakah risiko dihilangkan atau dikurangi sejauh yang dimungkinkan secara teknis melalui desain dan pengembangan sistem AI yang tepat?*
 - *Sub-pertanyaan: Apakah langkah-langkah mitigasi dan pengendalian yang tepat telah diambil untuk mengelola risiko yang tidak dapat dikesampingkan?*
 - *Sub-pertanyaan: Apakah informasi yang diperlukan telah diberikan sesuai dengan Pasal 13 atau apakah pengembang telah dilatih?*
 - *Pertanyaan penilaian: Apakah sistem AI telah diuji untuk menentukan langkah-langkah yang paling tepat?*
 - *Sub-pertanyaan: Apakah sistem tersebut telah diuji selama seluruh proses pengembangan atau setidaknya sebelum dipasarkan/dioperasikan?*
 - *Pertanyaan penilaian: Apakah telah dipertimbangkan apakah sistem AI kemungkinan akan berdampak buruk pada orang di bawah usia 18 tahun atau kelompok rentan lainnya?*
 - *Pertanyaan penilaian: Apakah ketentuan hukum lain yang berlaku telah dipertimbangkan dalam proses manajemen risiko?*

Data dan Tata Kelola Data

Data dan kumpulan data merupakan prasyarat wajib untuk penggunaan sistem AI. Jenis-jenis data telah dijelaskan pada bagian 3.1.

Untuk berbagai jenis data, yaitu kumpulan data pelatihan, validasi, dan pengujian, prosedur tata kelola data dan manajemen data harus ditetapkan sesuai dengan Pasal 10 UU AI yang sesuai untuk tujuan sistem AI berisiko tinggi. Oleh karena itu, data dan kumpulan data harus memenuhi kriteria kualitas yang disesuaikan dengan tujuan sistem AI berisiko tinggi. Tergantung pada tujuan penggunaannya, kumpulan data harus memiliki karakteristik

geografis, kontekstual, perilaku, atau fungsional khusus yang diperlukan dan khas untuk tujuan penggunaan sistem AI berisiko tinggi.

Pada dasarnya, Undang-Undang AI menjelaskan dua jenis tata kelola data, pertama tata kelola data umum dan kemudian tata kelola data pribadi, dengan fokus khusus pada kategori khusus data pribadi sesuai dengan Pasal 9 GDPR, jika hal ini melibatkan upaya memerangi bias.

Tata kelola data umum:

- Keputusan konseptual dengan mempertimbangkan tujuan sistem AI
- Metode pengumpulan data dan asal data (termasuk tujuan awal pengumpulan data jika itu adalah data pribadi)
- Proses persiapan data, seperti anotasi, pelabelan, pembersihan, pembaruan, pengayaan, dan agregasi
- Membuat asumsi, khususnya terkait informasi yang akan dikumpulkan dan disajikan bersama data
- Penilaian ketersediaan, kuantitas, dan kesesuaian kumpulan data yang dibutuhkan
- Pemeriksaan terkait kemungkinan bias, terutama jika hal ini berdampak pada kesehatan, keselamatan, atau hak-hak mendasar atau dapat menyebabkan diskriminasi
- Langkah-langkah untuk mendeteksi, mencegah, dan mengurangi distorsi ini
- Identifikasi kesenjangan atau kekurangan data yang relevan dan bagaimana hal tersebut dapat diperbaiki.

Penyedia dapat secara khusus memproses kategori khusus data pribadi untuk mendeteksi koreksi distorsi atau bias, di mana mereka juga harus mengambil langkah-langkah perlindungan yang sesuai.

Tata kelola data untuk kategori khusus data pribadi:

- Perlunya pemrosesan untuk deteksi dan koreksi, karena hal ini tidak dapat dilakukan secara efektif jika tidak dilakukan dengan cara ini
- Adanya pembatasan teknis yang mencegah penggunaan lebih lanjut, misalnya pseudonimisasi
- Adanya langkah-langkah keamanan yang tepat, seperti kontrol akses yang ketat dan dokumentasi, untuk mencegah penyalahgunaan dan memastikan bahwa hanya orang yang berwenang yang memiliki akses ke jenis data ini
- Tidak ada transmisi ke atau akses oleh pihak ketiga
- Penghapusan data segera setelah distorsi telah dikoreksi atau berakhirnya periode penyimpanan, mana pun yang terjadi lebih dulu
- Pemeliharaan direktori prosedur sesuai dengan Pasal 30 GDPR, termasuk dokumentasi alasan mengapa pemrosesan data diperlukan untuk deteksi dan koreksi bias

Dokumentasi Teknis

Sesuai dengan Pasal 11 UU AI, dokumentasi teknis sistem AI berisiko tinggi harus disiapkan sebelum dipasarkan/dioperasikan dan selalu diperbarui. Dokumentasi tersebut harus menunjukkan kepatuhan terhadap Pasal 8 dan seterusnya dan ditulis dalam bentuk yang

jasas dan mudah dipahami. Dokumentasi tersebut harus memuat setidaknya informasi yang ditentukan dalam Lampiran IV UU AI.

UKM dapat menyediakan dokumentasi ini dengan cara yang disederhanakan. Komisi Uni Eropa menyediakan formulir yang disederhanakan untuk tujuan ini.

Dalam kasus sistem AI berisiko tinggi sesuai dengan Lampiran I Bagian A UU AI, satu set dokumentasi harus disiapkan yang berisi persyaratan undang-undang khusus dan UU AI. Dokumentasi teknis bersama bersifat wajib, sedangkan pemeliharaan sistem manajemen risiko bersama sesuai dengan Pasal 9 UU AI merupakan persyaratan opsional.

Pencatatan dan Logisasi

Sistem AI berisiko tinggi harus dirancang sedemikian rupa sehingga pencatatan peristiwa secara otomatis dimungkinkan sepanjang siklus hidupnya.

Daftar Periksa: Spesifikasi untuk fungsi pencatatan

- Identifikasi fungsi yang mengarah pada prosedur sesuai dengan Pasal 79 UU AI (penanganan sistem AI yang menimbulkan risiko) atau pada perubahan signifikan
- Memfasilitasi pemantauan sistem AI setelah dipasarkan (lihat Pasal 72 UU AI)
- Memantau pengoperasian sistem AI berisiko tinggi (lihat Pasal 26 UU AI)

Persyaratan tambahan untuk sistem AI berisiko tinggi sesuai dengan Lampiran III huruf a UU AI (**Identifikasi Biometrik Jarak Jauh**)

- Pencatatan penggunaan sistem (tanggal dan waktu, periode penggunaan)
- Basis data referensi untuk sinkronisasi data
- Data masukan yang menghasilkan kecocokan dengan kueri
- Identitas orang yang terlibat dalam verifikasi hasil (lihat Pasal 14 ayat 5 UU AI)

Transparansi dan Penyediaan Informasi kepada Pengimplementasikan Kewajiban transparansi

Pengawasan Manusia

Sistem AI berisiko tinggi harus dirancang dan dikembangkan sedemikian rupa sehingga dapat diawasi **secara efektif** oleh manusia **sepanjang siklus hidupnya**, yang mungkin termasuk penggunaan alat antarmuka manusia-mesin. Pengawasan manusia berfungsi untuk mencegah atau meminimalkan risiko terhadap kesehatan, keselamatan, atau hak-hak dasar. Secara khusus, perhatian harus diberikan pada risiko yang muncul bahkan dalam kasus penggunaan yang dimaksudkan atau penyalahgunaan yang dapat diperkirakan dan yang tetap ada meskipun telah mematuhi Pasal 8 dan seterusnya dari UU AI.

Dalam menentukan **langkah-langkah pengawasan**, risiko, tingkat otonomi, dan konteks penggunaan sistem AI berisiko tinggi harus diperhitungkan. Pasal 14. UU AI mengatur jenis-jenis tindakan pencegahan berikut:

- Pemasangan tindakan pencegahan oleh penyedia, penempatan di pasar atau penugasan, jika secara teknis memungkinkan
- Penentuan pengaturan oleh penyedia sehingga dapat diimplementasikan oleh penyebar

Sistem AI harus dikembangkan dan disediakan sedemikian rupa sehingga pengawasan manusia dapat dilakukan **secara efektif**. Pengawasan manusia harus mampu melakukan hal-hal berikut:

- Memahami kemampuan dan keterbatasan sistem AI berisiko tinggi dan memantau operasinya, termasuk kemampuan untuk mendeteksi dan menyelesaikan anomali, malfungsi, dan kinerja yang tidak terduga
- Kesadaran akan bias otomatisasi (lihat bagian 7.1 Diskriminasi), terutama ketika sistem memberikan informasi atau rekomendasi yang menjadi dasar pengambilan keputusan oleh manusia
- Interpretasi yang benar terhadap hasil sistem, dengan mempertimbangkan alat dan metode interpretasi yang ada
- Keputusan untuk tidak menggunakan sistem dalam situasi tertentu atau untuk mengabaikan, mengesampingkan, atau membalikkan hasilnya
- Intervensi dalam sistem menggunakan tombol berhenti
- Sistem pengenalan biometrik jarak jauh sesuai dengan Lampiran III no. 1 huruf a UU AI tidak boleh dirancang sedemikian rupa sehingga hanya sistem yang membuat keputusan mengenai identifikasi, tetapi selalu melibatkan manusia yang memiliki kompetensi, pelatihan, dan otorisasi yang diperlukan untuk memeriksa identifikasi secara terpisah dan mengambil keputusan atasnya.

Akurasi, Ketahanan, dan Keamanan Siber

Pengembangan dan desain sistem sesuai dengan Pasal 15 UU AI dilakukan sedemikian rupa sehingga tingkat akurasi, ketahanan, dan keamanan siber yang sesuai terjamin dan dapat dipertahankan sepanjang masa pakai sistem. Angka-angka kunci akurasi harus ditentukan dalam petunjuk penggunaan sistem yang terlampir.

Mengenai ketahanan sistem, UU AI mensyaratkan bahwa sistem tersebut sekuat mungkin terhadap kesalahan, malfungsi, atau inkonsistensi. Untuk tujuan ini, langkah-langkah teknis dan organisasi yang diperlukan harus diambil untuk melindungi sistem. Ketahanan dapat dicapai melalui **redundansi teknis**, misalnya melalui rencana keamanan atau rencana keamanan kesalahan. Sistem yang "belajar" setelah dipasarkan/dioperasikan harus dikembangkan sedemikian rupa sehingga risiko hasil yang terdistorsi yang memengaruhi proses di masa mendatang ("lingkaran umpan balik") diminimalkan dan langkah-langkah mitigasi risiko diambil.

Sistem AI berisiko tinggi harus **tahan** terhadap upaya pihak ketiga untuk mengubah penggunaan, hasil, atau kinerjanya dengan mengeksploitasi kerentanan. Langkah-langkah keamanan siber yang diambil harus sesuai dengan kasus individual dan risiko sistem. Secara khusus, tujuannya adalah untuk mencegah:

- **Peracunan data:** Manipulasi kumpulan data pelatihan
- **Peracunan model:** Manipulasi komponen pra-terlatih yang digunakan selama pelatihan
- **Penghindaran model/Contoh adversarial:** Penggunaan data masukan yang dimaksudkan untuk mendorong model melakukan kesalahan

- Deteksi dan pencegahan serangan terhadap data rahasia atau cacat model

Kewajiban Penyedia, Penyebar, dan Pihak Lain yang terlibat

Tabel 3.3 Penyedia

Pasal	Kewajiban/Persyaratan
Pasal 6 dan seterusnya. Undang-Undang AI	Memenuhi persyaratan, khususnya: ▪ Pertimbangan terhadap kondisi terkini ▪ Persyaratan produk (lihat Lampiran I Bagian A) ▪ Sistem manajemen risiko ▪ Tata Kelola Data ▪ Dokumentasi (Teknis) ▪ Pencatatan dan pencatatan log
Pasal 16 huruf a Undang-Undang AI	Nama/nama dagang/merek dagang terdaftar dan alamat kontak pada sistem AI berisiko tinggi (jika tidak memungkinkan, pada kemasan/dokumentasi)
Pasal 17 Undang-Undang AI	Sistem manajemen mutu Dokumentasi tertulis yang memuat setidaknya poin-poin berikut: ▪ Konsep untuk kepatuhan terhadap UU AI dan peraturan lainnya (lihat Lampiran I dan III UU AI) ▪ Prosedur penilaian kesesuaian, manajemen perubahan ▪ Desain, pengendalian desain, tinjauan desain sistem ▪ Pengembangan, pengendalian mutu, jaminan mutu ▪ Prosedur pemeriksaan, pengujian, dan validasi ▪ Implementasi sebelum, selama, dan setelah pengembangan sistem, dokumentasi frekuensi pelaksanaan ▪ Spesifikasi dan standar teknis yang berlaku ▪ Manajemen data ▪ Pengumpulan, akuisisi, analisis, pelabelan, penyimpanan, penyaringan, evaluasi, agregasi, retensi data, dan lainnya. ▪ Sistem manajemen risiko sesuai dengan Pasal 9 UU AI ▪ Sistem pemantauan sesuai dengan Pasal 72 UU AI ▪ Prosedur pelaporan insiden serius sesuai dengan Pasal 72 UU AI. 73 UU AI ▪ Komunikasi dengan pihak berwenang yang relevan ▪ Sistem dan prosedur untuk mencatat semua dokumentasi dan informasi yang relevan ▪ Manajemen sumber daya, keamanan pasokan ▪ Kerangka akuntabilitas yang mengatur tanggung jawab manajemen dan staf lainnya terkait dengan manajemen mutu (misalnya matriks RACI) Sistem manajemen mutu dapat didasarkan pada ukuran organisasi penyedia, tetapi perlu dicatat bahwa tingkat ketelitian dan tingkat perlindungan sistem harus diperhitungkan. Sistem manajemen mutu sesuai dengan UU AI dapat diintegrasikan ke dalam sistem manajemen mutu untuk peraturan perundang-undangan khusus

	sektor lainnya (lihat khususnya Lampiran 1 UU AI). Oleh karena itu, tidak perlu mempertahankan sistem manajemen mutu "ganda" atau kedua untuk kepatuhan terhadap UU AI; sistem tersebut dapat digabungkan atau diperluas.
Pasal 18 Undang-Undang AI	Penyimpanan dokumentasi: ▪ Dokumentasi teknis sesuai dengan Pasal 11 UU AI ▪ Dokumentasi sistem manajemen mutu sesuai dengan Pasal 17 UU AI ▪ Dokumentasi tentang perubahan yang disetujui oleh badan yang berwenang ▪ Keputusan dan dokumen lain dari badan yang berwenang ▪ Deklarasi Kesesuaian UE sesuai dengan Pasal 47 UU AI Dokumen-dokumen tersebut harus disimpan setidaknya selama sepuluh tahun sejak tanggal dipasarkan/digunakan.
Seni. 19 UU AI, Pasal. 12 UU AI	Catatan sesuai dengan Pasal 12 UU AI Jangka waktu penyimpanan minimum adalah enam bulan, kecuali ketentuan hukum lain yang berlaku bagi penyedia menetapkan jangka waktu yang berbeda.
Seni. 43 UU AI	Prosedur penilaian kesesuaian untuk penempatan di pasar/pengoperasian
Seni. 47 UU AI	Penerbitan Deklarasi Kesesuaian Uni Eropa
Seni. 48 UU AI	Pemasangan tanda CE pada sistem/kemasan/dokumentasi
Seni. 49 ayat. 1 UU AI	Pemenuhan kewajiban pendaftaran
Seni. 20 UU AI, Pasal. 79 UU AI	Mengambil tindakan korektif Memberikan informasi yang diperlukan Jika penyedia memiliki alasan untuk percaya bahwa sistemnya tidak (atau tidak lagi) sesuai dengan UU AI, mereka harus memulihkan kepatuhan (misalnya, menginstal pembaruan) atau dapat menarik, menonaktifkan, atau menarik kembali sistem tersebut. Mereka juga harus memberi tahu distributor atau, jika berlaku, penyebar, perwakilan resmi, atau importir. Jika penyedia mengetahui bahwa sistemnya menimbulkan risiko (lihat Pasal 79 UU AI), mereka harus melakukan penyelidikan terhadap penyebabnya – jika perlu bersama dengan penyebar yang memberi tahu – dan memberi tahu otoritas yang berwenang dan, jika berlaku, badan yang diberi tahu yang menerbitkan sertifikat sesuai dengan Pasal 44 UU AI tentang sifat ketidakpatuhan dan tindakan yang telah diambil.
Seni. 21 UU AI	Bukti kepatuhan terhadap persyaratan Pasal 6 dan seterusnya UU AI, kerja sama dengan otoritas yang berwenang (jika ada penyelidikan) ▪ Penyampaian semua informasi dan dokumentasi yang diperlukan untuk menunjukkan kepatuhan terhadap sistem AI berisiko tinggi: ▪ Bahasa yang mudah dipahami ▪ Bahasa resmi Negara Anggota yang bersangkutan ▪ Akses ke log yang dihasilkan secara otomatis (atas permintaan)

Arahan (UE) 2016/2102 dan (UE) Memastikan **persyaratan aksesibilitas** terpenuhi
2019/882

Tabel 3.4 Perwakilan Resmi Penyedia Sistem AI Berisiko Tinggi

Artikel	Wajib
Seni. 22 ayat. 1, 2, 3 UU AI	Penyedia dengan cabang di negara ketiga/negara non-UE ▪ Penunjukan tertulis perwakilan resmi yang berkedudukan di UE ▪ Pemberian tugas ▪ Memungkinkan pelaksanaan tugas oleh perwakilan resmi ▪ Otorisasi perwakilan resmi untuk bertindak sebagai orang kontak bagi otoritas yang berwenang selain atau sebagai pengganti penyedia ▪ Pengakhiran kontrak jika penyedia memiliki alasan untuk percaya bahwa perwakilan resmi tidak memenuhi tugasnya (pemberitahuan kepada otoritas pengawasan pasar dan/atau badan yang diberi wewenang)
Seni. 22 ayat. 3 UU AI	Tugas-tugas perwakilan resmi ▪ Penyediaan tugas ▪ Bahasa resmi Negara Anggota ▪ Memeriksa apakah Deklarasi Kesesuaian UE dan dokumentasi teknis telah disusun sesuai dengan Pasal 11 ▪ Memastikan pelaksanaan prosedur penilaian kesesuaian
Seni. 22 ayat. 3 UU AI	Dokumen yang harus disiapkan oleh perwakilan resmi ▪ Penyimpanan detail kontak penyedia (setidaknya selama sepuluh tahun) ▪ Salinan Deklarasi Kesesuaian UE ▪ Dokumentasi teknis ▪ Sertifikat apa pun yang dikeluarkan oleh badan yang diberi wewenang ▪ Pengiriman dokumen-dokumen tersebut kepada otoritas yang berwenang (atas permintaan) ▪ Akses ke log otomatis sesuai dengan Pasal 12 UU AI (atas permintaan) ▪ Kerja sama dengan otoritas yang berwenang (atas permintaan) ▪ Memastikan kepatuhan terhadap kewajiban pendaftaran sesuai dengan Pasal 49 UU AI ▪ Memastikan keakuratan informasi yang tercantum dalam Lampiran VIII A UU AI

Tabel 3.5 Importir

Artikel	Wajib
Seni. 23 ayat. 1 UU AI	Pastikan sistem AI mematuhi Peraturan AI dengan memeriksa dokumen-dokumen berikut: ▪ Melakukan penilaian kesesuaian sesuai dengan Pasal 43 UU AI oleh penyedia ▪ Menyiapkan dokumentasi teknis sesuai dengan Pasal 11 UU AI dan Lampiran IV UU AI oleh penyedia ▪ Keberadaan tanda CE, Deklarasi Kesesuaian UE, dan petunjuk penggunaan ▪ Penunjukan perwakilan resmi sesuai dengan Pasal 22 ayat 1 UU AI
Seni. 23 ayat. 2 UU AI	Apabila terdapat dugaan ketidakpatuhan terhadap Regulasi AI, dugaan pemalsuan sistem AI, atau pemalsuan dokumentasi: ▪ Pemasaran hanya dilakukan setelah kesesuaian dipastikan ▪ Dalam kasus sistem AI berisiko tinggi (lihat Pasal 79 UU AI), importir wajib memberitahukan ▪ penyedia, ▪ perwakilan resmi, dan ▪ otoritas pengawasan pasar.
Seni. 23 ayat. 3 UU AI	Pengungkapan informasi berikut pada kemasan atau, jika berlaku, pada dokumentasi yang menyertainya: ▪ Nama ▪ Nama dagang terdaftar ▪ Merek dagang terdaftar ▪ Alamat tempat importir dapat dihubungi terkait dengan sistem
Seni. 23 ayat. 4 UU AI	Memastikan kondisi penyimpanan atau transportasi yang diperlukan (jika berlaku)
Seni. 23 ayat. 5 UU AI	Dokumen-dokumen berikut harus disimpan selama sepuluh tahun sejak dipasarkan atau dioperasikan: ▪ Salinan sertifikat dari badan yang berwenang ▪ Petunjuk penggunaan, jika berlaku ▪ Penilaian kesesuaian UE
Pasal 23 ayat 6 dan 7 UU AI	Kerja sama dengan otoritas yang berwenang (atas permintaannya): ▪ Pengiriman dokumen yang tersedia (Pasal 23 ayat 5 UU AI) ▪ Informasi dan dokumentasi yang diperlukan untuk menunjukkan kepatuhan sistem AI berisiko tinggi dalam bahasa yang mudah dipahami

	▪ Memastikan bahwa dokumentasi teknis dapat tersedia bagi otoritas ▪ Mengembangkan dan berkolaborasi dalam langkah-langkah untuk mengurangi atau memitigasi risiko yang ditimbulkan oleh sistem

Tabel 3.6 Distributor

Artikel	Wajib
Seni. 24 ayat. 1 UU AI	Sebelum dipasarkan: ▪ Pastikan sistem tersebut dilengkapi dengan tanda CE yang diperlukan. ▪ Salinan Deklarasi Kesesuaian UE terlampir. ▪ Petunjuk penggunaan terlampir. ▪ Pemenuhan kewajiban penyedia: ▪ Pengungkapan informasi berikut pada kemasan atau, jika berlaku, pada dokumentasi terlampir: – Nama – Nama dagang terdaftar – Merek dagang terdaftar – Alamat kontak ▪ Sistem manajemen mutu (lihat Pasal 17 UU AI) ▪ Pemenuhan kewajiban importir berikut: ▪ Pengungkapan informasi berikut pada kemasan atau, jika berlaku, pada dokumentasi terlampir: – Nama – Nama dagang terdaftar – Merek dagang terdaftar – Alamat tempat importir dapat dihubungi terkait dengan sistem
Seni. 24 ayat. 2 dan para. 4 UU AI	Jika dicurigai adanya ketidakpatuhan terhadap Peraturan AI berdasarkan informasi yang tersedia bagi pengecer: ▪ Pemasaran hanya dilakukan setelah kesesuaian telah ditetapkan ▪ Dalam kasus sistem AI berisiko tinggi (lihat Pasal 79 UU AI), importir wajib memberi tahu: ▪ penyedia, ▪ perwakilan resmi, dan ▪ otoritas pengawasan pasar ▪ Melakukan tindakan korektif yang diperlukan untuk mencapai kepatuhan ▪ Penarikan atau pengembalian sistem ▪ Memastikan bahwa pemasok, importir, atau pihak lain melakukan tindakan korektif yang diperlukan

	▪ Dalam kasus sistem AI berisiko tinggi (lihat Pasal 79 UU AI), pengecer wajib memberi tahu: ▪ penyedia, ▪ importir, ▪ otoritas yang berwenang di Negara Anggota tempat sistem tersebut tersedia
Seni. 24 ayat. 3 UU AI	Memastikan kondisi penyimpanan atau transportasi yang diperlukan (jika berlaku)
Seni. 24 ayat. 5 dan 6 UU AI	Kerja sama dengan otoritas yang berwenang (atas permintaan): ▪ Penyampaian semua informasi dan dokumentasi yang berkaitan dengan kewajiban di atas ▪ Bukti kesesuaian sistem AI ▪ Mengembangkan dan berkolaborasi dalam langkah-langkah untuk mengurangi atau memitigasi risiko yang ditimbulkan oleh sistem

Tabel 3.7 Tanggung Jawab di Sepanjang Rantai Nilai AI

Artikel	Wajib
Seni. 25 ayat. 1 dan para. 2 UU AI	Distributor, importir, penyebar, atau pihak ketiga lainnya menjadi penyedia sistem AI berisiko tinggi dalam kasus-kasus berikut dan oleh karena itu harus memenuhi kewajiban penyedia berdasarkan Pasal 16 UU AI: ▪ Sistem yang dipasarkan atau dioperasikan disediakan dengan nama/merek dagangnya sendiri (terlepas dari perjanjian kontraktual apa pun). ▪ Perubahan signifikan pada sistem AI (hanya jika masih merupakan sistem AI berisiko tinggi sesuai dengan Pasal 6 dan seterusnya.) ▪ Modifikasi sistem AI yang awalnya bukan berisiko tinggi atau sistem AI untuk tujuan umum sehingga diklasifikasikan sebagai sistem AI berisiko tinggi sesuai dengan Pasal 6 dan seterusnya. UU AI Klasifikasi ulang berarti bahwa penyedia asli tidak lagi dianggap sebagai penyedia. Penyedia awal wajib bekerja sama dengan penyedia baru dan memberikan semua informasi yang dibutuhkan untuk menetapkan kepatuhan, kecuali jika dapat membuktikan bahwa telah secara jelas menentukan bahwa sistem AI-nya tidak dapat diubah menjadi sistem AI berisiko tinggi dan oleh karena itu tidak wajib menyerahkan dokumentasi. Hak kekayaan intelektual, informasi bisnis rahasia, dan rahasia dagang harus dilindungi.

Seni. 25 ayat. 3 UU AI	Untuk komponen keselamatan sistem berisiko tinggi (lihat Lampiran 1 Bagian A UU AI), produsen produk dianggap sebagai penyedia sistem AI berisiko tinggi dan harus mematuhi kewajiban penyedia untuk: ▪ Memasarkan sistem bersama dengan produk dengan nama atau merek dagang produsen produk ▪ Mengoperasikan sistem bersama dengan produk dengan nama atau merek dagang produsen produk setelah produk dipasarkan Hak kekayaan intelektual, informasi bisnis rahasia, dan rahasia dagang harus dilindungi.
Seni. 23 para.4 UU AI	Perjanjian antara ▪ penyedia sistem AI berisiko tinggi dan ▪ pihak ketiga yang menyediakan sistem AI, alat, layanan, komponen, atau prosedur, yang digunakan atau diintegrasikan dalam sistem AI berisiko tinggi. Konten yang diperlukan agar penyedia sistem AI berisiko tinggi dapat memenuhi kewajibannya: ▪ Informasi tentang ▪ Keterampilan ▪ Akses teknis ▪ Dukungan ▪ Kondisi terkini yang diakui Tidak berlaku untuk alat, layanan, proses, atau komponen yang tidak tersedia untuk umum sebagai model AI tujuan umum di bawah lisensi sumber terbuka.

Tabel 3.8 Kewajiban Pengembang Sistem AI Berisiko Tinggi

Artikel	Wajib
Seni. 26 ayat. 1, para. 3, para. 6, para. 12 UU AI	Pengamanan: ▪ Langkah-langkah teknis dan organisasi yang tepat untuk memastikan bahwa sistem hanya digunakan sesuai dengan petunjuk penggunaan yang terlampir dan sesuai dengan paragraf 3 dan 6 ▪ Kewajiban lain dari pengembang berdasarkan hukum Uni Eropa atau nasional tetap tidak terpengaruh (lihat paragraf 3). ▪ Penyimpanan log yang dihasilkan secara otomatis untuk jangka waktu yang sesuai (bervariasi tergantung pada tujuan sistem, tetapi setidaknya enam bulan; lihat paragraf 6) ▪ Kerja sama dengan otoritas yang berwenang terkait implementasi Peraturan AI
Seni. 26 ayat. 2 UU AI	Pengawasan manusia:

	▪ Penggunaan orang-orang yang kompeten yang memiliki pelatihan dan otorisasi yang diperlukan ▪ Dukungan untuk orang-orang tersebut
Seni. 26 ayat. 4 UU AI	Penggunaan data masukan yang representatif Menjaga tujuan yang dimaksudkan dari sistem AI
Seni. 26 ayat. 5 UU AI	Memantau pengoperasian sistem AI berisiko tinggi: ▪ Patuhi petunjuk penggunaan ▪ Jika diperlukan, informasi penyedia sesuai dengan Pasal 72 UU ▪ Jika dicurigai adanya AI berisiko tinggi (lihat Pasal 79 UU AI), segera beri tahu pemasok atau distributor dan otoritas pengawasan pasar yang berwenang, termasuk penangguhan penggunaan ▪ Beri tahu pemasok, importir atau distributor dan otoritas pengawasan pasar yang berwenang jika terjadi insiden serius
Seni. 26 ayat. 7 UU AI	Penggunaan sistem AI berisiko tinggi di tempat kerja: ▪ Informasi untuk perwakilan karyawan ▪ Informasi untuk karyawan yang terdampak Hukum ketenagakerjaan nasional harus dipatuhi dan, jika perlu, perjanjian perusahaan harus dibuat.
Seni. 26 ayat. 8 UU AI	Kepatuhan terhadap kewajiban pendaftaran sesuai dengan Pasal 49 UU AI Periksa apakah sistem berisiko tinggi telah terdaftar dalam basis data Uni Eropa sesuai dengan Pasal 71 UU AI (jika belum, sistem tersebut tidak boleh digunakan dan penyedia atau pengecer harus diberitahu)
Seni. 26 ayat. 9 UU AI	Melakukan penilaian dampak perlindungan data sesuai dengan GDPR atau Arahan Perlindungan Data.
Seni. 26 ayat. 10 UU AI	Pihak yang menerapkan sistem AI berisiko tinggi untuk identifikasi biometrik jarak jauh selanjutnya: ▪ Meminta otorisasi atau penggunaan segera atau dalam waktu 48 jam kepada otoritas peradilan atau administratif yang berwenang, kecuali jika itu adalah identifikasi pertama dari calon tersangka berdasarkan fakta objektif dan terverifikasi yang terkait langsung dengan kejahatan. ▪ Pembatasan sebatas yang diperlukan. ▪ Jika permohonan ditolak, penggunaan dan penghapusan data pribadi yang telah dikumpulkan akan segera dihentikan. ▪ Tidak ada penggunaan sistem secara tidak terarah dan tidak terkait dengan tindak pidana, proses pidana, atau risiko tindak pidana yang ada atau

	aktual dan dapat diperkirakan, atau untuk pencarian orang hilang tertentu. ▪ Pasal 9 GDPR atau Pasal 10 GDPR atau Arahan Perlindungan Data harus dipatuhi. ▪ Dokumentasi penggunaan sistem dalam berkas kepolisian yang relevan ▪ Memberikan dokumentasi penggunaan kepada otoritas pengawasan pasar yang berwenang atau otoritas perlindungan data yang berwenang atas permintaan (kecuali untuk pengungkapan data operasional sensitif yang berkaitan dengan penegakan hukum) ▪ Laporan tahunan kepada otoritas pengawasan pasar dan otoritas perlindungan data yang berwenang (kecuali untuk pengungkapan data operasional sensitif yang berkaitan dengan penegakan hukum) ▪ Kepatuhan terhadap peraturan perundang-undangan nasional yang lebih ketat
Pasal 26 ayat 11 UU AI	Informasi kepada individu yang bersangkutan bahwa sistem AI telah membuat keputusan tentang mereka atau telah membantu sistem AI dalam membuat keputusan.

3.5 PENILAIAN DAMPAK HAK FUNDAMENTAL

Hak-hak fundamental, yang merupakan prinsip-prinsip mendasar yang menjadi landasan masyarakat demokratis, semakin berada di bawah tekanan. Perlindungan data, kebebasan berekspresi, kesetaraan, dan hak atas privasi hanyalah beberapa bidang di mana AI berpotensi memberikan dampak negatif. Dualitas AI sebagai alat untuk kemajuan dan sebagai ancaman potensial terhadap kebebasan individu menimbulkan pertanyaan kompleks bagi para legislator, pengembang, dan masyarakat, dan sampai batas tertentu, mencerminkan kebutuhan akan Undang-Undang AI: tujuannya adalah untuk mencapai keseimbangan antara kemajuan teknologi dan perlindungan hak-hak fundamental.

Sulit untuk menyebutkan hak fundamental yang berpotensi tidak terpengaruh dan mungkin dilanggar oleh AI. Peran teknologi dalam sistem pengawasan modern, risiko diskriminasi melalui pengambilan keputusan algoritmik, dan tantangan perlindungan data yang ditimbulkan oleh pengumpulan dan analisis sejumlah besar data merupakan hal yang sentral.

Undang-Undang AI dan Hak-Hak Fundamental

Untuk memastikan perlindungan hak-hak fundamental, Undang-Undang AI mengklarifikasi kepatuhan terhadap Piagam Hak-Hak Fundamental Uni Eropa (Piagam atau CFR) bahwa pengembangan, penerapan, dan penggunaan sistem AI di Uni Eropa sejalan dengan hak dan kebebasan fundamental dalam Piagam tersebut.

Relevansi perlindungan hak-hak fundamental dalam pengembangan dan penggunaan AI dapat disimpulkan dari **Pasal 1 ayat 1 Undang-Undang AI**, yang mendefinisikan tujuan regulasi:

*“... meningkatkan fungsi pasar internal dan mendorong adopsi kecerdasan buatan (AI) yang berpusat pada manusia dan dapat dipercaya, sambil memastikan tingkat perlindungan yang tinggi terhadap kesehatan, keselamatan, **hak-hak fundamental yang diabadikan dalam Piagam**, termasuk demokrasi, supremasi hukum, dan perlindungan lingkungan, terhadap dampak buruk sistem AI di Uni Eropa dan mendukung inovasi.”*

Hak-Hak Fundamental yang Terpengaruh oleh Piagam

Sebagian besar, jika tidak semua, Piagam Hak-Hak Fundamental Uni Eropa berpotensi terpengaruh oleh penerapan atau dampak AI, karena sistem AI semakin terintegrasi ke dalam berbagai aspek kehidupan sosial, ekonomi, dan pribadi. Cara sistem AI dirancang, dikembangkan, dan diterapkan secara langsung atau tidak langsung memengaruhi berbagai hak dan kebebasan. Dengan demikian, Pasal 48 Undang-Undang AI menyatakan bahwa *“sejauh mana dampak buruk yang disebabkan oleh sistem AI terhadap hak-hak fundamental yang dilindungi oleh Piagam sangat relevan ketika mengklasifikasikan sistem AI sebagai berisiko tinggi.”* Lebih lanjut, Pasal 48 UU AI juga mencantumkan hak-hak Piagam yang terpengaruh oleh sistem AI: *“hak atas martabat manusia, penghormatan terhadap kehidupan pribadi dan keluarga, perlindungan data pribadi, kebebasan berekspresi dan informasi, kebebasan berkumpul dan berasosiasi, hak untuk tidak diskriminasi, hak atas pendidikan, perlindungan konsumen, hak-hak pekerja, hak-hak penyandang disabilitas, kesetaraan gender, hak kekayaan intelektual, hak atas upaya hukum yang efektif dan pengadilan yang adil, hak untuk membela diri dan praduga tidak bersalah, dan hak atas pemerintahan yang baik”*. Pertimbangan kerentanan anak-anak ditekankan, dan penyebutan eksplisit hak fundamental *“atas tingkat perlindungan lingkungan yang tinggi yang diabadikan dalam Piagam dan diimplementasikan dalam kebijakan Uni Eropa juga harus dipertimbangkan ketika menilai tingkat keparahan kerusakan yang dapat ditimbulkan oleh sistem AI, termasuk dalam kaitannya dengan kesehatan dan keselamatan manusia”* patut diperhatikan.

Berikut beberapa contoh hak fundamental yang diabadikan dalam Piagam yang mungkin terpengaruh oleh AI dan bagaimana pelanggaran ini dapat terjadi:

- **Pasal 1 – Martabat manusia**

Sistem AI yang membuat keputusan yang memengaruhi aspek fundamental kehidupan manusia dapat membahayakan martabat manusia, terutama jika tidak transparan atau tidak menghormati martabat dan otonomi yang melekat pada individu.

- **Pasal 3 – Hak atas integritas**

Aplikasi AI, misalnya di bidang medis, dapat memengaruhi hak atas integritas fisik dan mental, misalnya melalui keputusan tentang metode pengobatan.

- **Pasal 8 – Perlindungan data pribadi**

Sistem AI yang memproses sejumlah besar data pribadi secara langsung memengaruhi hak atas perlindungan data terkait pengumpulan, penyimpanan, pemrosesan, dan pengungkapan data ini.

- **Pasal 21 – Non-diskriminasi**

Sistem AI dapat memperkuat ketidaksetaraan sosial dan ekonomi jika menggunakan data yang bias, yang dapat menyebabkan keputusan diskriminatif di bidang-bidang seperti perekrutan, pemberian pinjaman, atau penegakan hukum.

- **Pasal 23 – Kesetaraan antara perempuan dan laki-laki**

AI dapat secara tidak sengaja memperkuat bias gender jika didasarkan pada data pelatihan yang tidak setara, yang dapat memengaruhi kesetaraan gender.

- **Pasal 14 dan Pasal 11 – Hak atas pendidikan dan akses informasi**

AI dapat merevolusi akses ke pendidikan dan informasi melalui sistem pembelajaran personalisasi atau informasi yang efisien. penyaringan, tetapi juga menimbulkan risiko dalam hal akses ke lembaga pendidikan.

- **Pasal 13 – Kebebasan seni dan ilmu pengetahuan**

AI menimbulkan pertanyaan tentang hak cipta dan kebebasan kreatif, terutama ketika menghasilkan karya seni atau konten ilmiah, yang menyebabkan perdebatan tentang pengakuan dan perlindungan karya-karya tersebut.

- **Pasal 47 – Hak atas upaya hukum yang efektif dan pengadilan yang adil**

Penggunaan AI dalam sistem peradilan dan dalam proses pengambilan keputusan dapat meningkatkan efisiensi dan akurasi, tetapi juga dapat mengurangi transparansi dan akuntabilitas jika dasar keputusan AI tidak dapat dipahami.

Undang-Undang AI Memperluas Cakupan Piagam ke Sektor Swasta

Undang-Undang AI terutama merujuk pada Piagam sebagai titik acuan utama untuk perlindungan hak-hak fundamental, oleh karena itu diskusi ini juga berfokus pada hak-hak fundamental yang tercantum dalam Piagam.

Hak-hak fundamental terutama ditujukan kepada negara dan organ-organnya dan dipahami sebagai hak warga negara untuk membela diri terhadap campur tangan negara. Hak-hak tersebut menetapkan tindakan apa yang harus dihindari oleh negara atau bagaimana negara harus bertindak untuk melindungi hak-hak tertentu. Hak-hak tersebut mewajibkan negara untuk menghormati dan melindungi kebebasan dan hak-hak individu.

Meskipun hak-hak fundamental terutama dipahami sebagai hak-hak defensif terhadap campur tangan negara, efek pihak ketiga mengakui bahwa nilai-nilai dan prinsip-prinsip yang terkandung dalam hak-hak fundamental juga dapat relevan dalam hubungan hukum perdata. Hal ini terjadi di satu sisi melalui pemberlakuan undang-undang sederhana, misalnya dalam hukum ketenagakerjaan, dan di sisi lain melalui pengaruh hak-hak fundamental pada seluruh sistem hukum.

Piagam menetapkan hak-hak fundamental yang harus dihormati di Uni Eropa. Memang benar bahwa Piagam tersebut terutama mengikat lembaga, badan, kantor, dan badan Uni Eropa. Namun, Piagam tersebut juga berlaku untuk Negara Anggota, tetapi hanya jika mereka menerapkan hukum Uni Eropa. Ini termasuk situasi di mana otoritas atau pengadilan nasional menerapkan hukum Uni Eropa atau di mana hukum nasional didasarkan pada hukum Uni Eropa.

Undang-Undang AI secara tidak langsung memperluas cakupan hak-hak fundamental yang dilindungi oleh Piagam ke sektor swasta dengan menetapkan persyaratan dan larangan tertentu untuk pengembangan, penerapan, dan penggunaan sistem AI yang berlaku untuk operator publik dan swasta. Persyaratan hukum ini memastikan bahwa operator swasta harus mematuhi hak-hak fundamental ketika menerapkan teknologi AI di bidang-bidang tertentu, bahkan jika mereka awalnya tidak terikat langsung oleh Piagam tersebut.

Implementasi Penilaian Dampak Hak-Hak Fundamental

Teknologi bukanlah tujuan akhir. Tujuannya hanya untuk memberi manfaat bagi kita manusia dan planet kita. Oleh karena itu, pendekatan yang berpusat pada manusia adalah dasar kepercayaan pada AI dan dengan demikian Regulasi AI. Penerapan penilaian dampak hak-hak fundamental (FRIA) merupakan instrumen yang tepat untuk memastikan bahwa manusia ditempatkan sebagai pusat pembangunan teknologi, dari tahap konsepsi hingga operasional berkelanjutan. Komponen inti dari kerangka kerja ini adalah mengidentifikasi risiko potensi ancaman atau pelanggaran hak-hak fundamental dan hak asasi manusia sebelum pembangunan dan mengambil tindakan penanggulangan yang sesuai.

Untuk waktu yang lama, sektor swasta praktis mengabaikan implementasi penilaian dampak hak asasi manusia. Namun, pengenalan penilaian dampak hak asasi manusia dalam Undang-Undang AI menandai titik balik dengan menjadikan penilaian ini untuk area aplikasi tertentu sebagai bagian yang tak terpisahkan dari pengembangan dan pengenalan sistem AI berisiko tinggi khususnya. Persyaratan hukum ini memaksa perusahaan untuk mengatasi dampak mendalam teknologi mereka terhadap hak asasi manusia dan hak asasi manusia dan untuk mempertimbangkan bagaimana risiko ini dapat diatasi.

Pasal 27 ayat 1 Undang-Undang AI:

“Sebelum menerapkan sistem AI berisiko tinggi yang dimaksud dalam Pasal 6 ayat (2), kecuali sistem AI berisiko tinggi yang dimaksudkan untuk digunakan di area yang tercantum dalam poin 2 Lampiran III, pihak yang menerapkan sistem tersebut adalah badan yang diatur oleh hukum publik, atau entitas swasta yang menyediakan layanan publik, dan pihak yang menerapkan sistem AI berisiko tinggi yang dimaksud dalam poin 5 (b) dan (c) Lampiran III, wajib melakukan penilaian dampak terhadap hak asasi manusia yang mungkin ditimbulkan oleh penggunaan sistem tersebut.”

Dengan demikian, Pasal 27 ayat 1 Undang-Undang AI menetapkan bahwa Pasal 27 UU AI menetapkan persyaratan khusus untuk melakukan penilaian dampak hak asasi manusia terhadap penggunaan sistem AI berisiko tinggi sebelum dioperasikan. Ketentuan ini bertujuan untuk menilai dampak penggunaan sistem tersebut terhadap hak asasi manusia yang tercantum dalam Piagam dan untuk memastikan bahwa tindakan yang tepat diambil untuk melindungi hak-hak tersebut. Seperti yang dijelaskan di atas, kewajiban untuk melakukan penilaian dampak hak asasi manusia berlaku baik untuk pengembang yang merupakan entitas publik atau entitas swasta yang menyediakan layanan publik maupun untuk pengembang sistem AI berisiko tinggi di bidang-bidang tertentu yang tercantum dalam Lampiran III UU.

Menurut Pasal 27 UU AI, Berdasarkan Pasal 27 UU AI dan Pertimbangan 93 UU AI, tanggung jawab untuk melaksanakan penilaian dampak hak asasi manusia terutama terletak

pada pihak yang menerapkan sistem AI berisiko tinggi, karena mereka mengetahui kasus penggunaan spesifik sistem AI tersebut:

“Meskipun risiko yang terkait dengan sistem AI dapat timbul dari cara sistem tersebut dirancang, risiko juga dapat berasal dari cara sistem AI tersebut digunakan. Oleh karena itu, pihak yang menerapkan sistem AI berisiko tinggi memainkan peran penting dalam memastikan bahwa hak asasi manusia dilindungi, melengkapi kewajiban penyedia saat mengembangkan sistem AI. Pihak yang menerapkan berada pada posisi terbaik untuk memahami bagaimana sistem AI berisiko tinggi akan digunakan secara konkret dan oleh karena itu dapat mengidentifikasi potensi risiko signifikan yang tidak diperkirakan pada fase pengembangan, karena pengetahuan yang lebih tepat tentang konteks penggunaan, orang atau kelompok orang yang kemungkinan akan terpengaruh, termasuk kelompok rentan ...”

Hal ini sesuai dengan Pasal 27 UU AI. 27 Undang-Undang AI yang menyatakan bahwa hanya pihak-pihak tertentu yang menerapkan sistem AI berisiko tinggi yang wajib melakukan penilaian dampak hak asasi manusia sebelum melakukan pengoperasian:

1. Lembaga-lembaga di bawah hukum publik
2. Lembaga-lembaga swasta yang menyediakan layanan publik, misalnya pendidikan, perawatan kesehatan, layanan sosial, perumahan, dan administrasi peradilan
3. Pihak-pihak yang menerapkan sistem AI untuk penilaian kredit dan pemberian skor kredit kepada individu, misalnya bank (Lampiran III no. 5 huruf b)
4. Pengimplementasikan sistem AI untuk penilaian risiko dan penetapan harga asuransi kesehatan dan jiwa, misalnya perusahaan asuransi (Lampiran III no. 5 huruf b)

Area infrastruktur kritis secara eksplisit dikecualikan dari kewajiban untuk melakukan penilaian dampak hak-hak fundamental (Lampiran III no. 2). Pertimbangan 96 UU AI menjelaskan mengapa lembaga swasta yang menyediakan layanan publik juga tunduk pada kewajiban tersebut: *“Layanan penting bagi individu yang bersifat publik juga dapat disediakan oleh entitas swasta. Entitas swasta yang menyediakan layanan publik tersebut terkait dengan tugas-tugas untuk kepentingan publik seperti di bidang pendidikan, perawatan kesehatan, layanan sosial, perumahan, administrasi peradilan.”*

Penilaian dampak hak-hak fundamental bertujuan untuk mengidentifikasi *“risiko spesifik terhadap hak-hak individu atau kelompok individu yang kemungkinan akan terpengaruh”* sebelum penggunaan awal dan perubahan yang relevan pada sistem dan untuk menentukan terlebih dahulu langkah-langkah yang harus diambil jika risiko tersebut benar-benar terjadi. Penilaian dampak harus *“mengidentifikasi proses relevan dari pihak yang menerapkan sistem AI berisiko tinggi di mana sistem tersebut akan digunakan sesuai dengan tujuan yang dimaksudkan, dan harus mencakup deskripsi tentang jangka waktu dan frekuensi penggunaan sistem tersebut serta kategori spesifik orang dan kelompok yang kemungkinan akan terpengaruh dalam konteks penggunaan tertentu”* (Pasal 96 UU AI).

Pasal 27 ayat 1 UU AI juga menetapkan kerangka kerja yang harus diikuti oleh pihak yang menerapkan sistem untuk penilaian dampak hak-hak fundamental:

- a) **deskripsi tentang proses** pihak yang menerapkan sistem AI berisiko tinggi di mana sistem tersebut akan digunakan sesuai dengan tujuan yang dimaksudkan;

- b) *deskripsi tentang **jangka waktu** dan frekuensi penggunaan setiap sistem AI berisiko tinggi;*
- c) ***kategori orang dan kelompok** yang kemungkinan akan terpengaruh oleh penggunaannya dalam konteks tertentu;*
- d) *risiko bahaya **spesifik yang mungkin** berdampak pada kategori orang perseorangan atau kelompok orang yang diidentifikasi sesuai dengan poin (c) paragraf ini, dengan mempertimbangkan informasi yang diberikan oleh penyedia sesuai dengan Pasal 13;*
- e) *deskripsi implementasi langkah-langkah **pengawasan manusia**, sesuai dengan petunjuk penggunaan;*
- f) *langkah-langkah yang harus diambil jika risiko tersebut terwujud, termasuk pengaturan untuk tata kelola **internal dan mekanisme pengaduan**.*

Bentuk spesifik dari penilaian dampak hak asasi manusia ini dapat bervariasi tergantung pada konteks sistem AI dan hak asasi manusia yang terpengaruh. Rumusan yang lebih tepat tentang bagaimana penilaian dampak hak asasi manusia yang sesuai dengan Undang-Undang AI akan terlihat harus diumumkan oleh Kantor AI Eropa selambat-lambatnya tiga bulan sebelum ketentuan tentang sistem berisiko tinggi mulai berlaku, yaitu 21 bulan setelah Undang-Undang AI mulai berlaku, pada tanggal 2 Mei 2026.

Sebagai antisipasi terhadap persyaratan bagi para pengimplementasi, upaya pertama akan dilakukan di sini untuk menafsirkan proses penilaian dampak hak-hak fundamental sesuai dengan Pasal 27 ayat 1 UU AI:

1. **Analisis fungsi sistem AI (huruf a) dan implementasi (huruf b):** Analisis rinci tentang fungsi sistem AI, termasuk data yang digunakan, proses pengambilan keputusan, dan cara keluaran dihasilkan, diperlukan. Hal ini membantu untuk memahami bagaimana sistem tersebut secara khusus dapat memengaruhi hak-hak fundamental. Penjelasan tentang periode dan frekuensi penggunaan sistem. Pasal 96 UU AI mengharuskan para pengimplementasi untuk “ketika melakukan penilaian ini mempertimbangkan informasi yang relevan untuk penilaian dampak yang tepat, termasuk informasi yang diberikan oleh penyedia sistem AI berisiko tinggi dalam petunjuk penggunaan”.
2. **Identifikasi hak-hak fundamental dan kategori orang dan kelompok orang yang terdampak (huruf c):** Pertama, harus ditentukan hak-hak fundamental mana dari Piagam yang berpotensi terpengaruh oleh penggunaan sistem AI. Untuk tujuan ini, seseorang dapat meninjau hak-hak dalam Piagam secara individual dan melakukan analisis tentang hak mana yang mungkin terpengaruh oleh sistem yang mungkin diterapkan. Apakah kepatuhan terhadap setiap hak individu dijamin saat menggunakan aplikasi AI? Orang atau kelompok mana yang dapat terpengaruh secara negatif oleh sistem AI sehubungan dengan setiap hak yang diidentifikasi secara individual? Apakah ada kelompok yang sangat rentan (misalnya anak-anak atau orang dengan disabilitas fisik atau mental) yang perlu dipertimbangkan?
3. **Penilaian risiko dan dampak (huruf d):** Berdasarkan analisis fungsional, risiko untuk setiap hak fundamental yang diidentifikasi dan kelompok orang yang mungkin terpengaruh harus dinilai. Ini termasuk menilai kemungkinan dan tingkat keparahan

dampak negatif yang mungkin terjadi pada pelanggaran hak-hak fundamental individu dan seluruh kelompok. Seberapa besar kemungkinan pelanggaran satu atau lebih hak fundamental dan dapatkah campur tangan terhadap hak fundamental yang mungkin tersebut dibenarkan?

Menurut Pasal 27 UU AI bersamaan dengan Pertimbangan 96 UU AI, penilaian dampak harus mencakup “risiko kerugian spesifik”. Menurut interpretasi penulis, kerugian tersebut terletak pada pelanggaran hak-hak dalam Piagam. Untuk mengilustrasikan hal ini, digunakan contoh klasik yang berkaitan dengan sistem AI: Diskriminasi terhadap individu atau kelompok individu (lihat bagian 7.1, Diskriminasi), seperti yang dilakukan oleh alat rekrutmen AI Amazon, yang lebih mengutamakan kandidat laki-laki. Hal ini dapat merupakan pelanggaran terhadap Pasal 21 CFR (non-diskriminasi) dan Pasal 23 CFR (kesetaraan antara laki-laki dan perempuan), kecuali jika campur tangan terhadap hak fundamental tersebut dibenarkan oleh Pasal 52 ayat 1 CFR (cakupan hak yang dijamin).

Menurut Pasal 52 ayat 1 CFR, *“setiap pembatasan terhadap pelaksanaan hak dan kebebasan yang **diakui oleh Piagam** ini harus diatur oleh hukum dan **menghormati esensi hak dan kebebasan tersebut**. Dengan tunduk pada prinsip **proporsionalitas**, pembatasan hanya dapat dilakukan jika **diperlukan** dan benar-benar memenuhi **tujuan kepentingan umum yang diakui oleh Uni Eropa atau kebutuhan untuk melindungi hak dan kebebasan orang lain.**”*

Di sini, perlu diperiksa (1) apakah penggunaan AI dapat mengganggu hak fundamental berdasarkan Piagam dan orang atau kelompok orang mana yang haknya dapat dibatasi sebagai akibatnya dan (2) apakah gangguan tersebut juga dapat dibenarkan. Semakin tinggi kemungkinan bahwa hak fundamental akan dilanggar dan tidak ada alasan yang dapat dibenarkan untuk hal ini berdasarkan Pasal 52 ayat 1 Piagam, semakin tinggi risiko yang harus dinilai sebagai bagian dari penilaian dampak hak fundamental.

Berbeda dengan hak **fundamental relatif**, yang dapat dibatasi oleh alasan yang tercantum dalam Pasal 52 ayat 1 CFR, apa yang disebut **hak fundamental absolut** tidak dapat dibatasi dalam keadaan apa pun. Contoh hak fundamental absolut yang tidak dapat dibatasi dalam keadaan apa pun adalah Pasal 1 CFR: *“Martabat manusia tidak dapat dilanggar. Martabat manusia harus dihormati dan dilindungi.”* Jika suatu sistem AI seharusnya mengenali dan mengklasifikasikan orang dan objek dalam sebuah gambar dan menggambarkan orang-orang kulit berwarna sebagai “gorila”, penulis berpendapat bahwa ini merupakan pelanggaran terhadap Pasal 1 Piagam, karena individu dan seluruh kelompok orang digambarkan dengan cara yang merendahkan dan menghina sehingga martabat manusia dapat terpengaruh secara langsung. Tidak ada pembenaran yang sah untuk pelanggaran Pasal 1 Piagam tersebut.

Dalam artikel mereka “Kerangka Kerja untuk Memahami Sumber Kerugian Sepanjang Siklus Hidup Pembelajaran Mesin”, Harini Suresh dan John Gutttag menjelaskan apa yang disebut kerugian representasional, yang seringkali dapat menjadi dasar perlakuan diskriminatif selanjutnya. Menurut Pasal 96 UU AI, “penilaian juga harus mencakup identifikasi risiko kerugian spesifik yang kemungkinan akan berdampak pada hak-hak fundamental orang atau kelompok tersebut”. Dalam konteks ini, kerugian representasional harus dimasukkan dalam penilaian dampak dengan cara yang sama seperti kerugian distributif, di mana harus

dipastikan bahwa barang didistribusikan secara adil dan bahwa akses ke manfaat tertentu tersedia untuk semua.

Jika perlu, langkah ini juga dapat menentukan bahwa risiko pelanggaran hak fundamental terlalu besar untuk memulai pengembangan. Bagaimana dipastikan bahwa hak-hak yang berpotensi terpengaruh dilindungi?

Contoh penilaian potensi kerugian yang disebabkan oleh sistem AI dan dampaknya pada orang atau kelompok orang yang terpengaruh oleh Badan Hak Fundamental Eropa ditunjukkan pada Gambar 3.5.

CONTOH-CONTOH POTENSI BAHAYA					
Daerah	Potensi positif palsu - contoh		Contoh negatif palsu yang mungkin terjadi		Jika hasilnya lebih baik daripada keputusan manusia secara rata-rata - contoh
	Untuk seorang individu	Dalam skala/untuk masyarakat	Untuk seorang individu	Dalam skala/untuk masyarakat	
Kesejahteraan sosial	Jika seseorang menerima tunjangan tanpa berhak menerimanya atau menerima tunjangan melebihi jumlah yang berhak diterimanya		Jika seseorang tidak menerima hak manfaatnya atau kurang dari manfaatnya apa pun		- Akses yang lebih baik terhadap kesejahteraan sosial - Peningkatan administrasi publik
	Tidak ada konsekuensi negatif yang nyata, kecuali jika keputusan yang salah tersebut diketahui kemudian dan orang tersebut harus mengembalikan uang.	Konsekuensi negatif bagi administrasi publik, karena hal ini menyebabkan praktik-praktik yang tidak sejalan dengan tata kelola pemerintahan yang baik.	Meningkatnya kemiskinan dan kurangnya sumber daya bagi individu untuk menjalani kehidupan yang bermartabat.	Potensi pergeseran distribusi sumber daya dalam masyarakat, yang berpotensi meningkatkan ketidaksetaraan dan pengucilan sosial.	
Pemolisian prediktif	Seseorang yang tidak bersalah ditandai sebagai polisi sebagai tersangka		Seseorang yang terlibat dalam aktivitas kriminal tidak teridentifikasi		
	Berpotensi memalukan; dapat dikaitkan dengan diskriminasi.	Berpotensi meningkatkan ketidakpuasan dan kurangnya kepercayaan terhadap polisi; khususnya berdampak pada kelompok-kelompok tertentu.	Seseorang dapat melanjutkan aktivitas kriminal tanpa dikenai sanksi.	Potensi peningkatan kriminalitas di masyarakat, dengan implikasi signifikan terhadap keselamatan publik dan korban kejahatan.	- Kepolisian prediktif yang lebih akurat dapat menghasilkan hasil yang lebih tinggi. Tingkat penangkapan tersangka/pelaku kejahatan, dan berkurangnya risiko individu menjadi korban kejahatan. - Tingkat kejahatan menurun dan tingkat keamanan meningkat.
Diagnosa medis	Suatu penyakit salah didiagnosis		Suatu penyakit tidak terdiagnosis		
	Perawatan yang salah (berpotensi berbahaya) atau tidak perlu - berdampak negatif pada kesehatan dan martabat manusia.	Menurunnya kepercayaan terhadap sistem kesehatan, termasuk implikasi kesehatan negatif jika masyarakat berhenti berobat ke dokter. Tingkat kesehatan secara umum menurun.	Kurangnya pengobatan berdampak negatif pada kesehatan, termasuk harapan hidup.	Secara keseluruhan terjadi peningkatan masalah kesehatan di masyarakat, dan berpotensi meningkatkan angka kematian.	Tingkat kesehatan yang lebih tinggi
Iklan yang ditargetkan	Iklan disampaikan melalui situs web, tetapi tidak relevan bagi individu tersebut		Iklan yang berpotensi relevan tidaklah demikian disampaikan melalui situs web		
	Seseorang menerima iklan tertentu dan melewatkan informasi tentang penawaran yang mungkin menarik minat mereka.	Iklan mereplikasi stereotip sosial yang tidak menawarkan akses yang sama ke pasar. Potensi dampak ekonomi negatif	Calon konsumen tidak menerima iklan yang relevan dan kehilangan informasi tentang penawaran yang mungkin menarik bagi mereka.	Potensi dampak ekonomi negatif karena sebagian besar basis pelanggan potensial dikecualikan.	- Konsumen kini lebih terinformasi tentang penawaran di berbagai bidang, seperti produk, layanan, dan pekerjaan. - Peningkatan pendapatan ekonomi bagi perusahaan.

	Berpotensi menerima konten yang menyinggung.	karena sebagian besar basis pelanggan potensial dikecualikan. Potensi manipulasi terhadap konsumen dan warga negara. Penyebaran luas konten yang berpotensi menyinggung.	Iklan bertarget yang kurang efisien tidak akan berkontribusi pada peningkatan pendapatan perusahaan.		

Gambar 3.5 Contoh Penilaian Potensi Kerugian yang Disebabkan oleh Sistem AI dan Dampaknya pada Individu atau Kelompok Individu yang Terdampak.

- 1. Pengembangan strategi mitigasi melalui langkah-langkah pengawasan manusia (lit e) dan tata kelola internal serta mekanisme pengaduan (lit f):** Langkah ini melibatkan pertimbangan langkah-langkah yang harus diambil jika risiko tersebut terwujud, termasuk misalnya pengaturan tata kelola dalam konteks penggunaan spesifik tersebut, seperti pengaturan pengawasan manusia sesuai dengan petunjuk penggunaan atau, prosedur penanganan pengaduan dan ganti rugi, karena hal tersebut dapat berperan dalam mengurangi risiko terhadap hak-hak fundamental dalam kasus penggunaan konkret” (Pertimbangan 96 UU AI). Ini berarti bahwa strategi harus dikembangkan untuk risiko yang teridentifikasi guna mencegah kemungkinan terjadinya dan, jika ini tidak memungkinkan, untuk meminimalkannya. Ini dapat mencakup penyesuaian teknis pada sistem AI, revisi basis data, langkah-langkah perlindungan tambahan untuk pemrosesan data dan juga, misalnya, mengukur keadilan, tetapi juga mengacu pada prosedur untuk meninjau dan menantang keputusan AI tentang pengguna akhir.
- 2. Langkah-langkah pengawasan manusia (lit e)** Sistem AI berisiko tinggi harus dirancang sedemikian rupa sehingga dapat dipahami dan dipantau oleh manusia dengan cara sebaik mungkin. Harus diperiksa dan dievaluasi dengan cermat bagaimana manusia dapat dan harus campur tangan dalam sistem tersebut. Transparansi dan kemampuan menjelaskan memainkan peran yang sama pentingnya di sini seperti penyajian hasil sistem AI untuk menciptakan dasar bagi pengawasan manusia. Jika suatu sistem hanya mengatakan "ya" atau "tidak", manusia pada kenyataannya tidak memiliki cara untuk memeriksa sistem atau hasilnya. Di sini, disarankan untuk menyajikan keputusan yang dibuat oleh sistem AI sedemikian rupa sehingga seseorang membuat keputusan akhir sendiri, tetapi memiliki informasi yang relevan untuk membuat keputusan independen sejak awal. Demi transparansi, indikator kepercayaan dapat digunakan di sini, misalnya, untuk memberikan informasi kepada pengguna tentang seberapa andal sistem AI tersebut, misalnya untuk klasifikasi.
- 3. Tata kelola perusahaan internal dan mekanisme pengaduan (lit f)** Untuk memastikan kepatuhan berkelanjutan terhadap undang-undang AI, Diperlukan struktur tata kelola yang sesuai (lihat bagian 10.2) dan kode etik (lihat bagian 10.5). Pengenalan sistem AI di perusahaan memicu kekhawatiran di antara orang-orang, termasuk tentang

pekerjaan mereka sendiri, dan oleh karena itu seringkali menghadapi resistensi internal. Dengan kata lain, jika tujuannya adalah untuk mendampingi proses tertentu di perusahaan, karyawan juga perlu pelatihan untuk meredakan kekhawatiran mereka dan menunjukkan potensi untuk mempermudah pekerjaan dan untuk pengembangan lebih lanjut. Hanya apabila karyawan dilibatkan secara tepat dalam proses ini, mereka akan mampu menelaah sistem secara kritis dan tidak menerima begitu saja hasil yang dihasilkan secara otomatis. Ini adalah pertanyaan tentang tingkat kepercayaan yang tepat pada teknologi. Dalam konteks ini, pihak yang menerapkan juga perlu mempertimbangkan cara terbaik untuk membangun mekanisme pengaduan yang memungkinkan pemangku kepentingan seperti pelanggan, karyawan, atau pihak lain yang terkena dampak untuk menyampaikan kekhawatiran atau keluhan tentang fungsi sistem AI atau dampaknya. Berkaitan dengan pengguna akhir, komunikasi terbuka tentang fungsi, keterbatasan sistem AI, dan langkah-langkah pengaduan sangat penting untuk meminimalkan risiko pelanggaran hak-hak mendasar dan untuk bereaksi tepat waktu melalui saluran pengaduan jika hal ini terjadi.

Sebagai bagian dari penilaian dampak regulasi, sangat penting untuk melibatkan sebanyak mungkin pemangku kepentingan dalam proses ini – termasuk pengguna akhir, ahli hukum, dan kelompok orang yang berpotensi terkena dampak – untuk mengidentifikasi sepenuhnya potensi dampak dan risiko sejak awal. Seluruh penilaian dampak harus didokumentasikan dengan cermat, termasuk asumsi yang dibuat, analisis yang dilakukan, dan langkah-langkah mitigasi yang direncanakan.

Sebagai bagian dari penilaian dampak hak-hak fundamental, penting untuk melibatkan sebanyak mungkin pemangku kepentingan dalam proses ini – termasuk pengguna akhir, ahli hukum, dan kelompok orang yang berpotensi terkena dampak – untuk mengidentifikasi sepenuhnya potensi dampak dan risiko sejak awal. Seluruh penilaian dampak harus didokumentasikan dengan cermat, termasuk asumsi yang dibuat, analisis yang dilakukan, dan langkah-langkah mitigasi yang direncanakan. Pertimbangan ke-96 UU AI menyatakan sebagai berikut: *“Jika perlu, untuk mengumpulkan informasi yang relevan yang diperlukan untuk melakukan penilaian dampak, para pengimplementasikan sistem AI berisiko tinggi, khususnya ketika sistem AI digunakan di sektor publik, dapat melibatkan pemangku kepentingan yang relevan, termasuk perwakilan kelompok orang yang kemungkinan akan terpengaruh oleh sistem AI, pakar independen, dan organisasi masyarakat sipil dalam melakukan penilaian dampak tersebut dan merancang langkah-langkah yang harus diambil jika risiko tersebut terwujud.”*

Menurut Pasal 27 ayat 2 UU AI, kewajiban untuk melakukan penilaian dampak hak-hak fundamental yang diatur dalam Pasal 27 ayat 1 UU AI berlaku untuk penggunaan pertama sistem AI berisiko tinggi. Namun, penilaian dampak tidak harus dimulai dari awal setiap kali: *“Dalam kasus serupa, pihak yang menerapkan dapat mengandalkan penilaian dampak hak-hak fundamental yang telah dilakukan sebelumnya atau penilaian dampak yang ada yang dilakukan oleh penyedia. Jika, selama penggunaan sistem AI berisiko tinggi, pihak yang menerapkan menganggap bahwa salah satu elemen yang tercantum dalam paragraf 1 telah*

berubah atau tidak lagi mutakhir, pihak yang menerapkan harus mengambil langkah-langkah yang diperlukan untuk memperbarui informasi tersebut."

Kewajiban ini berlaku untuk pengenalan pertama sistem AI berisiko tinggi, meskipun dalam kasus serupa pihak yang menerapkan dapat mengandalkan penilaian dampak yang telah dilakukan sebelumnya – terutama oleh penyedia. Tinjauan berkala terhadap penilaian dampak direkomendasikan untuk memastikan bahwa penilaian tersebut tetap relevan dan risiko baru diperhitungkan. Jika keadaan berubah atau informasi tersebut tidak lagi mutakhir, pihak yang menerapkan harus mengambil langkah-langkah yang diperlukan untuk memperbarui informasi tersebut (Pertimbangan 96 UU AI). Ini berarti bahwa harus dinilai secara berkala apakah kondisi kerangka kerja untuk penggunaan sistem AI telah berubah atau dapat berdampak pada hak-hak fundamental. Hal ini memerlukan pemantauan oleh orang dan sistem yang ditunjuk dan bertanggung jawab yang mendokumentasikan dan memperlihatkan setiap perubahan dan pengembangan lebih lanjut dari sistem AI dan ruang lingkup aplikasinya.

(3) Setelah penilaian yang dimaksud dalam ayat 1 Pasal ini dilakukan, pihak yang menerapkan wajib memberitahukan hasilnya kepada otoritas pengawasan pasar, dengan menyerahkan templat yang telah diisi sebagaimana dimaksud dalam ayat 5 Pasal ini sebagai bagian dari pemberitahuan. Dalam kasus yang dimaksud dalam Pasal 46 ayat 1, pihak yang menerapkan dapat dibebaskan dari kewajiban untuk memberitahukan tersebut.

Sesuai dengan ayat 3, setelah melakukan penilaian, pihak yang menerapkan wajib memberitahukan hasilnya kepada otoritas pengawasan pasar, termasuk penyerahan kuesioner standar yang disediakan oleh Kantor AI untuk memfasilitasi kepatuhan terhadap kewajiban ini (lihat ayat 5 di bawah).

Pasal 46 ayat 1 Undang-Undang AI mendefinisikan pengecualian dari prosedur penilaian kesesuaian sesuai dengan Pasal 46 ayat 1 Undang-Undang AI. Pasal 43 UU AI menetapkan hal berikut: *"...atas permintaan yang beralasan, otoritas pengawasan pasar mana pun dapat mengizinkan penempatan di pasar atau pengoperasian sistem AI berisiko tinggi tertentu di wilayah Negara Anggota yang bersangkutan, karena alasan luar biasa terkait keamanan publik atau perlindungan jiwa dan kesehatan manusia, perlindungan lingkungan, atau perlindungan aset industri dan infrastruktur utama. Otorisasi tersebut berlaku untuk jangka waktu terbatas sementara prosedur penilaian kesesuaian yang diperlukan sedang dilakukan, dengan mempertimbangkan alasan luar biasa yang membenarkan pengecualian tersebut. Penyelesaian prosedur tersebut harus dilakukan tanpa penundaan yang tidak semestinya."* Ini berarti bahwa jika kriteria Pasal 46 ayat 1 UU AI terpenuhi, pihak yang menerapkan sistem tersebut dapat dibebaskan dari kewajiban pemberitahuan sesuai dengan Pasal 27 ayat 3 UU AI. Menurut pendapat penulis, ada risiko bahwa ketentuan ini dapat digunakan oleh Negara Anggota untuk melemahkan perlindungan hak-hak fundamental dan dapat digunakan sebagai pembenaran untuk setiap penggunaan sistem AI yang mengganggu hak-hak fundamental.

(4) Jika salah satu kewajiban yang ditetapkan dalam Pasal ini telah dipenuhi melalui penilaian dampak perlindungan data yang dilakukan berdasarkan Pasal 35 Peraturan

(EU) 2016/679 atau Pasal 27 Arahan (EU) 2016/680, maka penilaian dampak hak fundamental sebagaimana dimaksud dalam ayat 1 Pasal ini akan melengkapi penilaian dampak perlindungan data tersebut.

Jika penilaian dampak perlindungan data telah dilakukan sesuai dengan GDPR atau Direktif (UE) 2016/680, maka cukup bagi penilaian dampak perlindungan data tersebut untuk dilengkapi dengan penilaian dampak hak fundamental sesuai dengan Pasal 27 GDPR. Penting agar penilaian dampak perlindungan data mencakup penilaian komprehensif tentang dampak penggunaan sistem AI terhadap hak fundamental.

(5) Kantor AI akan mengembangkan templat kuesioner, termasuk melalui alat otomatis, untuk mempermudah para pengembang dalam memenuhi kewajiban mereka berdasarkan Pasal ini dengan cara yang disederhanakan.

Seperti yang telah disebutkan di atas, paragraf 5 Pasal 27 UU AI menetapkan bahwa Kantor AI Eropa akan mengembangkan kuesioner model untuk mempermudah para pengembang dalam melakukan penilaian dampak hak fundamental.

Sesuai dengan Pasal 77 ayat 2. Berdasarkan UU AI, setiap Negara Anggota harus menunjuk otoritas nasional atau badan publik yang bertanggung jawab atas kepatuhan terhadap hukum Uni Eropa tentang perlindungan hak-hak fundamental paling lambat tanggal 2 November 2024 dan menyediakannya dalam daftar publik yang mutakhir untuk dikomunikasikan kepada Komisi dan Negara Anggota lainnya.

Untuk memastikan implementasi hak-hak fundamental di tingkat nasional, Pasal 77 ayat 1 UU AI mengatur hal-hal berikut: *Otoritas atau badan publik nasional yang mengawasi atau menegakkan kepatuhan terhadap kewajiban berdasarkan hukum Uni Eropa yang melindungi hak-hak fundamental, termasuk hak untuk tidak didiskriminasi, sehubungan dengan penggunaan sistem AI berisiko tinggi yang disebutkan dalam Lampiran III, berwenang untuk meminta dan mengakses dokumentasi apa pun yang dibuat atau dipelihara berdasarkan Peraturan ini dalam bahasa dan format yang mudah diakses ketika akses ke dokumentasi tersebut diperlukan untuk secara efektif memenuhi mandat mereka dalam batas yurisdiksi mereka.* Otoritas atau badan publik yang bersangkutan harus memberi tahu otoritas pengawasan pasar Negara Anggota yang bersangkutan tentang permintaan tersebut. Jika dokumentasi ini tidak cukup untuk menentukan apakah telah terjadi pelanggaran hukum Uni Eropa tentang perlindungan hak-hak fundamental, otoritas nasional atau badan sektor publik dapat mengajukan permintaan untuk pengujian teknis sistem AI berisiko tinggi yang akan dilakukan oleh otoritas pengawasan pasar bekerja sama dengan otoritas atau badan yang meminta dalam jangka waktu yang wajar (Pasal 77 ayat 3 UU AI). Sesuai dengan paragraf 4, dokumentasi ini harus diperlakukan secara rahasia sesuai dengan Pasal 78 UU AI.

Pertimbangan 157 UU AI menyatakan bahwa Peraturan ini “tidak mengurangi kompetensi, tugas, wewenang, dan independensi otoritas atau badan publik nasional yang relevan yang mengawasi penerapan hukum Uni Eropa yang melindungi hak-hak fundamental, termasuk badan kesetaraan dan otoritas perlindungan data”.

Penilaian Dampak sebagai Bagian dari Tata Kelola AI

Melakukan penilaian dampak hak-hak fundamental merupakan langkah penting menuju tata kelola AI yang berpusat pada manusia (lihat Bab 10). Penilaian ini diperlukan untuk memastikan bahwa pengembangan dan penggunaan teknologi AI sejalan dengan hak-hak yang diabadikan dalam Piagam. Penilaian dampak tersebut berfungsi untuk meningkatkan kesadaran akan potensi dampak aplikasi AI tertentu pada berbagai bidang masyarakat dan untuk memastikan gambaran terstruktur tentang kemungkinan risiko dan pengelolaannya. Ini tentang mempromosikan perencanaan yang matang, desain etis, dan implementasi sistem AI yang bertanggung jawab. Ini termasuk mempromosikan transparansi dan akuntabilitas serta pengambilan keputusan yang etis. Penilaian dampak hak-hak fundamental harus dilakukan sebelum sistem AI diterapkan, tetapi juga harus dipantau secara berkala selama pengoperasian sistem AI dan ditinjau jika terjadi perubahan apa pun.

Inti dari penilaian tersebut adalah deteksi dini potensi pelanggaran hak-hak fundamental oleh aplikasi AI. Setiap risiko yang teridentifikasi harus dipertimbangkan dan dievaluasi dengan cermat untuk mengembangkan langkah-langkah mitigasi risiko yang sesuai. Hal ini juga mencakup penilaian probabilitas pelanggaran serta tingkat keparahan pelanggaran hak-hak fundamental yang mungkin terjadi. Pendekatan ini dapat mendorong penggunaan teknologi AI yang seimbang dan bertanggung jawab yang melindungi dan memperkuat hak dan kebebasan individu.

Melakukan penilaian dampak hak-hak fundamental dalam pengembangan dan penerapan teknologi AI merupakan elemen kunci dalam mencapai tujuan tata kelola AI yang berpusat pada manusia dan mendorong transparansi, akuntabilitas, dan pengambilan keputusan etis di seluruh proses perencanaan, desain, dan implementasi AI.

Alat yang Ada untuk Penilaian Dampak Hak-Hak Fundamental

Sudah ada daftar panjang alat dari berbagai organisasi dan lembaga yang menggambarkan proses untuk melakukan penilaian dampak hak-hak fundamental.

Daftar ini dimaksudkan untuk memberikan beberapa contoh penilaian dampak. Namun, perlu dicatat di sini bahwa alat-alat tersebut tidak merupakan penilaian dampak hak-hak fundamental sesuai dengan GDPR Uni Eropa.

Beberapa instrumen yang relevan untuk melakukan penilaian dampak hak-hak fundamental:

- *FRAIA* – Penilaian Dampak Hak-Hak Fundamental dan Algoritma saat ini digunakan oleh pemerintah Belanda untuk melakukan penilaian dampak.
- *DEDA* – Bantuan Pengambilan Keputusan Etika Data juga digunakan oleh pemerintah Belanda.
- *Sistem pengambilan keputusan otomatis di sektor publik* oleh Algorithm Watch Switzerland
- *Memeriksa Kotak Hitam* dari Ada Lovelace Institute dan Data Kind UK
- *Kerangka Kerja Manajemen Risiko AI Institut Standar dan Teknologi Nasional*
- (NIST AI RMF) oleh pemerintah AS
- *Kerangka Kerja Audit untuk Algoritma* dari Pengadilan Audit Belanda
- *Kelompok Dampak Etika AI: Dari Prinsip ke Praktik* dari Grup AIEI

- *Pedoman tentang administrasi dan etika digital* dari Kementerian Federal Seni, Budaya, Layanan Sipil dan Olahraga
- *Penilaian Dampak Etika: Alat Rekomendasi tentang Etika Kecerdasan Buatan* dari UNESCO untuk Evaluasi Dampak Etika
- *Daftar Penilaian AI Tepercaya ALTAI* dari Kelompok Pakar Tingkat Tinggi independen tentang Kecerdasan Buatan yang dibentuk oleh Komisi Eropa

3.6 STANDAR YANG HARMONIS, PENILAIAN KESESUAIAN, SERTIFIKAT DAN REGISTRASI

Bagian 5 dari Bab 3 Undang-Undang AI, yang terdiri dari Pasal 40–49 Undang-Undang AI, mendefinisikan kerangka kerja untuk menilai kesesuaian sistem AI. Bagian penting ini menjelaskan bagaimana penyedia harus memastikan bahwa sistem AI mereka mematuhi standar Uni Eropa yang ketat untuk keselamatan, transparansi, dan perlindungan hak-hak fundamental sebelum diluncurkan ke pasar.

Penilaian kesesuaian dimaksudkan untuk memperkuat kepercayaan pada teknologi AI dan memastikan tingkat perlindungan yang tinggi bagi semua orang. Hal ini seharusnya menjamin bahwa sistem AI aman, ramah privasi, dan tidak diskriminatif, sehingga mendorong penggunaan yang aman di Uni Eropa bagi masyarakat.

Contoh

Mari kita asumsikan bahwa sebuah perusahaan mengembangkan sistem AI untuk menganalisis dokumen aplikasi dalam proses rekrutmen. Sistem ini dapat diklasifikasikan sebagai AI berisiko tinggi, karena dapat berdampak signifikan pada peluang pelamar. Oleh karena itu, perusahaan harus melakukan penilaian kesesuaian sebelum meluncurkannya ke pasar. Ini termasuk memeriksa keakuratan sistem, melindungi data pelamar, dan memastikan bahwa sistem tidak membuat keputusan diskriminatif. Setelah penilaian berhasil, perusahaan mengeluarkan deklarasi kesesuaian dan mendaftarkan sistem tersebut di basis data Uni Eropa. Ini memastikan bahwa sistem tersebut mematuhi peraturan Uni Eropa dan dapat digunakan dengan aman.

Tabel berikut memberikan gambaran umum tentang elemen-elemen kunci Bagian 5, mulai dari standar yang diselaraskan dan persyaratan penilaian kesesuaian hingga pendaftaran sistem AI dalam basis data khusus Uni Eropa:

Pasal	Kata kunci	Penjelasan
Pasal 40 UU AI	Standar yang diselaraskan	Produsen dan pemasok sistem AI berisiko tinggi yang mematuhi standar yang harmonis dapat lebih mudah membuktikan bahwa produk mereka memenuhi persyaratan peraturan Uni Eropa.
Pasal 41 UU AI	Spesifikasi umum	Menjelaskan bagaimana Komisi Eropa menangani standardisasi sistem AI berisiko tinggi.
Pasal 42 UU AI	Asumsi kesesuaian	Mendefinisikan kriteria kapan persyaratan untuk data, akurasi, ketahanan, dan keamanan siber dapat diasumsikan untuk sistem AI berisiko tinggi.
Pasal 43 UU AI	Penilaian kesesuaian	Menjelaskan prosedur yang harus dilakukan oleh penyedia sistem AI berisiko tinggi untuk memastikan kesesuaian sistem mereka dengan persyaratan Peraturan.

Pasal 44 UU AI	Sertifikat	Menjelaskan sertifikat kesesuaian dan masa berlakunya.
Pasal 45 UU AI	Kewajiban informasi badan yang diberi wewenang	Menentukan kewajiban informasi dari badan yang diberi wewenang terhadap pemangku kepentingan lainnya.
Pasal 46 UU AI	Pengecualian dari prosedur penilaian kesesuaian	Mengatur keadaan di mana otoritas pengawasan pasar dapat menyetujui sistem AI berisiko tinggi.
Pasal 47 UU AI	Deklarasi Kesesuaian UE	Mewajibkan penyedia untuk menerbitkan deklarasi kesesuaian UE, yang membuktikan bahwa sistem AI memenuhi persyaratan sebelum dipasarkan.
Pasal 48 UU AI	Penandaan CE	Menjelaskan kriteria untuk pelabelan sistem AI.
Pasal 49 UU AI	Pendaftaran	Persyaratan ini mengharuskan penyedia atau perwakilan resminya untuk mendaftarkan sistem AI berisiko tinggi (dengan pengecualian tertentu) ke dalam basis data Uni Eropa sebelum dipasarkan atau dioperasikan. Pendaftaran oleh penyedia layanan publik tertentu sebelum penggunaannya juga diwajibkan.

Persyaratan utama bagi produsen, penyedia, dan pengimplementasikan sistem AI dibahas lebih rinci di bagian berikut.

Standar Terharmonisasi dan Penandaan CE

Pasal 40 Undang-Undang AI membahas standar terharmonisasi dan hasil standardisasi untuk sistem AI berisiko tinggi. Standar terharmonisasi adalah spesifikasi teknis (standar Eropa atau bagian-bagiannya) yang disusun oleh organisasi standardisasi Eropa seperti CEN, CENELEC, atau ETSI atas permintaan Komisi Eropa. Standar ini dimaksudkan untuk memfasilitasi kepatuhan terhadap persyaratan dasar dari arahan atau peraturan Uni Eropa tertentu. Suatu produk, layanan, atau proses yang sesuai dengan standar terharmonisasi dianggap sesuai dengan persyaratan yang relevan dari undang-undang Uni Eropa terkait.

Pada saat buku ini ditulis, belum ada standar khusus untuk Undang-Undang AI yang telah diselesaikan. Oleh karena itu, bagian ini hanya dapat membahas prinsip-prinsip dasar prosedur tersebut.

Standardisasi seharusnya memainkan peran kunci dalam menyediakan solusi teknis bagi para penyedia untuk memastikan kepatuhan terhadap Peraturan ini sesuai dengan perkembangan mutakhir ilmu pengetahuan dan teknologi, serta untuk mendorong inovasi, daya saing, dan pertumbuhan di pasar internal (Pertimbangan 121 AI Act).

Salah satu contoh standar yang terharmonisasi adalah EN ISO 12100, “Keselamatan mesin”. Standar ini memberikan pedoman untuk penilaian risiko dan pengurangan risiko dalam desain mesin. Tujuannya adalah untuk memastikan keselamatan para pengembang dan pengguna mesin. Kepatuhan terhadap standar yang terharmonisasi ini memungkinkan produsen untuk membubuhkan tanda CE pada produk mereka untuk menunjukkan bahwa produk tersebut sesuai dengan persyaratan undang-undang Uni Eropa yang relevan. Hal ini memfasilitasi pergerakan barang secara bebas di dalam Kawasan Ekonomi Eropa.

Sistem AI berisiko tinggi yang mematuhi standar yang terharmonisasi atau bagian-bagiannya yang diterbitkan dalam Jurnal Resmi Uni Eropa dianggap memenuhi persyaratan untuk sistem AI berisiko tinggi (Pasal 8 dan seterusnya Undang-Undang AI) atau, jika berlaku, dengan persyaratan melalui GPAI, asalkan persyaratan ini tercakup dalam standar tersebut.

Signifikansi bagi produsen dan penyedia sistem AI berisiko tinggi

Persyaratan ini berarti bahwa produsen dan penyedia sistem AI berisiko tinggi dapat lebih mudah menunjukkan bahwa produk mereka sesuai dengan persyaratan Undang-Undang AI dengan mematuhi standar yang terharmonisasi. Prosedur ini dimaksudkan untuk memastikan keamanan, transparansi, dan perlindungan hak-hak fundamental di dalam Uni Eropa, sekaligus mendorong inovasi dan pertumbuhan di bidang kecerdasan buatan.

Untuk siapa ini relevan?

Ini sangat relevan bagi pengembang dan penyedia sistem AI berisiko tinggi yang ingin menawarkan produk mereka di pasar Eropa, serta bagi organisasi standarisasi dan pengambil keputusan politik di bidang teknologi digital.

Ringkasan Persyaratan Terpenting

1. Asumsi kesesuaian melalui kepatuhan terhadap standar yang harmonis (Pasal 40 ayat 1 Undang-Undang AI)

Jika sistem AI berisiko tinggi mematuhi standar harmonis yang diterbitkan sesuai dengan Peraturan (UE) 1025/2012, maka sistem tersebut dianggap mematuhi persyaratan yang relevan dari Undang-Undang AI. Ini berlaku selama standar tersebut mencakup persyaratan atau kewajiban khusus.

2. Mandat standarisasi dari Komisi (Pasal 40 ayat 2 Undang-Undang AI)

Komisi Eropa akan mengeluarkan mandat standarisasi untuk mencakup semua persyaratan yang relevan dari Undang-Undang AI. Mandat ini juga mencakup pertimbangan efisiensi sumber daya dan pengembangan model AI yang hemat energi. Komisi akan berkonsultasi dengan Dewan dan pemangku kepentingan terkait.

3. Konsistensi dan pemenuhan persyaratan (Pasal 40 ayat 2 Undang-Undang AI)

Mandat standarisasi yang dikeluarkan oleh Komisi dimaksudkan untuk memastikan bahwa standar yang dikembangkan jelas dan konsisten dan bahwa sistem AI atau model AI yang dipasarkan atau digunakan di Uni Eropa memenuhi persyaratan yang ditetapkan dalam Peraturan. Organisasi standarisasi Eropa diminta untuk menunjukkan komitmen mereka untuk mencapai tujuan ini.

4. Promosi investasi dan inovasi (Pasal 40 ayat 3 Undang-Undang AI)

Mereka yang terlibat dalam proses standarisasi harus mempromosikan investasi dan inovasi di bidang AI, khususnya dengan meningkatkan kepastian hukum dan memperkuat daya saing pasar Uni Eropa. Mereka juga harus berkontribusi pada kerja sama global dalam standarisasi dan memastikan bahwa standar internasional di bidang AI sejalan dengan nilai-nilai, hak-hak fundamental, dan kepentingan Uni Eropa.

5. Wewenang Komisi (Pasal 41 UU AI)

Pasal 41 memungkinkan Uni Eropa untuk menanggapi secara fleksibel tantangan standardisasi sistem AI sehingga standar keselamatan dan etika yang tinggi dapat dipertahankan bahkan tanpa standar yang harmonis.

Tanda CE

Tanda CE adalah simbol yang ditempelkan pada produk untuk menunjukkan bahwa produk tersebut sesuai dengan peraturan Uni Eropa yang berlaku. Namun, tanda CE untuk sistem AI berisiko tinggi tidak hanya menunjukkan kepatuhan terhadap persyaratan khusus Peraturan AI, tetapi juga kesesuaian dengan peraturan Uni Eropa lainnya yang berlaku. Penempelan dan sifat tanda CE harus dirancang sedemikian rupa sehingga mudah dikenali dan diakses oleh pengguna, terlepas dari apakah itu produk fisik atau layanan yang disediakan secara digital.

Pasal 48 UU AI mengatur kriteria:

1. Prinsip umum (ayat 1)

Prinsip-prinsip untuk penandaan CE didasarkan pada prinsip-prinsip umum yang ditetapkan dalam Pasal 30 Peraturan (EC) No. 765/2008. Prinsip-prinsip ini mengatur, misalnya, pemasangan penandaan CE, termasuk visibilitas, keterbacaan, dan daya tahannya.

2. Penandaan CE digital untuk sistem AI yang dipasang secara digital (ayat 2)

Untuk sistem AI berisiko tinggi yang tersedia secara digital, bentuk digital penandaan CE dapat digunakan. Ini harus mudah diakses, baik secara langsung melalui antarmuka pengguna, melalui kode yang dapat dibaca mesin, atau melalui cara elektronik lainnya.

3. Pemasangan penandaan CE (ayat 3)

Penandaan CE harus dipasang pada sistem AI berisiko tinggi dengan cara yang terlihat, terbaca, dan tidak dapat dihapus. Jika sifat sistem AI tidak memungkinkan atau membenarkannya (misalnya karena ukurannya atau jenis penggunaannya), penandaan tersebut dapat dipasang pada kemasan atau dokumen yang menyertainya.

4. Nomor Identifikasi Badan yang Diberi Notifikasi (ayat 4)

Jika penilaian kesesuaian sistem AI berisiko tinggi memerlukan penggunaan badan yang diberi notifikasi untuk penilaian kesesuaian sistem AI berisiko tinggi, nomor identifikasinya harus dicantumkan bersama dengan tanda CE. Nomor identifikasi tersebut harus ditempelkan oleh badan yang diberi notifikasi itu sendiri atau, atas instruksinya, oleh penyedia atau perwakilan resminya. Nomor ini juga harus muncul pada materi promosi apa pun yang menunjukkan bahwa sistem AI memenuhi persyaratan untuk tanda CE.

5. Kepatuhan terhadap peraturan perundang-undangan Uni Eropa lainnya (ayat 5)

Jika sistem AI berisiko tinggi juga tunduk pada peraturan perundang-undangan Uni Eropa lainnya yang juga mengatur tentang tanda CE, tanda CE menunjukkan bahwa sistem AI juga memenuhi persyaratan lainnya tersebut.

Penandaan CE merupakan tanda administratif yang menunjukkan kesesuaian suatu produk dengan peraturan perundang-undangan Uni Eropa, sehingga memungkinkan produk

tersebut untuk diperdagangkan secara bebas di dalam Wilayah Ekonomi Eropa. Bagi sistem AI, khususnya yang diklasifikasikan sebagai berisiko tinggi, penandaan CE menandakan bahwa sistem tersebut telah memenuhi persyaratan khusus sebagaimana ditetapkan dalam peraturan Uni Eropa yang berlaku.

Prosedur Penilaian Kesesuaian

Prosedur penilaian kesesuaian terutama relevan bagi penyedia sistem AI berisiko tinggi untuk memastikan bahwa sistem ini memenuhi persyaratan ketat Peraturan AI sebelum ditawarkan di pasar atau dioperasikan. Sistem AI lainnya tunduk pada peraturan yang kurang ketat, di mana persyaratan pastinya dapat bervariasi tergantung pada area aplikasi dan profil risiko.

Untuk siapa ini relevan?

Artikel ini relevan bagi penyedia sistem AI berisiko tinggi yang perlu memastikan bahwa sistem mereka mematuhi persyaratan Undang-Undang AI. Artikel ini membantu mengidentifikasi prosedur mana yang perlu dilakukan untuk menilai kesesuaian sistem ini dan memberikan panduan untuk memilih prosedur yang tepat, tergantung pada penerapan standar harmonisasi atau spesifikasi umum dan jenis sistem AI.

Signifikansi bagi penyedia sistem AI berisiko tinggi

Pasal 43 Undang-Undang AI mengatur tentang prosedur penilaian kesesuaian untuk sistem AI berisiko tinggi. Prosedur berikut harus diikuti:

1. Pilihan prosedur penilaian kesesuaian (Pasal 43 ayat 1 UU AI)

Pemasok sistem AI berisiko tinggi tertentu (tercantum dalam Lampiran III/1 UU AI) dapat memilih antara dua prosedur penilaian kesesuaian, dengan syarat mereka telah menerapkan standar harmonisasi atau spesifikasi umum:

- a) pengendalian internal sesuai dengan Lampiran VI UU AI
- b) Penilaian sistem manajemen mutu dan dokumentasi teknis oleh badan yang berwenang sesuai dengan Lampiran VII UU AI

2. Kebutuhan prosedur penilaian kesesuaian khusus (Pasal 43 ayat 1 UU AI)

Jika tidak ada standar harmonisasi atau spesifikasi umum yang tersedia atau pemasok belum (sepenuhnya) menerapkannya, prosedur penilaian kesesuaian harus dilakukan dengan melibatkan badan yang berwenang.

3. Pemilihan badan yang diberi wewenang (Pasal 43 ayat 1 UU AI)

Pemasok dapat menunjuk badan yang diberi wewenang untuk penilaian kesesuaian, kecuali jika sistem tersebut dioperasikan oleh otoritas publik tertentu (misalnya, penegak hukum, otoritas suaka, dan badan-badan Uni Eropa lainnya), dalam hal ini otoritas pengawasan pasar tertentu mengambil peran ini (Pasal 74 ayat 8 UU AI dan Pasal 74 ayat 9 UU AI).

4. Pengawasan internal untuk sistem AI berisiko tinggi lainnya (Pasal 43 ayat 2 UU AI)

Untuk sistem AI berisiko tinggi lainnya yang tercantum dalam Lampiran III UU AI (no. 2 hingga 8), penilaian kesesuaian dilakukan oleh pengawasan internal tanpa melibatkan badan yang diberi wewenang. Ini termasuk sistem AI untuk:

- Infrastruktur kritis

- Pendidikan dan pelatihan kejuruan
- Ketenagakerjaan, manajemen pekerja, dan akses ke wirausaha
- Aksesibilitas dan penggunaan layanan dan manfaat swasta dan publik dasar
- Penegakan hukum, sejauh penggunaannya diizinkan berdasarkan hukum Uni Eropa atau nasional yang relevan
- Migrasi, suaka, dan kontrol perbatasan, sejauh penggunaannya diizinkan berdasarkan hukum Uni Eropa atau nasional yang relevan
- Administrasi peradilan dan proses demokrasi

5. Kepatuhan terhadap peraturan perundang-undangan Uni Eropa lainnya (Pasal 43 ayat 3 Undang-Undang AI)

Sistem AI yang tercakup dalam peraturan perundang-undangan harmonisasi Uni Eropa lainnya harus mengikuti prosedur penilaian kesesuaian yang relevan dan persyaratan Undang-Undang AI termasuk dalam penilaian ini.

6. Penilaian Ulang Jika Terjadi Perubahan Material (Pasal 43 ayat 4 UU AI)

Sistem AI berisiko tinggi yang telah dimodifikasi secara substansial akan kembali menjalani prosedur penilaian kesesuaian, terlepas dari apakah sistem yang dimodifikasi tersebut masih akan dipasarkan atau terus digunakan oleh pengguna saat ini. Perubahan yang telah diperkirakan sebagai bagian dari proses pembelajaran berkelanjutan setelah dipasarkan tidak dianggap sebagai perubahan signifikan.

7. Pembaruan Lampiran dan Prosedur (Pasal 43 ayat 5 UU AI)

Komisi Eropa dapat mengadopsi tindakan delegasi untuk memperbarui Lampiran VI dan VII serta prosedur penilaian kesesuaian, khususnya terkait dengan kemajuan teknis dan evaluasi efektivitas prosedur.

Sistem AI Lainnya

Untuk sistem AI yang tidak diklasifikasikan sebagai berisiko tinggi, tidak ada kewajiban eksplisit untuk menjalani prosedur penilaian kesesuaian. Namun, sistem ini juga harus memenuhi persyaratan umum peraturan, khususnya terkait transparansi dan hak-hak mendasar. Pemasok sistem tersebut diharapkan untuk menilai sendiri apakah produk mereka sesuai dengan ketentuan yang relevan dari Peraturan AI, tetapi mereka tidak diharuskan untuk memberikan bukti kesesuaian formal atau membubuhkan tanda CE.

Perbedaan antara penggunaan suatu sistem AI dan penyediaannya merupakan hal yang penting. Kewajiban untuk melaksanakan prosedur penilaian kesesuaian berada pada penyedia (yaitu pihak yang menempatkan sistem di pasar atau mulai mengoperasikannya), bukan pada pengguna yang hanya menggunakan sistem tersebut.

Namun demikian, pengguna (deployer) sistem AI berisiko tinggi harus memahami persyaratan khusus yang berlaku serta memastikan bahwa sistem yang mereka gunakan telah memenuhi ketentuan (patuh terhadap regulasi) dan memiliki penandaan CE.

Contoh

Untuk mengilustrasikan penerapan Pasal 43 UU AI, mari kita lihat contoh fiktif: sistem AI berisiko tinggi dalam diagnostik medis, suatu bidang yang biasanya dianggap berisiko tinggi.

Langkah 1: Penentuan sistem AI berisiko tinggi

- Sebuah perusahaan, sebut saja Medai, sedang mengembangkan sistem AI untuk diagnosis penyakit langka berdasarkan data pencitraan. Sistem ini termasuk dalam sistem AI berisiko tinggi yang tercantum dalam Lampiran I Bagian A/1 UU AI.

Langkah 2: Tinjauan standar harmonisasi dan spesifikasi umum

- Medai memeriksa apakah ada standar harmonisasi untuk sistem AI Anda sesuai dengan Pasal 40 UU AI atau spesifikasi umum sesuai dengan Pasal 41 UU AI yang dapat memenuhi persyaratan. Anda akan menemukan standar harmonisasi untuk keamanan dan kinerja perangkat lunak medis.

Langkah 3: Keputusan tentang prosedur penilaian kesesuaian

- Karena Medai dapat sepenuhnya menerapkan standar yang harmonis, mereka mengikuti prosedur penilaian kesesuaian yang relevan dari peraturan perundang-undangan yang berlaku ini.

Langkah 4: Implementasi pengendalian internal

- Medai melakukan pengendalian internal yang meliputi hal-hal berikut:
- Penilaian risiko dan pengurangan risiko sesuai dengan standar yang harmonis
- Pembuatan dokumentasi teknis komprehensif yang menunjukkan bagaimana sistem AI memenuhi persyaratan
- Melakukan pengujian internal dan proses validasi untuk memastikan keamanan dan efektivitas sistem

Langkah 5: Pemasangan tanda CE

- Setelah inspeksi internal berhasil diselesaikan, Medai memasang tanda CE pada produknya, yang berarti bahwa sistem AI mematuhi peraturan Uni Eropa dan dapat dipasarkan di Uni Eropa.

Langkah 6: Peluncuran dan pemantauan pasar

- Medai membawa sistem AI ke pasar. Mereka juga berkewajiban untuk melakukan pemantauan terus-menerus untuk memastikan bahwa sistem terus memenuhi persyaratan, terutama jika ada pembaruan atau perubahan pada sistem.

Dengan menerapkan standar yang harmonis, Medai mampu menyederhanakan prosedur penilaian kesesuaian dan melaksanakannya berdasarkan kontrol internal. Hal ini memungkinkan untuk mendapatkan tanda CE dan memasarkan sistem AI berisiko tinggi di dalam Wilayah Ekonomi Eropa.

Pengecualian dari Prosedur Penilaian Kesesuaian

Pasal 46 UU AI mengatur pengecualian dari prosedur penilaian kesesuaian untuk sistem AI berisiko tinggi tertentu dalam keadaan luar biasa.

Untuk siapa dan apa yang dimaksud pasal ini?

Otoritas pengawasan pasar dapat mengizinkan penempatan di pasar atau pengoperasian sistem AI berisiko tinggi tertentu jika (Pasal 46 ayat 1 UU AI):

- terdapat alasan luar biasa untuk keselamatan publik atau perlindungan jiwa, kesehatan, lingkungan, atau fasilitas industri dan infrastruktur penting
- otorisasi ini dibatasi waktunya hingga durasi prosedur penilaian kesesuaian yang diperlukan.

Dalam kasus mendesak, penegak hukum dan otoritas perlindungan sipil dapat mengoperasikan sistem AI berisiko tinggi tertentu tanpa otorisasi sebelumnya, tetapi harus mengajukan permohonan otorisasi segera setelahnya (Pasal 46 ayat 2 UU AI).

Langkah-langkah apa yang perlu diambil?

Permohonan (Pasal 46 ayat 3 UU AI). Permohonan yang didukung dengan bukti yang memadai harus diajukan kepada otoritas pengawasan pasar jika ingin mendapatkan pengecualian dari prosedur penilaian kesesuaian.

- Prosedur persetujuan (Pasal 46 ayat 3 UU AI)
Otoritas pengawasan pasar memeriksa apakah sistem AI memenuhi persyaratan dan, jika perlu, mengeluarkan persetujuan sementara.
- Pemberitahuan dan peninjauan (Pasal 46 ayat 4 dan 5 UU AI)
Otoritas pengawasan pasar akan memberitahukan kepada Komisi dan Negara Anggota lainnya tentang setiap persetujuan yang diberikan. Keberatan dapat diajukan dalam waktu 15 hari kalender.
- Konsultasi dan pengambilan keputusan (Pasal 46 ayat 5 UU AI)
Jika terdapat keberatan, konsultasi akan diadakan antara Komisi, Negara Anggota yang bersangkutan, dan, jika berlaku, operator yang bersangkutan. Komisi kemudian memutuskan apakah otorisasi tersebut dibenarkan. Keputusan ini dikomunikasikan kepada semua pihak yang terkait.
- Pencabutan otorisasi (Pasal 46 ayat 6 UU AI)
Jika persetujuan dianggap tidak dibenarkan oleh Komisi, otoritas pengawasan pasar Negara Anggota yang memberikan persetujuan tersebut harus mencabutnya.
- Peraturan khusus untuk produk tertentu (Pasal 46 ayat 7 UU AI)
Untuk sistem AI berisiko tinggi yang terkait dengan produk yang tercakup dalam peraturan harmonisasi Uni Eropa tertentu (tercantum dalam Lampiran I Bagian A UU AI), hanya pengecualian dari prosedur penilaian kesesuaian yang ditetapkan dalam peraturan khusus tersebut yang berlaku.

Deklarasi Kesesuaian UE

Deklarasi Kesesuaian UE merupakan langkah penting untuk peluncuran sistem AI berisiko tinggi di pasar UE. Deklarasi ini berfungsi sebagai bukti bahwa sistem AI memenuhi persyaratan ketat Undang-Undang AI dan dengan demikian menjamin keselamatan publik, perlindungan kesehatan, dan hak-hak fundamental.

Penerbitan dan penyimpanan deklarasi ini dengan cermat tidak hanya memastikan kepatuhan terhadap peraturan, tetapi juga memperkuat kepercayaan terhadap keamanan dan keandalan sistem AI di pasar.

Pasal 47 Undang-Undang AI mengatur penerbitan dan penyimpanan deklarasi kesesuaian UE untuk sistem AI berisiko tinggi. Deklarasi ini merupakan bagian penting dari prosedur penilaian kesesuaian dan sangat penting bagi penyedia sistem tersebut.

Untuk siapa ini relevan?

Deklarasi kesesuaian UE sangat penting bagi penyedia sistem AI berisiko tinggi. Dengan deklarasi ini, mereka menegaskan bahwa sistem AI mereka sesuai dengan persyaratan yang ditetapkan dalam Undang-Undang AI.

Deklarasi ini merupakan dokumen kunci yang menjadi dasar otorisasi sistem AI berisiko tinggi di Wilayah Ekonomi Eropa.

Kriteria dan langkah-langkah

1. Penerbitan deklarasi (Pasal 47 ayat 1 UU AI)

- Penyedia harus menerbitkan deklarasi kesesuaian UE tertulis, yang dapat dibaca mesin, ditandatangani secara fisik atau elektronik untuk setiap sistem AI berisiko tinggi.
- Deklarasi harus disimpan selama sepuluh tahun setelah sistem dipasarkan atau dioperasikan dan tersedia bagi otoritas nasional jika diminta.

2. Isi deklarasi (Pasal 47 ayat 2 UU AI)

- Deklarasi harus mengkonfirmasi bahwa sistem AI memenuhi persyaratan khusus yang didefinisikan dalam Bagian 2 UU AI.
- Deklarasi harus memuat informasi yang tercantum dalam Lampiran V dan harus diterjemahkan ke dalam bahasa yang dapat dipahami oleh otoritas nasional Negara Anggota.

3. Peraturan Harmonisasi (Pasal 47 ayat 3 UU AI)

Jika sistem AI berisiko tinggi juga tunduk pada peraturan harmonisasi Uni Eropa lainnya yang memerlukan deklarasi kesesuaian, maka satu deklarasi kesesuaian Uni Eropa diterbitkan untuk semua peraturan yang berlaku.

4. Tanggung Jawab (Pasal 47 ayat 4 UU AI)

Dengan menerbitkan deklarasi kesesuaian Uni Eropa, penyedia bertanggung jawab atas kesesuaian sistem AI dengan persyaratan yang ditentukan. Deklarasi tersebut harus diperbarui jika perlu untuk mencerminkan status terbaru.

5. Pembaruan (Pasal 47 ayat 5 UU AI)

Komisi Eropa berwenang untuk memperbarui isi Deklarasi Kesesuaian Uni Eropa melalui tindakan delegasi untuk menyesuaikannya dengan kemajuan teknologi.

***Deklarasi Kesesuaian Uni Eropa** merupakan dokumen yang esensial untuk pemasaran dan pengoperasian sistem AI berisiko tinggi di Eropa. Dokumen ini menegaskan bahwa sistem tersebut telah memenuhi ketentuan AI Act, sehingga menjamin keselamatan serta perlindungan kesehatan dan hak-hak fundamental. Pengelolaan deklarasi ini secara cermat memastikan kepatuhan terhadap regulasi dan sekaligus meningkatkan kepercayaan terhadap keamanan serta keandalan sistem AI yang beredar di pasar.*

Deklarasi Kesesuaian Uni Eropa sangat penting untuk pengenalan sistem AI berisiko tinggi di Eropa. Deklarasi ini menegaskan kepatuhan terhadap Undang-Undang AI dan dengan demikian menjamin keamanan serta perlindungan kesehatan dan hak-hak fundamental. Penanganan yang cermat terhadap deklarasi ini memastikan kepatuhan terhadap peraturan dan meningkatkan kepercayaan terhadap keamanan dan keandalan sistem AI di pasaran.

Pendaftaran

Pasal 49 UU AI mengatur tentang kewajiban pendaftaran untuk sistem AI berisiko tinggi dalam basis data khusus Uni Eropa. Hal ini harus dilakukan sebelum peluncuran atau pengoperasiannya di pasar. Persyaratan ini sangat penting karena memastikan transparansi dan ketertelusuran untuk sistem AI berisiko tinggi di pasar tunggal Eropa. Persyaratan dan langkah-langkah berikut harus diambil oleh pihak-pihak yang terlibat:

Untuk siapa ini relevan?

Penyedia (atau perwakilan resmi mereka) dan pengimplementasikan sistem AI berisiko tinggi adalah kelompok sasaran utama dari pasal ini.

Kriteria dan langkah-langkah

1. Pendaftaran sistem AI berisiko tinggi (Pasal 49 ayat 1 UU AI)

Penyedia (atau perwakilan resmi mereka) harus mendaftarkan sistem AI berisiko tinggi mereka dalam basis data Uni Eropa sebelum memasarkannya atau mengoperasikannya, kecuali untuk sistem yang tercantum dalam Lampiran III/2 UU AI.

2. Pendaftaran untuk sistem yang tidak diklasifikasikan sebagai berisiko tinggi (Pasal 49 ayat 2 UU AI)

Jika penyedia memutuskan bahwa suatu sistem tidak memenuhi kriteria berisiko tinggi berdasarkan Pasal 6 ayat 3 UU AI, penyedia tetap harus mendaftarkannya dalam basis data Uni Eropa (Pasal 71 UU AI).

3. Pendaftaran oleh pengembang (Pasal 49 ayat 3 UU AI)

Pengembang sistem AI berisiko tinggi yang merupakan otoritas atau lembaga publik juga harus mendaftarkan diri dalam basis data Uni Eropa (Pasal 71 UU AI), kecuali untuk sistem yang tercantum dalam Lampiran II/2 UU AI.

4. Pendaftaran khusus untuk area tertentu (Pasal 49 ayat 4 UU AI)

Untuk sistem AI berisiko tinggi tertentu yang digunakan di area sensitif seperti penegakan hukum dan pengawasan perbatasan, pendaftaran dilakukan di bagian non-publik dari basis data Uni Eropa. Hanya Komisi dan otoritas nasional tertentu yang memiliki akses.

5. Pendaftaran Nasional (Pasal 49 ayat 5 UU AI)

Sistem AI berisiko tinggi yang secara khusus disebutkan dalam Lampiran III/2 UU AI harus didaftarkan di tingkat nasional.

Pentingnya pendaftaran

Pendaftaran merupakan proses penting untuk menunjukkan kepatuhan sistem AI berisiko tinggi terhadap persyaratan UU AI. Hal ini memungkinkan pengawasan pasar yang efektif oleh otoritas yang berwenang dan membantu meningkatkan kepercayaan pada sistem AI dengan memastikan bahwa sistem ini aman dan sesuai dengan hukum. Pendaftaran yang

terperinci juga membantu menjaga gambaran yang jelas tentang sistem AI berisiko tinggi di pasar Eropa dan memfasilitasi kerja sama antara Negara Anggota dan Komisi Eropa dalam hal pemantauan dan penegakan hukum.

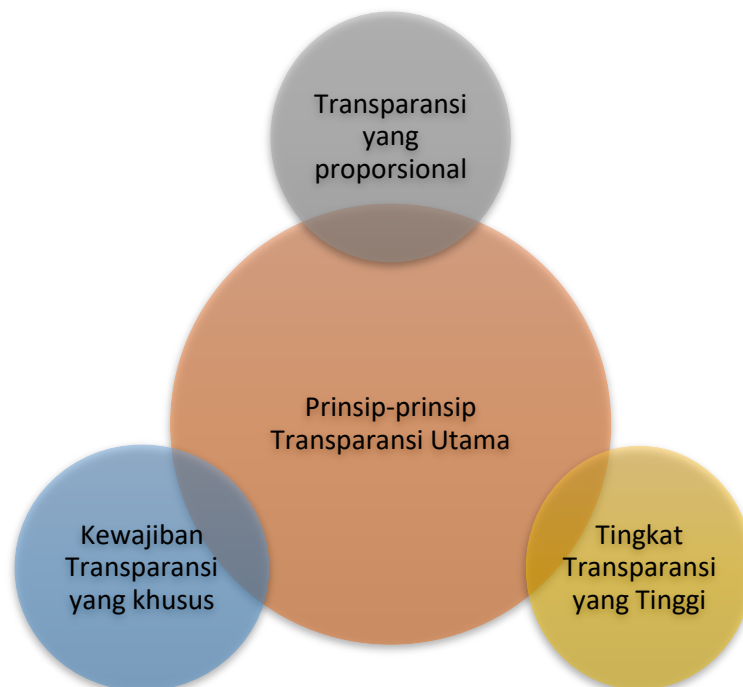
Kewajiban pendaftaran bertujuan untuk menjamin tingkat keamanan yang tinggi serta perlindungan hak-hak fundamental dengan memastikan bahwa tersedia gambaran menyeluruh mengenai seluruh sistem AI berisiko tinggi yang beredar di pasar Eropa, dan bahwa hanya sistem AI berisiko tinggi yang telah memenuhi ketentuan yang dapat ditempatkan di pasar atau mulai dioperasikan di Uni Eropa.

3.7 KEWAJIBAN TRANSPARANSI DALAM UNDANG-UNDANG AI

Undang-Undang AI memberlakukan kewajiban transparansi untuk mengurangi dampak negatif, menjaga kepercayaan publik, memastikan akuntabilitas, dan menyediakan solusi hukum yang efektif untuk menciptakan lingkungan yang saling percaya dan akuntabel bagi pengenalan dan penggunaan AI.

Dalam konteks Undang-Undang AI, **transparansi** berarti bahwa *sistem AI dikembangkan dan diterapkan dengan cara yang memungkinkan keterlacakan dan penjelasan yang memadai, membuat masyarakat menyadari bahwa mereka berkomunikasi atau berinteraksi dengan sistem AI dan memberi tahu pihak yang menerapkan tentang kemampuan dan keterbatasan sistem AI tersebut serta subjek data tentang hak-hak mereka.*

Transparansi sangat penting untuk menghindari dampak negatif, menjaga kepercayaan publik, dan memastikan akuntabilitas serta solusi yang efektif.



Gambar 3.6 Prinsip-prinsip Transparansi dalam Undang-Undang AI

Meskipun Undang-Undang AI tidak secara eksplisit menjelaskan kerangka kerja teoretis atau tipologi transparansi, undang-undang ini menetapkan persyaratan transparansi yang berbeda berdasarkan tingkat risiko dan kasus penggunaan spesifik sistem AI, yang secara efektif menggabungkan **prinsip-prinsip kewajiban transparansi yang proporsional, tingkat tinggi, dan spesifik.**

- **Prinsip transparansi yang proporsional**

Prinsip **proporsionalitas** adalah prinsip umum hukum Uni Eropa. Prinsip ini membatasi otoritas publik dalam menjalankan kekuasaan mereka dengan mengharuskan mereka untuk mencapai keseimbangan antara cara yang digunakan dan tujuan yang dikejar. Dalam konteks hak-hak fundamental, seperti hak atas perlindungan data pribadi, proporsionalitas adalah kunci untuk setiap pembatasan hak-hak ini.

Peraturan AI mensyaratkan bahwa tingkat transparansi harus proporsional dengan risiko yang ditimbulkan oleh sistem AI, yang merupakan inti dari **transparansi yang proporsional**: oleh karena itu, langkah-langkah transparansi yang proporsional harus disediakan, termasuk pembuatan dan pembaruan dokumentasi dan penyediaan informasi tentang model AI umum untuk digunakan oleh penyedia hilir.

- **Prinsip transparansi tinggi**

Model AI untuk tujuan umum yang dipublikasikan di bawah lisensi sumber terbuka dan gratis harus dipertimbangkan untuk memastikan **tingkat transparansi dan keterbukaan yang tinggi** jika parameter-parameternya, termasuk bobot, informasi arsitektur model, dan informasi penggunaan model, tersedia untuk umum (lihat Pasal 54 ayat 5 UU AI).

Untuk sistem AI yang menimbulkan risiko signifikan atau berdampak signifikan pada hak individu dan nilai-nilai masyarakat, UU AI mensyaratkan tingkat keterbukaan yang lebih tinggi. Ini termasuk dokumentasi terperinci, penjelasan yang jelas tentang kemampuan sistem AI, keterbatasannya, dan logika terkait, terutama untuk sistem yang diklasifikasikan sebagai berisiko tinggi. Hal ini memastikan bahwa para pemangku kepentingan memiliki akses ke informasi komprehensif untuk sepenuhnya menilai, meneliti, dan memahami dampak sistem AI.

- **Prinsip kewajiban transparansi khusus**

Sistem AI yang dimaksudkan untuk berinteraksi dengan orang perseorangan atau menghasilkan konten, baik yang diklasifikasikan sebagai sistem berisiko tinggi atau tidak, dapat menimbulkan risiko peniruan identitas atau penipuan tertentu. Dalam keadaan tertentu, penggunaan sistem tersebut harus tunduk pada **kewajiban transparansi khusus**, tanpa mengurangi persyaratan dan kewajiban untuk sistem AI berisiko tinggi, dengan pengecualian yang ditargetkan untuk mempertimbangkan kebutuhan khusus penegakan hukum.

Pasal 50 UU AI memperkenalkan kewajiban transparansi khusus untuk kategori AI tertentu, seperti yang berinteraksi dengan manusia atau menghasilkan konten yang dapat menyesatkan atau manipulatif. Pendekatan ini dirancang untuk mengatasi

kekhawatiran khusus yang terkait dengan berbagai aplikasi AI dan mengurangi potensi dampak negatifnya.

Semua ketentuan ini mencerminkan komitmen Uni Eropa untuk memastikan bahwa teknologi AI digunakan dengan cara yang aman, etis, dan menghormati hak asasi manusia fundamental. Pasal 6 dan seterusnya. Undang-Undang AI, yang berjudul **Persyaratan untuk sistem AI berisiko tinggi**, persyaratan transparansi diatur dalam pasal-pasal berikut:

- Pasal 10 Undang-Undang AI: **Data dan manajemen data**
- Pasal 13 Undang-Undang AI: **Transparansi dan penyediaan informasi kepada pengembang**

Selain itu, Pasal 53 Undang-Undang AI: **Kewajiban transparansi bagi penyedia dan pengguna sistem AI tertentu dan GPAI** serta informasi dari Lampiran XI Undang-Undang AI yang disebutkan dalam Pasal 53 ayat 1 Undang-Undang AI: dokumentasi teknis untuk penyedia model AI untuk tujuan umum kepada penyedia hilir yang mengintegrasikan model tersebut ke dalam sistem AI mereka.

Pedoman untuk Implementasi Kewajiban Transparansi untuk Data dan Manajemen Data

Perlindungan data dan **tata kelola data** berarti bahwa sistem AI dikembangkan dan diterapkan sesuai dengan peraturan privasi dan perlindungan data yang berlaku, memproses data yang memenuhi standar kualitas dan integritas yang tinggi.

Panduan berikut dimaksudkan untuk memberikan pendekatan terstruktur kepada penyedia sistem AI untuk mematuhi Pasal 10 Undang-Undang AI. 10 Undang-Undang AI, dengan fokus pada persyaratan data dan tata kelola data untuk sistem AI berisiko tinggi.

Tabel 3.9 Gambaran Umum Pasal 10 Undang-Undang AI

Ketentuan Pasal 10 UU AI	Tujuan Terpenting	Tindakan
Pengembangan berdasarkan kumpulan data berkualitas tinggi (ayat 1)	Menentukan apakah sistem AI dapat diklasifikasikan sebagai sistem AI berisiko tinggi sesuai dengan ketentuan Regulasi AI. Mengklasifikasikan data.	Tentukan apakah sistem AI berisiko tinggi. Klasifikasikan kumpulan data ke dalam kategori pelatihan, validasi, dan pengujian.
Praktik manajemen data yang tepat (paragraf 2)	Mengembangkan kerangka kerja manajemen data yang sesuai dengan persyaratan Pasal 10.	Tetapkan proses yang jelas untuk pengumpulan data, termasuk sumber dan tujuan awal pengumpulan data. Terapkan proses persiapan data seperti anotasi, pelabelan, pembersihan, dan agregasi yang sesuai dengan tujuan sistem AI. Evaluasi kumpulan data untuk relevansi, keterwakilan, dan akurasi sehubungan dengan tujuan sistem AI. Pastikan bahwa kumpulan data mempertimbangkan karakteristik spesifik populasi target atau konteks penggunaan.
Deteksi dan koreksi bias (paragraf 2 huruf f, 2 huruf g)	Pengenalan mekanisme untuk mendeteksi dan mengurangi bias dalam sistem AI.	Melakukan peninjauan berkala terhadap kumpulan data dan hasil AI untuk potensi bias yang dapat memengaruhi keselamatan atau hak atau menyebabkan diskriminasi.

		Menerapkan langkah-langkah yang sesuai untuk mendeteksi, menghindari, dan memperbaiki distorsi.
Relevansi dan keterwakilan kumpulan data (paragraf 3)	Memastikan kualitas dan keterwakilan data	Verifikasi bahwa kumpulan data akurat dan komprehensif. Konfirmasi bahwa kumpulan data mencerminkan tujuan penggunaan dan demografi pengguna.
Pertimbangan fitur khusus (paragraf 4)	Pertimbangkan relevansi kontekstual	Sertakan faktor geografis, kontekstual, dan perilaku yang relevan dalam kumpulan data.
Pemrosesan kategori khusus data pribadi (paragraf 5)	Pengolahan kategori data khusus dalam kondisi ketat	Menilai kebutuhan untuk memproses kategori data khusus guna mengoreksi bias. Menerapkan langkah-langkah keamanan dan perlindungan data tingkat lanjut. Memastikan kebijakan kontrol akses dan penghapusan data yang ketat. Membenarkan pemrosesan kategori data khusus dalam dokumentasi.
Penerapan pada pengembangan model non-pelatihan (paragraf 6)	Penerapan pada pengujian kumpulan data	Untuk sistem AI yang tidak berbasis pada pelatihan model, kumpulan data pengujian harus diselaraskan dengan praktik tata kelola yang telah dijelaskan.

Prinsip panduan umum untuk implementasi Pasal 10 UU AI:

- Dokumentasi terperinci dari semua langkah dan tindakan tidak hanya memastikan kepatuhan, tetapi juga berkontribusi pada transparansi dan akuntabilitas.
- Tata kelola data dan pengurangan bias adalah proses berkelanjutan. Tinjau dan perbarui praktik secara berkala untuk memastikan bahwa praktik tersebut sesuai dengan kemajuan teknologi dan perubahan persyaratan hukum.
- Para pemangku kepentingan yang relevan harus dilibatkan dalam pengembangan dan peninjauan kerangka kerja dan strategi tata kelola data untuk menghindari bias. Ini termasuk ilmuwan data, tim hukum dan kepatuhan, serta kelompok pengguna yang berpotensi terpengaruh.
- Harus dipastikan bahwa praktik tersebut tidak hanya mematuhi GDPR, tetapi juga peraturan relevan lainnya seperti GDPR. Perhatian khusus harus diberikan pada pemrosesan kategori khusus data pribadi.
- Sebelum menggunakan kategori khusus data pribadi untuk mendeteksi dan memperbaiki bias, harus diperiksa apakah tujuan yang sama dapat dicapai dengan data sintetis atau anonim.

Pedoman Pelaksanaan Ketentuan Transparansi yang Tercantum dalam Pasal 13 UU AI

Tabel 3.10 Gambaran Umum Pasal 13 UU AI

Ketentuan Pasal 13 UU AI	Tujuan Terpenting	Tindakan
Desain dan pengembangan untuk transparansi (ayat 1)	Menilai dan merancang untuk transparansi, memastikan bahwa desain dan pengembangan sistem AI berisiko tinggi mendorong transparansi.	Evaluasi cara kerja sistem untuk memastikan bahwa pihak yang menerapkan sistem tersebut memahami dan dapat menggunakan hasil sistem dengan tepat. Tentukan tingkat transparansi yang dibutuhkan berdasarkan kompleksitas sistem dan kasus penggunaannya.

Petunjuk penggunaan dalam format digital atau format lainnya (paragraf 2)	Pengembangan instruksi yang komprehensif dan mudah digunakan untuk sistem AI berisiko tinggi.	Buat petunjuk dalam format yang mudah diakses dan berisi semua informasi yang diperlukan. Pastikan bahasa yang digunakan jelas, ringkas, dan mudah dipahami oleh semua pengguna.
Isi detail petunjuk penggunaan (paragraf 3)	Memberikan informasi komprehensif tentang sistem AI untuk memastikan implementasi dan penggunaan yang tepat.	Berikan detail kontak penyedia dan, jika berlaku, perwakilan resmi. Jelaskan tujuan sistem AI, metrik kinerja, keterbatasan, dan tingkat akurasi, ketahanan, dan keamanan siber yang diharapkan. Soroti keadaan di mana kinerja sistem dapat bervariasi dan jelaskan cara teknis untuk menjelaskan kinerjanya. Tentukan spesifikasi untuk data masukan dan semua informasi yang relevan tentang kumpulan data pelatihan, validasi, dan pengujian. Catat semua perubahan yang diketahui pada kinerja sistem sejak penilaian kesesuaian pertama. Jelaskan langkah-langkah untuk pengawasan manusia dan dukungan teknis dalam menafsirkan hasil sistem AI. Berikan informasi tentang persyaratan komputer dan perangkat keras, perkiraan masa pakai sistem, dan log pemeliharaan. Jika berlaku, jelaskan mekanisme dalam sistem AI untuk merekam, menyimpan, dan menganalisis log.
Memastikan kepatuhan terhadap peraturan dan memungkinkan interpretasi oleh layanan darurat (sepanjang paragraf 3)	Memungkinkan penggunaan yang efektif dan kepatuhan terhadap peraturan.	Menyelenggarakan pelatihan bagi personel darurat tentang cara menafsirkan hasil sistem AI. Memberikan dukungan dan sumber daya untuk mengklarifikasi masalah penggunaan sistem. Memperbarui petunjuk penggunaan secara berkala untuk mencerminkan setiap perubahan atau pembaruan pada sistem.

Prinsip panduan umum untuk implementasi Pasal 13 UU AI:

- Pastikan bahwa petunjuk penggunaan dan semua informasi yang diberikan dapat diakses oleh orang-orang dengan berbagai tingkat pengetahuan teknis. Pertimbangkan penggunaan elemen multimedia atau petunjuk interaktif untuk pemahaman yang lebih baik.
- Tetapkan mekanisme untuk memperbarui informasi yang diberikan secara berkala berdasarkan umpan balik dari pengguna, kemajuan teknologi, dan perubahan peraturan.
- Simpan catatan rinci tentang semua langkah yang diambil untuk mematuhi Pasal 13 UU AI, termasuk keputusan desain, proses pengembangan, dan pembuatan petunjuk penggunaan. Dokumentasi ini sangat penting untuk menunjukkan kepatuhan kepada otoritas pengawas.

- Buat saluran untuk pertukaran berkelanjutan dengan pengguna untuk mendapatkan wawasan tentang transparansi sistem AI, kemungkinan perbaikan, dan kebutuhan klarifikasi.
- Saat memberikan informasi rinci, pastikan bahwa keamanan dan perlindungan data tidak terganggu.

Pedoman Implementasi Kewajiban Transparansi untuk Penyedia dan Pemasok Sistem AI dan Model GPAI Tertentu

Tabel 3.11 Gambaran Umum Pasal 13 UU AI 52 Undang-Undang AI

Ketentuan Pasal 52 UU AI	Tujuan Terpenting	Tindakan
Transparansi untuk interaksi langsung (ayat 1 dan 2)	Memberi informasi kepada individu	Rancang sistem AI sehingga mudah dikenali ketika pengguna berinteraksi dengan AI. Terapkan dan dokumentasikan sistem pelabelan yang dapat dibaca mesin untuk konten yang dihasilkan AI yang menunjukkan pembuatan atau manipulasi buatan.
Pengungkapan konten palsu (paragraf 4)	Memberi sinyal konten buatan	Ungkapkan jika konten dihasilkan oleh AI, terutama dalam kasus deep fake, kecuali jika itu merupakan bagian dari kegiatan legal yang diizinkan atau telah ditinjau secara editorial.
Aksesibilitas informasi (paragraf 5)	Memastikan kejelasan dan aksesibilitas	Berikan informasi yang jelas dan mudah dipahami tentang interaksi AI pada titik kontak pertama. Kepatuhan terhadap standar aksesibilitas untuk memastikan bahwa informasi tersebut dapat dipahami oleh semua pengguna.
Pengembangan kode etik (paragraf 7)	Pengembangan dan kepatuhan terhadap kode etik	Berpartisipasi dalam atau mematuhi kode etik yang telah ditetapkan untuk identifikasi dan pelabelan konten yang dihasilkan oleh AI. Berkoordinasi dengan kelompok industri atau badan pengatur yang terlibat dalam pengembangan standar ini.
Dokumentasi teknis untuk model GPAI (Lampiran XI)	Penyusunan dokumentasi komprehensif	Buat dokumentasi teknis terperinci untuk model GPAI, termasuk deskripsi model, proses pengembangan, dan data yang digunakan. Pastikan dokumentasi tersebut mudah diakses oleh penyedia hilir yang mengintegrasikan model tersebut.

Prinsip-prinsip panduan umum untuk implementasi Pasal 50 UU AI:

- Secara teratur memperoleh umpan balik dari pengguna dan pengembang untuk meningkatkan praktik transparansi dan menyesuaikannya jika perlu.
- Secara teratur meninjau pembaruan UU AI dan standar serta kode etik terkait untuk memastikan kepatuhan berkelanjutan.

- Berkolaborasi dengan kelompok industri, regulator, dan organisasi standar untuk berkontribusi atau tetap mendapatkan informasi tentang praktik terbaik untuk transparansi AI.
- Melatih karyawan dan pemangku kepentingan tentang pentingnya transparansi dalam penerapan AI dan cara menerapkan persyaratan ini secara efektif.
- Memelihara catatan lengkap tentang upaya kepatuhan, termasuk keputusan desain yang dibuat untuk memberi tahu pengguna tentang interaksi AI, upaya untuk memberi label pada konten yang dihasilkan AI, dan dokumentasi teknis model GPAI yang dibuat untuk model GPAI.

3.8 KECERDASAN BUATAN SERBAGUNA (GPAI)

Usulan Peraturan yang menetapkan aturan harmonisasi tentang kecerdasan buatan (**usulan Undang-Undang AI** atau **draf pertama**) diterbitkan pada 21 April 2021. Meningkatnya kehadiran aplikasi AI generatif seperti ChatGPT & Co membalikkan jadwal bagi legislator Eropa. Legislator belum mempertimbangkan peraturan untuk apa yang disebut "*model AI serbaguna*" (GPAI) dalam draf pertama.

Kebutuhan akan peraturan terpisah menjadi jelas selama proses legislatif. Namun, para legislator tidak sepakat untuk waktu yang lama dalam negosiasi tentang tingkat peraturan yang diperlukan, sehingga model AI serbaguna baru kemudian dimasukkan dalam Undang-Undang AI. Bagian ini membahas lebih detail tentang model dan sistem AI serbaguna dalam arti Undang-Undang AI.

ChatGPT: Awal dari "revolusi AI"? – Implikasi bagi Proses Legislatif

Pada tanggal 30 November 2022, Open AI merilis chatbot ChatGPT dan menimbulkan kehebohan yang luar biasa – lebih dari hampir semua teknologi lainnya. Perusahaan itu sendiri sebelumnya mengklasifikasikan ChatGPT secara internal sebagai *pratinjau penelitian ambang batas rendah*. Namun, kisah sukses seputar penggunaan ChatGPT datang bertubi-tubi: ChatGPT lulus ujian pengacara Amerika, "Matura" Austria atau "Abitur" Jerman (keduanya merupakan ujian akhir di sekolah menengah atas), atau menciptakan preseden dalam hukum kasus Anglo-Amerika yang digunakan pengacara dalam kasus pengadilan yang sedang berlangsung.

Aplikasi AI telah ada selama bertahun-tahun. Namun, publikasi ChatGPT pada akhir tahun 2022 membantu sistem bantuan AI mendapatkan visibilitas, membuatnya lebih mudah diakses oleh masyarakat umum dan dengan demikian menandai *tonggak penting dalam penerimaan sosial solusi AI*.

Sampai batas tertentu, *kecerdasan buatan* dalam arti luas telah dikomersialkan dengan bantuan ChatGPT, sehingga menurut pendapat saya istilah "kecerdasan buatan" sekarang digunakan hampir secara berlebihan dalam bahasa sehari-hari. Teknologi yang mendasari ChatGPT adalah bidang khusus kecerdasan buatan: Model Bahasa Besar (LLM), yang merupakan bidang khusus dalam AI generatif.

Apa kata ChatGPT?

“**ChatGPT dan sistem** serupa memang telah berkontribusi pada **popularisasi dan penggunaan komersial** kecerdasan buatan (AI). Perkembangan ini telah membawa istilah “kecerdasan buatan” lebih ke depan dalam bahasa sehari-hari. Namun, penting untuk dipahami bahwa **ChatGPT adalah contoh AI terapan di bidang khusus**, yaitu pemahaman bahasa alami dan pembangkitan ucapan. Teknologi yang mendasarinya, **pembelajaran mesin (pembelajaran mendalam)**, hanyalah satu aspek dari **lanskap penelitian dan aplikasi AI yang luas dan beragam**. Perhatian dan aplikasi yang luas dari sistem tersebut [dapat] **menyebabkan penggunaan istilah yang berlebihan, tetapi juga harus dilihat sebagai peluang untuk meningkatkan kesadaran akan kedalaman dan kompleksitas bidang ini.**”

Open AI, ChatGPT Plus, Versi 4.0 (2023), ditanyakan pada 10.03.2024 (dalam bahasa Jerman), pertanyaan pertama: “Menurut pendapat saya, “kecerdasan buatan” dalam arti luas telah dikomersialkan dengan bantuan ChatGPT, sehingga istilah kecerdasan buatan digunakan hampir secara berlebihan dalam bahasa sehari-hari. Namun, teknologi yang mendasari ChatGPT adalah bidang khusus dari kecerdasan buatan. Ringkaslah sudut pandang Anda secara singkat.”

ChatGPT: Menanggapi permintaan untuk mengkaji secara kritis pernyataan sebelumnya.

“Pernyataan tersebut dapat dilihat secara kritis dari beberapa perspektif:

1. **Definisi dan pemahaman tentang AI:** AI adalah bidang luas yang mencakup banyak teknologi dan pendekatan berbeda, dari algoritma sederhana hingga jaringan saraf kompleks. Fakta bahwa ChatGPT dan teknologi serupa telah dipopulerkan sebenarnya dapat **berkontribusi pada peningkatan minat publik dan pemahaman tentang AI**. Alih-alih penggunaan yang berlebihan, dapat dikatakan bahwa peningkatan kehadiran AI dalam kehidupan sehari-hari mendorong diskusi yang lebih tepat dan terdiferensiasi tentang berbagai aspek AI.
2. **Komersialisasi dan aksesibilitas:** [...] teknologi AI seperti ChatGPT telah memperluas akses ke alat-alat canggih ini dan memungkinkan tidak hanya perusahaan tetapi juga individu untuk mendapatkan manfaat dari aplikasi bertenaga AI. Ini dapat dilihat sebagai demokratisasi teknologi AI [...]
3. **Mendorong inovasi:** Karena [...] minat yang luas terhadap teknologi AI [...], penelitian dan pengembangan di bidang AI didorong maju. Hal ini menyebabkan siklus inovasi yang lebih cepat, teknologi yang lebih baik, dan kasus penggunaan baru yang mungkin tidak akan tercapai tanpa popularisasi dan dukungan finansial melalui kesuksesan komersial.
4. **Tanggung jawab dan etika:** Pandangan kritis juga harus mencakup aspek etika. dan tanggung jawab dalam menangani teknologi AI. Popularisasi AI menimbulkan pertanyaan tentang perlindungan data, potensi penyalahgunaan, dan dampaknya terhadap pasar tenaga kerja. [...]

*Singkatnya, popularisasi AI melalui teknologi seperti ChatGPT memiliki **aspek positif dan menantang**. Tinjauan kritis harus mempertimbangkan berbagai implikasi dari perkembangan ini dan mempertimbangkan baik peluang maupun risiko untuk mempromosikan pendekatan yang bertanggung jawab terhadap AI.”*

Inklusi GPAI dalam Undang-Undang AI

Usulan Regulasi AI diterbitkan pada 21 April 2021, sebelum kehebohan seputar AI generatif. Mengingat perkembangan teknologi yang pesat sejak saat itu, versi pertama Regulasi AI segera dianggap ketinggalan zaman.

Seperti yang telah disebutkan di awal, keberhasilan LLM membuat regulasi terpisah menjadi perlu dan terdapat perbedaan pendapat yang besar, karena pembuat undang-undang tidak ingin mempersulit inovasi di satu sisi, tetapi di sisi lain ingin menangkal risiko yang diketahui, seperti pengungkapan rahasia dagang atau data pribadi. Dengan pengumuman kesepakatan politik pada 9 Desember 2023 (siaran pers), diumumkan untuk pertama kalinya bahwa untuk model AI tujuan umum (**general-purpose AI atau general-purpose Artificial Intelligence models atau model GPAI singkatnya**) akan diperkenalkan regulasi khusus dengan tujuan menciptakan transparansi di sepanjang rantai nilai (*AI Value Chain*). Pengenalan pendekatan dua tahap untuk GPAI juga diumumkan.

Pada tahap akhir, definisi model dan sistem GPAI, kewajiban lebih lanjut, khususnya kewajiban transparansi, sebenarnya dimasukkan ke dalam Undang-Undang AI. Karakteristik klasifikasi spesifik GPAI disajikan bersama dengan kewajiban terkait. Untuk model berkinerja sangat tinggi yang dapat menimbulkan risiko sistemik (model GPAI dengan risiko sistemik), terdapat kewajiban mengikat tambahan terkait manajemen risiko, pemantauan insiden serius, evaluasi model, dan uji serangan.

AI Generatif dan Model Bahasa Besar

AI Analitik & AI Generatif

Solusi AI di bidang kecerdasan buatan analitik telah banyak dicoba dan diuji. Teknologi AI yang matang meliputi analisis data, solusi intelijen bisnis (untuk pembuatan visualisasi, dasbor, storyboard secara otomatis), deteksi anomali, pemeriksaan kualitas data, validasi data, dan deteksi penipuan. Model klasifikasi, misalnya untuk tujuan mengenali dan mengkategorikan data numerik, teks, atau gambar, juga termasuk.

AI analitik berbeda dengan AI generatif. Jenis kecerdasan buatan ini digunakan untuk menghasilkan konten. Model Bahasa Besar (LLM) untuk membuat teks (misalnya ChatGPT atau Google Gemini [sebelumnya Google Bard]), model untuk menghasilkan gambar (teks ke gambar), format audio, atau video adalah contohnya.

Model Bahasa Besar (LLM)

Model bahasa besar adalah salah satu bentuk AI. Sistem yang terkenal antara lain GPT-4 (seri Generative Pre-Trained Transformer yang dikembangkan oleh OpenAI) dan aplikasi ChatGPT yang berbasis padanya, PaLM 2 (Google), LLaMA 2 (Meta), Tongyi Qianwen 2.0 (Alibaba) dan Luminous (Aleph Alpha).

LLM dapat melakukan melalui perhitungan statistik apa yang dapat dilakukan manusia secara linguistik melalui semantik dan pemahaman kausalitas. Mereka mengenali pola dalam data bahasa atau teks dan memanfaatkannya dengan bantuan perhitungan probabilitas. Mereka semakin banyak digunakan di bidang pemrosesan bahasa alami (NLP). Di sini, LLM memberikan hasil yang luar biasa, sebagian karena jumlah data yang sangat besar yang telah digunakan untuk melatih model-model ini. Hal ini memungkinkan sistem untuk menghasilkan konten yang tampak seperti ditulis oleh manusia.

Model AI dan Sistem AI untuk Penggunaan Umum

Aturan Klasifikasi untuk Model GPAI

Model GPAI didefinisikan dalam Pasal 3 No. 63 UU AI:

Model AI Serbaguna sesuai dengan Pasal 3 No. 63 UU AI

Model AI Serbaguna berarti model AI, termasuk yang dilatih dengan sejumlah besar data menggunakan pengawasan mandiri dalam skala besar, yang menunjukkan generalitas yang signifikan dan mampu secara kompeten melakukan berbagai tugas yang berbeda terlepas dari cara model tersebut dipasarkan dan yang dapat diintegrasikan ke dalam berbagai sistem atau aplikasi hilir, kecuali model AI yang digunakan untuk kegiatan penelitian, pengembangan, atau pembuatan prototipe sebelum dipasarkan (Pasal 3 No. 63 UU AI).

Definisi ini terbatas pada karakteristik fungsional penting dari model GPAI:

- I. Kegunaan umum
- II. Kemampuan untuk melakukan berbagai tugas yang berbeda (lihat Pasal 97 UU AI)

Biasanya, model GPAI dilatih menggunakan sejumlah besar data dengan berbagai metode, misalnya:

- I. Pembelajaran mandiri (self-supervised learning)
- II. Pembelajaran tanpa pengawasan (unsupervised learning)
- III. Pembelajaran penguatan (reinforcement learning) (lihat Pasal 97 UU AI)

Model ini dapat dipasarkan dengan berbagai cara:

- I. di perpustakaan
- II. melalui antarmuka pemrograman aplikasi (API)
- III. melalui unduhan langsung
- IV. sebagai salinan fisik (lihat Pasal 97 UU AI)

Model-model tersebut dapat dimodifikasi atau disempurnakan menjadi model-model baru. Istilah model GPAI harus didefinisikan dan dibedakan secara jelas dari istilah sistem AI untuk menciptakan kepastian hukum (Pertimbangan 97 UU AI). Model AI generatif besar untuk menghasilkan konten (teks, audio, gambar, video) adalah contoh tipikal model GPAI (Pertimbangan 99 UU AI).

Definisi: Sistem AI Serbaguna

Sistem AI serbaguna (“Sistem AI serbaguna”) *berarti sistem AI yang didasarkan pada model AI serbaguna dan memiliki kemampuan untuk melayani berbagai tujuan, baik untuk penggunaan langsung maupun untuk integrasi dalam sistem AI lainnya* (lihat Pasal 3 No. 66 UU AI).

Model AI merupakan komponen dari sistem AI, tetapi bukan merupakan sistem AI itu sendiri. Hal ini memerlukan komponen tambahan (misalnya, antarmuka pengguna). Bagaimanapun, peraturan untuk GPAI berlaku terlepas dari apakah model tersebut terintegrasi ke dalam sistem AI atau tidak.

Kewajiban berlaku bagi penyedia segera setelah model GPAI diluncurkan di pasar. Jika penyedia model GPAI mengintegrasikannya ke dalam sistem AI miliknya sendiri dan membuatnya tersedia di pasar atau mengoperasikannya, kewajiban GPAI juga berlaku di samping kewajiban sistem AI (Pertimbangan 97 UU AI).

PENGECUALIAN: Optimalisasi Proses Internal Semata

Apabila suatu model AI tujuan umum (General-Purpose AI/GPAI) yang terpisah digunakan semata-mata untuk proses internal, maka kewajiban yang dimaksud tidak berlaku. Hal yang sama berlaku bagi model AI yang digunakan secara eksklusif untuk tujuan **penelitian, pengembangan, dan pembuatan prototipe sebelum model tersebut ditempatkan di pasar** (Pertimbangan 97 AI Act; Pasal 3 angka 63 AI Act).

Pasal 25 ayat 1 huruf c UU AI (tanggung jawab AI di sepanjang rantai nilai AI) telah dilengkapi sehingga GPAI terikat pada pendekatan berbasis risiko UU AI. Penyedia sistem tersebut wajib memberikan kepada penyedia hilir (*downstream providers*) sistem AI berisiko tinggi semua informasi dan elemen (Pasal 25 ayat 1 huruf c UU AI, Pasal 53 ayat 1 huruf b UU AI, Pertimbangan 101 UU AI, Lampiran XII UU AI).

Penyedia Hilir (Downstream Providers)

Penyedia suatu sistem AI, termasuk sistem AI tujuan umum, yang mengintegrasikan suatu model AI, terlepas dari apakah model AI tersebut disediakan oleh dirinya sendiri dan terintegrasi secara vertikal, atau disediakan oleh entitas lain berdasarkan hubungan kontraktual (Pasal 3 angka 68 AI Act).

Jika model GPAI diintegrasikan ke dalam sistem AI atau merupakan bagian dari sistem AI, sistem ini harus dianggap sebagai sistem GPAI jika dapat digunakan untuk berbagai tujuan karena integrasi ini. Sistem GPAI dapat digunakan secara langsung atau diintegrasikan ke dalam sistem AI lainnya (Pertimbangan 100 UU AI).

Komitmen

Komitmen untuk semua model GPAI dan model GPAI dengan risiko sistemik telah dimasukkan dalam perjanjian kompromi untuk pertama kalinya, seperti mengevaluasi model,

melakukan penilaian risiko, mengambil langkah-langkah mitigasi risiko, memastikan tingkat perlindungan keamanan siber yang memadai, dan melaporkan insiden serius kepada Kantor Kecerdasan Buatan dan otoritas nasional yang berwenang. **Kewajiban terpenting** bagi semua penyedia *model AI tujuan umum* adalah sebagai berikut dalam versi final Undang-Undang AI:

- **Persiapan dan pembaruan dokumentasi teknis yang tercantum dalam** Lampiran XI (Pasal 53 ayat 1 huruf a Undang-Undang AI)
- Kewajiban untuk menyediakan dokumentasi tersebut kepada **Kantor Kecerdasan Buatan Eropa (Kantor AI)** dan otoritas nasional yang berwenang **atas permintaan** (Pasal 53 ayat 1 huruf a Undang-Undang AI)
- Penyediaan informasi dan dokumentasi tertentu (kemampuan dan keterbatasan model AI dan Lampiran VII) kepada **penyedia hilir** untuk tujuan kepatuhan terhadap Undang-Undang AI (Pasal 53 ayat 1 huruf b Undang-Undang AI)
- Kepatuhan terhadap **hukum hak cipta “UE”** (Pasal 53 ayat 1 huruf c Undang-Undang AI)
- **Penyebaran ringkasan rinci tentang konten yang digunakan** (Pasal 53 ayat 1 huruf d Undang-Undang AI)

Kewajiban-kewajiban tersebut di atas tidak berlaku untuk penyedia model AI yang disediakan di bawah lisensi bebas dan terbuka. Pengecualian ini tidak berlaku untuk model AI tujuan umum dengan risiko sistemik (lihat Pasal 52 ayat 2 UU AI). Komisi Uni Eropa berwenang untuk mengubah lampiran melalui tindakan delegasi (perubahan perkembangan teknologi) (Pertimbangan 101 UU AI, Pasal 97 ayat 2 UU AI).

Kewajiban dalam UU AI pada dasarnya bergantung pada peran pihak yang berkewajiban. Sebagian besar kewajiban dalam Peraturan AI berlaku untuk penyedia.

Penyedia (Provider)

Penyedia adalah orang perseorangan atau badan hukum, otoritas publik, lembaga, atau badan lainnya yang:

- **mengembangkan** atau meminta **dikembangkannya suatu sistem AI atau model AI tujuan umum**; dan
- menempatkannya atas **nama** atau **merek dagangnya** sendiri; serta
 - **menempatkannya di pasar** atau mulai **mengoperasikannya**;
 - tanpa memandang apakah hal tersebut dilakukan dengan imbalan atau tanpa imbalan (lihat Pasal 3 angka 3 AI Act).

Distributor, importir, penyebar, atau pihak ketiga lainnya dianggap sebagai penyedia sistem AI berisiko tinggi jika mereka mengubah tujuan penggunaan sistem AI yang tidak diklasifikasikan sebagai berisiko tinggi dan telah dipasarkan atau dioperasikan, termasuk sistem AI *tujuan umum*, sedemikian rupa sehingga sistem AI tersebut menjadi sistem AI berisiko tinggi sesuai dengan Pasal 6 UU AI (Pasal 25 ayat 1 huruf c UU AI).

Penyedia model AI tujuan umum memiliki peran dan tanggung jawab khusus di sepanjang rantai nilai AI: model yang mereka sediakan dapat menjadi dasar bagi sejumlah

sistem hilir, yang seringkali disediakan oleh **penyedia** hilir. Hal ini membutuhkan pemahaman yang baik tentang model dan kemampuannya untuk memungkinkan integrasi model tersebut ke dalam produk mereka dan untuk memenuhi kewajiban mereka (Pertimbangan 101 UU AI).

Model GPAI dengan Risiko Sistemik

Untuk model berkinerja tinggi dengan efek sistemik (“model sistemik”), terdapat persyaratan tambahan. Karena risiko sistemik muncul dari kemampuan yang sangat tinggi, model GPAI harus dianggap menimbulkan risiko sistemik jika memiliki kemampuan berdampak tinggi atau memiliki dampak signifikan pada pasar internal karena cakupannya. Hal ini harus dinilai berdasarkan alat dan metodologi teknis yang sesuai. Rentang penuh kemampuan suatu model dapat dipahami lebih baik setelah dirilis ke pasar atau ketika pengguna berinteraksi dengan model tersebut (Pertimbangan 111 Undang-Undang AI).

Aturan Klasifikasi untuk Model AI Tujuan Umum dengan Risiko Sistemik menurut Pasal 51 Undang-Undang AI

Menurut Komisi Uni Eropa, “kemampuan berdampak tinggi” dianggap ada jika upaya komputasi kumulatif untuk pelatihannya, yang diukur dalam operasi floating point (FLOPs), lebih besar dari 10^{25} (Pasal 51 ayat 2 Undang-Undang AI).

“Operasi titik mengambang” atau “FLOP” (floating-point operation) menggambarkan setiap operasi aritmatika atau setiap penugasan dengan bilangan titik mengambang, yang merupakan himpunan bagian dari bilangan riil yang biasanya direpresentasikan pada komputer dengan hasil perkalian bilangan bulat dengan presisi tetap dan basis tetap dengan eksponen bilangan bulat (Pasal 3 no 67 UU AI).

Dari sudut pandang Uni Eropa, 10^{25} FLOP adalah nilai ambang batas yang sesuai:

- Ambang batas yang disebutkan mencakup model GPAI paling canggih saat ini, yaitu GPT-4 dari OpenAI dan mungkin Gemini dari Google DeepMind. Kemampuan model di atas ambang batas ini belum cukup diketahui. Mereka dapat menimbulkan risiko sistemik dan oleh karena itu masuk akal untuk mengenakan kewajiban tambahan kepada penyedia. Undang-Undang AI dapat diubah untuk memperbarui ambang batas FLOP (melalui tindakan delegasi sesuai dengan Pasal 97 Undang-Undang AI).
- Komisi Uni Eropa berkewajiban untuk menyesuaikan ambang batas, dengan mempertimbangkan perkembangan teknologi dan kemampuan model GPAI paling canggih untuk mengikuti perkembangan teknologi terkini, misalnya:
 - peningkatan algoritma atau
 - peningkatan efisiensi perangkat keras (Pasal 51 ayat 3 Undang-Undang AI)

Kewajiban untuk Model GPAI dengan Risiko Sistemik berdasarkan Pasal 55

Penyedia model AI tujuan umum dengan risiko sistemik dapat mengandalkan kode etik hingga standar yang harmonis diterbitkan (Pasal 55 ayat 2 UU AI). Kode etik diatur dalam Pasal 56 UU AI dan Bab 10 (Pasal 95 dan 96 UU AI).

Model GPAI dan Sistem Berisiko Tinggi

Sistem AI tujuan umum didefinisikan sebagai sistem AI yang berbasis pada model GPAI dan dapat digunakan untuk berbagai tujuan. Sistem GPAI itu sendiri dapat diklasifikasikan sebagai sistem AI berisiko tinggi atau bertindak sebagai bagian dari sistem tersebut

(Pertimbangan 85 UU AI). Penyedia sistem GPAI tersebut wajib menyediakan semua informasi dan elemen kepada penyedia sistem AI berisiko tinggi di hilir agar mereka dapat memenuhi persyaratan yang relevan (termasuk penilaian kesesuaian; Pertimbangan 86 Peraturan AI, Pasal 25 ayat 1 huruf c UU AI). Pasal 25 mencakup ketentuan untuk menyelaraskannya dengan pendekatan berbasis risiko dari Peraturan AI (lihat Pasal 25 ayat 1 huruf c UU AI).

Jika sistem AI tujuan umum yang dapat digunakan langsung oleh penyebar untuk setidaknya satu tujuan diklasifikasikan sebagai berisiko tinggi, otoritas pengawasan pasar harus bekerja sama dengan Kantor AI untuk melakukan penilaian kesesuaian dan memberi tahu Komite dan otoritas pengawasan pasar lainnya (Pertimbangan 161 UU AI, Pasal 75 ayat 2 UU AI).

Periode Implementasi dan Sanksi

Batas waktu transisi dalam Undang-Undang AI dilakukan secara bertahap. Ketentuan yang berkaitan dengan model dan sistem GPAI berlaku hingga 2 Agustus 2025 (Pasal 113 huruf b Undang-Undang AI, Pertimbangan 179 Undang-Undang AI). Untuk sistem AI yang sudah dipasarkan atau dioperasikan, batas waktu transisi 2 Agustus 2027 berlaku sesuai dengan Pasal 111 ayat 3 Undang-Undang AI.

Pasal 101 Undang-Undang AI menetapkan denda bagi penyedia model AI tujuan umum jika terjadi pelanggaran kewajiban atau ketidakpatuhan terhadap tindakan penegakan hukum. Komisi Eropa dapat mengenakan denda kepada penyedia model AI tujuan umum hingga 3% dari total omset tahunan mereka di seluruh dunia pada tahun keuangan sebelumnya atau Rp. 150.000.000.000 (lihat Pasal 101 ayat 1 Undang-Undang AI). **Jumlah maksimum denda telah diselaraskan dengan jumlah denda untuk penyedia sistem AI berisiko tinggi** (lihat Pasal 99 ayat 4 Undang-Undang AI). Terdapat masa tenggang tambahan bagi penyedia model AI untuk tujuan umum, karena tidak ada denda yang dapat dikenakan pada tahun pertama setelah ketentuan tersebut berlaku (Pasal 113 huruf b UU AI)

3.9 SANDBOX AI

UU AI seharusnya tidak memperlambat atau mencegah **ide, pengembangan, atau teknologi inovatif** meskipun tingkat regulasi AI sudah tinggi. Untuk memperkuat dan mempromosikan inovasi, dibuatlah apa yang disebut "sandbox regulasi". Sandbox ini dimaksudkan untuk menyediakan lingkungan terkontrol di mana sistem AI inovatif dapat dikembangkan, diuji, atau divalidasi untuk jangka waktu terbatas sebelum dipasarkan atau dioperasikan. Sandbox juga dapat mencakup pengujian di dunia nyata, yang dipantau di dalam sandbox.

Pasal 57 dan seterusnya UU AI mengatur sandbox AI. Menurut definisi dalam Pasal 3 ayat 55 UU AI, ini adalah kerangka kerja terkontrol yang dibuat oleh otoritas yang berwenang yang memberi penyedia atau calon penyedia sistem AI kesempatan untuk mengembangkan, melatih, memvalidasi, dan menguji sistem AI inovatif untuk jangka waktu terbatas di bawah pengawasan resmi dan, jika perlu, dalam kondisi dunia nyata sesuai dengan apa yang disebut **rencana pengujian dunia nyata**. Penyedia dan otoritas yang berwenang menyepakati rencana sandbox tersebut. Ini menjelaskan tujuan, kondisi, kerangka waktu, metode, dan persyaratan

untuk kegiatan yang akan dilakukan di dalam sandbox. Rencana pengujian dunia nyata, di sisi lain, adalah dokumen yang menjelaskan tujuan, metodologi, cakupan geografis, terkait populasi, dan temporal, serta pemantauan, pengorganisasian, dan implementasi pengujian dalam kondisi dunia nyata sesuai dengan Pasal 3 ayat 53 UU AI.

Pengaturan dan Fungsionalitas

Setiap Negara Anggota harus memiliki **setidaknya satu sandbox AI di tingkat nasional**, yang harus beroperasi 24 bulan setelah UU AI mulai berlaku, yaitu paling lambat tanggal 2 Agustus 2026. Namun, sandbox ini dapat dioperasikan oleh satu atau lebih Negara Anggota Uni Eropa lainnya. Komisi Uni Eropa dapat memberikan dukungan teknis, saran, atau alat untuk pengenalan atau pengoperasian sandbox. Laboratorium nyata tambahan dapat didirikan di tingkat regional atau lokal atau bersama dengan otoritas dari Negara Anggota lainnya. Negara Anggota harus memastikan bahwa otoritas tersebut diberikan sumber daya yang sesuai tepat waktu untuk mengoperasikan laboratorium nyata tersebut. Otoritas juga dapat mengoperasikan sandbox secara bersama-sama, sehingga dapat dibayangkan bahwa otoritas AI yang berwenang dapat mengoperasikan sandbox bersama dengan otoritas perlindungan data yang berwenang.

Untuk menggunakan sandbox, penyedia harus menyepakati rencana sandbox dengan otoritas yang berwenang. Otoritas tersebut, jika perlu, dapat memberikan panduan, pemantauan, dan dukungan untuk mengidentifikasi risiko yang terkait dengan hak-hak fundamental, kesehatan, dan keselamatan. Otoritas tersebut juga harus memberikan dukungan terkait proses pengujian, langkah-langkah pengurangan risiko, dan efektivitasnya sehubungan dengan kewajiban dan persyaratan Undang-Undang AI.

Otoritas yang berwenang juga harus membimbing penyedia dan calon penyedia sistem AI terkait harapan regulasi dan bagaimana mereka harus memenuhi persyaratan dan kewajiban Undang-Undang AI. Atas permintaan penyedia, otoritas harus mengeluarkan **konfirmasi tertulis** tentang kegiatan yang berhasil dilakukan di sandbox. Dalam hal apa pun, otoritas harus mengeluarkan laporan yang menjelaskan kegiatan yang dilakukan, termasuk hasil dan pengalaman pembelajaran. Dokumentasi ini dapat digunakan oleh penyedia untuk menunjukkan kepatuhan terhadap Undang-Undang AI dalam prosedur penilaian kesesuaian atau prosedur pengawasan pasar lainnya. Oleh karena itu, otoritas atau badan yang diberi wewenang harus dilibatkan secara positif dalam penilaian sejauh yang wajar. Laporan akhir dapat diperiksa oleh Komisi Uni Eropa, dan jika otoritas dan penyedia setuju, laporan tersebut juga dapat dipublikasikan. Pembentukan sandbox bertujuan untuk mencapai **tujuan-tujuan** berikut:

- Meningkatkan kepastian hukum terkait kepatuhan terhadap Undang-Undang AI atau, jika berlaku, undang-undang Uni Eropa atau Negara Anggota lainnya
- Mendukung dengan berbagi praktik terbaik melalui kerja sama dengan otoritas
- Mendorong inovasi dan persaingan serta memungkinkan pengembangan ekosistem AI
- Berkontribusi pada pembelajaran berbasis bukti di bidang regulasi
- Memungkinkan dan mempercepat akses sistem AI ke pasar Eropa, khususnya untuk UKM dan perusahaan rintisan

Jika sistem AI memproses data pribadi, otoritas AI yang berwenang harus memastikan bahwa otoritas perlindungan data terlibat dalam pengoperasian sandbox. Penggunaan sandbox tidak memengaruhi wewenang otoritas lainnya. Risiko signifikan terhadap kesehatan, keselamatan, dan hak-hak mendasar yang teridentifikasi selama pengembangan atau pengujian sistem AI harus dimitigasi melalui langkah-langkah pengurangan risiko. Jika hal ini tidak memungkinkan, otoritas dapat menangguhkan operasi di lingkungan uji coba (sandbox) untuk jangka waktu tertentu atau secara permanen.

Penyedia atau calon penyedia tetap **bertanggung jawab atas kerusakan yang terjadi pada pihak ketiga** selama eksperimen di dalam sandbox. Namun, jika mereka mematuhi rencana dan ketentuan partisipasi mereka serta mengikuti instruksi otoritas dengan itikad baik, tidak ada sanksi administratif yang dapat dikenakan. Hal ini juga berlaku untuk otoritas lain yang terlibat dalam sandbox.

Otoritas nasional memberi tahu Kantor AI dan dewan pengurusnya untuk mendirikan sandbox dan dapat meminta dukungan. Daftar laboratorium dunia nyata yang direncanakan tersedia untuk umum di Kantor AI untuk mempromosikan interaksi dan kerja sama lintas batas.

Otoritas nasional juga melaporkan kepada Kantor AI dan dewan pengurusnya setiap tahun, dimulai satu tahun setelah pendirian sandbox dan selanjutnya selama sandbox beroperasi. Laporan tersebut mencakup kemajuan dan hasil implementasi sandbox, termasuk praktik terbaik, insiden, pelajaran yang dipetik, dan rekomendasi untuk mendirikan sandbox.

Komisi Uni Eropa sedang mengembangkan antarmuka dengan informasi tentang laboratorium dunia nyata untuk memungkinkan para pemangku kepentingan berinteraksi dengan laboratorium dunia nyata. Mereka juga dapat mengajukan keberatan kepada pihak berwenang untuk mendapatkan panduan yang tidak mengikat tentang kepatuhan produk, layanan, dan model bisnis inovatif yang menggabungkan teknologi AI.

Spesifikasi konkret untuk fungsionalitas dan mode operasi sandbox diatur dalam Pasal 58 Undang-Undang AI untuk memastikan keseragaman di dalam Uni Eropa. Untuk tujuan ini, Komisi Uni Eropa mengeluarkan **peraturan** perundang-undangan yang mengatur pendirian, pengembangan, implementasi, pengoperasian, dan pemantauan laboratorium nyata. Peraturan perundang-undangan tersebut menerapkan prinsip-prinsip berikut:

- Kelayakan dan seleksi untuk partisipasi dalam sandbox
- Prosedur untuk aplikasi, partisipasi, pemantauan, dan penghentian sandbox, rencana sandbox, dan laporan akhir
- Syarat partisipasi bagi pelamar

Peraturan perundang-undangan ini dimaksudkan untuk memastikan bahwa sandbox terbuka untuk semua calon penyedia, asalkan mereka memenuhi persyaratan kelayakan dan partisipasi. Persyaratan ini harus transparan dan adil. Otoritas yang menawarkan sandbox harus memberi tahu pelamar tentang keputusan atas aplikasi tersebut dalam waktu tiga bulan. Laboratorium dunia nyata harus memungkinkan akses yang luas dan setara serta memenuhi permintaan. Para pelamar juga dapat mengajukan permohonan dalam kemitraan dengan pengguna dan pihak ketiga lainnya. Tata cara dan persyaratan partisipasi harus dijaga sefleksibel mungkin. Akses ke sandbox gratis untuk UKM dan perusahaan rintisan, tetapi

otoritas dapat meminta biaya luar biasa dengan cara yang adil dan proporsional. Undang-undang ini dimaksudkan untuk memungkinkan calon penyedia menggunakan hasil pembelajaran untuk kewajiban yang berkaitan dengan penilaian kesesuaian atau aplikasi sukarela untuk standar industri sesuai dengan Pasal 95 UU AI. Laboratorium dunia nyata juga harus dapat digunakan untuk melibatkan operator relevan lainnya dalam ekosistem AI, seperti badan yang diberi wewenang atau lembaga standardisasi. UKM, perusahaan rintisan, perusahaan, inovator, fasilitas pengujian dan eksperimental, penelitian, laboratorium, pusat inovasi digital, pusat kompetensi, atau peneliti juga harus diberikan akses. Prosedur, proses, dan persyaratan administratif untuk aplikasi, seleksi, partisipasi, dan penghentian partisipasi dalam sandbox harus sederhana, mudah dipahami, dan dikomunikasikan dengan jelas sehingga UKM dan perusahaan rintisan dengan sumber daya hukum dan administratif yang terbatas pun dapat dengan mudah memahaminya. Persyaratan ini akan seragam di seluruh Eropa untuk mencegah fragmentasi dan memastikan bahwa partisipasi diakui secara setara di Uni Eropa dan memiliki efek hukum yang sama. Partisipasi dalam sandbox dibatasi untuk jangka waktu tertentu yang sesuai dengan kompleksitas dan ukuran proyek, tetapi dapat diperpanjang oleh otoritas. Sandbox memungkinkan pengembangan alat dan infrastruktur untuk pengujian, benchmarking, evaluasi, dan penjelasan dimensi sistem AI, khususnya dalam hal pembelajaran regulasi tentang akurasi, ketahanan, dan keamanan siber, langkah-langkah yang dapat diambil untuk mengatasi risiko terhadap hak-hak fundamental, lingkungan, dan masyarakat secara keseluruhan.

Jika otoritas mempertimbangkan pengujian dalam kondisi dunia nyata yang diawasi dalam sandbox, mereka harus menyepakati dengan peserta tentang kondisi partisipasi dan mengambil langkah-langkah pengamanan untuk melindungi hak-hak fundamental, kesehatan, dan keselamatan. Mereka juga dapat bekerja sama dengan otoritas lain untuk memastikan konsistensi di dalam Uni Eropa.

Pemrosesan Lebih Lanjut Data Pribadi

Pemrosesan lebih lanjut data pribadi dalam sistem AI tertentu yang menjadi kepentingan publik di dalam sandbox dimungkinkan berdasarkan ketentuan Pasal 59 UU AI. Data pribadi yang telah dikumpulkan secara sah untuk tujuan lain dapat digunakan untuk tujuan **pengembangan, pelatihan, dan pengujian sistem AI** tertentu di dalam sandbox. Namun, syarat-syarat tertentu harus dipenuhi.

Sistem AI harus dikembangkan untuk melindungi kepentingan publik yang penting oleh otoritas publik atau orang perseorangan atau badan hukum lainnya berdasarkan hukum publik atau swasta di salah satu bidang berikut:

- Keamanan publik, kesehatan publik, termasuk pencegahan, pengendalian, dan pengobatan penyakit serta peningkatan sistem kesehatan
- Memastikan tingkat perlindungan lingkungan yang tinggi dan meningkatkan kualitas lingkungan, melindungi keanekaragaman hayati, polusi, perubahan hijau, dan perlindungan iklim
- Keberlanjutan energi

- Keamanan dan ketahanan sistem transportasi dan mobilitas, infrastruktur dan jaringan penting
- Efisiensi dan kualitas administrasi publik dan layanan publik

Data yang diproses harus diperlukan untuk memenuhi persyaratan dalam Bagian III, Bab 2 Undang-Undang AI (persyaratan untuk sistem AI berisiko tinggi). Namun, pemrosesan hanya diizinkan jika persyaratan ini tidak dapat dipenuhi dengan data anonim, sintetis, atau data non-pribadi lainnya.

Langkah-langkah pemantauan yang efisien juga harus diambil untuk mengurangi risiko tinggi terhadap hak dan kebebasan subjek data (lihat Pasal 4 ayat 1 GDPR) yang mungkin timbul selama eksperimen sandbox atau, jika perlu, untuk menghentikan pemrosesan sama sekali. Semua data pribadi yang akan diproses sehubungan dengan sandbox harus disimpan di lingkungan yang terpisah, terisolasi, dan terlindungi di bawah kendali penyedia yang bertanggung jawab dan hanya dapat dilihat oleh orang yang berwenang. Penyedia dapat membagikan data yang awalnya dikumpulkan sesuai dengan GDPR, tetapi data yang dibuat di sandbox tidak boleh dibagikan di luar sandbox. Ini berarti bahwa hasil pemrosesan dari sandbox yang bersifat pribadi tidak boleh digunakan kembali. Setiap pemrosesan data pribadi sehubungan dengan sandbox tidak boleh menyebabkan tindakan atau keputusan yang merugikan subjek data atau membatasi hak mereka sehubungan dengan pemrosesan data pribadi. Data pribadi harus dilindungi oleh langkah-langkah teknis dan organisasi yang tepat dan dihapus segera setelah partisipasi dalam sandbox berakhir atau periode penyimpanan telah berakhir. Data log dan protokol yang dihasilkan selama pemrosesan di dalam sandbox dapat disimpan selama masa partisipasi di dalam sandbox, kecuali ditentukan lain oleh hukum Uni Eropa atau hukum nasional. Deskripsi rinci tentang proses dan justifikasi pelatihan, pengujian, dan validasi sistem AI harus disimpan bersama dengan hasil pengujian sebagai bagian dari dokumentasi teknis sesuai dengan Lampiran IV Undang-Undang AI. Ringkasan singkat proyek AI yang dikembangkan di dalam sandbox, tujuannya, dan hasil yang diharapkan harus dipublikasikan di situs web otoritas yang berwenang. Kewajiban ini tidak termasuk data operasional sensitif yang terkait dengan kegiatan penegakan hukum, pengawasan perbatasan, imigrasi, atau otoritas suaka.

Persyaratan ini juga berlaku untuk sistem AI di dalam sandbox untuk tujuan pencegahan, investigasi, deteksi, atau penuntutan tindak pidana atau pelaksanaan hukuman pidana, termasuk perlindungan dan pencegahan ancaman terhadap keamanan publik. Pemrosesan data pribadi juga dilakukan berdasarkan undang-undang khusus dari Negara Anggota atau Uni Eropa.

Pengujian di Luar Sandbox AI

Pasal 60 UU AI juga mengatur tentang **pengujian sistem AI berisiko tinggi dalam kondisi dunia nyata** di luar sandbox. Penyedia atau calon penyedia dapat melakukan pengujian tersebut sesuai dengan rencana pengujian, dengan tunduk pada kondisi tertentu. Namun, larangan Pasal 5 UU AI berlaku. Unsur-unsur pasti dari rencana pengujian dunia nyata dikeluarkan oleh Komisi Uni Eropa dalam sebuah peraturan perundang-undangan.

Penyedia atau calon penyedia dapat menguji sistem AI berisiko tinggi dalam kondisi dunia nyata kapan saja sebelum memasarkannya atau mengoperasikannya, baik sendiri maupun bersama dengan yang lain. Pengujian tidak mengurangi tinjauan etika apa pun yang dipersyaratkan berdasarkan hukum nasional atau Uni Eropa.

Pelaksanaan pengujian dunia nyata hanya dapat dilakukan oleh penyedia atau calon penyedia dalam kondisi tertentu: Penyedia atau calon penyedia memiliki **rencana pengujian** dan telah menyerahkannya kepada otoritas pengawasan pasar Negara Anggota tempat pengujian akan dilakukan. Otoritas pengawasan pasar harus **menyetujui** pengujian dalam kondisi dunia nyata dan rencana pengujian dunia nyata tersebut. Jika otoritas pengawasan pasar tidak memberikan tanggapan dalam waktu 30 hari, pengujian dianggap telah disetujui. Jika hukum nasional tidak mengatur persetujuan eksplisit, pengujian setidaknya harus diotorisasi. Jika itu adalah sistem AI berisiko tinggi sesuai dengan Lampiran III, poin 1, 6 dan 7 dalam penegakan hukum, migrasi, suaka dan manajemen kontrol perbatasan dan sistem AI berisiko tinggi sesuai dengan Lampiran III, poin 2 Undang-Undang AI, pengujian harus didaftarkan dalam basis data Uni Eropa yang tidak bersifat publik dengan nomor identifikasi unik di seluruh Uni Eropa (lihat Lampiran IX Undang-Undang AI). Penyedia atau calon penyedia harus memiliki **kantor terdaftar** atau setidaknya perwakilan hukum di Uni Eropa. Data yang dikumpulkan dan diproses untuk tujuan pengujian dunia nyata hanya dapat ditransfer ke **negara ketiga di luar** Uni Eropa jika perlindungan yang berlaku berdasarkan hukum Uni Eropa dipatuhi (lihat Pasal 48 dan seterusnya GDPR). Pengujian dalam kondisi dunia nyata tidak boleh berlangsung lebih lama dari yang diperlukan untuk mencapai tujuan yang relevan, tetapi dalam keadaan apa pun tidak lebih dari enam bulan, yang selanjutnya dapat diperpanjang maksimal **enam bulan**. Hal ini harus dilakukan dengan pemberitahuan sebelumnya kepada otoritas pengawas pasar yang berwenang dan harus mencakup penjelasan mengapa perpanjangan tersebut diperlukan. Orang-orang yang termasuk dalam **kelompok rentan** karena usia atau disabilitas fisik atau mental mereka harus dilindungi sesuai dengan ketentuan. Jika penyedia atau calon penyedia menyelenggarakan pengujian dalam kondisi nyata dengan satu atau lebih calon pengguna, pengguna tersebut harus diinformasikan tentang semua aspek pengujian yang diperlukan untuk keputusan mereka untuk berpartisipasi. Mereka juga harus diberi instruksi tentang penggunaan sistem AI. Penyedia atau calon penyedia dan pengguna harus membuat **perjanjian** yang mendefinisikan peran dan tanggung jawab untuk pengujian di dunia nyata. Subjek pengujian harus memberikan persetujuan berdasarkan informasi sesuai dengan Pasal 61 UU AI. Jika pengujian terkait dengan penegakan hukum dan memperoleh persetujuan akan bertentangan dengan pengujian, hal itu dapat dikesampingkan jika pengujian di dunia nyata tidak memiliki efek negatif pada subjek pengujian dan data pribadi dihapus setelah pengujian. Pengujian harus dilakukan di bawah pengawasan penyedia atau calon penyedia dan pelaksana dengan bantuan orang-orang yang berkualifikasi. Prediksi, rekomendasi, atau keputusan sistem AI dapat dibatalkan atau diabaikan.

Setiap **subjek pengujian** dapat menarik diri dari pengujian dalam kondisi dunia nyata tanpa memberikan alasan, mencabut persetujuan mereka, dan meminta penghapusan data pribadi mereka. Otoritas pengawasan pasar yang berwenang dapat melakukan investigasi di

tempat atau jarak jauh untuk memantau kemajuan pengujian. Setiap insiden serius harus dilaporkan kepada otoritas pengawasan pasar. Penyedia atau calon penyedia harus segera mengambil tindakan untuk mengurangi atau, jika ini gagal, menanggguhkan atau mengakhiri pengujian. Penyedia atau calon penyedia harus menetapkan proses untuk segera menarik kembali sistem AI jika pengujian tersebut diakhiri. Otoritas pengawasan pasar harus diberitahu tentang berakhirnya atau penangguhan pengujian dan hasil akhirnya. Penyedia atau calon penyedia bertanggung jawab atas **setiap kerusakan** yang disebabkan selama berpartisipasi dalam pengujian di lingkungan nyata.

Persetujuan untuk Pengujian di Luar Sandbox

Pasal 61 UU AI menjelaskan aturan untuk persetujuan berdasarkan informasi untuk pengujian dunia nyata di luar sandbox. Persetujuan tersebut harus diberikan secara **sukarela** dan berdasarkan **informasi** oleh subjek pengujian sebelum berpartisipasi. Informasi tersebut harus ringkas, jelas, relevan, dan mudah dipahami. Ini berarti bahwa **sifat** dan **tujuan** pengujian serta **kemungkinan ketidaknyamanan** yang terkait dengan partisipasi harus dinyatakan dengan jelas. Kondisi di mana pengujian akan berlangsung dan **durasi** partisipasi harus dijelaskan. Hak dan jaminan subjek data sehubungan dengan partisipasi harus dijelaskan, khususnya hak untuk menolak partisipasi atau menarik persetujuan untuk pengujian kapan saja tanpa konsekuensi negatif atau memerlukan justifikasi. Tata cara untuk meminta penarikan atau pengabaian prediksi, rekomendasi, atau keputusan sistem AI harus ditetapkan, serta nomor identifikasi unik pengujian di seluruh Uni Eropa dalam kondisi nyata dan detail kontak penyedia atau perwakilan hukumnya yang dapat memberikan informasi lebih lanjut. Persetujuan harus diberi tanggal dan **didokumentasikan**, dan subjek data atau perwakilan hukumnya harus menerima salinannya.

Fasilitasi untuk UKM

Pasal 62 UU AI memuat fasilitasi untuk penyedia dan penyebar kecil, khususnya UKM dan perusahaan rintisan. Negara-negara Anggota Uni Eropa wajib mengambil langkah-langkah berikut: UKM dan perusahaan rintisan yang memiliki kantor atau cabang di Uni Eropa diberikan **akses prioritas ke sandbox**, dengan syarat mereka memenuhi persyaratan dan kriteria seleksi. Akses prioritas tidak boleh menghalangi UKM dan perusahaan rintisan lain untuk mendapatkan akses ke sandbox. Negara-negara Anggota juga harus menyelenggarakan **kegiatan peningkatan kesadaran khusus** tentang penerapan UU AI, yang disesuaikan dengan kebutuhan UKM dan perusahaan rintisan, tetapi juga penyebar dan, jika perlu, badan pemerintahan lokal. Selain itu, Negara Anggota dapat membangun saluran komunikasi (baru) dengan UKM dan perusahaan rintisan, inovator lain, dan, jika perlu, badan pemerintahan lokal untuk memberi nasihat dan menanggapi permintaan terkait implementasi Undang-Undang AI, termasuk sandbox. Negara Anggota dapat melibatkan partisipasi UKM dan pemangku kepentingan terkait lainnya dalam pengembangan proses standarisasi.

Kantor AI yang baru juga melakukan upaya: Atas permintaan, kantor ini menawarkan templat standar untuk Undang-Undang AI, mengembangkan dan memelihara platform yang menyediakan informasi tentang Undang-Undang AI. Kantor AI menyelenggarakan kampanye

komunikasi untuk meningkatkan kesadaran akan kewajiban Undang-Undang AI. Kantor ini mengevaluasi dan mempromosikan penggabungan praktik terbaik.

Usaha mikro sebagaimana didefinisikan dalam Pasal 2 ayat 3 Lampiran Rekomendasi Komisi 2003/361/EC tentang definisi usaha mikro, kecil, dan menengah dapat memenuhi persyaratan Pasal 17 Peraturan Investasi Modal dengan cara yang disederhanakan. Komisi Uni Eropa sedang mengembangkan pedoman sendiri untuk tujuan ini.

3.10 OTORITAS

Pasal 28 dan seterusnya UU AI membedakan antara otoritas pemberi pemberitahuan, badan penilaian kesesuaian, dan badan pemberi pemberitahuan. Negara-negara Anggota dapat memutuskan bahwa pemantauan dilakukan oleh badan akreditasi nasional sesuai dengan Arahan (EC) No. 765/2008.

Otoritas Pemberi Pemberitahuan

Otoritas pemberi pemberitahuan dibentuk di setiap negara anggota Uni Eropa. Definisinya dapat ditemukan dalam Pasal 3 no. 19 UU AI. Otoritas ini bertanggung jawab atas pembentukan badan penilaian kesesuaian dan pemantauannya. Otoritas ini juga dapat berupa badan akreditasi sesuai dengan Peraturan Pengawasan Pasar (Peraturan (EC) No. 765/2008). Di Austria, otoritas ini berbeda-beda, tergantung pada bidang hukum, tanggung jawab federal atau negara bagian. Misalnya, AGES, Kantor Pasar Wina, atau bagian yang bertanggung jawab dari kementerian federal. Koordinasi nasional dilakukan oleh Kantor Metrologi dan Survei Federal. Situasinya serupa di Jerman, di mana Komite Kerja Pengawasan Pasar dibentuk untuk memastikan penegakan yang seragam. Daftar lengkap semua otoritas pengawasan pasar tersedia dari Komisi Uni Eropa.

Negara-negara anggota harus membentuk otoritas pemberi pemberitahuan sedemikian rupa sehingga mereka dapat bekerja secara terstruktur dan terorganisir. Konflik kepentingan dengan badan penilai kesesuaian harus dihindari dan objektivitas serta ketidakberpihakan otoritas harus dijamin. Orang yang bekerja untuk otoritas tidak boleh secara bersamaan bekerja untuk badan penilai kesesuaian, dan otoritas juga tidak boleh mengambil alih kegiatan badan penilai kesesuaian. Pemisahan yang ketat harus dipatuhi. Otoritas secara eksplisit tidak boleh menawarkan layanan konsultasi dan harus menjamin kerahasiaan. Negara-negara Anggota harus menyediakan sumber daya yang sesuai kepada otoritas dan staf harus memiliki keahlian yang relevan.

Badan Penilaian Kesesuaian dan Badan yang Diberi Pemberitahuan

Badan penilaian kesesuaian melaksanakan semua kegiatan yang berkaitan dengan pengujian, sertifikasi, dan inspeksi serta bertindak sebagai pihak ketiga independen (lihat definisi dalam Pasal 3 no. 21 UU AI). Badan tersebut merupakan **badan yang diberi pemberitahuan** jika telah ditunjuk sesuai dengan UU AI (atau peraturan atau arahan UE lainnya). (bdk. Pasal 3 no. 22 UU AI). Badan penilaian kesesuaian harus mengajukan permohonan pemberitahuan di Negara Anggota tempat mereka didirikan.

Dokumen-dokumen berikut harus dilampirkan dengan **permohonan**:

- Deskripsi kegiatan penilaian kesesuaian

- Deskripsi prosedur penilaian kesesuaian
- Deskripsi teknologi AI yang menjadi kompetensi badan penilaian kesesuaian
- Jika tersedia, sertifikat akreditasi yang menyatakan bahwa badan tersebut memenuhi persyaratan Pasal 31 UU AI
- Jika tersedia, penunjukan yang ada sebagai badan yang diberi pemberitahuan sesuai dengan peraturan atau arahan UE lainnya.

Jika tidak ada sertifikat akreditasi sesuai dengan Pasal 31 UU AI, maka badan tersebut tidak memenuhi persyaratan. Berdasarkan Pasal 31 UU AI, badan tersebut harus membuktikan bahwa mereka memenuhi persyaratan Pasal 31 UU AI.

Badan yang diberi wewenang memverifikasi **kesesuaian sistem AI berisiko tinggi**, yang berarti bahwa badan tersebut harus memiliki sumber daya yang diperlukan, manajemen mutu yang sesuai, dan persyaratan prosedural untuk melaksanakan tugas ini. Struktur organisasi harus dirancang sedemikian rupa sehingga badan tersebut dapat menjamin hasil yang dapat dipercaya dalam kegiatan penilaian kesesuaiannya. Badan tersebut harus independen dari penyedia, yaitu tidak boleh ada tumpang tindih personel, kepentingan ekonomi, atau hubungan kompetitif. Tidak seorang pun dari badan tersebut, baik manajemen tingkat atas maupun staf, boleh terlibat langsung dalam perancangan, pengembangan, pemasaran, atau penggunaan AI berisiko tinggi atau mewakili pihak yang terlibat dalam kegiatan ini. Hal ini berlaku khususnya untuk layanan konsultasi.

Badan yang diberi wewenang mendokumentasikan pelaksanaan prosedur dan memastikan kerahasiaan. Selama prosedur, badan tersebut mempertimbangkan ukuran, sektor, dan struktur penyedia serta kompleksitas sistem AI yang akan diuji. Tujuannya adalah untuk mengurangi biaya dan beban administratif, khususnya untuk usaha kecil dan mikro (lihat Pasal 34 UU AI). Kepatuhan terhadap persyaratan Pasal 31 UU AI dianggap terpenuhi jika badan tersebut memenuhi persyaratan dalam peraturan perundang-undangan Uni Eropa yang relevan. Asuransi tanggung jawab wajib bagi badan yang telah dinotifikasi.

Prosedur pemberitahuan diatur dalam Pasal 30 UU AI. Otoritas yang berwenang hanya dapat memberitahukan badan-badan yang memenuhi persyaratan Pasal 31 UU AI. Komisi Uni Eropa harus diberitahu tentang pemberitahuan yang dibuat oleh badan-badan penilaian kesesuaian. **Pemberitahuan** berisi rincian lengkap tentang:

- kegiatan penilaian kesesuaian
- modul penilaian kesesuaian yang bersangkutan
- teknologi AI yang relevan
- bukti kompetensi yang relevan (baik akreditasi sesuai dengan Pasal 29 ayat 2 UU AI atau bukti kepatuhan terhadap Pasal UU AI)

Badan yang diberitahukan bertanggung jawab penuh atas setiap kantor cabang yang digunakan atau subkontrak yang diberikan. Kegiatan hanya dapat dialihkan dengan persetujuan penyedia. Badan yang diberitahukan hanya dapat memulai kegiatannya jika Komisi Uni Eropa maupun Negara Anggota lainnya tidak mengajukan keberatan dalam waktu dua minggu dalam kasus pemberitahuan sesuai dengan Pasal 29 ayat 2 UU AI, atau dalam waktu dua bulan dalam kasus bukti sesuai dengan Pasal 30 ayat 3 UU AI. Jika ada keberatan

yang diajukan, Komisi Uni Eropa harus segera memulai konsultasi dengan Negara Anggota yang bersangkutan. Komisi Uni Eropa memutuskan apakah keberatan tersebut beralasan atau tidak dan menyampaikan keputusan tersebut kepada Negara Anggota dan badan yang diberi pemberitahuan.

Komisi Uni Eropa juga memberikan **nomor identifikasi** kepada badan-badan yang diberi pemberitahuan yang selalu sama, meskipun badan tersebut telah diberi pemberitahuan berdasarkan beberapa peraturan perundang-undangan Uni Eropa. Daftar badan-badan tersebut, termasuk nomor identifikasi dan aktivitasnya, dipublikasikan.

Otoritas harus segera memberitahukan Komisi Uni Eropa tentang setiap **perubahan**. Perluasan ruang lingkup pemberitahuan harus dilakukan sesuai dengan prosedur yang ditetapkan dalam Pasal 29 dan 30 UU AI. Jika suatu badan ingin mengakhiri aktivitas penilaiannya, otoritas yang memberi pemberitahuan dan penyedia layanan harus diberitahu. Jika suatu otoritas memiliki alasan yang wajar untuk mencurigai bahwa suatu badan tidak lagi memenuhi persyaratan Pasal 31 UU AI atau tidak memenuhi kewajibannya, otoritas tersebut harus segera melakukan investigasi. Otoritas tersebut menyampaikan kekhawatirannya kepada badan tersebut dan memberinya kesempatan untuk memberikan komentar. Pemberitahuan tersebut selanjutnya dapat dibatasi, ditangguhkan, atau dicabut sebagian atau seluruhnya. Otoritas juga memberi tahu Komisi Uni Eropa dan badan yang diberi pemberitahuan memberi tahu produsen AI paling lambat dalam sepuluh hari. Otoritas juga memastikan bahwa dokumen dan berkas prosedural badan tersebut disimpan dan tersedia untuk otoritas lain atau badan pengawasan pasar jika diminta. Dalam hal **pembatasan, penangguhan, atau pencabutan status sebagai badan** yang diberi pemberitahuan, otoritas wajib untuk:

- memeriksa pengaruhnya terhadap sertifikasi yang diberikan kepada badan tersebut;
- menyampaikan laporan kepada Komisi Uni Eropa dan Negara Anggota lainnya tentang perubahan pada pemberitahuan tersebut dalam waktu tiga bulan;
- mewajibkan badan-badan tersebut untuk menangguhkan atau mencabut sertifikat yang telah diterbitkan secara salah;
- memberi tahu Komisi Uni Eropa dan Negara-negara Anggota tentang Negara-negara Anggota yang sertifikatnya ditangguhkan atau dicabut;
- memberi tahu otoritas kompeten nasional Negara-negara Anggota tempat penyedia layanan berada tentang sertifikat yang telah ditangguhkan atau dicabut. Otoritas di sana kemudian akan mengambil langkah-langkah yang diperlukan untuk mencegah risiko terhadap kesehatan, keselamatan, atau hak-hak dasar.

Dalam kondisi tertentu, sertifikat dapat dipertahankan sesuai dengan Pasal 36 UU AI: Otoritas yang memberi pemberitahuan mengkonfirmasi dalam waktu satu bulan setelah penangguhan atau pembatasan bahwa tidak ada risiko terhadap kesehatan, keselamatan, atau hak-hak dasar dan otoritas tersebut memberikan jadwal dan tugas untuk mencabut penangguhan atau pembatasan tersebut. Opsi kedua adalah bahwa otoritas tersebut mengkonfirmasi bahwa tidak ada sertifikat yang ditangguhkan dan badan yang diberi pemberitahuan masih memiliki kemungkinan untuk mengawasi sertifikat yang diterbitkan. Jika

tidak demikian, penyedia layanan memiliki opsi untuk memberi tahu otoritas tersebut dalam waktu tiga bulan tentang badan yang diberi pemberitahuan lain yang akan mengawasi sertifikat tersebut di masa mendatang.

Meskipun demikian, sertifikat dari badan yang sebelumnya telah dinotifikasi tetap berlaku selama sembilan bulan jika otoritas yang berwenang mengkonfirmasi kepada penyedia bahwa tidak ada risiko terhadap kesehatan, keselamatan, dan hak-hak mendasar sehubungan dengan sistem AI yang bersangkutan; atau, badan yang dinotifikasi lainnya mengkonfirmasi secara tertulis bahwa mereka akan segera mengambil alih tanggung jawab atas sistem ini dan melakukan penilaian dalam waktu dua belas bulan sejak pencabutan. Dalam kasus pertama, batas waktu dapat diperpanjang hingga tiga bulan lagi.

Otoritas yang berwenang atau badan yang dinotifikasi yang mengambil alih fungsi badan yang dinotifikasi sebelumnya harus segera memberitahukan Komisi Uni Eropa, Negara-negara Anggota, dan badan-badan yang dinotifikasi lainnya tentang pengambilalihan tersebut.

Selain itu, sesuai dengan Pasal 37 UU AI, Komisi Uni Eropa dapat menyelidiki semua kasus di mana Komisi Uni Eropa meragukan kompetensi badan yang dinotifikasi atau kepatuhan berkelanjutan badan tersebut terhadap persyaratan Pasal 31 UU AI. Otoritas yang melakukan notifikasi harus memberikan Komisi Uni Eropa semua informasi yang relevan sehubungan dengan notifikasi atau pemeliharaan kompetensi badan yang dinotifikasi atas permintaan. Komisi Uni Eropa menjamin kerahasiaan penyelidikan tersebut. Jika Komisi Uni Eropa sampai pada kesimpulan bahwa badan yang diberi pemberitahuan tidak lagi memenuhi persyaratan, Komisi segera memberitahukan Negara Anggota yang memberi pemberitahuan agar Negara Anggota tersebut dapat mengambil tindakan korektif yang diperlukan, termasuk, jika perlu, menangguhkan atau mencabut pemberitahuan tersebut. Jika Negara Anggota tidak mengambil tindakan yang diperlukan, Komisi Uni Eropa dapat menangguhkan, membatasi, atau mencabut pemberitahuan tersebut melalui tindakan pelaksana sesuai dengan Pasal 98 ayat 2 UU AI. Sesuai dengan Pasal 38 UU, Komisi Uni Eropa memastikan koordinasi dan kerja sama antara badan-badan yang diberi pemberitahuan.

Badan penilaian kesesuaian dari negara ketiga yang telah menjalin perjanjian dengan Komisi Uni Eropa dalam hal ini dapat mengambil alih tugas badan yang diberi pemberitahuan berdasarkan Undang-Undang AI, dengan syarat mereka memenuhi persyaratan Pasal 31 Undang-Undang AI atau menjamin tingkat yang setara.

3.11 TATA KELOLA DALAM UNDANG-UNDANG AI

Undang-Undang AI menyediakan berbagai mekanisme untuk memastikan interpretasi dan kerja sama yang seragam antar Negara Anggota.

Kantor AI

Menurut Pasal 64 Undang-Undang AI, Komisi Uni Eropa wajib mengembangkan keahlian dan keterampilannya sendiri di bidang AI. Negara-negara anggota harus menyediakan **Kantor AI**. Kantor AI didirikan berdasarkan Keputusan Komisi tanggal 24 Januari 2024.

Dewan AI

Komponen kunci tata kelola adalah **Dewan Kecerdasan Buatan Eropa** atau “Dewan AI” yang juga baru. Sesuai dengan Pasal 65 Undang-Undang AI, dewan ini terdiri dari satu perwakilan per Negara Anggota. Pengawas Perlindungan Data Eropa berpartisipasi sebagai pengamat. Kantor AI juga ikut serta dalam rapat, tetapi tidak memiliki hak suara. Otoritas atau badan nasional atau Uni Eropa lainnya dapat diundang jika Dewan AI membahas topik yang relevan bagi mereka.

Komposisi

Para anggota, yaitu **wakil dari negara-negara anggota**, diangkat untuk jangka waktu tiga tahun, di mana pengangkatan dapat diperpanjang hingga total enam tahun. Negara-negara Anggota harus memastikan bahwa wakil mereka memiliki tanggung jawab dan wewenang yang relevan untuk secara aktif mewakili Negara Anggota dan berkontribusi pada Dewan AI. Wakil juga merupakan satu-satunya titik kontak dengan komite dan pemangku kepentingan lainnya. Wakil harus diberi wewenang untuk memastikan konsistensi dan koordinasi antara berbagai otoritas nasional sehubungan dengan implementasi Undang-Undang AI. Mereka dapat mengumpulkan data dan informasi untuk memenuhi tugas mereka terhadap Komite.

Salah satu tugas pertama anggota komite yang ditunjuk adalah mengadopsi **peraturan prosedur** dengan mayoritas dua pertiga. Secara khusus, proses seleksi, durasi penunjukan dan tugas ketua, modalitas pemungutan suara dan organisasi kegiatan komite dan kelompok kerjanya harus didefinisikan. Komite harus memastikan bahwa ia bekerja secara objektif dan tidak memihak.

Dalam hal apa pun, **dua kelompok kerja tetap** akan dibentuk untuk berfungsi sebagai platform pertukaran bagi otoritas pengawasan pasar dan otoritas pemberi pemberitahuan untuk topik masing-masing. Kelompok kerja lain dapat dibentuk oleh Dewan secara permanen atau untuk jangka waktu tertentu untuk mengklarifikasi masalah tertentu. Ketua adalah perwakilan terpilih dari negara anggota. Kantor AI menyediakan sekretariat untuk Dewan, mengatur pertemuan dan menyiapkan agenda.

Tugas Dewan AI

Tugas badan penasihat didefinisikan dalam Pasal 66 UU AI. Dewan AI memberikan nasihat dan bantuan kepada Komisi Uni Eropa dan Negara-negara Anggota untuk memastikan penerapan UU AI yang konsisten dan efisien. Tugas-tugas berikut didefinisikan secara eksplisit: Dewan AI berkontribusi pada **koordinasi otoritas nasional yang berwenang** dan, tergantung pada kesepakatan dengan otoritas pengawasan pasar yang bersangkutan, memberikan dukungan untuk kegiatan bersama otoritas pengawasan pasar sesuai dengan Pasal 74 ayat 11 UU AI.

Dewan mengumpulkan keahlian teknis dan regulasi serta praktik terbaik di antara Negara-negara Anggota. Dewan memberikan nasihat tentang implementasi UU AI, khususnya terkait dengan penegakan aturan tentang model AI untuk tujuan umum. Dewan berkontribusi pada **harmonisasi praktik administrasi** di Negara-negara Anggota, termasuk prosedur untuk penilaian kesesuaian sesuai dengan Pasal 46 UU AI, fungsi laboratorium nyata dan pengujian dunia nyata sesuai dengan Pasal 57 dan seterusnya UU AI.

Atas permintaan Komisi Uni Eropa atau atas inisiatifnya sendiri, Dewan AI dapat mengeluarkan **rekomendasi dan opini tertulis** tentang topik relevan apa pun yang berkaitan dengan implementasi Undang-Undang AI dan penerapannya yang konsisten dan efisien. Rekomendasi atau opini ini harus berkaitan dengan pengembangan dan penerapan kode etik dan praktik sesuai dengan Undang-Undang AI atau sesuai dengan pedoman Komisi Uni Eropa. Dewan juga dapat mengeluarkan opini tentang evaluasi Peraturan AI, insiden serius, tindakan delegasi, dan amandemen Lampiran I Undang-Undang AI. Opini juga dimungkinkan mengenai spesifikasi teknis dan standar yang ada serta standar yang harmonis. Komite juga dapat memberikan komentar tentang tren, seperti daya saing Uni Eropa, pengembangan keterampilan digital, rantai nilai AI, dan lainnya.

Dewan AI juga mendukung Komisi Uni Eropa dalam **mempromosikan keterampilan AI**, kesadaran publik, dan pemahaman tentang manfaat, risiko, perlindungan, hak, dan kewajiban yang terkait dengan penggunaan sistem AI. Dewan AI mengembangkan kriteria umum dan membantu membangun pemahaman bersama di antara pelaku pasar dan otoritas yang berwenang tentang konsep-konsep yang diatur dalam Undang-Undang AI dan berkontribusi pada pengembangan tolok ukur. Dewan akan bekerja sama dengan lembaga, badan, kantor, dan badan Uni Eropa lainnya sebagaimana mestinya dan, jika perlu, secara internasional, serta dengan kelompok dan jaringan ahli yang relevan di Uni Eropa, khususnya di bidang keamanan produk, keamanan siber, persaingan, layanan digital dan media, layanan keuangan, perlindungan konsumen, perlindungan data, dan perlindungan hak-hak fundamental.

Dewan AI mendukung otoritas nasional yang berwenang dan Komisi Uni Eropa dalam membangun keahlian organisasi dan teknis yang diperlukan untuk implementasi Peraturan AI, termasuk dengan membantu mengidentifikasi kebutuhan pelatihan bagi staf Negara Anggota yang terlibat dalam implementasi Undang-Undang AI. Dewan membantu Kantor AI, yang mendukung otoritas nasional yang berwenang dalam mendirikan dan mengembangkan sandbox, serta memfasilitasi kerja sama dan pertukaran informasi antar sandbox. Dewan memberikan nasihat kepada Komisi Uni Eropa tentang masalah internasional yang berkaitan dengan AI dan mengeluarkan pendapat kepada Komisi Uni Eropa mengenai pemberitahuan yang memenuhi syarat tentang model AI untuk tujuan umum. Negara-negara anggota juga memberikan pendapat kepada Dewan tentang pemberitahuan yang memenuhi syarat tentang model AI untuk tujuan umum, tetapi juga tentang pengalaman nasional, praktik mengenai pemantauan dan penegakan sistem AI.

Forum Penasihat

Pasal 67 Undang-Undang AI juga mengatur forum penasihat teknis. Forum ini terutama memberikan **keahlian teknis** kepada Dewan AI dan Komisi Uni Eropa. Anggota ditunjuk oleh Komisi Uni Eropa dan mereka ditunjuk untuk forum penasihat selama dua tahun, tetapi setelah diperpanjang satu kali untuk maksimal empat tahun. **Anggota tetap** forum penasihat adalah Badan Hak Fundamental FRA, Badan Keamanan Siber Eropa, Komite Standardisasi Eropa CEN, Komite Standardisasi Elektroteknik Eropa CENELEC, dan Institut Standar Telekomunikasi Eropa ETSI. Forum penasihat memiliki dua ketua, yang juga dipilih untuk masa jabatan dua tahun, dan dapat diperpanjang untuk dua tahun berikutnya. Untuk memenuhi tugasnya, forum

penasihat bertemu setidaknya dua kali setahun, menyiapkan pernyataan atas permintaan Dewan AI atau Komisi Uni Eropa, dan menyusun laporan tahunan, yang juga dipublikasikan.

Panel Ilmiah

Sebuah **panel ilmiah yang terdiri dari para ahli independen** juga direncanakan sesuai dengan Pasal 68 UU AI. Badan ini dibentuk oleh Komisi Uni Eropa untuk membantu tugas-tugas penegakan hukum. Para anggotanya ditunjuk oleh Komisi Uni Eropa berdasarkan keahlian ilmiah atau teknis mereka. Mereka harus independen dari penyedia sistem AI. Panel ilmiah memberikan nasihat dan dukungan kepada Kantor AI terkait implementasi dan penegakan UU AI, kemungkinan risiko, evaluasi model AI untuk tujuan umum, klasifikasi sistem AI, pengembangan alat dan model, pekerjaan otoritas pengawasan pasar, Kantor AI terkait tugas-tugasnya sesuai dengan Pasal 66 UU AI. Panel ilmiah bertindak secara imparial, objektif, rahasia, dan tanpa instruksi.

Negara-negara Anggota dapat menggunakan para ahli dari panel ilmiah untuk membantu mereka dalam tugas-tugas penegakan UU AI. Komisi Uni Eropa menyediakan akses tepat waktu kepada para ahli untuk Negara-negara Anggota dan memastikan bahwa kombinasi kegiatan pendukung melalui apa yang disebut "dukungan pengujian AI Uni" sesuai dengan Pasal 68 UU AI dapat memberikan dukungan yang memadai bagi Negara-negara Anggota. 84 Undang-Undang AI dan para ahli menawarkan nilai tambah terbaik.

Otoritas Nasional

Pengangkatan otoritas kompeten nasional diatur dalam Pasal 70 Undang-Undang AI. Setiap Negara Anggota harus menetapkan atau menunjuk setidaknya satu **otoritas pemberitahuan** dan setidaknya satu **otoritas pengawasan pasar** sebagai otoritas kompeten nasional. Otoritas-otoritas ini harus menjalankan tanggung jawab mereka secara independen, tidak memihak, objektif, dan tanpa bias. Anggota otoritas-otoritas ini harus menahan diri dari kegiatan yang tidak sesuai. Negara-negara Anggota harus memberitahukan kepada Komisi Uni Eropa tentang pengangkatan, tugas, dan setiap perubahan pada otoritas pemberitahuan dan otoritas pengawasan pasar. Informasi tentang cara menghubungi otoritas harus dipublikasikan dalam waktu dua belas bulan sejak Undang-Undang AI mulai berlaku. Setiap negara anggota menunjuk otoritas pengawasan pasar sebagai "**titik kontak tunggal**". Komisi Uni Eropa pada gilirannya menerbitkan daftar lengkap semua detail kontak ini. Komisi juga mendukung pertukaran pengalaman antar otoritas.

Otoritas nasional harus memiliki tingkat langkah-langkah keamanan siber yang memadai. Mereka wajib menjaga kerahasiaan saat melakukan kegiatan mereka. Dalam melaksanakan kegiatannya, otoritas yang berwenang dapat memberikan panduan dan nasihat, khususnya kepada UKM dan perusahaan rintisan. Dalam melakukannya, mereka harus mempertimbangkan panduan apa pun yang diberikan oleh Dewan AI dan Komisi Uni Eropa. Otoritas nasional yang menerapkan Undang-Undang AI harus, jika undang-undang Uni Eropa lainnya juga berlaku, berkonsultasi dengan otoritas yang bertanggung jawab atas undang-undang tersebut. Misalnya, jika sistem AI memproses data pribadi, otoritas AI yang berwenang atau otoritas perlindungan data yang berwenang harus dikonsultasikan, tergantung pada keadaan.

Basis Data UE untuk Sistem AI Berisiko Tinggi

Bersama dengan Negara-negara Anggota, Komisi UE membuat dan memelihara basis data tentang sistem AI berisiko tinggi yang telah terdaftar sesuai dengan Pasal 49 dan 60 Undang-Undang AI. Mengenai spesifikasi basis data, Komisi UE berkoordinasi dengan Dewan AI.

Basis data tersebut berisi sistem AI berisiko tinggi sesuai dengan Lampiran VIII Undang-Undang AI. Sistem AI sesuai dengan Bagian A didaftarkan oleh penyedia atau perwakilan mereka. Sistem AI sesuai dengan Bagian C didaftarkan oleh pengembang yang bertindak atas nama otoritas, kantor, atau lembaga.

Pada prinsipnya, basis data tersebut tersedia untuk umum dan juga harus dapat dibaca oleh mesin. Data pribadi hanya boleh diproses dalam basis data jika hal ini diperlukan sesuai dengan Undang-Undang AI. Rincian kontak orang perseorangan yang bertanggung jawab atas pendaftaran sistem AI dan yang dapat mewakili penyedia atau pemasok dicantumkan dalam basis data.

Pemantauan Pasca-Pemasaran

Setelah sistem AI dipasarkan, penyedia harus memastikan bahwa sistem AI dipantau sesuai dengan Pasal 72 UU AI dan mendokumentasikannya dengan tepat. **Pendekatan berbasis risiko** dapat diikuti. Langkah-langkah pemantauan harus sesuai dengan jenis teknologi AI dan risiko sistem AI berisiko tinggi.

Tujuan dari sistem pemantauan pasca-pemasaran adalah untuk secara aktif dan sistematis mengumpulkan, mendokumentasikan, dan menganalisis data yang relevan untuk menilai sistem AI berisiko tinggi **sepanjang siklus hidupnya**. Penyedia harus dapat terus-menerus memeriksa kepatuhan terhadap persyaratan UU AI. Pemeriksaan interaksi dengan sistem AI lain juga dapat menjadi bagian dari sistem pemantauan. Ini berarti bahwa sistem AI berisiko tinggi setidaknya harus secara teratur berhubungan dengan penyedia untuk memberikan data yang relevan. Hal ini harus sudah diperhitungkan saat merancang sistem AI.

Sistem pemantauan pasca-pemasaran harus didasarkan pada rencana. Rencana ini merupakan bagian dari dokumentasi teknis sesuai dengan Lampiran IV UU AI. Komisi Uni Eropa menyediakan templat untuk rencana tersebut, termasuk elemen-elemen yang harus disertakan, melalui tindakan implementasi. Model ini harus dipublikasikan paling lambat enam bulan sebelum Undang-Undang AI mulai berlaku.

Jika sistem pemantauan telah dibentuk untuk sistem AI berisiko tinggi sesuai dengan Lampiran I, Bagian A Undang-Undang AI dan sesuai dengan peraturan perundang-undangan yang disebutkan di dalamnya, elemen-elemen Undang-Undang AI juga harus disertakan.

Berbagi Informasi tentang Insiden Serius

Menurut Pasal 73 UU AI, penyedia sistem AI berisiko tinggi yang dipasarkan di Uni Eropa harus melaporkan insiden tertentu. Insiden serius dari sistem AI tersebut harus dilaporkan kepada otoritas pengawasan pasar di Negara Anggota tempat insiden tersebut terjadi. Secara umum, **pemberitahuan** bergantung pada tingkat keparahan insiden. Oleh karena itu, insiden yang sangat serius harus dilaporkan secepat mungkin. Pemberitahuan dilakukan segera setelah penyedia telah menetapkan hubungan sebab akibat antara sistem AI

dan insiden atau setidaknya telah mengidentifikasi kemungkinan yang jelas. Namun, paling lambat 15 hari setelah penyedia mengetahui insiden tersebut, laporan harus dibuat. Namun, dalam kasus pelanggaran yang meluas atau insiden serius sesuai dengan Pasal 3 ayat 49 UU AI, laporan harus dibuat segera, tetapi paling lambat dua hari. Jika insiden tersebut mengakibatkan kematian seseorang, laporan juga harus dibuat segera atau sesegera mungkin setelah penyedia atau pemasok mencurigai adanya insiden serius, tetapi dalam hal apa pun tidak lebih dari sepuluh hari setelah mengetahui insiden tersebut. Penyedia atau pemasok juga memiliki opsi untuk membuat laporan awal dan memberikan laporan akhir di kemudian hari.

Setelah melaporkan insiden serius, penyedia harus melakukan investigasi yang diperlukan. Ini termasuk **penilaian risiko** insiden dan tindakan korektif. Penyedia harus bekerja sama dengan otoritas yang berwenang atau badan pelapor selama investigasi. Setiap perubahan pada sistem AI yang akan mempersulit atau mencegah evaluasi penyebab insiden tidak diizinkan tanpa memberi tahu otoritas yang berwenang terlebih dahulu. Oleh karena itu, "tindakan penutupan" dalam bentuk apa pun tidak diizinkan.

Sistem AI berisiko tinggi sesuai dengan Lampiran III UU AI atau sistem AI berisiko tinggi yang mengandung komponen keselamatan sesuai dengan Peraturan UE 2017/745 (perangkat medis) dan 2017/746 (diagnostik in vitro) yang telah dipasarkan atau dioperasikan hanya diwajibkan untuk menyampaikan laporan jika terjadi insiden sesuai dengan Pasal 3 ayat 49 UU AI, yaitu pelanggaran hak asasi manusia atau kerusakan serius terhadap properti atau lingkungan.

Penegakan Hukum

Pengawasan dan pengendalian pasar sistem AI di pasar Eropa diatur dalam Pasal 74 UU AI. **Peraturan Pengawasan Pasar** 2019/1020 berlaku untuk sistem AI yang termasuk dalam peraturan ini. Pelaku ekonomi menurut Peraturan Pengawasan Pasar adalah semua pelaku menurut Pasal 2 ayat 1 (pemasok, penyedia, importir, produsen produk) UU AI, dan sistem AI menurut UU AI juga dianggap sebagai produk.

Peraturan Pengawasan Pasar memberikan hak yang luas kepada otoritas yang berwenang, seperti **persyaratan bukti tertentu** (khususnya akses ke dokumentasi, data pengujian, langkah-langkah keamanan, antarmuka, alat untuk akses jarak jauh), **inspeksi di tempat tanpa pemberitahuan**, dan penghapusan konten daring. Jika penyedia atau pemasok mencurigai bahwa suatu produk atau sistem AI berbahaya, otoritas pengawasan pasar harus diberitahu dan tindakan korektif harus dimulai jika perlu. Dalam kondisi tertentu, otoritas pengawasan pasar juga dapat mengakses kode sumber. Akses harus diperlukan untuk memeriksa kesesuaian sistem AI berisiko tinggi dengan persyaratan yang relevan dari Undang-Undang AI dan jika dokumentasi penyedia tidak memadai terkait dengan prosedur pengujian dan audit.

Berkaitan dengan sistem AI untuk tujuan umum, ada persyaratan tambahan dalam Pasal 75. Jika sistem AI dan model AI dioperasikan oleh penyedia yang sama, Kantor AI memiliki hak untuk memantau sistem AI ini. Dalam hal ini, Kantor AI memiliki hak sebagai otoritas pengawasan pasar berdasarkan Peraturan Pengawasan Pasar. Jika otoritas nasional berpendapat bahwa sistem AI dapat digunakan untuk setidaknya satu tujuan berisiko tinggi

dan sistem ini tidak memenuhi persyaratan Undang-Undang AI, maka otoritas tersebut bekerja sama dengan Kantor AI.

Pemantauan pengujian dalam kondisi nyata dilakukan oleh otoritas pengawasan pasar sesuai dengan Pasal 76 Undang-Undang AI. Jika pengujian dilakukan dalam kondisi nyata di dalam sandbox AI, otoritas pengawasan pasar memeriksa kepatuhan terhadap Undang-Undang AI sebagai bagian dari fungsi pengawasannya untuk sandbox tersebut.

Jika otoritas pengawasan pasar diberitahu oleh calon penyedia, penyedia, atau pihak ketiga tentang insiden atau malfungsi serius, atau jika memiliki alasan untuk percaya bahwa persyaratan untuk pengujian di dunia nyata tidak dipenuhi, maka otoritas tersebut dapat menanggapi atau menghentikan pengujian ini atau menginstruksikan penyedia untuk menyesuaikan pengujian. Alasan harus diberikan untuk keputusan tersebut sehingga penyedia dapat mengajukan banding.

Otoritas untuk perlindungan hak-hak fundamental memiliki kemungkinan untuk meminta akses ke dokumentasi apa pun dari sistem AI berisiko tinggi. Otoritas tersebut memberitahukan otoritas pengawasan pasar tentang langkah tersebut. Negara-negara anggota mengidentifikasi otoritas tersebut, mempublikasikannya, dan memberitahukan kepada Komisi Uni Eropa dan semua Negara Anggota lainnya. Jika dokumentasi tidak memadai, otoritas hak fundamental dapat mengajukan permintaan yang beralasan kepada otoritas pengawasan pasar dan meminta pengujian AI berisiko tinggi.

Kerahasiaan Prosedur

Kerahasiaan prosedur berulang kali disebutkan dalam Undang-Undang AI, tetapi persyaratan utama ditetapkan dalam Pasal 78 Undang-Undang AI. Komisi Uni Eropa, otoritas pengawasan pasar, badan yang diberi pemberitahuan, dan orang atau badan hukum lain yang dipercayakan dengan penerapan Undang-Undang AI harus menjaga **kerahasiaan data dan informasi**. Hal ini berlaku untuk pelaksanaan tugas dan aktivitas mereka, tetapi khususnya mereka harus melindungi informasi dan hak-hak berikut:

- Kekayaan intelektual, informasi bisnis rahasia atau rahasia dagang dari orang perseorangan atau badan hukum, kode sumber
- Implementasi efektif Undang-Undang AI, khususnya inspeksi, investigasi, dan audit
- Kepentingan keamanan publik dan nasional
- Proses pidana dan administratif
- Informasi yang diklasifikasikan sesuai dengan hukum Uni Eropa atau nasional

Saat meminta informasi dan data, pihak berwenang wajib hanya meminta apa yang benar-benar diperlukan untuk melaksanakan tugas mereka atau untuk menentukan risiko sistem AI. Pihak berwenang dan badan-badan terkait wajib menerapkan **langkah-langkah keamanan siber** untuk menjamin keamanan dan kerahasiaan data dan informasi. Data dan informasi juga harus dihapus segera setelah tidak lagi diperlukan. Undang-Undang AI tidak menetapkan periode penghapusan tertentu; pihak berwenang dan badan-badan terkait harus merujuk pada peraturan perundang-undangan Uni Eropa atau nasional lainnya.

Untuk hal-hal yang berkaitan dengan penegakan hukum, imigrasi, atau otoritas suaka, terdapat mekanisme kerahasiaan tambahan jika pengungkapan dapat membahayakan

kepentingan keamanan nasional dan internasional. Pertukaran informasi antara pihak berwenang atau dengan Komisi Uni Eropa memerlukan konsultasi dengan otoritas nasional yang berwenang atau pengguna. Selain itu, dokumentasi teknis tetap berada di otoritas ini dan otoritas pengawasan pasar menerima akses atau salinannya. Di otoritas pengawasan pasar, hanya personel dengan izin keamanan yang sesuai yang dapat mengaksesnya.

Prosedur di Tingkat Nasional untuk menangani Sistem AI yang Menimbulkan Risiko

Menurut Pasal 3.10.11 79 Undang-Undang AI, sistem AI merupakan produk yang menimbulkan risiko sesuai dengan Pasal 3 ayat 19 Peraturan Pengawasan Pasar jika menimbulkan risiko terhadap **kesehatan, keselamatan, atau perlindungan hak-hak fundamental**. Produk atau sistem AI tersebut memengaruhi kepentingan-kepentingan tersebut dalam skala yang lebih besar daripada yang dianggap wajar dan dapat dibenarkan sehubungan dengan tujuan penggunaannya atau dalam penggunaan normal atau yang dapat diperkirakan secara wajar dari produk atau sistem AI yang bersangkutan.

Jika otoritas pengawasan pasar memiliki alasan yang wajar untuk menganggap adanya risiko tersebut, maka otoritas tersebut memeriksa sistem AI untuk memastikan kepatuhannya terhadap Undang-Undang AI. Jika terdapat **risiko terhadap hak-hak fundamental**, otoritas pengawasan pasar akan menginformasikan dan bekerja sama dengan otoritas terkait untuk memastikan kepatuhan terhadap hak fundamental yang relevan. Otoritas pengawasan pasar juga akan menginformasikan badan yang diberi wewenang, atau jika ketidakpatuhan meluas di luar wilayahnya sendiri, maka otoritas tersebut juga akan menginformasikan Komisi Uni Eropa dan Negara Anggota lainnya tentang hasil pemeriksaan dan tindakan apa pun yang wajib dilakukan oleh pemasok/penyedia jasa/importir. Pihak terakhir memastikan bahwa tindakan tersebut diimplementasikan. Jika ia gagal melakukannya, otoritas dapat **melarang** sistem AI atau **membatasi penyediaannya** atau menarik produk dari pasar atau menariknya kembali. Otoritas memberi tahu operator tentang langkah-langkah yang diambil. Otoritas menunjukkan apakah ketidakpatuhan tersebut merupakan sistem AI terlarang, kegagalan untuk mematuhi persyaratan untuk sistem AI berisiko tinggi, atau kegagalan untuk mematuhi kewajiban transparansi bagi penyedia dan penyebar sistem AI dan model GPAI tertentu sesuai dengan Pasal 52 Undang-Undang AI.

Jika baik Negara Anggota maupun Komisi Uni Eropa tidak mengajukan keberatan terhadap pemberitahuan ini, tindakan yang diambil oleh otoritas pengawasan pasar yang berwenang dianggap dibenarkan. Jika diduga bahwa sistem AI terlarang terlibat, jangka waktu dikurangi menjadi 30 hari. Setiap upaya hukum berdasarkan Peraturan Pengawasan Pasar tetap tidak terpengaruh (lihat Pasal 18 Peraturan Pengawasan Pasar).

Prosedur untuk Sistem AI yang Diklasifikasikan sebagai AI Non-berisiko Tinggi oleh Penyedia

Pasal 80 UU AI mengatur aturan prosedural jika otoritas pengawasan pasar menyimpulkan bahwa sistem AI tersebut merupakan sistem AI berisiko tinggi, sementara penyedia belum mengidentifikasi sistem AI tersebut sebagai AI berisiko tinggi dan mengklasifikasikannya sesuai dengan Lampiran III UU AI. Otoritas pengawasan pasar harus segera memberitahukan kesimpulan ini kepada penyedia dan mewajibkan penyedia untuk mengambil langkah-langkah yang tepat untuk memastikan bahwa sistem AI tersebut

mematuhi persyaratan untuk sistem AI berisiko tinggi. Jika sistem AI tersebut tidak dibatasi di wilayahnya sendiri, otoritas tersebut akan memberitahukan kepada Komisi Uni Eropa. Jika penyedia tidak mengambil **tindakan korektif** yang diperlukan, hal yang sama berlaku seperti untuk sistem AI berisiko tinggi yang masih menimbulkan risiko. Jika otoritas menetapkan bahwa penyedia telah sengaja salah mengklasifikasikan sistem AI untuk menghindari kewajiban mematuhi persyaratan yang relevan dari Peraturan AI, otoritas tersebut dapat mengenakan **sanksi**.

Pasal 81 UU AI mengatur **prosedur pengamanan** Uni Eropa. Jika suatu negara anggota mengajukan keberatan terhadap pemberitahuan suatu tindakan yang dimaksud dalam Pasal 81 ayat 5 UU AI dalam waktu tiga bulan atau jika Komisi Uni Eropa berpendapat bahwa suatu tindakan tidak sesuai, Komisi Uni Eropa akan memeriksa tindakan tersebut dan memutuskan dalam waktu sembilan bulan. Tindakan yang dibenarkan akan dilanjutkan sesuai rencana, tindakan yang tidak dibenarkan harus ditarik oleh Negara Anggota.

Sistem AI yang Sesuai tetapi Menimbulkan Risiko

Mungkin juga terjadi bahwa suatu sistem AI mematuhi Undang-Undang AI tetapi masih menimbulkan risiko terhadap kesehatan atau keselamatan atau hak-hak fundamental. Dalam hal ini, sesuai dengan Pasal 82 Undang-Undang AI, otoritas pengawasan pasar mewajibkan penyedia/pengguna/importir yang bersangkutan untuk mengambil semua **tindakan** yang sesuai yang ditentukan olehnya untuk memastikan bahwa sistem AI tersebut tidak lagi menimbulkan risiko tersebut ketika dipasarkan atau dioperasikan, atau bahwa sistem AI tersebut ditarik dari pasar atau ditarik kembali. Negara Anggota harus segera memberi tahu Komisi Uni Eropa dan Negara Anggota lainnya tentang hal tersebut. Komisi Uni Eropa harus segera melakukan **konsultasi** dan memeriksa tindakan nasional yang diambil dan memutuskan apakah tindakan tersebut dibenarkan atau tidak dan, jika perlu, mengusulkan tindakan sendiri.

Ketidaksesuaian Formal

Kriteria berikut menyebabkan ketidaksesuaian formal sesuai dengan Pasal 82 Undang-Undang AI. 83 Undang-Undang AI dan menghasilkan **permintaan** untuk memperbaiki ketidaksesuaian yang dimaksud:

- Tanda CE ditempelkan melanggar Pasal 49 Undang-Undang AI.
- Tanda CE belum ditempelkan.
- Pendaftaran dalam basis data Uni Eropa belum dilakukan.
- Jika berlaku, belum ada perwakilan resmi yang ditunjuk.
- Dokumentasi teknis tidak tersedia.

Jika ketidakpatuhan berlanjut, otoritas pengawasan pasar harus mengambil langkah-langkah yang diperlukan dan proporsional untuk membatasi atau melarang sistem AI berisiko tinggi atau menarik atau mencabutnya dari pasar.

Upaya Hukum

Sesuai dengan Pasal 85 Undang-Undang AI, hak untuk mengajukan pengaduan kepada **otoritas pengawasan pasar**. Tanpa mengurangi upaya hukum administratif atau peradilan lainnya, setiap orang atau badan hukum yang memiliki alasan untuk meyakini bahwa telah terjadi pelanggaran terhadap Undang-Undang AI dapat mengajukan pengaduan kepada

otoritas pengawasan pasar yang berwenang. Pengaduan ini akan dipertimbangkan dan diproses sesuai dengan Peraturan Pengawasan Pasar.

Hak untuk Mendapatkan Penjelasan tentang Pengambilan Keputusan

Setiap subjek data yang menjadi subjek keputusan yang dibuat oleh penyedia berdasarkan keluaran dari **sistem AI berisiko tinggi** dapat meminta dari penyedia penjelasan yang jelas dan masuk akal tentang peran sistem AI dalam proses pengambilan keputusan dan elemen utama keputusan tersebut (lihat Pasal 86 UU AI). **Prasyaratnya** adalah bahwa

- keputusan ini memiliki efek hukum, atau
- keputusan tersebut secara signifikan terpengaruh sedemikian rupa sehingga berdampak buruk pada kesehatan, keselamatan, atau hak-hak fundamental.

Hak ini tidak berlaku untuk sistem AI yang memiliki pengecualian atau pembatasan berdasarkan hukum nasional atau Uni Eropa. Jika hak ini sudah ada dalam dasar hukum lain (misalnya Pasal 22 GDPR), hak untuk mengajukan pengaduan sesuai dengan Pasal 86 UU AI tidak berlaku.

Upaya Hukum untuk GPAI

Sesuai dengan Pasal 86 UU AI, Berdasarkan Pasal 88 UU AI, **Komisi Uni Eropa** secara eksklusif berwenang untuk, tetapi dapat mendelegasikan tugas ini kepada Kantor AI. Negara-negara Anggota dapat meminta Komisi Uni Eropa untuk memenuhi tugasnya.

Penyedia hilir berhak untuk mengajukan pengaduan tentang dugaan pelanggaran Peraturan AI. **Pengaduan** harus berdasar dan memuat poin-poin berikut:

- Kontak penyedia GPAI
- Deskripsi fakta yang relevan, ketentuan yang relevan dari UU AI, dan alasan mengapa penyedia hilir menganggap model AI melanggar ketentuan tersebut
- Informasi lain yang dianggap relevan oleh penyedia hilir dan, jika berlaku, informasi yang diperolehnya atas inisiatif sendiri

Panel ilmiah dapat mengeluarkan peringatan berkualifikasi kepada Kantor AI jika memiliki alasan untuk percaya bahwa GPAI menimbulkan risiko spesifik yang dapat diidentifikasi di tingkat Uni Eropa atau bahwa GPAI memenuhi persyaratan untuk klasifikasi sebagai GPAI dengan risiko sistemik. Setelah peringatan berkualifikasi tersebut, Komisi Uni Eropa dapat, melalui Kantor AI dan setelah memberi tahu Dewan AI, menggunakan wewenang berikut untuk menilai masalah tersebut. **Peringatan yang memenuhi syarat** setidaknya memuat poin-poin berikut:

- Titik kontak penyedia GPAI dengan risiko sistem
- Deskripsi fakta yang relevan dan dasar kecurigaan
- Informasi lain yang dianggap relevan oleh panel ilmiah dan, jika berlaku, informasi yang diperoleh atas inisiatif sendiri

Komisi Uni Eropa dapat meminta penyedia untuk mendokumentasikan GPAI dan meminta informasi tambahan apa pun untuk menilai apakah penyedia mematuhi Undang-Undang AI. Sebelum mengajukan permintaan informasi, Kantor AI dapat memulai dialog terstruktur dengan penyedia GPAI, di mana pengujian internal dan langkah-langkah perlindungan dibahas dengan penyedia. Sebagai tanggapan atas permintaan yang beralasan

dari panel ilmiah, Komisi Uni Eropa dapat mengirimkan permintaan informasi kepada penyedia. Permintaan informasi akan menyatakan dasar hukum dan tujuan, informasi yang dibutuhkan, tenggat waktu untuk memberikan informasi, dan pernyataan bahwa denda dapat dikenakan jika informasi yang diberikan salah, tidak lengkap, atau menyesatkan.

Kantor AI dapat, setelah berkonsultasi dengan Dewan AI, **mengevaluasi GPAI**. Komisi Uni Eropa menilai kepatuhan penyedia terhadap Undang-Undang AI berdasarkan informasi yang diperoleh atau memeriksa risiko sistemik di tingkat Uni Eropa. Komisi Uni Eropa dapat menunjuk pakar independen untuk melakukan evaluasi atas namanya. Komisi juga dapat meminta akses ke antarmuka, alat teknis, dan bahkan kode sumber. Komisi harus memberikan justifikasi untuk hal ini. Prosedur pengujian yang tepat akan ditentukan dalam peraturan perundang-undangan terpisah.

Jika perlu dan sesuai, Komisi Uni Eropa dapat meminta penyedia untuk mengambil **tindakan** yang tepat atau mewajibkan implementasi tindakan perbaikan jika penilaian yang dilakukan telah menimbulkan kekhawatiran serius dan beralasan mengenai risiko sistemik di tingkat Uni Eropa. Jika perlu, penyedia bahkan dapat diminta untuk membatasi model AI di pasar, menariknya, atau mencabutnya. Sebelum tindakan diberlakukan, Kantor AI kembali melakukan **dialog terstruktur** dengan penyedia. Jika tindakan untuk mengurangi risiko sistemik diambil selama dialog terstruktur, Komisi Uni Eropa dapat menyatakan kewajiban ini mengikat dan tidak perlu tindakan lebih lanjut.

3.12 SANKSI DAN HUKUMAN

Pasal 99 dan seterusnya UU AI mengatur sanksi. Tergantung pada jenis pelanggaran UU AI, berbagai tingkat atau jenis hukuman dapat dikenakan. Menurut Pasal 99 UU AI, Negara Anggota wajib menetapkan hukuman dan mengambil semua tindakan yang diperlukan untuk **penegakan UU AI yang tepat dan efektif**. Ini dapat berupa denda tetapi juga peringatan dan tindakan non-finansial lainnya. Sanksi harus **efektif, proporsional, dan bersifat pencegahan**. Namun, sanksi juga harus mempertimbangkan kepentingan UKM dan perusahaan rintisan serta kelangsungan ekonomi mereka. Jika hukuman akan dikenakan kepada mereka, maka dasar perhitungan yang lebih rendah dari berikut ini harus digunakan.

Jumlah Denda (mana yang lebih tinggi)	Sifat Pelanggaran
Hingga ▪ Rp. 300 miliar atau ▪ 7% dari total penjualan tahunan global pada tahun keuangan sebelumnya	▪ Pasal 5 UU AI (sistem AI yang dilarang)
Hingga ▪ Rp. 150 miliar atau ▪ 3% dari total omset tahunan di seluruh dunia pada tahun keuangan sebelumnya	▪ Kewajiban penyedia sesuai dengan Pasal 16 UU AI ▪ Kewajiban perwakilan resmi sesuai dengan Pasal 22 UU AI ▪ Kewajiban importir sesuai dengan Pasal 23 UU AI

	▪ Kewajiban distributor sesuai dengan Pasal 24 UU AI ▪ Persyaratan dan kewajiban badan yang diberi wewenang sesuai dengan Pasal 31, 33 ayat 1, 3, 4 dan Pasal 34 UU AI ▪ Kewajiban transparansi bagi penyedia dan pengguna sesuai dengan Pasal 50 UU AI
Hingga ▪ Rp. 75 miliar dan ▪ 1% dari total omset tahunan di seluruh dunia pada tahun keuangan sebelumnya	▪ Memberikan informasi yang salah, tidak lengkap, atau menyesatkan kepada badan yang berwenang dan otoritas nasional yang kompeten atas permintaan informasi mereka.

Jika sanksi akan dijatuhkan, pihak berwenang wajib mempertimbangkan setiap kasus secara individual dan harus memperhitungkan semua keadaan dan situasi spesifik. Mereka harus mempertimbangkan poin-poin berikut:

- Sifat, tingkat keparahan, dan durasi pelanggaran serta konsekuensinya: Dengan mempertimbangkan tujuan sistem AI dan, jika berlaku, jumlah orang yang terpengaruh dan besarnya kerugian yang mereka derita.
- Sanksi yang dijatuhkan oleh otoritas pengawasan pasar: Jika otoritas pengawasan pasar telah menjatuhkan denda kepada operator dalam kasus yang sama.
- Sanksi yang dijatuhkan: Apakah otoritas lain telah menjatuhkan denda kepada produsen atau pemasok yang sama berdasarkan aktivitas atau kelalaian yang sama?
- Ukuran, omset tahunan, dan pangsa pasar operator yang melakukan pelanggaran.
- Faktor-faktor yang meringankan atau memberatkan lainnya: Keuntungan yang diperoleh atau kerugian yang dihindari secara langsung atau tidak langsung sebagai akibat dari pelanggaran harus diperhitungkan.
- Jenis kerja sama dengan pihak berwenang: Sejauh mana operator telah bekerja sama dengan pihak berwenang yang berwenang untuk mengakhiri pelanggaran dan mengurangi kemungkinan dampak negatif.
- Tanggung jawab operator: Pertimbangan langkah-langkah teknis dan organisasi yang diambil.
- Pemberitahuan pelanggaran kepada pihak berwenang: Bagaimana pelanggaran tersebut sampai ke perhatian pihak berwenang dan sejauh mana penyedia melaporkan pelanggaran tersebut.
- Niat dan kelalaian pelanggaran.
- Langkah-langkah yang diambil oleh penyedia untuk mengurangi kerugian yang diderita oleh pihak yang bersangkutan.

Mirip dengan GDPR, terserah kepada Negara Anggota untuk menentukan sejauh mana denda dapat dikenakan kepada otoritas dan badan publik yang didirikan di Negara Anggota yang bersangkutan. Namun, Pengawas Perlindungan Data Eropa dapat mengenakan denda

kepada lembaga, badan, kantor, dan badan Uni Eropa dalam kondisi serupa sesuai dengan Pasal 100 UU AI, meskipun denda tersebut ditetapkan pada tingkat yang lebih rendah.

Bergantung pada struktur sistem hukum negara anggota, hal ini menentukan apakah otoritas atau pengadilan dapat mengenakan denda. Namun, tidak boleh ada perbedaan dalam dampak hukuman. **Upaya hukum** yang sesuai harus diatur **dalam hukum nasional** terhadap tindakan penegakan hukum oleh otoritas pengawasan pasar. Selain itu, Negara Anggota melaporkan semua denda yang dikenakan dan sengketa hukum atau proses pengadilan terkait kepada Komisi Uni Eropa.

Terdapat persyaratan tambahan untuk **hukuman yang berkaitan dengan GPAI** sesuai dengan Pasal 101 Undang-Undang AI.

Komisi Uni Eropa dapat mengenakan denda kepada penyedia model AI untuk tujuan umum. Denda tidak boleh melebihi **3% dari omset tahunan di seluruh dunia** pada tahun keuangan sebelumnya atau Rp.150 miliar, mana pun yang lebih tinggi. Sanksi dapat dikenakan paling cepat satu tahun setelah berlakunya Undang-Undang AI agar penyedia memiliki waktu untuk menyesuaikan model AI mereka jika perlu, apabila Komisi Uni Eropa menetapkan adanya kesengajaan atau kelalaian:

- pelanggaran terhadap ketentuan yang relevan dalam Undang-Undang AI,
- kegagalan untuk menindaklanjuti permintaan dokumen atau informasi atau penyediaan dokumen palsu, tidak lengkap, atau menyesatkan;
- Kegagalan untuk memberikan akses kepada Komisi Uni Eropa terhadap model AI dengan risiko sistemik untuk melakukan penilaian.
- Saat menentukan denda atau pembayaran sanksi berkala, Komisi Uni Eropa harus mempertimbangkan hal-hal berikut:
 - Sifat, tingkat keparahan, dan durasi pelanggaran
 - Prinsip proporsionalitas dan kesesuaian
 - kode etik apa pun

Sebelum Komisi Uni Eropa mengenakan denda, Komisi harus memberitahukan penyedia model AI dengan risiko sistemik tentang temuan pendahuluan dan memberikan **kesempatan untuk memberikan komentar**. Komisi juga mengkomunikasikan hasil investigasi kepada Dewan AI. Mahkamah Eropa (ECJ) memiliki kewenangan untuk meninjau keputusan Komisi Uni Eropa. Mahkamah dapat mencabut, mengurangi, atau meningkatkan denda. Tata cara pasti dari prosedur tersebut masih akan ditentukan oleh Komisi Uni Eropa melalui peraturan pelaksana.

3.13 UKM DAN PERUSAHAAN RINTISAN DALAM UNDANG-UNDANG AI

Undang-Undang AI dimaksudkan tidak hanya untuk mengatur sistem AI dan memastikan tingkat perlindungan kepentingan publik yang tinggi seperti kesehatan dan keselamatan serta perlindungan hak-hak fundamental, tetapi juga untuk mempromosikan pengembangan, penggunaan, dan penyebaran AI. Undang-Undang AI mempertimbangkan UKM (usaha kecil dan menengah) dan perusahaan rintisan sehingga mereka juga dapat mengejar pendekatan inovatif. Hal ini telah disebutkan dalam Pasal 1 ayat 2 huruf g Undang-

Undang AI, yang menyatakan bahwa ada “*langkah-langkah untuk mendukung inovasi, dengan fokus khusus pada UKM, termasuk perusahaan rintisan*”. Ini tidak berarti bahwa UKM dan perusahaan rintisan sebagian besar dikecualikan atau bahwa ada pengecualian yang jelas terhadap penerapannya, tetapi Uni Eropa telah mempertimbangkan kebutuhan UKM dan perusahaan rintisan ketika menyusun Undang-Undang AI. Pembuat undang-undang menyadari bahwa mereka seringkali tidak memiliki departemen hukum sendiri dan umumnya memiliki sedikit karyawan.

Oleh karena itu, bagian ini merangkum berbagai pengecualian dan penyederhanaan untuk UKM dan perusahaan rintisan. Menurut Rekomendasi 2003/61 dari Komisi Uni Eropa, UKM didefinisikan sebagai berikut:

	Jumlah maksimum karyawan	Omzet maksimum	Total neraca maksimum
Perusahaan menengah	250	Rp. 500 miliar	Rp. 430 miliar
Perusahaan kecil	50	Rp. 100 miliar	Rp. 100 miliar
Usaha mikro	10	Rp. 20 miliar	Rp. 20 miliar

Tidak ada definisi istilah “start-up” yang berlaku di seluruh Eropa, tetapi permohonan pendanaan dapat menentukan berapa lama perusahaan Rp.tersebut telah berdiri atau seberapa besar ukurannya.

Fasilitasi dan Pengecualian untuk UKM dan Start-up

Memfasilitasi Dokumentasi Teknis

Sesuai dengan Pasal 11 UU AI, dokumentasi teknis harus disiapkan untuk sistem AI berisiko tinggi sebelum dipasarkan atau dioperasikan. Dokumentasi tersebut juga harus selalu mutakhir, yaitu perkembangan lebih lanjut harus selalu diperhitungkan. Konten minimum diatur dalam Lampiran IV UU AI.

UKM dan start-up dapat menyediakan konten ini dengan cara yang disederhanakan. Komisi Uni Eropa menyediakan formulir yang disederhanakan sebagai templat untuk tujuan ini. UKM atau start-up dapat memilih untuk menggunakan formulir yang disederhanakan atau Lampiran IV. Namun, jika memilih dokumentasi yang disederhanakan, formulir Komisi Uni Eropa harus digunakan. Badan yang diberi wewenang kemudian harus menerima hal ini untuk tujuan penilaian kesesuaian.

Akses Sederhana ke Sandbox AI

Sandbox AI harus tersedia di seluruh Uni Eropa dan hambatan bagi UKM harus dihilangkan. Pasal 57 UU AI mengatur sandbox AI dengan tujuan eksplisit untuk mempromosikan inovasi (lihat bagian 3.8 Sandbox AI). Sesuai dengan Pasal 57 ayat 9 huruf e UU AI, UKM dan perusahaan rintisan diberikan akses yang lebih mudah dan cepat ke laboratorium nyata sehingga sistem AI dapat dipasarkan atau dioperasikan lebih cepat. Hal ini harus diperhitungkan oleh otoritas yang berwenang saat mendirikan sandbox AI. Pertimbangan 139 UU AI juga menekankan hal ini. Partisipasi dalam sandbox AI harus berfokus pada isu-isu di mana terdapat ketidakpastian hukum di antara penyedia dan calon penyedia.

Fokusnya juga pada pengembangan, pelatihan, pengujian, dan validasi sebelum sistem AI dipasarkan atau dioperasikan.

Menurut Pasal 58 ayat 2 huruf d UU AI, akses ke laboratorium AI umumnya gratis untuk UKM dan perusahaan rintisan; namun, otoritas yang berwenang dapat meminta biaya luar biasa, tetapi biaya tersebut harus adil dan proporsional. Selain itu, prosedur, proses, dan persyaratan administratif untuk aplikasi, seleksi, partisipasi, dan keluar dari sandbox AI harus dirancang sedemikian rupa sehingga UKM dan perusahaan rintisan dengan kapasitas hukum dan administratif yang terbatas juga dapat dengan mudah memenuhi hak dan kewajiban mereka. Prosedur, aplikasi, dan lainnya. harus mudah dipahami dan dikomunikasikan dengan jelas (lihat Pasal 58 ayat 2 huruf g UU AI). Otoritas yang mengoperasikan laboratorium AI juga harus merujuk UKM dan perusahaan rintisan ke lembaga yang menawarkan panduan tentang implementasi UU AI, memberikan bantuan dengan dokumen standarisasi, dan lainnya., jika diperlukan.

Langkah-langkah untuk UKM dan Perusahaan Rintisan

Pasal 62 UU AI mengatur langkah-langkah untuk UKM dan perusahaan rintisan yang bertindak sebagai penyedia dan pengembang. Namun, hal-hal ini harus terlebih dahulu diimplementasikan ke dalam hukum nasional, di sinilah peran negara-negara anggota dan khususnya Kantor AI. **Negara-negara anggota** harus mengambil langkah-langkah berikut:

- **Akses prioritas ke sandbox AI:** UKM dan perusahaan rintisan yang berbasis atau memiliki cabang di Uni Eropa memiliki akses prioritas, tetapi tetap harus memenuhi persyaratan penerimaan dan kriteria seleksi meskipun memiliki akses prioritas. Namun, akses prioritas tidak boleh menghalangi penyedia lain untuk mendapatkan akses.
- **Langkah-langkah peningkatan kesadaran dan pelatihan:** Negara-negara anggota harus menyediakan langkah-langkah peningkatan kesadaran dan pelatihan tentang penerapan Undang-Undang AI yang disesuaikan dengan kebutuhan UKM, perusahaan rintisan, pengembang, dan pemerintah daerah. Langkah-langkah ini belum diimplementasikan di negara-negara anggota.
- **Saluran komunikasi:** Negara-negara anggota harus menggunakan saluran komunikasi yang ada atau membangun saluran komunikasi baru untuk memberikan saran tentang implementasi Undang-Undang AI dan untuk menjawab pertanyaan mengenai partisipasi dalam sandbox AI. Tujuannya adalah untuk memberikan dukungan selama seluruh proses pengembangan, menawarkan panduan, dan menjawab pertanyaan tentang implementasi Undang-Undang AI. Jika terdapat saluran yang berbeda, mereka harus bekerja sama jika perlu untuk menciptakan sinergi dan memastikan homogenitas.
- **Partisipasi dalam pengembangan standar:** Negara-negara Anggota harus mendorong partisipasi UKM dan pemangku kepentingan terkait lainnya dalam pengembangan standar.
- **Biaya untuk penilaian kesesuaian:** Saat menetapkan biaya sesuai dengan Pasal 43 UU AI, perhatian diberikan untuk memastikan bahwa biaya tersebut ditetapkan secara

proporsional dengan ukuran perusahaan, ukuran pasarnya, dan angka-angka kunci yang relevan. Komisi Uni Eropa harus secara teratur menilai biaya sertifikasi dan kepatuhan untuk UKM dan perusahaan rintisan dan bekerja sama dengan Negara-negara Anggota untuk membatasi biaya ini.

Kantor AI juga mengambil langkah-langkah khusus untuk UKM dan perusahaan rintisan:

- **Contoh dan templat:** Kantor AI menyediakan templat standar.
- **Platform informasi pusat:** Kantor AI memperkenalkan platform informasi pusat yang akan menyediakan informasi yang mudah digunakan tentang Undang-Undang AI kepada semua pemangku kepentingan di Uni Eropa.
- **Kampanye informasi:** Kampanye ini bertujuan untuk meningkatkan kesadaran akan kewajiban yang timbul dari Undang-Undang AI.
- **Prosedur pengadaan:** Kantor AI mengevaluasi dan mempromosikan konsolidasi praktik terbaik dalam prosedur pengadaan yang melibatkan sistem AI.

Usaha Mikro

Pasal 63 UU AI memberikan penyederhanaan lebih lanjut untuk usaha mikro. Ini dapat mencakup elemen-elemen tertentu sesuai dengan Pasal 17 UU AI (sistem manajemen mutu, Kewajiban Penyedia, Penyebar, dan Pihak Lain yang Terlibat) dengan cara yang disederhanakan. Untuk tujuan ini, Komisi Uni Eropa akan menyusun pedoman yang mempertimbangkan kebutuhan usaha mikro di satu sisi, tetapi juga tingkat perlindungan atau kebutuhan untuk mematuhi persyaratan yang berkaitan dengan AI berisiko tinggi. Namun, kemudahan ini tidak boleh diartikan sebagai pengecualian dari kewajiban berdasarkan Pasal 9 dan seterusnya UU AI.

Sanksi

Menurut Pasal 99 UU AI, sanksi harus efektif, proporsional, dan bersifat mencegah. Namun, pada saat yang sama, kepentingan dan khususnya kelangsungan ekonomi UKM dan perusahaan rintisan juga harus dipertimbangkan. Ketika menjatuhkan denda, jumlah yang lebih rendah dari paragraf 3, 4 dan 5 harus dikenakan sesuai dengan Pasal 99 ayat 6 UU AI (lihat bagian 3.10). Sesuai dengan Pertimbangan 168 UU AI, denda dinilai berdasarkan kasus per kasus dan keadaan yang relevan dari situasi tersebut harus diperhitungkan, khususnya sifat, tingkat keparahan dan durasi pelanggaran serta konsekuensinya dan juga ukuran penyedia.

Daftar Periksa: Meluncurkan Sistem AI Baru Sesuai dengan UU AI

Berikut ini adalah garis besar pertanyaan yang harus dijawab oleh UKM atau perusahaan rintisan ketika ingin memasarkan atau memesan sistem AI baru. Langkah-langkah pengujian harus didokumentasikan dalam setiap kasus. Fokusnya adalah pada langkah-langkah yang diperlukan sesuai dengan UU AI.

Apakah sistem AI sesuai dengan Pasal 3 ayat 1 UU AI sudah ada?

Sistem AI adalah *“sistem berbasis mesin yang dirancang untuk beroperasi dengan berbagai tingkat otonomi dan yang dapat menunjukkan kemampuan adaptasi setelah diterapkan, dan yang, untuk tujuan eksplisit atau implisit, menyimpulkan, dari masukan yang*

diterimanya, bagaimana menghasilkan keluaran seperti prediksi, konten, rekomendasi, atau keputusan yang dapat memengaruhi lingkungan fisik atau virtual” (lihat detail bagian 3.1).

- Jika **ya**, lanjutkan.
- Jika **tidak**, akhiri di sini.

Apakah sistem AI menggunakan data pribadi?

Lihat Pasal 4 ayat 1 GDPR, yang menyatakan bahwa data pribadi adalah *“setiap informasi yang berkaitan dengan orang perseorangan yang teridentifikasi atau dapat diidentifikasi (‘subjek data’); orang perseorangan yang dapat diidentifikasi adalah orang yang dapat diidentifikasi, secara langsung atau tidak langsung, khususnya dengan merujuk pada pengenal seperti nama, nomor identifikasi, data lokasi, pengenal daring atau satu atau lebih faktor spesifik yang berkaitan dengan identitas fisik, fisiologis, genetik, mental, ekonomi, budaya atau sosial dari orang perseorangan tersebut”*. Tidak masalah apakah data pribadi diperlukan untuk pengembangan, pengujian, pelatihan, dan/atau penggunaan.

- Jika **ya**, kepatuhan terhadap GDPR diperlukan, lihat bab 4.
- Jika **tidak**, misalnya saat menggunakan data anonim, kepatuhan terhadap GDPR tidak diperlukan.

Sistem Kecerdasan Artifisial yang Dilarang atau Berisiko Tinggi

Apakah terdapat sistem kecerdasan artifisial yang dilarang berdasarkan Pasal 5 Undang-Undang Kecerdasan Artifisial (AI Act)?

Sistem kecerdasan artifisial yang dilarang, misalnya, adalah sistem yang secara sengaja memanipulasi atau menyesatkan sehingga menyebabkan seseorang mengambil keputusan yang dalam kondisi normal tidak akan diambilnya; sistem yang mengeksploitasi kelompok rentan; sistem pemeringkatan sosial (*social scoring*); dan lain sebagainya.

- Jika **ya**, proses dihentikan pada tahap ini, karena sistem kecerdasan artifisial tersebut sangat mungkin tidak dapat dioperasikan atau diedarkan di pasar.
- Jika **tidak**, lanjutkan ke tahap berikutnya.

Apakah terdapat AI berisiko tinggi sesuai dengan Pasal 6 AI Act?

Sistem AI berisiko tinggi dianggap ada apabila sistem tersebut merupakan produk atau komponen keselamatan sesuai dengan peraturan harmonisasi yang tercantum dalam Lampiran I (daftar peraturan perundang-undangan yang diharmonisasikan); atau Sistem tersebut merupakan sistem AI sebagaimana dimaksud dalam Lampiran III AI Act (daftar “kasus penggunaan”).

- Jika **ya**, apakah terdapat pengecualian?
Pasal 6 ayat (3) AI Act menetapkan sejumlah pengecualian mengenai kondisi di mana suatu sistem AI berisiko tinggi tidak dianggap ada, misalnya apabila sistem AI tersebut hanya melaksanakan tugas prosedural yang didefinisikan secara sempit, atau apabila sistem tersebut dimaksudkan untuk mengenali pola tanpa menggantikan atau memengaruhi penilaian manusia yang telah diselesaikan sebelumnya. Namun demikian, pembuatan profil (*profiling*) terhadap orang perseorangan selalu mengakibatkan klasifikasi sebagai AI berisiko tinggi.

- Jika terdapat AI berisiko tinggi dan tidak ada pengecualian yang berlaku, lihat bagian berikut mengenai kepatuhan serta mengenai kewajiban dan persyaratan.
- Dokumentasikan proses pengujian dan hasilnya, terlepas dari apakah sistem AI berisiko tinggi tersebut ada atau tidak.

Apakah diperlukan Penilaian Dampak terhadap Hak-Hak Fundamental (Fundamental Rights Assessment/FRA)?

Untuk sistem AI berisiko tinggi tertentu, wajib dilakukan penilaian dampak terhadap hak-hak fundamental sesuai dengan Pasal 27 AI Act, yaitu terhadap:

- Sistem AI yang tercantum dalam Lampiran III, dalam hal digunakan oleh badan hukum publik dan badan swasta yang menyediakan layanan publik.
- Sistem AI sebagaimana dimaksud dalam Lampiran III angka 5 huruf b dan c (aksesibilitas dan penggunaan layanan serta manfaat dasar swasta dan publik), apabila digunakan oleh *deployer*, tanpa memandang apakah merupakan badan hukum publik atau badan swasta penyedia layanan publik.

Pengecualian:

- Lampiran III angka 2 (infrastruktur kritis) — tidak memerlukan penilaian dampak terhadap hak-hak fundamental.

Berdasarkan peran apa perusahaan atau rintisan (start-up) beroperasi?

- Penyedia (Provider) *“adalah orang perseorangan atau badan hukum, otoritas publik, lembaga, atau badan lainnya yang mengembangkan sistem AI atau model AI tujuan umum, atau yang mengembangkan sistem AI atau model AI tujuan umum dan menempatkannya di pasar atau mulai mengoperasikannya atas nama atau merek dagangnya sendiri, baik dengan imbalan maupun tanpa imbalan”* sebagaimana dimaksud dalam Pasal 3 angka 3 AI Act.
- Pengguna (Deployer) menurut Pasal 3 angka 4 AI Act adalah *“orang perseorangan atau badan hukum, otoritas publik, lembaga, atau badan lainnya yang menggunakan sistem AI di bawah kewenangannya, kecuali apabila sistem AI tersebut digunakan dalam rangka kegiatan pribadi yang bersifat nonprofessional”*.
- Perwakilan Resmi (Authorized Representative) sesuai Pasal 3 angka 5 AI Act adalah *“orang perseorangan atau badan hukum yang berlokasi atau didirikan di Uni Eropa dan telah menerima serta menyetujui mandat tertulis dari penyedia sistem AI atau model AI tujuan umum untuk, atas namanya, melaksanakan kewajiban dan prosedur yang ditetapkan dalam peraturan ini”*.
- Importir (Importer) menurut Pasal 3 angka 6 AI Act adalah *“orang perseorangan atau badan hukum yang berlokasi atau didirikan di Uni Eropa yang menempatkan di pasar suatu sistem AI yang menggunakan nama atau merek dagang dari orang perseorangan atau badan hukum yang didirikan di negara ketiga”*.
- Distributor (Distributor) menurut Pasal 3 angka 7 AI Act adalah *“orang perseorangan atau badan hukum dalam rantai pasok, selain penyedia atau importir, yang menyediakan sistem AI di pasar Uni Eropa”*.

- Operator (Operator) menurut Pasal 3 angka 8 AI Act adalah “*penyedia, produsen produk, pengguna, perwakilan resmi, importir, atau distributor*”.

Penetapan Kepatuhan Sistem AI Berisiko Tinggi (lihat Pasal 8 dan seterusnya AI Act)

- Kewajiban umum bagi sistem AI berisiko tinggi sesuai dengan Pasal 8 dan seterusnya AI Act.
 - Sistem manajemen risiko sesuai dengan Pasal 9 AI Act.
 - Data dan tata kelola data sesuai dengan Pasal 10 AI Act.
 - Dokumentasi teknis sesuai dengan Pasal 11 AI Act (termasuk pengecualian bagi usaha kecil dan menengah/UKM serta perusahaan rintisan, yang dapat menggunakan formulir sederhana yang disediakan oleh Komisi Eropa).
 - Kewajiban pencatatan (logging) sesuai dengan Pasal 12 AI Act.
 - Transparansi dan penyediaan informasi kepada pengguna (deployer) sesuai dengan Pasal 13 AI Act.
 - Pengawasan manusia sesuai dengan Pasal 14 AI Act.
 - Akurasi, ketahanan (robustness), dan keamanan siber sesuai dengan Pasal 15 AI Act.
- Kepatuhan tergantung pada peran
 - **Penyedia, lihat Pasal 16 UU AI**
 - Sistem manajemen mutu sesuai dengan Pasal 17 UU AI
 - Penyimpanan dokumentasi sesuai dengan Pasal 18 UU AI
 - Protokol sesuai dengan Pasal 19 UU AI
 - Tindakan korektif dan kewajiban untuk memberi informasi sesuai dengan Pasal 20 UU AI
 - Kerja sama dengan otoritas yang berwenang sesuai dengan Pasal 21 UU AI
 - Jika berlaku, peran perwakilan resmi penyedia sesuai dengan Pasal 22 UU AI
 - Jika berlaku, perjanjian dengan pihak ketiga dari mana sistem AI atau bagian-bagiannya berasal, lihat Pasal 25 ayat 4 UU AI
 - Kepatuhan terhadap standar yang harmonis sesuai dengan Pasal 40 UU AI,
 - Jika berlaku, prosedur penilaian kesesuaian sesuai dengan Pasal 42 UU AI,
 - Deklarasi Kesesuaian UE sesuai dengan Pasal 40 UU AI 47 UU AI,
 - Pendaftaran sistem AI berisiko tinggi sesuai dengan Pasal 49 UU AI
 - Jika sistem AI berinteraksi dengan orang perseorangan, kepatuhan terhadap kewajiban transparansi sesuai dengan Pasal 50 ayat 1 UU AI, lihat bagian 3.6
 - Kepatuhan terhadap kewajiban transparansi dalam kasus “deep fake” sesuai dengan Pasal 50 ayat 2 UU AI, lihat bagian 3.6
 - Pemantauan sistem AI setelah dipasarkan sesuai dengan Pasal 72 UU AI
 - **Importir, lihat Pasal 23 UU AI**
 - Jika sistem AI atau bagian-bagiannya berasal dari pihak ketiga, lihat Tanggung Jawab di sepanjang rantai nilai AI sesuai dengan Pasal 25 UU AI
 - **Pedagang, lihat Pasal 24 UU AI**
 - Jika sistem AI atau bagian-bagiannya berasal dari pihak ketiga, lihat Tanggung Jawab di sepanjang rantai nilai AI sesuai dengan Pasal 25 UU AI

▪ **Pengguna, lihat Pasal 26 UU AI**

- Jika sistem AI atau bagian-bagiannya berasal dari pihak ketiga, lihat tanggung jawab di sepanjang rantai nilai AI sesuai dengan Pasal 25 UU AI
- Langkah-langkah teknis dan organisasi untuk pengoperasian sistem AI, memastikan literasi AI, dan lainnya. (lihat bagian 3.2)
- Pendaftaran sistem AI berisiko tinggi sesuai dengan Pasal 49 UU AI
- Kewajiban transparansi untuk sistem pengenalan emosi atau sistem untuk kategorisasi biometrik sesuai dengan Pasal 50 ayat 3 UU AI (lihat bagian 3.6)
- Kepatuhan terhadap kewajiban transparansi untuk “deep fake” sesuai dengan Pasal 50 ayat 4 UU AI, lihat bagian 3.6
- Jika berlaku, hak untuk penjelasan sesuai dengan Pasal 50 ayat 4 UU AI. Pasal 86 UU AI ketika sistem AI membuat keputusan tentang individu

Sistem AI dengan Tujuan Umum

Apakah terdapat sistem AI dengan tujuan umum atau GPAI (Kecerdasan Buatan Tujuan Umum) sesuai dengan Pasal 3 ayat 63 UU AI?

GPAI adalah “*model AI, termasuk di mana model AI tersebut dilatih dengan sejumlah besar data menggunakan pengawasan mandiri dalam skala besar, yang menunjukkan generalitas yang signifikan dan mampu secara kompeten melakukan berbagai tugas yang berbeda terlepas dari cara model tersebut dipasarkan dan yang dapat diintegrasikan ke dalam berbagai sistem atau aplikasi hilir, kecuali model AI yang digunakan untuk kegiatan penelitian, pengembangan, atau pembuatan prototipe sebelum dipasarkan*”. Saat ini, banyak sistem yang merupakan GPAI, terutama AI generatif untuk teks, gambar, kode pemrograman, dan lainnya.

- Jika **ya**, lihat bagian 3.7 (GPAI) dan bagian 3.5 (Standar Terharmonisasi, Penilaian Kesesuaian, Sertifikat dan Registrasi)
- Jika **ya**, sub-pertanyaan apakah ada GPAI dengan apa yang disebut “risiko sistemik”: Menurut Pasal 3 No. 65 UU AI, risiko sistemik adalah “*risiko yang spesifik terhadap kemampuan berdampak tinggi dari model AI tujuan umum, yang memiliki dampak signifikan pada pasar Uni Eropa karena jangkauannya, atau karena dampak negatif yang sebenarnya atau yang dapat diperkirakan secara wajar terhadap kesehatan masyarakat, keselamatan, keamanan publik, hak-hak dasar, atau masyarakat secara keseluruhan, yang dapat menyebar dalam skala besar di seluruh rantai nilai*”.
- Jika **ya**, lihat di bawah untuk kewajiban atau bagian 3.7 GPAI.

Menetapkan kepatuhan model GPAI sesuai dengan Pasal 3 No. 65 UU AI. 51 UU AI
Pemberitahuan kepada Komisi Uni Eropa sesuai dengan Pasal 52 UU AI

- Kewajiban **penyedia** sesuai dengan Pasal 53 UU AI
 - Dokumentasi teknis model (lihat Lampiran XI UU AI)
 - Informasi dan dokumentasi untuk penyedia hilir
 - Kerja sama dengan Komisi Uni Eropa (lihat khususnya Pasal 91 UU AI) atau otoritas yang berwenang
 - Penggunaan standar yang harmonis sesuai dengan Pasal 56 UU AI atau panduan praktis untuk menunjukkan kepatuhan terhadap Pasal 53 ayat 1 UU AI

- Penggunaan tindakan delegasi sesuai dengan Pasal 97 UU AI untuk menunjukkan kepatuhan terhadap Lampiran XI UU AI
- Langkah-langkah implementasi yang diberikan oleh Komisi Uni Eropa sesuai dengan Pasal 93 UU AI
- Kewajiban **perwakilan resmi** penyedia model GPAI sesuai dengan Pasal 54 UU AI
 - (Hanya berlaku jika penyedia berkedudukan di negara ketiga!)
 - Penunjukan tertulis perwakilan resmi
 - Peninjauan dokumentasi teknis
 - Penyediaan salinan dokumentasi teknis
 - Penyediaan semua dokumen yang diperlukan untuk membuktikan kepatuhan terhadap kewajiban berdasarkan UU AI
 - Kerja sama dengan Kantor AI dan otoritas yang berwenang
 - Kewajiban perwakilan resmi untuk mengakhiri pesanan jika ia berpendapat atau memiliki alasan untuk percaya bahwa penyedia melanggar kewajibannya berdasarkan UU AI, termasuk kewajiban untuk memberi tahu Kantor AI

Kewajiban tambahan untuk GPAI dengan risiko sistemik sesuai dengan Pasal 54 UU AI. 53 UU AI

- Evaluasi model
- Menilai dan mengurangi potensi risiko sistemik
- Informasi tentang insiden serius dan kemungkinan tindakan perbaikan, termasuk pelaporan ke kantor AI dan, jika berlaku, otoritas yang berwenang
- Langkah-langkah keamanan siber yang tepat
- Penggunaan standar yang harmonis sesuai dengan Pasal 56 UU AI atau panduan praktis untuk menunjukkan kepatuhan terhadap Pasal 55 ayat 1 UU AI

BAB 4

PERLINDUNGAN DATA

4.1 PENDAHULUAN

Di dunia saat ini, di mana manusia dan mesin semakin banyak bekerja sama dan menghasilkan sejumlah besar data, kepatuhan terhadap Peraturan Perlindungan Data Umum (GDPR) merupakan salah satu tantangan dan peluang terbesar bagi pengembang, perusahaan, dan masyarakat. Peraturan Uni Eropa yang utama ini, yang mulai berlaku di semua negara anggota pada tanggal 25 Mei 2018, mengatur pemrosesan data pribadi yang sepenuhnya atau sebagian otomatis, serta pemrosesan data pribadi yang tidak otomatis yang disimpan atau dimaksudkan untuk disimpan dalam sistem file (Pasal 2 ayat 1 GDPR).

Tujuan utamanya adalah untuk menstandarisasi dan memperkuat hak perlindungan data individu di era digital tanpa menghambat inovasi. Aspek lainnya adalah untuk memfasilitasi pergerakan data secara bebas di dalam pasar Eropa (Pasal 1 GDPR).

GDPR menggantikan Arahan Perlindungan Data sebelumnya dari tahun 1995 dan membawa perubahan signifikan bagi semua perusahaan dan lembaga publik, karena peraturan ini berlaku untuk semua organisasi yang memproses data pribadi, terlepas dari ukuran, omset, bentuk perusahaan, atau industri. Ini berlaku untuk pedagang individu maupun perusahaan multinasional.

Meskipun GDPR adalah peraturan Uni Eropa, dampaknya bersifat global. Setiap perusahaan di seluruh dunia yang menawarkan layanan di Uni Eropa atau memproses data warga negara Uni Eropa harus mematuhi peraturan ini, terlepas dari di mana organisasi tersebut berkantor pusat.

Penegakan GDPR dilakukan oleh otoritas perlindungan data lokal di setiap negara anggota Uni Eropa. Otoritas ini memiliki wewenang untuk melakukan investigasi dan menjatuhkan sanksi. Peraturan ini memberi wewenang kepada otoritas perlindungan data nasional untuk menjatuhkan hukuman yang signifikan kepada organisasi atas pelanggaran, termasuk denda hingga 20 juta euro atau 4% dari omset global tahunan, mana pun yang lebih tinggi.

Saat memproses data menggunakan kecerdasan buatan, GDPR memberlakukan standar tinggi yang sama yang berlaku untuk semua jenis pemrosesan data lainnya. Ini termasuk kepatuhan terhadap prinsip-prinsip pemrosesan, kebutuhan akan dasar hukum untuk pemrosesan, perlindungan hak-hak subjek data, dan aturan khusus untuk pengambilan keputusan otomatis dan pembuatan profil. Oleh karena itu, disarankan untuk melibatkan pakar perlindungan data dalam proyek AI. Jika petugas perlindungan data telah ditunjuk, mereka harus menjadi bagian dari tim proyek sejak awal.

Pentingnya perlindungan data dalam konteks AI muncul dari beberapa skenario:

1. Pelatihan dan pengoperasian AI dengan data pribadi

Sistem AI sering memproses sejumlah besar data pribadi untuk belajar, mengenali pola, dan membuat keputusan. GDPR mengatur bagaimana data tersebut dapat dikumpulkan, disimpan, diproses, dan ditransfer untuk melindungi privasi individu.

2. Transparansi dan akuntabilitas

GDPR mengharuskan organisasi untuk transparan tentang bagaimana dan untuk tujuan apa data pribadi diproses. Dalam kasus sistem AI, ini berarti bahwa algoritma dan prosedur pemrosesan data yang mendasarinya harus diungkapkan sampai batas tertentu untuk memastikan kepatuhan terhadap hukum.

3. Hak untuk penjelasan

GDPR memberi individu hak untuk mendapatkan penjelasan atas keputusan otomatis yang memengaruhi mereka. Ini sangat relevan untuk keputusan AI, yang sering kali didasarkan pada perhitungan yang kompleks dan sulit dipahami oleh orang awam. Oleh karena itu, perusahaan harus dapat menjelaskan bagaimana sistem AI mereka bekerja.

4. Privasi Berdasarkan Desain dan Privasi Secara Default

GDPR mewajibkan perlindungan data untuk diintegrasikan ke dalam pengembangan produk dan layanan sejak awal. Untuk AI, ini berarti pertimbangan perlindungan data harus diperhitungkan sejak awal pengembangan sistem.

5. Hak untuk penghapusan dan koreksi

Individu memiliki hak untuk meminta penghapusan atau koreksi data mereka. Oleh karena itu, sistem AI harus dirancang sedemikian rupa sehingga dapat memenuhi persyaratan ini. Hal ini dapat menjadi tantangan teknis, karena meskipun data telah dianonimkan, data tersebut tetap merupakan data pribadi menurut Pasal 26 GDPR.

6. Risiko diskriminasi

AI dapat secara sadar atau tidak sadar memperkuat prasangka dan diskriminasi jika dilatih dengan data yang bias. Namun, GDPR bertujuan untuk mempromosikan keadilan dan perlakuan yang sama dalam penanganan data pribadi. Implementasi yang benar sangat penting dalam pengembangan dan penggunaan sistem AI.

Singkatnya, GDPR bertujuan untuk membentuk pengembangan dan penggunaan teknologi sedemikian rupa sehingga privasi dan hak-hak mendasar terlindungi. Regulasi ini menciptakan kerangka hukum yang menyeimbangkan perlindungan individu dan promosi teknologi inovatif, termasuk AI.

4.2 PERSYARATAN UMUM GDPR

Oleh karena itu, GDPR didasarkan pada beberapa prinsip utama yang mengatur pemrosesan data pribadi. Prinsip-prinsip ini mengharuskan organisasi untuk memproses data pribadi secara sah, adil, dan transparan, menggunakannya hanya untuk tujuan yang ditentukan, dan memastikan bahwa data tersebut disimpan secara akurat dan hanya selama diperlukan.

Tidak semua persyaratan GDPR dapat dibahas secara luas dalam buku ini, tetapi aspek-aspek berikut khususnya relevan ketika AI digunakan untuk memproses data pribadi:

1. Prinsip-prinsip untuk pemrosesan data pribadi

Semua aktivitas pemrosesan harus mematuhi prinsip-prinsip GDPR, seperti legalitas, keadilan, transparansi, pembatasan tujuan, minimalisasi data, keakuratan, pembatasan penyimpanan, integritas dan kerahasiaan serta akuntabilitas (Pasal 5 GDPR).

2. Keabsahan pemrosesan

Setiap pemrosesan data pribadi harus didasarkan pada dasar hukum yang sah, seperti persetujuan subjek data, kebutuhan untuk pelaksanaan kontrak, kewajiban hukum, perlindungan kepentingan vital, pelaksanaan tugas yang dilakukan untuk kepentingan umum atau pengejaran kepentingan yang sah (Pasal 6 GDPR).

3. Kewajiban untuk memberikan informasi jika data pribadi dikumpulkan

Jika data pribadi dikumpulkan, subjek data harus diberitahu tentang nama dan detail kontak pengontrol. Selain itu, tujuan pemrosesan, dasar hukum, dan durasi penyimpanan data harus dijelaskan (Pasal 13–14 GDPR).

4. Hak-hak subjek data

Individu yang datanya diproses memiliki hak-hak khusus berdasarkan GDPR, termasuk hak akses, koreksi, penghapusan (“hak untuk dilupakan”), pembatasan pemrosesan, portabilitas data, dan keberatan. Ketika AI memproses data pribadi, hak-hak ini harus dijamin (Pasal 15–21 GDPR).

5. Pengambilan keputusan otomatis termasuk pembuatan profil

Subjek data berhak untuk tidak tunduk pada keputusan yang hanya didasarkan pada pemrosesan otomatis yang menghasilkan efek hukum yang menyangkut mereka atau secara signifikan memengaruhi mereka. Ada pengecualian terhadap hak ini jika, misalnya, keputusan otomatis diperlukan untuk Penyelesaian atau pelaksanaan kontrak, didasarkan pada undang-undang atau dibuat dengan persetujuan eksplisit (Pasal 22 GDPR).

6. Perlindungan data melalui desain dan pengaturan default yang ramah perlindungan data

Saat mengembangkan dan menerapkan sistem AI, prinsip-prinsip perlindungan data harus dipertimbangkan dan diintegrasikan sejak awal (Pasal 25 GDPR).

7. Tanggung jawab atas pemrosesan sesuai dengan hukum

“Pengontrol” berarti setiap orang atau badan hukum, otoritas publik, lembaga atau badan lain yang, sendiri atau bersama-sama dengan orang lain, menentukan tujuan dan cara pemrosesan data pribadi sesuai dengan Pasal 4 ayat 7 GDPR. Oleh karena itu, orang ini juga bertanggung jawab atas implementasi semua persyaratan yang dijelaskan di atas dan harus membuktikannya jika ada keraguan.

Pengembang dan pengguna sistem TI dan AI wajib memastikan bahwa aplikasi dan proses pemrosesan data mereka mematuhi persyaratan GDPR. Hal ini dapat dicapai, misalnya, dengan:

- Dokumentasi rinci dari semua langkah pemrosesan

- Penyajian data yang digunakan dan alur data selama pemrosesan, pencatatan dalam register pemrosesan data perusahaan yang menggunakan data
 - Implementasi penilaian dampak perlindungan data
 - Memastikan transparansi dalam proses pengambilan keputusan otomatis
 - Implementasi langkah-langkah teknis dan organisasi (“TOM”) yang memadai untuk melindungi data pribadi dari akses tidak sah, kehilangan, penghancuran, atau kerusakan.
- Ini termasuk:

- Enkripsi
- Anonimisasi
- Pemeriksaan keamanan berkala
- Kontrol akses

Sekarang mari kita lihat lebih detail dampak penggunaan AI di perusahaan terhadap tujuh persyaratan dasar untuk penggunaan data pribadi seperti yang diuraikan di atas.

Prinsip-Prinsip Pengolahan Data Pribadi

Prinsip-prinsip pengolahan data pribadi berdasarkan Pasal 5 GDPR membentuk dasar penanganan data pribadi, termasuk pengolahan oleh kecerdasan buatan. Oleh karena itu, prinsip-prinsip ini dapat diterapkan dalam konteks pengolahan AI:

1. Keabsahan, pengolahan dengan itikad baik, transparansi

Pengolahan data harus didasarkan pada dasar hukum, seperti persetujuan subjek data, kebutuhan akan kontrak, atau persyaratan hukum. Dalam konteks AI, ini berarti bahwa pengguna harus diberi informasi yang jelas tentang bagaimana data mereka diproses oleh sistem AI, termasuk tujuan dan metode pengolahan.

Pertimbangan 58 GDPR menjelaskan bahwa semua informasi yang ditujukan kepada publik atau subjek data harus ringkas, mudah diakses, dan mudah dipahami, serta harus menggunakan bahasa yang jelas dan sederhana, dan jika perlu, visualisasi tambahan.

2. Pembatasan tujuan

Data hanya boleh dikumpulkan untuk tujuan yang ditentukan, eksplisit, dan sah, dan tidak boleh diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan tersebut. Jika data akan digunakan untuk pelatihan sistem AI, pemeriksaan harus dilakukan terlebih dahulu untuk menetapkan dasar pengumpulan dan penyimpanan data. Sistem AI juga harus dirancang sedemikian rupa sehingga hanya memproses data yang relevan dan diperlukan untuk tujuan spesifik pengumpulannya. Pemrosesan lebih lanjut untuk tujuan pengarsipan demi kepentingan umum, tujuan penelitian ilmiah atau sejarah, atau tujuan statistik (Pasal 89 ayat 1 GDPR) dapat dikecualikan dari ketidaksesuaian dengan tujuan awal.

3. Minimisasi Data

Hanya data yang diperlukan yang boleh dikumpulkan dan diproses. Dalam pengembangan dan penggunaan AI, ini berarti hanya jumlah minimum data yang diperlukan untuk tujuan pemrosesan tertentu yang boleh digunakan.

Ada area ketegangan khusus dengan AI di sini. Menurut Sartor, prinsip minimisasi data harus selalu dipertimbangkan dalam konteks proporsionalitas. Hal ini memungkinkan dimasukkannya data pribadi tambahan dalam operasi pemrosesan jika manfaat yang dihasilkan lebih besar daripada potensi risiko bagi subjek data. Potensi manfaat dari pemrosesan data di masa mendatang juga dapat membenarkan penyimpanan data ini, dengan syarat bahwa langkah-langkah keamanan yang tepat, seperti pseudonimisasi dan mekanisme perlindungan lainnya, diterapkan. Selain itu, pemrosesan data pribadi untuk tujuan statistik semata dapat tunduk pada persyaratan minimalisasi yang lebih longgar.

4. Akurasi

Data harus akurat dan, jika perlu, selalu diperbarui. Sistem AI yang didasarkan pada analisis data pribadi harus mencakup mekanisme untuk memastikan keakuratan data dan untuk mengoreksi atau menghapus data yang salah.

Menurut Sartor, hal ini juga berlaku untuk data pribadi yang digunakan sebagai input untuk sistem AI, terutama ketika data pribadi digunakan untuk membuat kesimpulan atau keputusan tentang subjek data. Data yang tidak akurat dapat membahayakan subjek data jika data tersebut dilihat dan diperlakukan dengan cara yang tidak mencerminkan identitas mereka.

Dalam model bahasa yang besar, ini adalah tantangan yang tidak mudah dipecahkan. OpenAI¹⁾ menyatakan bahwa “akurasi faktual dalam model bahasa skala besar tetap menjadi area penelitian aktif”. Untuk mengklarifikasi persyaratan hukum, noyb mengajukan pengaduan terhadap OpenAI kepada otoritas perlindungan data Austria pada April 2024. Rincian lebih lanjut tentang proses ini dijelaskan di bagian 4.6.

5. Batasan penyimpanan

Data tidak boleh disimpan dalam bentuk yang dapat diidentifikasi lebih lama dari yang diperlukan untuk tujuan pemrosesan. Oleh karena itu, aplikasi AI harus mengambil tindakan pencegahan untuk menganonimkan atau menghapus data pribadi setelah tujuan pemrosesan tercapai.

Jika informasi subjek data hanya dianggap sebagai masukan untuk kumpulan data pelatihan dan tidak digunakan untuk prediksi atau keputusan mengenai individu, ketentuan yang disederhanakan berlaku. Hal ini didukung oleh Pasal 162 GDPR, yang menyatakan bahwa pemrosesan data tersebut terutama ditujukan untuk produksi survei atau hasil statistik. Namun, hasil ini tidak boleh bersifat pribadi, tetapi harus memberikan data agregat yang tidak digunakan untuk membuat keputusan yang memengaruhi individu.

6. Integritas dan kerahasiaan (Keamanan data)

Pemrosesan harus dilakukan dengan cara yang memastikan keamanan yang tepat untuk data pribadi, termasuk perlindungan terhadap pemrosesan yang tidak sah atau melanggar hukum, kehilangan, penghancuran, atau kerusakan yang tidak disengaja. Untuk sistem AI, pendekatan ini harus disertakan dalam desain model untuk memastikan integritas data dan perlindungan privasi.

7. Akuntabilitas

Pengendali pemrosesan data harus dapat menunjukkan kepatuhan terhadap prinsip-prinsip di atas. Untuk AI, ini berarti bahwa pengembang dan penyebar harus mendokumentasikan bagaimana sistem mereka dirancang dan dioperasikan untuk memastikan kepatuhan terhadap GDPR.

Dalam konteks pemrosesan AI, prinsip-prinsip ini memerlukan perencanaan dan implementasi sistem AI yang cermat untuk memastikan kepatuhan terhadap peraturan perlindungan data. Hal ini mencakup, antara lain, pengembangan pedoman etika untuk AI, melakukan penilaian dampak perlindungan data, dan menetapkan prosedur untuk melindungi hak-hak subjek data.

Saat membuat pedoman internal, Tabel 4.1 dapat membantu.

Tabel 4.1 Isi Kebijakan Perusahaan Terkait AI Dan Perlindungan Data

Prinsip	Penjelasan
Kepatuhan hukum	- Apakah pemrosesan didasarkan pada persyaratan hukum? Lihat juga Pasal 6 ayat 1 GDPR - Bukti dan dokumentasi dasar hukum. - Jika tidak, bukti persetujuan yang diperlukan dari subjek data. Catatan: Persetujuan tidak dibatasi waktu, tetapi dapat ditarik kapan saja. Oleh karena itu, harus diterapkan proses untuk menarik persetujuan.
Keadilan	Memberi tahu subjek data tentang keberadaan pemrosesan data. Jika data dikumpulkan, subjek data harus diberi tahu secara lengkap dan benar tentang kondisi aktivitas pemrosesan data ini.
Transparansi	- Subjek data harus diinformasikan tentang pemrosesan data mereka saat ini dan di masa mendatang. - Tujuan pemrosesan harus dijelaskan. Informasi tersebut harus mudah ditemukan dan ditulis dalam bahasa yang mudah dipahami oleh orang awam.
Pembatasan tujuan	- Pemrosesan data pribadi hanya untuk tujuan tertentu, yang didefinisikan dengan jelas dan sah. - Dokumentasi tujuan pemrosesan data pribadi. - Definisi dan dokumentasi tujuan pemrosesan data AI. - Pemrosesan tidak boleh dilakukan dengan cara yang tidak sesuai dengan tujuan yang telah didefinisikan (dan dikomunikasikan). Untuk pemrosesan data yang lebih luas, persetujuan mungkin perlu diperoleh dari subjek data atau data harus dianonimkan.
Minimalisasi data	Pengumpulan dan pemrosesan harus relevan dan memadai secara langsung untuk tujuan yang ditentukan.

	• Jumlah data pribadi yang diproses harus dibatasi hanya pada yang benar-benar diperlukan. Berhati-hatilah saat “memperkaya” atau melengkapi atau menghubungkan data dengan data dari sumber lain (dokumentasi legalitas).
Akurasi	• Data pribadi harus dijaga keakuratannya secara faktual dan, jika perlu untuk aktivitas pemrosesan, harus selalu diperbarui. • Data pribadi yang tidak akurat harus segera dihapus atau dikoreksi sehubungan dengan tujuan pemrosesan. • Apakah mekanisme telah diimplementasikan dalam sistem AI yang dapat mengidentifikasi dan mengoreksi data yang tidak akurat?
Keterbatasan penyimpanan	• Penyimpanan dalam bentuk yang memungkinkan identifikasi subjek data hanya selama diperlukan untuk tujuan pemrosesan awal. • Penyimpanan data yang lebih lama hanya dimungkinkan untuk pengecualian yang ditentukan secara hukum. • Setelah masa penggunaan berakhir, data harus dihapus atau dianonimkan, atau alternatifnya, persetujuan harus diperoleh dari subjek data. • Jika persetujuan ditarik oleh subjek data, catatan data harus dihapus atau dianonimkan (tidak ada penyimpanan yang memungkinkan dalam sistem). Data harus selalu benar, bahkan dengan periode penyimpanan yang lama, dan integritas harus dijaga.
Integritas	• Integritas data harus dijaga selama aktivitas pemrosesan. • Integritas data harus dipastikan selama seluruh siklus hidup aktivitas pemrosesan data (hati-hati dengan periode penyimpanan yang lama). • Implementasi langkah-langkah yang dapat mendokumentasikan dan membuktikan integritas (contohnya termasuk enkripsi, pemeriksaan nilai hash, anonimisasi, dan lainnya.), pemeriksaan keamanan rutin, akses sesuai prinsip kebutuhan untuk mengetahui, dan lainnya.).
Kerahasiaan	• Perlindungan data pribadi dari akses, pengungkapan, modifikasi, atau transfer yang tidak sah. • Implementasi langkah-langkah perlindungan (TOM) terhadap kehilangan, penghancuran, atau kerusakan data yang tidak disengaja.

Akuntabilitas	• Pengendali harus mampu secara aktif menunjukkan kepatuhan terhadap prinsip-prinsip di atas. • Dokumentasi, prosedur, dan langkah-langkah yang memadai untuk menunjukkan kepatuhan terhadap prinsip-prinsip tersebut. • Dokumentasi keberhasilan implementasi pengendalian internal untuk menunjukkan kepatuhan terhadap prinsip-prinsip tersebut. • Tinjauan berkala terhadap pengendalian oleh auditor internal/audit internal/petugas perlindungan data/petugas kepatuhan. • Jika perlu, sertifikasi berkala oleh pihak ketiga independen.

Keabsahan Pemrosesan

Keabsahan pemrosesan data pribadi didefinisikan dalam Pasal 6 ayat 2 GDPR yang menetapkan berbagai kondisi di mana pemrosesan dianggap sah:

1. Persetujuan

Subjek data telah memberikan persetujuannya untuk pemrosesan data pribadinya untuk satu atau lebih tujuan tertentu.

Untuk aplikasi AI, memperoleh persetujuan yang jelas, terinformasi, dan sukarela dari subjek data sangat penting, terutama jika pemrosesannya ekstensif atau melibatkan data sensitif. Persetujuan harus diperoleh secara khusus untuk aktivitas pemrosesan yang diaktifkan oleh AI.

2. Pemenuhan Kontrak

Aktivitas pemrosesan diperlukan untuk pelaksanaan kontrak di mana subjek data adalah pihak atau untuk mengambil langkah-langkah atas permintaan subjek data sebelum memasuki kontrak.

Saat menggunakan sistem AI untuk memenuhi kontrak, seperti rekomendasi yang dipersonalisasi dalam e-commerce, harus ada kebutuhan yang jelas untuk pemrosesan untuk layanan yang disepakati secara kontraktual.

3. Kewajiban hukum

Aktivitas pemrosesan diperlukan untuk memenuhi kewajiban hukum yang harus dipatuhi oleh pengontrol data.

Jika sistem AI digunakan untuk tujuan ini, seperti sistem deteksi penipuan di perbankan, sistem tersebut harus secara tepat memenuhi persyaratan hukum dan pemrosesan harus diperlukan untuk memenuhi kewajiban tersebut.

4. Kepentingan vital

Aktivitas pemrosesan diperlukan untuk melindungi kepentingan vital subjek data atau orang lain.

Dalam hal ini, penggunaan AI memerlukan pertimbangan yang sangat cermat, terutama dalam situasi di mana subjek data tidak dapat memberikan persetujuan.

5. Kepentingan publik atau pelaksanaan wewenang resmi

Aktivitas pemrosesan diperlukan untuk pelaksanaan tugas yang dilakukan untuk kepentingan publik atau dalam pelaksanaan wewenang resmi yang diberikan kepada pengontrol data.

Aplikasi AI di sektor publik harus dibenarkan secara jelas untuk kepentingan publik atau dilaksanakan dalam kerangka wewenang publik.

6. Kepentingan yang Sah

Aktivitas pemrosesan diperlukan untuk tujuan kepentingan sah yang dikejar oleh pengontrol atau pihak ketiga, kecuali jika kepentingan tersebut dikesampingkan oleh kepentingan atau hak dan kebebasan mendasar subjek data yang memerlukan perlindungan data pribadi.

Jika sistem AI dioperasikan berdasarkan kepentingan sah pengontrol atau pihak ketiga, pertimbangan yang cermat diperlukan. Harus dipastikan bahwa kepentingan, hak dan kebebasan mendasar subjek data, yang memerlukan perlindungan data pribadi, tidak lebih diutamakan. Transparansi pemrosesan dan kemungkinan bagi subjek data untuk mengajukan keberatan sangat penting di sini.

Penting bagi pengontrol untuk dengan cermat memilih dan mendokumentasikan dasar hukum yang tepat untuk pemrosesan data guna memastikan kepatuhan terhadap GDPR. Dasar hukum yang dipilih harus spesifik, eksplisit, dan sah, dan pemrosesan harus dibatasi untuk mencapai tujuan yang ditentukan.

Pasal 6 ayat 4 GDPR menetapkan kondisi di mana pemrosesan data pribadi untuk tujuan yang melampaui tujuan awal pengumpulan diizinkan. Paragraf ini memberikan pedoman untuk menilai apakah pemrosesan data baru tersebut sesuai dengan tujuan semula dengan mempertimbangkan berbagai kriteria.

Secara khusus, berbagai faktor harus dipertimbangkan ketika menilai apakah pemrosesan lebih lanjut untuk tujuan baru diperbolehkan:

- Seberapa erat keterkaitan tujuan-tujuan tersebut? Apakah tujuan baru tersebut merupakan kelanjutan logis dari tujuan semula?
- Harapan apa yang dimiliki subjek data mengenai kemungkinan pemrosesan lebih lanjut pada saat pengumpulan data?
- Apakah ini data yang sangat sensitif sehingga memerlukan tindakan perlindungan yang lebih ketat?
- Dapatkah pemrosesan lebih lanjut berdampak negatif pada orang yang bersangkutan?

Apakah tindakan perlindungan yang sesuai seperti pseudonimisasi diterapkan untuk melindungi hak dan kebebasan subjek data?

Pasal 6 ayat 4 GDPR memungkinkan penanganan yang fleksibel terhadap pemrosesan lebih lanjut data pribadi, dengan syarat kompatibilitas tujuan pemrosesan baru tersebut diperiksa dan dibenarkan secara cermat. Ketentuan ini berkontribusi pada kepastian hukum dengan memberikan kriteria yang jelas untuk menilai kebolehan operasi pemrosesan lebih lanjut sambil memastikan perlindungan subjek data.

Kewajiban Memberikan Informasi Saat Data Pribadi Dikumpulkan

Kewajiban untuk memberi tahu saat mengumpulkan data pribadi diatur dalam Pasal 13 dan 14 GDPR. Kewajiban ini bertujuan untuk memastikan transparansi dalam pemrosesan data pribadi dan untuk memungkinkan subjek data untuk secara efektif menggunakan hak-hak mereka. Persyaratan sedikit berbeda tergantung pada apakah data dikumpulkan langsung dari subjek data (Pasal 13 GDPR) atau tidak (Pasal 14 GDPR).

Dalam konteks kecerdasan buatan, kewajiban informasi ini menjadi lebih penting, karena sistem AI sering melakukan operasi pemrosesan data yang kompleks yang tidak selalu mudah dipahami oleh subjek data. Area-area berikut ini sangat penting:

I. Pengumpulan data langsung (Pasal 13 GDPR)

Dalam hal pengumpulan data langsung, pengontrol data harus memberikan informasi komprehensif kepada subjek data pada saat pengumpulan data:

- I. Identitas dan detail kontak pengontrol data dan, jika berlaku, perwakilan pengontrol data dan petugas perlindungan data jika tersedia
- II. Tujuan pemrosesan data dan dasar hukumnya, jika berlaku, penjelasan lebih lanjut tentang kepentingan sah pengontrol data
- III. Penerima atau kategori penerima data pribadi
- IV. Informasi tentang apakah data ditransfer ke negara ketiga dan mekanisme perlindungan apa yang diterapkan
- V. Durasi penyimpanan atau kriteria untuk menentukan durasi ini
- VI. Informasi tentang hak-hak subjek data, termasuk hak akses, koreksi, penghapusan, pembatasan pemrosesan, hak untuk keberatan, dan hak untuk mengajukan pengaduan kepada otoritas pengawas
- VII. Keberadaan proses pengambilan keputusan otomatis termasuk pembuatan profil dan informasi yang bermakna tentang logika yang terlibat, serta signifikansi dan konsekuensi yang diperkirakan dari pemrosesan tersebut bagi subjek data

II. Pengumpulan data tidak langsung (Pasal 14 GDPR)

Jika data pribadi tidak dikumpulkan langsung dari subjek data, kewajiban informasi yang serupa berlaku seperti pada Pasal 13 GDPR, tetapi dengan beberapa penyesuaian. Selain itu, pengontrol data harus, misalnya, memberikan informasi tentang sumber data.

Pertimbangan Khusus Saat Menggunakan AI

Saat menggunakan AI, pengendali harus memberikan penekanan khusus pada transparansi pemrosesan data. Ini termasuk:

- Penjelasan yang jelas tentang bagaimana sistem AI memproses data dan membuat keputusan
- Informasi tentang catatan data pelatihan yang digunakan untuk melatih AI, terutama jika hal ini dapat berdampak pada subjek data
- Rincian langkah-langkah yang diambil untuk mengatasi ketidakakuratan, bias, dan diskriminasi oleh sistem AI

Kepatuhan terhadap kewajiban informasi saat memproses data pribadi oleh sistem AI tidak hanya berkontribusi pada kepatuhan hukum, tetapi juga memperkuat kepercayaan pengguna dan subjek data terhadap teknologi tersebut.

Hak subjek data

GDPR memperkuat hak individu dengan memberi mereka kendali atas data pribadi mereka. Hak-hak ini sangat penting dalam konteks pemrosesan oleh kecerdasan buatan, karena sistem AI sering memproses sejumlah besar data dan membuat keputusan kompleks yang berdampak signifikan pada individu. Hak-hak utama dan implikasinya saat menggunakan AI diuraikan di bawah ini:

1. Hak atas informasi (Pasal 15 GDPR)

Subjek data berhak untuk mengetahui apakah data mereka sedang diproses dan, jika demikian, untuk mendapatkan akses ke data ini dan informasi tambahan.

Dalam konteks AI, ini berarti bahwa individu dapat meminta informasi tentang bagaimana data mereka digunakan dalam sistem AI, termasuk deskripsi logika di balik keputusan otomatis (Pasal 15 ayat 1 huruf h GDPR).

2. Hak untuk perbaikan (Pasal 16 GDPR)

Hak ini memungkinkan individu untuk meminta perbaikan data pribadi yang tidak akurat mengenai mereka. Sistem AI yang memproses data yang tidak lengkap dapat membuat keputusan yang salah, dengan konsekuensi negatif bagi subjek data.

3. Hak untuk penghapusan (“Hak untuk dilupakan”, Pasal 17 GDPR)

Dalam kondisi tertentu, individu dapat meminta penghapusan data mereka. Untuk aplikasi AI yang memproses data pribadi, mekanisme harus tersedia untuk menghapus data atas permintaan subjek data, terutama jika data tersebut tidak lagi diperlukan untuk tujuan semula atau persetujuan telah dicabut.

4. Hak untuk pembatasan pemrosesan (Pasal 18 GDPR)

Subjek data dapat meminta pembatasan pemrosesan data mereka dalam keadaan tertentu, misalnya jika keakuratan data tersebut diperdebatkan. Untuk sistem AI, ini mungkin berarti bahwa data tertentu untuk sementara tidak dapat digunakan untuk proses pengambilan keputusan.

5. Hak atas portabilitas data (Pasal 20 GDPR)

Setiap individu berhak menerima data mereka dalam format terstruktur, umum digunakan, dan dapat dibaca mesin, serta mentransfer data tersebut ke pengontrol data lain. Dalam konteks AI, ini memungkinkan pengguna untuk mentransfer data mereka dari satu layanan ke layanan lain, yang sangat relevan untuk layanan yang menggunakan AI untuk rekomendasi yang dipersonalisasi.

6. Hak untuk menolak (Pasal 21 GDPR)

Subjek data berhak untuk menolak pemrosesan data pribadi mereka kapan saja, khususnya jika pemrosesan ini didasarkan pada kepentingan sah pengontrol data atau untuk tujuan pemasaran langsung. Saat menggunakan AI, ini berarti individu dapat menolak pemrosesan data mereka oleh sistem AI, khususnya terkait dengan pembuatan profil dalam kasus pemasaran langsung (Pasal 21 ayat 2 GDPR).

Penerapan hak-hak ini dalam sistem AI memerlukan perencanaan yang cermat dan langkah-langkah teknis untuk memastikan bahwa sistem tersebut dapat memenuhi persyaratan. Hal ini dapat dicapai melalui praktik pemrosesan data yang transparan, penyediaan antarmuka pengguna untuk pelaksanaan hak-hak tersebut, dan pengintegrasian prinsip-prinsip perlindungan data ke dalam proses perancangan sistem AI.

4.3 PRIVASI BERDASARKAN DESAIN

Pasal 25 GDPR merupakan elemen sentral untuk mempromosikan perlindungan data dalam fase pengembangan dan penggunaan produk, layanan, dan sistem. Pasal ini sangat relevan ketika menggunakan kecerdasan buatan, karena mendorong pengembang dan pengguna sistem AI untuk mengintegrasikan langkah-langkah perlindungan data ke dalam sistem mereka sejak awal dan menetapkan pengaturan yang ramah perlindungan data sebagai standar. Aspek-aspek kuncinya adalah:

- **Privasi Berdasarkan Desain**

Prinsip ini mensyaratkan bahwa perlindungan data sudah diperhitungkan selama pengembangan dan desain prosedur pemrosesan. Dalam konteks AI, ini berarti bahwa pertimbangan perlindungan data harus menjadi bagian integral dari proses desain sistem AI, mulai dari pemilihan data yang digunakan untuk melatih AI hingga algoritma yang membuat keputusan.

- **Privasi Secara Default**

Prinsip ini mensyaratkan bahwa hanya data pribadi yang benar-benar diperlukan untuk tujuan tertentu yang diproses. Bagi sistem AI, ini berarti bahwa sistem tersebut harus dikonfigurasi secara default untuk menghormati privasi, misalnya dengan mempraktikkan minimalisasi data, membatasi pengumpulan dan penyimpanan data hanya pada apa yang benar-benar diperlukan, dan membatasi aksesibilitas data.

Pasal 25 GDPR menggarisbawahi pentingnya perlindungan data yang proaktif dan preventif. Saat menggunakan AI, ini berarti bahwa langkah-langkah perlindungan data harus direncanakan dan diimplementasikan dengan cermat - di setiap tahap siklus hidup sistem AI, mulai dari pengumpulan data dan pelatihan model hingga penerapan praktis AI. Prinsip-prinsip "privasi berdasarkan desain" dan "privasi secara default" berfungsi untuk memastikan perlindungan privasi dan memperkuat kepercayaan pengguna dan publik terhadap sistem AI.

Implementasi

Implementasi prinsip-prinsip "privasi berdasarkan desain" dan "privasi secara default" sesuai dengan Peraturan Perlindungan Data Umum (GDPR) dan pertimbangan Undang-Undang AI sangat penting untuk pengembangan dan pengoperasian aplikasi AI.

1. Privasi Sejak Awal (Privacy by Design)

"Privasi Sejak Awal" berarti bahwa perlindungan data diintegrasikan ke dalam desain dan arsitektur sistem AI sejak awal. Ini mencakup beberapa aspek:

- Teknologi yang ramah perlindungan data: Penggunaan teknologi yang memfasilitasi minimalisasi data seperti anonimisasi dan pseudonimisasi data untuk menghindari identifikasi individu.
- Minimalkan pengumpulan data: Hanya kumpulkan data yang benar-benar diperlukan. Model AI harus dilatih dengan jumlah data minimum yang diperlukan untuk melakukan tugas.
- Keamanan: Implementasi langkah-langkah keamanan yang kuat untuk melindungi data dari akses dan penyalahgunaan yang tidak sah. Ini termasuk enkripsi, transmisi data yang aman, dan kontrol akses.
- Transparansi dan akuntabilitas: Pastikan bahwa fungsi dan pemrosesan data aplikasi AI dapat dipahami dan dimengerti oleh pengguna.

2. Privasi Secara Default (Privacy by Default)

“Privasi Secara Default” berarti bahwa pengaturan perlindungan data yang paling aman diaktifkan secara default tanpa pengguna harus melakukan pengaturan apa pun sendiri. Untuk aplikasi AI, ini berarti:

- Penghematan data secara default: Secara default, hanya data yang benar-benar diperlukan untuk fungsi spesifik AI yang diproses.
- Pembatasan akses data: Pembatasan standar tentang siapa yang dapat mengakses data mana dan dalam keadaan apa, terutama untuk informasi sensitif.
- Penghapusan otomatis: Data yang tidak lagi diperlukan harus dihapus secara otomatis untuk meminimalkan risiko pelanggaran data

3. Undang-Undang AI

Undang-Undang AI, yang secara khusus ditujukan untuk kecerdasan buatan, melengkapi GDPR dengan memperkenalkan peraturan khusus untuk sistem AI:

- Klasifikasi berbasis risiko: Sistem AI diklasifikasikan menurut risikonya terhadap hak dan kebebasan individu. Aplikasi berisiko tinggi tunduk pada persyaratan yang lebih ketat.
- Kewajiban transparansi: Penyedia AI harus memastikan bahwa pengguna diberi informasi tentang cara kerja AI dan faktor-faktor pengambilan keputusan.
- Pemantauan dan kepatuhan: Mematuhi pedoman etika dan memastikan bahwa sistem AI dikembangkan dan dioperasikan sesuai dengan persyaratan hukum.

Lalu bagaimana prinsip-prinsip ini dapat dipraktikkan? Penyedia, produsen produk, dan pengembang lainnya harus selalu mengembangkan aplikasi AI mereka dalam sebuah proyek bersama orang-orang dengan beragam pengetahuan. Ini termasuk:

- Keterlibatan awal pakar perlindungan data dalam perancangan AI
- Melakukan penilaian dampak perlindungan data untuk mengidentifikasi dan mengurangi potensi risiko
- Saat mengembangkan sistem AI, prinsip-prinsip perlindungan data seperti minimalisasi data, pembatasan tujuan, dan transparansi harus dipertimbangkan sejak awal.

- Sistem AI harus dirancang sedemikian rupa sehingga membatasi pengumpulan dan pemrosesan data pribadi hanya pada apa yang diperlukan untuk mencapai tujuan pemrosesan.
- Dokumentasi berkelanjutan tentang fungsionalitas dan pemantauan sistem AI yang beroperasi untuk membuktikan kepatuhan. Pengembang dan penyedia AI harus dapat menunjukkan bagaimana prinsip-prinsip perlindungan data telah diintegrasikan ke dalam sistem mereka untuk memenuhi persyaratan GDPR.
- Pasal 25 GDPR menekankan pentingnya perlindungan data yang proaktif dan preventif. Saat menggunakan AI, hal ini memerlukan perencanaan dan implementasi langkah-langkah perlindungan data yang cermat di semua fase siklus hidup sistem AI, mulai dari pengumpulan data hingga pelatihan model dan penggunaan AI dalam praktik. Kepatuhan terhadap prinsip “privasi berdasarkan desain” dan “privasi secara default” akan memastikan bahwa sistem AI melindungi privasi dan memperkuat kepercayaan pengguna serta masyarakat.

Tanggung Jawab atas Pemrosesan Sesuai dengan Hukum

Pasal 4 ayat 7 GDPR mendefinisikan istilah “pengontrol”. Istilah ini didefinisikan sebagai orang perseorangan atau badan hukum, otoritas publik, lembaga atau badan lain yang, sendiri atau bersama-sama dengan orang lain, menentukan tujuan dan cara pemrosesan data pribadi. Oleh karena itu, pengontrol adalah otoritas pengambilan keputusan utama mengenai mengapa (tujuan) dan bagaimana (cara) data pribadi diproses.

Dalam konteks kecerdasan buatan, peran pengontrol sangat penting, karena sistem AI sering melakukan aktivitas pemrosesan data yang kompleks yang dapat memiliki implikasi luas terhadap privasi dan hak subjek data. Berikut beberapa aspek spesifik yang perlu dipertimbangkan:

1. Pengambilan Keputusan dalam Pengembangan AI

Penyedia dan pengembang sistem AI yang menggunakan data pribadi untuk melatih model AI atau menyediakan layanan yang didukung AI biasanya dianggap sebagai pengontrol data, karena mereka memutuskan penggunaan teknologi ini dan penggunaan data tersebut.

2. Transparansi dan Akuntabilitas

Sebagai pengendali data, penyedia dan pengimplementasikan AI harus memastikan bahwa aktivitas pemrosesan mereka transparan dan sesuai dengan prinsip-prinsip perlindungan data GDPR. Mereka harus mendokumentasikan data mana yang diproses untuk tujuan apa, bagaimana pemrosesan dilakukan, dan harus dapat menunjukkan kepatuhan terhadap GDPR kepada otoritas pengawas.

3. Penilaian Dampak dan Langkah-langkah Perlindungan

Pengendali data yang menggunakan sistem AI harus melakukan penilaian dampak perlindungan data jika jenis pemrosesan dapat menimbulkan risiko tinggi terhadap hak dan kebebasan subjek data. Mereka harus mengambil langkah-langkah teknis dan organisasi yang tepat untuk mengurangi risiko dan memastikan perlindungan data pribadi.

4. Kepatuhan terhadap Hak Subjek Data

Pengendali data harus memastikan bahwa hak-hak subjek data, seperti hak akses, koreksi, penghapusan, dan keberatan (Pasal 15–21 GDPR), sepenuhnya dijamin. Saat menggunakan AI, perhatian khusus harus diberikan untuk memastikan bahwa subjek data dapat menggunakan hak-hak mereka secara efektif, terutama terkait dengan keputusan otomatis. Saat merancang sistem AI, kewajiban-kewajiban ini harus menjadi dasar persyaratan implementasi.

Kesimpulan

Dalam konteks AI, Pasal 4 ayat 7 GDPR menekankan peran sentral pengontrol dalam memastikan perlindungan data dan kepatuhan terhadap GDPR. Penyedia dan pengembang AI harus mengambil pendekatan proaktif untuk mengintegrasikan prinsip-prinsip perlindungan data ke dalam sistem mereka, memastikan transparansi pemrosesan data, dan melindungi hak-hak subjek data. Mengidentifikasi dan bertanggung jawab atas aktivitas pemrosesan data yang didukung AI sangat penting untuk meningkatkan kepercayaan pengguna dan kepatuhan hukum.

4.4 PERSYARATAN UNTUK DATA PENGUJIAN

Penerapan GDPR pada data pengujian untuk kecerdasan buatan menimbulkan persyaratan khusus, terutama jika data ini berisi informasi pribadi. Berikut adalah beberapa persyaratan terpenting yang dapat diatasi dengan menggunakan poin-poin berikut:

Keabsahan pemrosesan data

Menurut GDPR, pemrosesan data pribadi harus dilakukan atas dasar hukum. Untuk data pengujian AI, ini berarti harus ada dasar hukum yang jelas untuk pengumpulan dan penggunaan data ini, seperti persetujuan tegas dari subjek data, pelaksanaan kontrak, kewajiban hukum, atau kepentingan sah (lihat Pasal 6 GDPR). Jika ragu, data harus dianonimkan sebelum pengujian dilakukan.

Minimalisasi Data dan Pembatasan Tujuan

GDPR mensyaratkan bahwa hanya data yang benar-benar diperlukan (minimalisasi data) yang diproses dan data tersebut hanya digunakan untuk tujuan yang ditentukan, eksplisit, dan sah. Untuk data pengujian AI, ini berarti bahwa hanya jumlah informasi yang diperlukan untuk tujuan pengujian spesifik AI yang boleh digunakan. Lebih lanjut, data tersebut tidak boleh digunakan untuk tujuan lain.

Kewajiban Transparansi dan Informasi

Organisasi harus transparan dan proaktif tentang bagaimana dan mengapa data pribadi digunakan. Dalam kasus pengujian AI, ini termasuk penyediaan dokumen informasi tentang pemrosesan data yang dimaksudkan kepada subjek data. Informasi perlindungan data tambahan dapat dibuat untuk tujuan khusus ini atau informasi yang ada dapat dilengkapi.

Keamanan Data

GDPR mensyaratkan bahwa langkah-langkah teknis dan organisasi yang tepat harus diambil untuk melindungi data pribadi.

Untuk data pengujian AI, ini berarti bahwa langkah-langkah keamanan seperti enkripsi, kontrol akses, dan pemeriksaan keamanan rutin harus diterapkan untuk melindungi data dari akses tidak sah atau kehilangan. Sedapat mungkin, data pengujian juga harus dianonimkan atau setidaknya dipseudonimkan untuk melindunginya secara memadai dari pengembang dan penguji. Ini mengurangi risiko bahwa data dapat dikaitkan dengan orang tertentu.

Hak Subjek Data

Individu yang datanya digunakan untuk pengujian AI mempertahankan hak mereka berdasarkan GDPR, termasuk hak akses, koreksi, penghapusan, dan pembatasan pemrosesan. Organisasi harus menyediakan mekanisme untuk memastikan hak-hak ini. Oleh karena itu, keterlibatan petugas perlindungan data dalam tim proyek mengurangi kesalahan dalam pelaporan yang sesuai saat menjalankan hak subjek data.

Penilaian Dampak Perlindungan Data (DPIA)

Penilaian dampak perlindungan data diperlukan jika suatu jenis pemrosesan, khususnya penggunaan teknologi baru, kemungkinan besar akan menimbulkan risiko tinggi terhadap hak dan kebebasan individu karena sifat, cakupan, keadaan, dan tujuannya (Pasal 35 GDPR). Pengontrol data wajib berkonsultasi dengan otoritas pengawas sebelum melakukan pemrosesan jika penilaian dampak perlindungan data menunjukkan bahwa pemrosesan tersebut akan menimbulkan risiko tinggi, kecuali pengontrol data mengambil langkah-langkah untuk mengurangi risiko tersebut (Pasal 35 GDPR).

Oleh karena itu, GDPR mewajibkan DPIA untuk proyek AI yang dapat menimbulkan risiko tinggi terhadap hak dan kebebasan individu. DPIA ini harus menilai dan mendokumentasikan risiko spesifik yang terkait dengan pemrosesan data pengujian serta langkah-langkah untuk mengurangi risiko tersebut.

Untuk proyek AI, sangat penting untuk mengintegrasikan pertimbangan perlindungan data sejak tahap pengembangan, termasuk pemilihan dan penggunaan data pengujian. Dokumentasikan seluruh proses penilaian dampak perlindungan data, termasuk risiko yang diidentifikasi, penilaian yang dilakukan, dan langkah-langkah mitigasi yang diambil. Ini berfungsi sebagai bukti kepatuhan terhadap GDPR.

4.5 PENGAMBILAN KEPUTUSAN OTOMATIS

Pasal 22 GDPR menyediakan mekanisme penting untuk melindungi individu dari risiko dan potensi kerugian pengambilan keputusan otomatis, terutama yang berbasis pada kecerdasan buatan atau sistem pemrosesan otomatis lainnya. Pasal ini membatasi penggunaan pengambilan keputusan otomatis semata dengan memberikan hak kepada subjek data untuk tidak tunduk pada keputusan yang memiliki dampak hukum atau dampak signifikan serupa tanpa tinjauan manusia.

Pasal 4 ayat 4 GDPR mendefinisikan istilah pembuatan profil sebagai segala bentuk pemrosesan otomatis data pribadi yang terdiri dari penggunaan data pribadi untuk mengevaluasi aspek-aspek pribadi tertentu yang berkaitan dengan seseorang, khususnya untuk menganalisis atau memprediksi aspek-aspek yang berkaitan dengan kinerja orang

tersebut di tempat kerja, situasi ekonomi, kesehatan, preferensi pribadi, minat, keandalan, perilaku, lokasi, atau pergerakan.

Faktanya, semakin banyak data yang dikumpulkan yang memetakan setiap aktivitas manusia. Melalui berbagai teknologi AI, individu dapat dipantau dan dipengaruhi berdasarkan berbagai karakteristik pribadi dalam banyak kasus dan konteks. Dengan mengkorelasikan data tentang individu dengan klasifikasi dan prediksi yang sesuai, AI meningkatkan potensi pembuatan profil, yaitu memperoleh informasi tentang individu atau kelompok dan membuat penilaian serta keputusan berdasarkan hal tersebut.

Pasal 22 GDPR membahas pengambilan keputusan individu secara otomatis, termasuk pembuatan profil. Artikel ini sangat relevan dalam konteks kecerdasan buatan, karena sistem AI sering digunakan untuk pengambilan keputusan dan pembuatan profil secara otomatis.

Larangan pengambilan keputusan individual secara otomatis

Pasal 22 ayat 1 GDPR menyatakan bahwa individu memiliki hak untuk tidak tunduk pada keputusan yang didasarkan semata-mata pada pemrosesan otomatis, termasuk pembuatan profil, yang menghasilkan efek hukum atau secara signifikan mempengaruhi mereka.

Oleh karena itu, empat karakteristik diperlukan untuk penerapan larangan tersebut:

1. Keputusan harus dibuat tentang orang perseorangan, misalnya penetapan peringkat kredit.
2. Keputusan harus didasarkan secara eksklusif pada pemrosesan otomatis; manusia tidak boleh memiliki pengaruh yang relevan terhadap hasil proses pengambilan keputusan.
3. Teknologi tersebut harus mencakup pembuatan profil. Persyaratan ini lebih lanjut dijelaskan dalam Pasal 71 GDPR.
4. Hasilnya harus memiliki efek hukum atau setidaknya efek yang signifikan.

Pada prinsipnya, sistem TI tidak diizinkan untuk membuat keputusan penting tentang orang perseorangan. Namun, ada pengecualian terhadap larangan ini, yang diatur dalam Pasal 22 ayat 2. Keputusan tersebut dapat dibuat jika:

- diperlukan untuk Penyelesaian atau pelaksanaan kontrak antara subjek data dan pengontrol data,
- diizinkan oleh hukum Uni Eropa atau Negara Anggota yang juga menetapkan langkah-langkah yang sesuai untuk melindungi hak dan kebebasan serta kepentingan sah subjek data, atau
- dengan persetujuan eksplisit dari subjek data.

Langkah-langkah perlindungan yang diperlukan dalam kasus-kasus tersebut tercantum dalam Pasal 22 ayat 3 dan 4 GDPR. Jika keputusan didasarkan pada pemrosesan otomatis dan termasuk dalam pengecualian, langkah-langkah yang tepat harus diterapkan untuk melindungi hak dan kebebasan serta kepentingan sah subjek data. Ini termasuk, misalnya:

- hak untuk intervensi manusia dari pihak pengontrol
- hak untuk menyampaikan sudut pandang sendiri
- hak untuk mengajukan banding atas keputusan tersebut

Bagaimana hal ini terlihat secara konkret dalam interaksi dengan sistem AI? Pertimbangan berikut harus didiskusikan oleh tim proyek dan langkah-langkah harus diputuskan dan didokumentasikan:

1. Pengambilan keputusan otomatis

Banyak sistem AI mampu mengambil keputusan tanpa intervensi manusia, yang secara langsung termasuk dalam Pasal 22 GDPR. Hal ini sangat relevan di bidang-bidang seperti penilaian kredit, sumber daya manusia (misalnya, seleksi pelamar otomatis) dan diagnostik kesehatan.

Oleh karena itu, risiko terhadap subjek data harus dinilai dalam penilaian dampak perlindungan data dan langkah-langkah yang tepat harus diambil. Contoh dari langkah-langkah ini termasuk peninjauan berkala atas keputusan oleh seorang ahli manusia, implementasi opsi keberatan dalam sistem AI, atau kontrol internal yang secara acak memilih masalah yang diproses oleh AI dan meneruskannya kepada manusia untuk ditinjau.

2. Pembuatan Profil

AI sering digunakan untuk pembuatan profil, yaitu mengumpulkan informasi tentang individu dan membuat prediksi atau keputusan berdasarkan informasi tersebut. Pasal 22 GDPR membatasi penggunaan teknik tersebut jika berdampak signifikan pada individu. Contohnya termasuk kinerja seseorang di tempat kerja, situasi ekonomi, kondisi kesehatan, preferensi pribadi, minat, keandalan, kemungkinan perilaku dalam situasi tertentu, atau pola pergerakan.

Pembuatan profil digunakan dalam banyak skenario aplikasi yang berbeda karena memungkinkan sejumlah besar data untuk dianalisis secara efisien dan temuan spesifik tentang individu atau kelompok dapat diperoleh darinya. Dalam perawatan kesehatan, pembuatan profil dapat membantu mengidentifikasi pasien yang berisiko lebih tinggi terkena penyakit tertentu, dan dalam keuangan, hal itu membantu menilai risiko kredit peminjam.

Meskipun pembuatan profil merupakan teknik yang ampuh untuk mengidentifikasi dan memanfaatkan pola dan tren dalam sejumlah besar data, teknik ini juga memiliki keterbatasan, karena hasilnya dapat dipengaruhi oleh faktor eksternal seperti perubahan ekonomi, peristiwa politik, atau perkembangan teknologi yang mungkin tidak termasuk dalam data yang ada. Selain itu, peristiwa tunggal atau acak yang berada di luar pola dan tren yang diidentifikasi dalam data tidak dapat diprediksi.

3. Persetujuan dan transparansi

Penggunaan AI untuk pengambilan keputusan otomatis seringkali memerlukan persetujuan yang jelas dan eksplisit dari subjek data. Selain itu, prosedur dan kriteria yang menjadi dasar proses pengambilan keputusan harus transparan. Bersama dengan petugas perlindungan data, oleh karena itu harus diperiksa apakah persetujuan yang diperlukan telah diperoleh, apakah langkah-langkah teknis telah diterapkan secara memadai, dan apakah hak-hak subjek data dapat dilaksanakan. Ini juga termasuk deskripsi yang mudah dipahami tentang proses yang digunakan.

4. Intervensi manusia

Dalam kasus di mana keputusan otomatis diizinkan, masih harus ada kemungkinan intervensi manusia untuk memastikan bahwa hak-hak subjek data dilindungi. Secara konseptual harus diperhitungkan bahwa pengendali data dapat campur tangan dalam pemrosesan dan memperbaiki hasilnya.

4.6 PEDOMAN OTORITAS DATA: GDPR & AI

Penggunaan AI yang bertanggung jawab sesuai dengan GDPR saat ini menimbulkan banyak masalah kompleks. Terdapat potensi konflik yang beragam dan terkadang cukup besar yang belum sepenuhnya diklarifikasi. Berbagai inisiatif dari para ahli perlindungan data saat ini bertujuan untuk mengembangkan solusi praktis untuk tantangan ini dan mencapai kepastian hukum.

Bagian ini berfungsi sebagai panduan bagi perusahaan dan menunjukkan beberapa pendekatan tentang bagaimana sistem AI dapat diimplementasikan dan dioperasikan sesuai dengan peraturan perlindungan data. Penekanan khusus diberikan pada pemenuhan persyaratan GDPR dan pada saat yang sama memanfaatkan potensi inovasi teknologi AI sebaik mungkin. Panduan dan studi kasus mencerminkan status terkini pada Juli 2024. Keputusan atau pendapat dan rekomendasi lain yang dibuat setelah tanggal ini bukan bagian dari tinjauan ini.

Publikasi Dewan Perlindungan Data Eropa (Kutipan)

Dalam Opini 3/2024, EDPB menjelaskan pandangannya tentang peran otoritas perlindungan data nasional dalam konteks Undang-Undang AI dan menekankan bahwa hukum perlindungan data Uni Eropa sepenuhnya berlaku untuk pemrosesan data pribadi dalam konteks siklus hidup sistem AI, sebagaimana secara eksplisit diakui dalam Pasal 13 GDPR. 2 ayat 7 UU AI (lihat juga Pertimbangan 9 dan 10).

EDPB menunjukkan bahwa pemrosesan data pribadi dalam siklus hidup sistem AI menimbulkan risiko tinggi terhadap hak-hak fundamental, terutama karena seringkali terkait erat dengan data non-pribadi. Oleh karena itu, otoritas kompeten nasional harus bekerja sama erat dengan otoritas perlindungan data untuk menegakkan UU AI. Gugus tugas ini dibentuk karena OpenAI tidak memiliki kantor di Uni Eropa hingga 15 Februari 2024 dan oleh karena itu tidak ada satu pun otoritas perlindungan data nasional yang bertanggung jawab atas layanan ChatGPT, yang disediakan oleh perusahaan AS OpenAI OpCo, LLC.

Oleh karena itu, EDPB memutuskan pada April 2023 untuk membentuk gugus tugas untuk mempromosikan kerja sama antara otoritas nasional dan mengkoordinasikan informasi tentang kemungkinan tindakan penegakan hukum terkait dengan pemrosesan data pribadi sehubungan dengan ChatGPT. Dalam laporan sementara ini, anggota gugus tugas ChatGPT melaporkan analisis mereka tentang penerapan GDPR terhadap layanan ChatGPT dan sampai pada kesimpulan awal sebagai berikut:

1. Keabsahan

Pemrosesan data pribadi harus memenuhi setidaknya satu dari persyaratan yang ditentukan dalam Pasal 6 ayat 1 GDPR. Keabsahan harus dinilai untuk setiap fase berikut dan dapat berbeda:

- I. Fase: “Pengumpulan data pelatihan”, “Pra-pemrosesan data” dan “Pelatihan”. Selama fase-fase ini, terdapat risiko khusus terhadap hak dan kebebasan mendasar individu, karena data pribadi dapat dikumpulkan dan diproses melalui web scraping (pengumpulan dan ekstraksi otomatis informasi tertentu dari berbagai sumber yang dapat diakses publik di internet). Dalam beberapa kasus, ini bahkan dapat mencakup kategori data khusus sesuai dengan Pasal 9 ayat 1 GDPR, misalnya ketika orang membagikan riwayat medis mereka di saluran media sosial. Penilaian keabsahan masih tertunda dan OpenAI telah diminta untuk memberikan beberapa bukti kepatuhan GDPR.
- II. Fase: “Input prompt”, “Output hasil” dan “Pelatihan ChatGPT dengan prompt”. OpenAI mengklasifikasikan masukan dan umpan balik pengguna terhadap hasil sebagai "konten" dan menyatakan bahwa mereka akan menggunakan informasi ini untuk melatih dan meningkatkan model, di mana penggunaan "konten" untuk tujuan pelatihan dapat ditolak. Hal ini harus dipertimbangkan ketika menimbang kepentingan sesuai dengan Pasal 6 ayat 1 huruf f GDPR.

2. Keadilan

Prinsip GDPR ini mensyaratkan bahwa data pribadi tidak boleh diproses dengan cara yang merugikan subjek data secara tidak adil, diskriminatif secara tidak sah, tidak terduga, atau menyesatkan. Lebih lanjut, tidak boleh ada pengalihan risiko dari perusahaan sebagai pengontrol kepada subjek data. Gugus tugas menyimpulkan bahwa, sehubungan dengan ChatGPT, tanggung jawab untuk kepatuhan terhadap GDPR tidak boleh dialihkan kepada subjek data, misalnya dengan memasukkan klausul dalam syarat dan ketentuan umum bahwa subjek data bertanggung jawab atas entri obrolan mereka. OpenAI telah memberikan prospek untuk menerapkan prosedur yang lebih baik untuk memeriksa masukan.

3. Kewajiban Transparansi dan Informasi

Satuan tugas mencatat bahwa dalam kasus pengumpulan data melalui web scraping, subjek data tidak diinformasikan dan pengecualian sesuai dengan Pasal 14 ayat 5 huruf b GDPR dapat berlaku jika OpenAI menerapkan langkah-langkah yang tepat untuk melindungi hak dan kebebasan serta kepentingan sah subjek data, termasuk penyediaan informasi ini kepada publik. Sehubungan dengan input pengguna, orang-orang harus diberitahu bahwa "konten" (input pengguna) tersebut dapat digunakan untuk tujuan pelatihan.

4. Prinsip Akurasi Data

Perlu dicatat bahwa pendekatan pelatihan OpenAI saat ini, karena sifat probabilistik sistem, menghasilkan model yang juga dapat menghasilkan hasil yang bias atau dibuat-buat. Sesuai dengan prinsip transparansi berdasarkan Pasal 5 ayat 1 huruf a GDPR,

pengontrol harus memberikan informasi yang memadai tentang mekanisme probabilistik untuk menghasilkan output dan keandalannya yang terbatas. Ini termasuk referensi eksplisit terhadap fakta bahwa teks yang dihasilkan mungkin benar secara sintaksis, tetapi mungkin terdistorsi atau fiktif. Meskipun langkah-langkah saat ini dianggap bermanfaat untuk menghindari salah tafsir hasil ChatGPT, langkah-langkah tersebut tidak cukup untuk mematuhi prinsip akurasi data.

5. Hak subjek data

Dalam versi kebijakan privasi Eropa, OpenAI menyediakan opsi untuk menghubungi mereka melalui email, di mana beberapa hak subjek data juga dapat dilaksanakan melalui pengaturan akun. OpenAI menawarkan prospek untuk menerapkan langkah-langkah lebih lanjut untuk melaksanakan hak subjek data.

Laporan ini hanyalah hasil sementara dan gugus tugas telah mengirimkan daftar pertanyaan kepada OpenAI untuk dijawab guna lebih memahami dan menilai prosedur dan langkah-langkah yang diterapkan di ChatGPT.

Rekomendasi DSK

Banyak perusahaan dan organisasi menghadapi tantangan karena tidak mengetahui kondisi apa yang memungkinkan mereka menggunakan aplikasi AI sesuai dengan peraturan perlindungan data. Model Bahasa Besar (LLM), yang sering disebut sebagai chatbot tetapi juga dapat berfungsi sebagai dasar untuk aplikasi lain, merupakan pengenalan AI yang hemat biaya.

Pada awal Mei 2024, DSK menerbitkan pedoman yang memberikan “gambaran umum tentang kriteria perlindungan data yang harus dipatuhi untuk penggunaan aplikasi AI yang sesuai dengan perlindungan data”, dengan fokus pada LLM dan chatbot. Ini dapat berfungsi sebagai panduan bagi organisasi dalam memilih, menerapkan, dan menggunakan aplikasi AI. *“Panduan ini terutama ditujukan kepada mereka yang bertanggung jawab yang ingin menggunakan aplikasi AI”*, tetapi juga kepada pengembang dan teknisi yang ingin merancang dan mengoperasikan sistem AI sesuai dengan peraturan perlindungan data.

Bab pertama memberikan bantuan untuk desain dan pemilihan aplikasi AI, bab kedua membahas implementasi, dan bab ketiga memberikan informasi tentang penggunaan yang sesuai dengan perlindungan data. Isu-isu berikut dibahas:

1. Konsepsi dan pemilihan aplikasi AI

Pengontrol data berdasarkan GDPR harus secara eksplisit mendefinisikan area aplikasi dan tujuan AI sebelum menggunakan aplikasi AI dan menentukan apakah data pribadi diperlukan untuk ini. Kemudian harus diperiksa apakah sistem ini termasuk dalam sistem yang dilarang menurut Undang-Undang AI, misalnya pemantauan biometrik waktu nyata di ruang publik.

Jika tidak ada atau hanya sebagian data pribadi yang diproses secara langsung, masih harus dinilai apakah data pribadi tidak langsung diproses atau terjadi dalam model AI. Pemeriksaan ini berkaitan dengan seluruh siklus hidup data dan sistem AI, dimulai dengan pelatihan AI. Jika data pribadi digunakan untuk pelatihan AI, dasar hukum untuk pemrosesan data ini harus dipertanyakan.

“Keputusan yang memiliki kekuatan hukum hanya dapat diambil oleh manusia sesuai dengan Pasal 22 ayat 1 GDPR. Pengecualian hanya diperbolehkan dalam kasus-kasus tertentu, seperti persetujuan subjek data. Jika aplikasi AI mengembangkan usulan yang memiliki kekuatan hukum bagi subjek data, prosedur harus dirancang sedemikian rupa sehingga orang yang mengambil keputusan memiliki ruang gerak yang nyata dan keputusan tersebut tidak terutama didasarkan pada usulan AI.”

DSK juga membedakan antara sistem AI terbuka dan tertutup, di mana sistem AI tertutup berkaitan dengan kelompok pengguna dan kasus penggunaan yang ditentukan dan oleh karena itu lebih disukai dari perspektif perlindungan data. Dalam kasus sistem AI terbuka, yang tersedia untuk sejumlah besar peserta di internet, misalnya, masukan dari individu juga dapat menjadi tanggapan dari individu lain. Dalam hal ini, lebih sulit untuk memastikan kepatuhan perlindungan data.

Lebih lanjut, penggunaan aplikasi AI dalam kaitannya dengan kewajiban informasi dan transparansi yang dipertimbangkan oleh pengontrol GDPR:

- Jika pengontrol tidak mengembangkan aplikasi AI sendiri, mereka harus menerima informasi yang cukup dari penyedia untuk memenuhi persyaratan transparansi sesuai dengan Pasal 12 dan seterusnya GDPR. Pengembang harus menyediakan dokumentasi yang sesuai dan, sebagai pengolah sesuai dengan Pasal 28 ayat 3 kalimat 2 huruf e GDPR, mendukung pengontrol dalam menerapkan hak-hak subjek data.
- Pengontrol juga harus memberikan informasi tentang logika yang terlibat dalam pengambilan keputusan otomatis sesuai dengan Pasal 28 ayat 3 kalimat 2 huruf e GDPR. Pasal 22 ayat 1 GDPR dan ruang lingkup serta kemungkinan dampaknya bagi subjek data. Hal ini memerlukan penjelasan tentang metode pemrosesan data dan cara kerja program. Visualisasi dan teknik interaktif dapat berguna untuk menyajikan kompleksitas AI dengan cara yang mudah dipahami.
- Jika data input dan output dari AI (misalnya LLM) akan digunakan untuk pelatihan AI lebih lanjut, subjek data harus diberitahu. Jika mereka tidak mengecualikan penggunaan tersebut dan jika data pribadi dapat terpengaruh, maka diperlukan dasar hukum.
- Jika aplikasi AI dikendalikan oleh input teks dan input ini disimpan untuk diproses kemudian, subjek data harus diberitahu tentang hal ini. Secara khusus, jika orang lain juga memiliki akses ke dialog ini, subjek data harus dapat menghapus riwayat input.

Salah satu fokus GDPR adalah hak-hak subjek data. Pedoman tersebut menyatakan: “Pengontrol data harus memastikan bahwa subjek data dapat menggunakan hak mereka untuk perbaikan berdasarkan Pasal 16 GDPR dan penghapusan berdasarkan Pasal 17 GDPR. Langkah-langkah organisasi dan teknis harus dirancang untuk kedua hak tersebut sehingga dapat digunakan secara efektif.” Tentu saja, persyaratan ini juga berlaku untuk hak-hak subjek data lainnya.

Khusus untuk penggunaan LLM dan chatbot, DSK menyatakan bahwa hak untuk perbaikan juga ada di sini. “Harus dimungkinkan untuk menerapkan perbaikan ini dalam aplikasi AI, misalnya dengan mengoreksi data atau melalui pelatihan ulang/penyetelan halus.”

Prosedur berikut direkomendasikan untuk menghapus data pribadi. “Penekanan keluaran yang tidak diinginkan melalui filter hilir umumnya tidak merupakan penghapusan dalam arti Pasal 17 GDPR. Hal ini karena data yang menghasilkan keluaran tertentu setelah masukan tertentu masih dapat tersedia untuk model AI dalam bentuk yang dipersonalisasi. Namun, teknologi filter dapat membantu menghindari keluaran tertentu dan dengan demikian melayani hak dan kebebasan orang-orang yang terpengaruh oleh keluaran tertentu.” Selain itu, DSK merekomendasikan keterlibatan petugas perlindungan data serta dewan pekerja dan staf.

2. Implementasi aplikasi AI

Dalam hal perlindungan data, penting untuk menentukan siapa yang bertanggung jawab atas data pribadi. Hal ini mudah ditentukan jika organisasi mengoperasikan aplikasi AI di servernya sendiri dan untuk tujuan sendiri. Akan lebih sulit jika aplikasi AI digunakan sebagai layanan. Dalam hal ini, mungkin juga ada tanggung jawab bersama.

“Sesuai dengan Pasal 26 ayat 1 kalimat 2 GDPR, badan-badan yang terlibat harus secara transparan menentukan dalam sebuah perjanjian mana dari mereka yang harus mematuhi kewajiban mana berdasarkan GDPR, khususnya pemenuhan hak-hak subjek data dan kewajiban informasi sesuai dengan Pasal 13 dan 14 GDPR.”

Meskipun klarifikasi tanggung jawab sesuai dengan GDPR penting untuk hubungan eksternal, hal itu harus diklarifikasi secara internal dengan karyawan mengenai aplikasi AI mana yang dapat digunakan dan bagaimana, dan khususnya bagaimana data pribadi ditangani. Untuk tujuan ini, instruksi khusus harus disusun dan karyawan harus diberi pemahaman. Selain itu, organisasi harus memberikan karyawan ID pengguna perusahaan untuk sistem AI eksternal yang tidak memuat nama lengkap orang tersebut.

Penilaian risiko harus dilakukan sebelum pemrosesan data pribadi dimulai. Jika hal ini menunjukkan bahwa mungkin ada risiko tinggi bagi individu, penilaian dampak perlindungan data (DPIA) harus dilakukan sesuai dengan Pasal 26 ayat 14 GDPR. Pasal 35 GDPR diwajibkan, yang sering terjadi pada aplikasi AI. Otoritas perlindungan data juga menerbitkan daftar dan informasi yang diperbarui secara berkala tentang kapan DPIA diperlukan dan kapan tidak. Pengontrol data yang bukan pengembang sistem AI memerlukan informasi dari penyedia untuk hal ini dan harus mempertimbangkannya saat memilih aplikasi AI.

DSK juga merekomendasikan “desain yang sesuai dengan perlindungan data dalam arti “privasi berdasarkan desain” dan “privasi secara default”, yang mempertimbangkan fitur khusus sistem AI, serta implementasi langkah-langkah keamanan TI sehingga tidak ada yang dapat mengakses aplikasi AI tanpa otorisasi. Untuk tetap patuh secara hukum di masa mendatang, harus diimplementasikan suatu proses yang secara berkala menilai kesesuaian langkah-langkah yang diimplementasikan dan memperbaruinya jika perlu.

3. Penggunaan aplikasi AI

Bagian terakhir dari panduan ini berkaitan dengan penggunaan aplikasi AI. Peringatan pertama di sini adalah terhadap memasukkan data pribadi ke dalam sistem AI, terutama jika model AI yang digunakan tidak berada di Uni Eropa. Subjek data harus diinformasikan tentang penggunaan data mereka dan dasar hukum diperlukan untuk transfer tersebut. Kategori khusus data pribadi sesuai dengan Pasal 9 ayat 1 GDPR, yang mencakup asal ras dan etnis, keanggotaan serikat pekerja, opini politik, keyakinan agama atau filosofis, serta pemrosesan data genetik dan biometrik, data kesehatan atau data tentang orientasi seksual, sangat layak diperhatikan. untuk tujuan perlindungan. Pemrosesan data ini pada umumnya dilarang dan hanya diizinkan dalam kasus-kasus luar biasa berdasarkan ketentuan Pasal 9 ayat 2 sampai 4 GDPR.

“Hasil aplikasi AI dengan referensi pribadi harus diteliti secara kritis. Penyedia LLM khususnya sering menjelaskan bahwa teks yang dihasilkan oleh aplikasi mereka tidak mengklaim kebenaran dan harus selalu diteliti. Selain itu, aplikasi AI dapat memiliki berbagai tingkat informasi.”

Selain itu, DSK menekankan bahwa hasil dan prosedur AI perlu dinilai untuk memastikan tidak ada diskriminasi sehingga, misalnya, Undang-Undang Perlakuan Setara Umum Jerman (AGG) tidak dilanggar.

Otoritas Data Baden-Württemberg

Pada November 2023, LfDI BW menerbitkan makalah diskusi komprehensif yang menguraikan penilaiannya tentang penanganan sistem AI yang sesuai dengan GDPR. Berkaitan dengan pemrosesan data pribadi dalam sistem AI, LfDI BW menunjukkan bahwa penilaian tersebut bergantung pada waktu evaluasi. “Orang-orang dapat diidentifikasi sejak awal atau hanya pada titik waktu selanjutnya dengan informasi tambahan. Dalam setiap kasus, metode pembelajaran mesin yang digunakan harus dianalisis serta probabilitas bahwa orang-orang dapat (kembali) diidentifikasi melalui pengaruh yang tidak lazim pada sistem.”

Penilaian LfDI BW berkaitan dengan fase-fase pemrosesan individual (dari pengumpulan data pelatihan hingga keluaran AI), penilaian tanggung jawab GDPR, membahas dasar hukum untuk badan publik dan non-publik serta pemrosesan kategori khusus data pribadi. Sangat membantu untuk digunakan dalam proyek AI adalah pertanyaan panduan dalam dokumen untuk sebagian besar wwwws, yang mencakup pertanyaan-pertanyaan kunci untuk konten yang dibahas. Selain itu, daftar pemeriksaan singkat untuk pemrosesan dengan lima pertanyaan terpenting disertakan dalam lampiran, serta kumpulan materi yang menyediakan poin referensi untuk analisis lebih lanjut dan lebih mendalam.

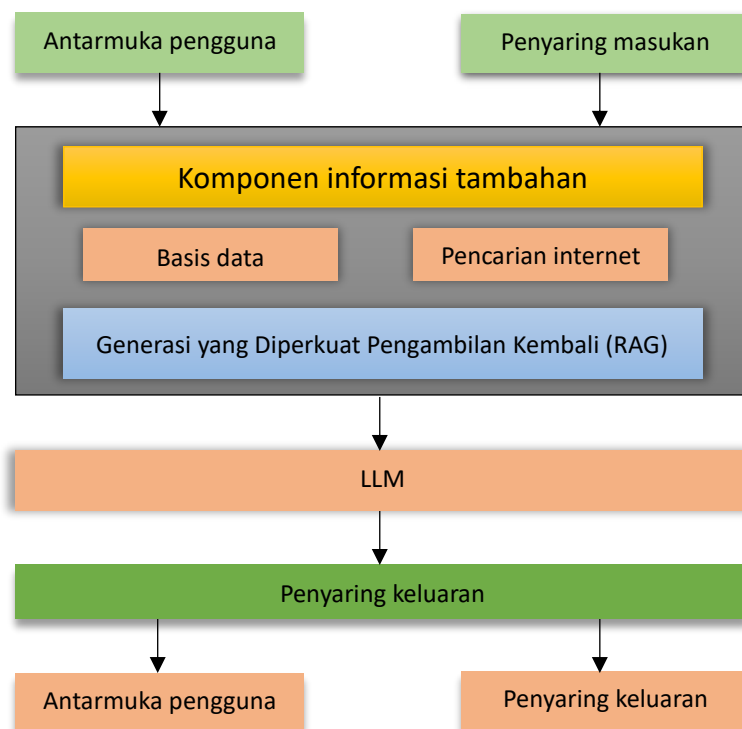
Komisioner Perlindungan Data Hamburg tentang LLM

Pada Juli 2024, Komisioner Perlindungan Data dan Kebebasan Informasi Hamburg (HmbBfDI) menerbitkan makalah diskusi tentang penerapan GDPR pada model bahasa besar (LLM). HmbBfDI menyatakan bahwa “makalah ini merupakan pendorong untuk debat. Tujuannya adalah untuk membantu perusahaan dan otoritas untuk lebih memahami kompleksitas hukum perlindungan data”.

Makalah diskusi merangkum tiga poin berikut:

1. Penyimpanan LLM semata tidak merupakan pemrosesan dalam arti Pasal 4 ayat 2 GDPR. Hal ini karena tidak ada data pribadi yang disimpan dalam LLM. Se jauh data pribadi diproses dalam sistem AI yang didukung LLM, operasi pemrosesan harus mematuhi persyaratan GDPR. Ini berlaku khususnya untuk output dari sistem AI tersebut.
2. Karena tidak adanya penyimpanan data pribadi dalam LLM, hak-hak subjek data berdasarkan GDPR tidak dapat dikaitkan dengan model itu sendiri. Namun, klaim untuk akses, penghapusan, atau perbaikan setidaknya dapat dikaitkan dengan input dan output dari sistem AI penyedia atau pengembang yang bertanggung jawab.
3. Pelatihan LLM dengan data pribadi harus mematuhi peraturan perlindungan data. Hak-hak subjek data juga harus dihormati. Namun, pelatihan yang mungkin melanggar peraturan perlindungan data tidak memengaruhi keabsahan penggunaan model tersebut dalam sistem AI.

Dengan ketiga poin ini, HmbHfDI berupaya memberikan kejelasan lebih lanjut pada diskusi terkini seputar penggunaan ChatGPT dan Copilot yang sesuai dengan hukum di perusahaan. Pertama, sistem AI “Chatbot” diuraikan menjadi komponen-komponennya dan dijelaskan sehingga masing-masing modul dapat dinilai secara terpisah:



Gambar 4.1 Interaksi dan Aliran Informasi antara Berbagai Komponen Sistem AI yang Menggunakan LLM

Komponen-komponen individual tersebut menjalankan fungsi-fungsi berikut:

Antarmuka pengguna: memungkinkan pengguna untuk berinteraksi dengan sistem AI.

Filter input: memproses input pengguna sebelum diteruskan ke LLM.

Komponen informasi tambahan:

Basis data: melengkapi input pengguna dengan informasi tambahan. Pencarian internet: mencari informasi yang relevan di internet.

Generasi Tambahan Pengambilan (RAG): menggabungkan dan mengintegrasikan informasi yang ditemukan.

LLM (Model Bahasa Besar): memproses input pengguna yang telah dimodifikasi dan menghasilkan respons yang sesuai.

Filter output: memproses output langsung dari LLM sebelum ditampilkan kepada pengguna.

Selanjutnya, dijelaskan bahwa elemen sentral pemrosesan informasi linguistik dalam LLM adalah tokenisasi. Di sini, teks dipecah menjadi unit-unit kecil yang telah ditentukan sebelumnya, yang disebut token, yang biasanya lebih kecil dari kata tetapi lebih besar dari huruf individual. Hal ini memungkinkan untuk bekerja dengan sejumlah elemen dasar terbatas yang dapat ditempatkan dalam hubungan satu sama lain.

Misalnya, kalimat “Perlindungan data itu penting” dibagi menjadi token seperti [Dat] [aprot] [ection] [is] [impo] [rtant], Token-token ini kemudian dipetakan ke nilai numerik dan diproses lebih lanjut dalam model. Teks ada dalam model sebagai fragmen dalam bentuk token numerik ini dan yang disebut embedding-nya. Ini membuat hubungan yang dipelajari dapat diakses dengan menghubungkan token satu sama lain dan mengaturnya sesuai dengan probabilitas.

Ketika model merespons masukan seseorang, ia menggunakan representasi matematis dari masukan yang dipelajari. Keluaran LLM pertama kali dihasilkan sebagai urutan token, yang kemudian diubah menjadi urutan huruf. Misalnya, LLM dapat menghasilkan kata “proyek” dari token “pro” dan “ject” atau kata “proyektil” dari “pro” dan “ject” dan “il”, tergantung pada konteksnya. Ini menunjukkan bagaimana tokenisasi yang fleksibel dan bergantung pada konteks serta pembangkitan teks berdasarkan tokenisasi tersebut bekerja dalam LLM.

HmbBfDI mencatat bahwa LLM itu sendiri tidak menyimpan data pribadi apa pun dalam arti Pasal 4 ayat 1, 2 GDPR bersamaan dengan Pertimbangan 26, karena model tersebut hanya berisi representasi matematis dari teks yang diproses.

Secara khusus ditekankan bahwa pelatihan LLM dengan data pribadi harus mematuhi peraturan perlindungan data, tetapi pelatihan yang melanggar peraturan perlindungan data tidak memengaruhi keabsahan penggunaan model tersebut, tetapi hanya memengaruhi penyedia LLM. Untuk hak-hak subjek data, ini berarti bahwa akses, penghapusan, atau perbaikan tidak boleh terkait langsung dengan model, tetapi dengan input dan output sistem AI. Hal ini dapat berupa pelatihan, kode etik atau pedoman lain untuk karyawan.

FAQ dari Otoritas Perlindungan Data Austria

Pada awal Juli 2024, dsb menerbitkan FAQ di situs webnya yang membahas isu-isu utama yang berkaitan dengan implementasi AI di perusahaan. Pertanyaan-pertanyaan ini terus diperluas untuk mencakup topik dan temuan lebih lanjut.

Menanggapi pertanyaan apakah pengembang yang belum mengembangkan sistem AI juga harus mematuhi GDPR, jawabannya adalah sebagai berikut: “Segera setelah seseorang atau badan hukum memutuskan tujuan dan cara pemrosesan data, mereka harus memenuhi syarat sebagai pengendali data berdasarkan hukum perlindungan data dan wajib mematuhi

GDPR. Meskipun spesifikasi teknis mungkin berasal dari penyedia atau pengembang, hal ini umumnya tidak mengubah fakta bahwa entitas yang menggunakan sistem AI harus dianggap sebagai pengendali data berdasarkan hukum perlindungan data.”

Menanggapi pertanyaan tentang hubungan antara GDPR dan Undang-Undang AI, berikut ini jawabannya: “Pasal 2 ayat 7 Undang-Undang AI menyatakan bahwa GDPR, pekerjaan otoritas perlindungan data, dan kewajiban penyedia dan pengembang sistem AI dalam peran mereka sebagai pengendali atau pengolah data tetap tidak terpengaruh oleh Undang-Undang AI. GDPR tetap berlaku (secara paralel) jika data pribadi diproses. Oleh karena itu, otoritas perlindungan data bertanggung jawab atas masalah perlindungan data yang berkaitan dengan sistem AI.”

Jawaban atas pertanyaan-pertanyaan tersebut sering kali berisi tautan ke otoritas dan keputusan lain yang sesuai untuk analisis lebih lanjut.

4.7 CHATGPT DAN PENGADUAN PERLINDUNGAN DATA DARI NOYB

Contoh konkret dari konflik antara GDPR dan penggunaan AI generatif adalah kasus pengaduan oleh noyb - Pusat Hak Digital Eropa, Wina, terhadap OpenAI OpCo LLC, San Francisco. Seorang karyawan pengadu menemukan bahwa ChatGPT memberikan informasi yang salah tentang tanggal lahirnya. Permintaannya untuk penghapusan data yang salah dijawab oleh pengembang AI generatif OpenAI dengan alasan bahwa mereka tidak dapat sepenuhnya menghapus atau memperbaiki data yang berkaitan dengan tanggal lahir. Mereka hanya dapat mencegah tampilan data tersebut untuk pengguna ChatGPT. Menurut pengadu, ini merupakan pelanggaran terhadap Pasal 5 ayat 1 huruf d GDPR.

Secara Detail:

Menurut pengaduan tersebut, ChatGPT telah memberikan tanggal lahir pengadu secara salah, yang menurut pendapat mereka menunjukkan bahwa data yang digunakan tidak akurat. Hal ini merupakan pelanggaran terhadap kewajiban keakuratan data sebagaimana diatur dalam GDPR. Ketika pengadu mengajukan permintaan akses dan penghapusan, OpenAI hanya fokus pada data akun pengadu dan tidak memberikan informasi apa pun tentang data pribadi yang diproses dalam Model Bahasa Besar ChatGPT.

Dalam tanggapannya, OpenAI menjelaskan bahwa secara teknis tidak mungkin untuk memperbaiki data tanpa memengaruhi informasi relevan lainnya. Namun, ini bertentangan dengan persyaratan GDPR, yang mensyaratkan koreksi atau penghapusan segera data pribadi yang tidak akurat. OpenAI lebih lanjut berpendapat bahwa pembatasan informasi yang diberikan oleh ChatGPT akan melanggar kebebasan berekspresi dan kebebasan informasi publik, karena pengadu adalah tokoh publik.

Kasus ini menggambarkan kesulitan yang dapat muncul dalam mematuhi GDPR dalam konteks sistem AI yang kompleks. Ketidakmampuan OpenAI untuk sepenuhnya menghapus atau memperbaiki data yang salah menunjukkan tantangan yang terkait dengan pemrosesan data pribadi dalam model AI skala besar. Pada saat yang sama, Undang-Undang AI menekankan perlunya sistem AI untuk beroperasi secara bertanggung jawab dan transparan,

yang tidak sepenuhnya dipastikan dalam kasus ini. Masih perlu dilihat bagaimana pengadilan akan memutuskan kasus ini.

BAB 5

HAK KEKAYAAN INTELEKTUAL

5.1 PENDAHULUAN

Hak kekayaan intelektual (“hak kekayaan intelektual”; secara internasional juga disebut “hak kekayaan intelektual” atau “hak kekayaan intelektual”) mengacu pada ciptaan manusia yang tidak berwujud seperti teks, gambar, perangkat lunak, basis data, pengetahuan teknis, atau penemuan. Hal ini dapat tunduk pada berbagai hak perlindungan berdasarkan hukum kekayaan intelektual jika persyaratan yang relevan dipenuhi sesuai dengan hukum yang berlaku :

- Hak kekayaan industri terdaftar seperti paten dan model utilitas, merek dagang atau desain;
- Hak cipta atau hak cipta tambahan;
- Perlindungan rahasia dagang.

Pencipta atau pemilik hak kekayaan intelektual menikmati perlindungan terhadap akses atau penggunaan yang tidak sah oleh pihak ketiga.

UU Kekayaan Intelektual tidak memengaruhi peraturan hak kekayaan intelektual yang ada, tetapi mempertimbangkannya dalam berbagai konteks sebagai hak fundamental yang ditentukan (lihat Pertimbangan 1 UU Kekayaan Intelektual, Pertimbangan 48 UU Kekayaan Intelektual, Pasal 17 Piagam Hak Fundamental Uni Eropa). Korelasi kekayaan intelektual yang paling penting meliputi Berikut ini:

- Luasnya dampak negatif sistem AI terhadap hak-hak fundamental yang dilindungi oleh Piagam – termasuk hak kekayaan intelektual – relevan untuk klasifikasi AI berisiko tinggi berdasarkan Pasal 6 dan seterusnya dari UU AI dan AI Tujuan Umum menurut Pasal 51 UU AI. Selain itu, ketika mengadopsi tindakan delegasi, Komisi harus mempertimbangkan dampak terhadap hak-hak fundamental, termasuk hak kekayaan intelektual (misalnya, ketika mengubah klasifikasi risiko sebagai AI berisiko tinggi menurut Lampiran III sesuai dengan Pasal 7 UU AI).
- Perlindungan hak kekayaan intelektual pihak ketiga juga tercermin dalam banyak kewajiban para pengembang, penyedia, importir, dan produsen (misalnya, manajemen risiko, penggunaan dan tata kelola data, penilaian dampak hak-hak fundamental untuk AI berisiko tinggi, pelaporan insiden serius). Hal ini sangat penting ketika menggunakan AI generatif. Penyedia AI Tujuan Umum khususnya harus menerapkan kebijakan untuk melindungi hak cipta dan membuat ringkasan yang cukup rinci tentang konten yang digunakan untuk pelatihan (Pasal 53 ayat 1 UU AI bersamaan dengan Pertimbangan). 106 dan seterusnya dari UU AI) tersedia. Hal ini seharusnya mencegah distribusi ilegal karya yang dilindungi hak cipta. Namun, di sepanjang rantai nilai AI, kewajiban harus dipenuhi sedemikian rupa sehingga masing-masing pihak yang menerapkannya tidak membahayakan hak kekayaan intelektual mereka sendiri (Pertimbangan 88 UU AI).

- Komisi, otoritas pengawasan pasar, dan badan yang diberi pemberitahuan, serta semua orang atau badan hukum lain yang terlibat dalam penerapan Peraturan HKI wajib menjaga kerahasiaan dalam kegiatan mereka. Mereka harus melindungi hak kekayaan intelektual dari akses, penggunaan, dan pengungkapan yang melanggar hukum (Pasal 78 Peraturan HKI).
- Akses oleh badan yang memberi pemberitahuan dalam konteks penilaian kesesuaian AI berisiko tinggi, yaitu akses ke model pelatihan dan model terlatih dari sistem AI, termasuk parameter yang relevan, tunduk pada hukum Uni Eropa yang ada tentang perlindungan HKI dan rahasia dagang (Lampiran VII UU AI).
- Perlindungan hak kekayaan intelektual juga merupakan titik pemeriksaan dalam konteks laboratorium nyata AI (Pasal 57 ayat 6 UU AI). (UU AI).
- Dalam praktiknya, penyedia atau pengembang dihadapkan pada pertanyaan, apakah
- sistem AI, komponennya, dan dokumentasi yang menyertainya dilindungi oleh hukum kekayaan intelektual dan
- penggunaan AI sesuai dengan hukum kekayaan intelektual.

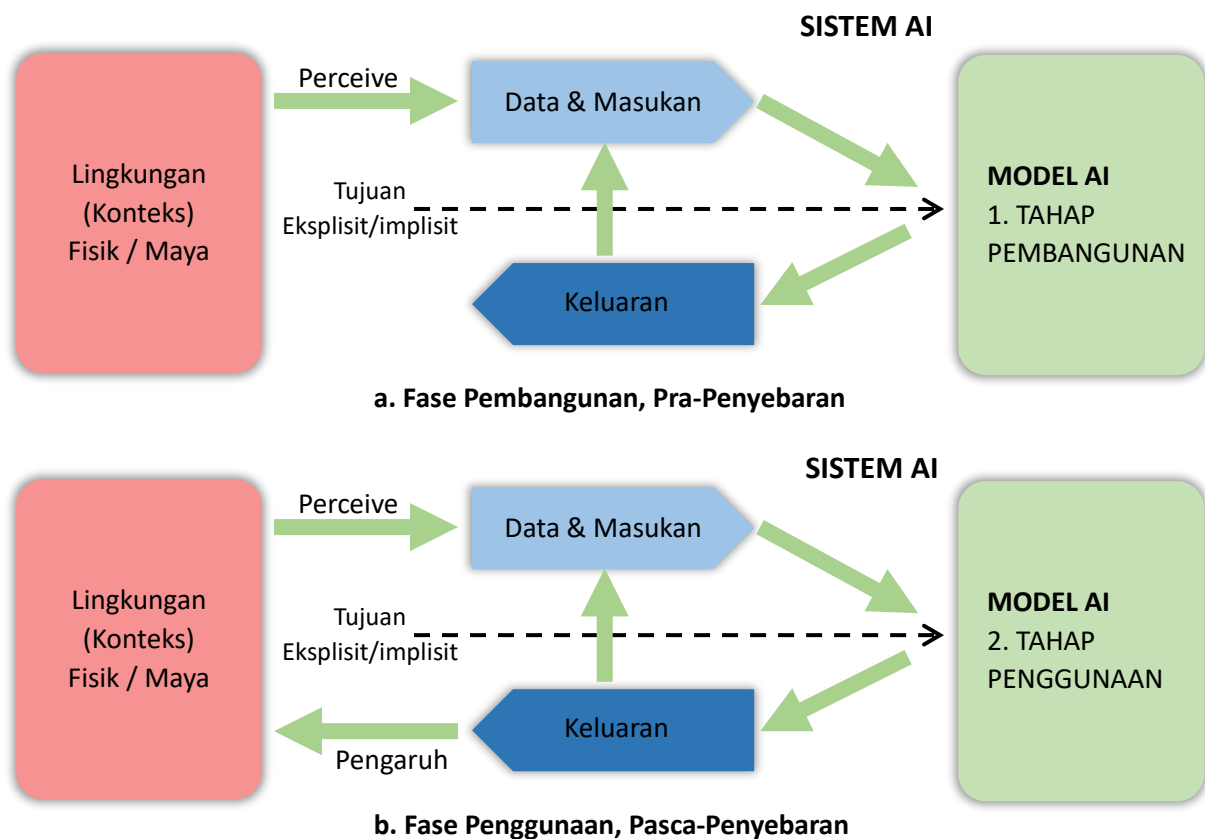
Yang terakhir harus dievaluasi baik dari sisi input maupun output terkait hak pihak ketiga. Oleh karena itu, berikut ini kami akan membahas kedua masalah ini.

5.2 PERLINDUNGAN AI DAN KOMPONENNYA

Untuk menilai kelayakan perlindungan, diperlukan pemeriksaan teknis awal. Definisi sistem AI dalam arti UU AI didasarkan pada definisi AI OECD. Dengan demikian, sistem AI adalah sistem berbasis mesin yang terdiri dari model AI, input (data), dan output, yang dirancang untuk berbagai tingkat operasi otonom, dapat beradaptasi, dan yang menghasilkan pengaruh terhadap lingkungan fisik atau virtual dari input yang diterima untuk tujuan eksplisit atau implisit (Pasal 3 ayat 1 UU AI).

Apakah AI dapat dikualifikasikan sebagai perangkat lunak merupakan subjek perdebatan yang beragam. Namun, pertimbangan dalam Undang-Undang AI berupaya membedakan sistem AI dari perangkat lunak tradisional (Pertimbangan 12 Undang-Undang AI). Peraturan tambahan, seperti Arahan Tanggung Jawab Produk yang telah diubah, juga berlaku untuk sistem AI dengan memperluas definisi produk termasuk perangkat lunak. Menurut pendapat saya, ini tidak menyisakan keraguan tentang klasifikasi AI sebagai perangkat lunak.

Namun, komponen sistem AI secara keseluruhan harus dibedakan: (i) model AI, yang dalam banyak kasus mewakili kumpulan algoritma, model, dan metode yang mungkin; (ii) data masukan dan (iii) keluaran, yang dapat bermanifestasi dalam berbagai bentuk (misalnya sebagai prediksi, konten, rekomendasi, atau keputusan).



Gambar 5.1 Representasi Visual Definisi AI OECD

Berdasarkan pemahaman ini, sistem AI dan, dalam beberapa kasus, komponennya dapat dilindungi terutama oleh hak cipta atau hak cipta tambahan. Di sisi lain, hukum paten atau model utilitas seringkali dikesampingkan. Hal ini dijelaskan secara rinci di bagian berikut.

Hak Cipta dan Hak Cipta Tambahan

Informasi Umum

Karya intelektual menikmati perlindungan hak cipta. Oleh karena itu, karya tersebut harus berbeda dari karya sehari-hari, umum, biasa, dan memiliki karakteristik pribadi. Karya di bidang sastra, seni suara, seni visual, dan sinematografi memenuhi syarat untuk perlindungan. Perlindungan hak cipta muncul dengan tindakan penciptaan dan tidak memerlukan pendaftaran terpisah, seperti halnya dengan kekayaan intelektual terdaftar.

Fakta, ide semata termasuk ide bisnis, proses, metode, konsep matematika, gaya dan cara tidak dilindungi oleh hak cipta.

Program komputer dapat dilindungi sebagai karya sastra, jika merupakan hasil kreasi asli dan merupakan karya individu. Menurut hukum kasus Austria, program komputer harus menunjukkan tingkat kompleksitas tertentu, artinya solusi untuk tugas tersebut dapat dikuasai dengan beberapa cara dan pemrogram memiliki kebebasan untuk mengembangkan fitur individual. Perlindungan hak cipta atas program komputer mencakup semua bentuk ekspresi, seperti kode sumber, kode biner, kode objek, kode byte, kode assembler, dan materi kompilasi dan pengembang. Program komputer sehari-hari yang biasa, di sisi lain, yang pembuatannya

tidak memerlukan usaha dan biaya atau pencapaian intelektual yang signifikan, tidak dilindungi oleh hak cipta. Atas dasar ini, perlindungan hak cipta AI dapat dinilai sebagai berikut.

Sistem AI yang Dikembangkan Secara Individual

Sistem AI yang dikembangkan secara individual umumnya dilindungi oleh hak cipta secara keseluruhan karena kompleksitas dan ruang lingkup desain yang ada. Lagipula, mereka membutuhkan keahlian khusus di bidang tersebut dan berbeda dari yang biasa.

Model AI yang Dikembangkan Secara Individual

Perlindungan hak cipta atas model AI, di sisi lain, masih kontroversial. Model AI seringkali didasarkan pada metode dan perhitungan matematika yang umum dikenal. Hal ini umumnya tidak dilindungi oleh hak cipta. Bahkan dalam kasus model yang kompleks, masih dipertanyakan apakah ada cukup ruang untuk kreasi orisinal dan dengan demikian perlindungan hak cipta dapat diasumsikan untuk model AI dalam kasus urutan yang murni teknis.

Hal ini harus dibedakan dari implementasi algoritma dalam kode program dan struktur program. Kombinasi banyak langkah program dan solusi masalah yang dibentuk secara individual dapat memenuhi syarat untuk perlindungan.

Contoh

Contoh pembelajaran mesin mengilustrasikan kesulitan mengklasifikasikan model AI sebagai program komputer milik pribadi. Di satu sisi, topologi jaringan dan pembobotan yang ditentukan untuk pelatihan dan eksekusi dapat bervariasi dan kompleks tergantung pada model pembelajaran mesin. Semakin banyak lapisan dan neuron yang dimiliki jaringan dan semakin efisien dan andal model yang dirancang, semakin menonjol komponen tersebut dari yang biasa. Biaya investasi yang tinggi juga dapat mendukung hal ini. Namun, patut dipertanyakan apakah optimasi urutan komputasi ini bukan hanya bersifat teknis dan sebenarnya tidak memungkinkan kebebasan kreatif apa pun, karena kemungkinan untuk merancang jaringan saraf terbatas.

Kumpulan Data Masukan dan Pelatihan

Tidak hanya sistem AI sebagai program komputer yang dapat dilindungi, tetapi juga kumpulan data masukan dan pelatihannya serta pengaturan data tersebut. Hukum hak cipta memberikan perlindungan khusus untuk basis data. Basis data adalah kumpulan karya, data, atau elemen independen lainnya yang diatur secara sistematis atau metodis dan dapat diakses secara individual melalui sarana elektronik atau lainnya. Namun, perlindungan hak cipta hanya berlaku jika pemilihan atau pengaturan konten tersebut merupakan ciptaan asli. Hal ini membutuhkan pencapaian kreatif, yang dapat muncul dari keputusan untuk memasukkan konten ke dalam basis data atau untuk menyusunnya. Karena ada ruang untuk bermanuver ketika mengatur kumpulan data masukan dan pelatihan, saya percaya bahwa perlindungan hak cipta pada umumnya dimungkinkan.

Sebagai alternatif, konten yang diatur dalam kumpulan data masukan dan pelatihan dapat menikmati perlindungan sui generis sebagai basis data sederhana. Hal ini membutuhkan keberadaan basis data dan investasi substansial dalam hal jenis atau ruang lingkup untuk pengadaan, peninjauan, atau presentasi kontennya. Ketentuan umum ini memberikan

perlindungan investasi kepada pengembang dan perlindungan terhadap akuisisi layanan mereka atau bagian-bagian penting dari basis data oleh pihak ketiga.

Dokumentasi Pengguna dan Manual Pengguna

Dokumentasi pengguna dan manual pengguna dapat mencapai karakter karya dan menikmati perlindungan sebagai karya sastra, jika merupakan ciptaan asli.

Contoh

Namun menurut pendapat saya, masih dipertanyakan apakah petunjuk penggunaan untuk AI berisiko tinggi dapat dianggap sebagai ciptaan intelektual asli sesuai dengan Pasal 13 ayat 2 UU AI. Petunjuk tersebut, misalnya, harus menjelaskan karakteristik, kemampuan, dan keterbatasan kinerja sistem AI serta keadaan penggunaan yang diketahui dan kemungkinan risikonya. Hal ini memiliki kesamaan dengan brosur kemasan produk obat, yang perlindungan hak ciptanya telah ditolak di masa lalu.

Hak dan Klaim Penulis

Penulis menikmati hak eksklusif dan moral. Oleh karena itu, pemanfaatan karya sepenuhnya menjadi hak penulis, selama belum ada pihak ketiga yang diberikan izin untuk menggunakan karya tersebut.

Penulis menikmati hak pemanfaatan yang tercantum di bawah ini. Dalam praktiknya, dalam kasus aplikasi AI, hal-hal berikut sangat relevan:

- Hak reproduksi: Penulis memiliki hak eksklusif untuk mereproduksi karya tersebut dengan cara apa pun, dalam jumlah berapa pun, sementara atau permanen. Pengecualian berlaku dalam konteks penggunaan karya secara bebas, khususnya reproduksi sementara atau yang menyertainya, penambahan teks dan data dan, dalam kasus program komputer, juga dalam kasus penggunaan dan dekompilasi sesuai dengan tujuan yang dimaksud.
- Hak distribusi: Hanya penulis yang dapat mendistribusikan karyanya dan, misalnya, memasarkannya. Namun, hak distribusi perangkat lunak berakhir ketika perangkat lunak tersebut dipasarkan di EEA dengan persetujuan penulis.
- Hak untuk menyediakan: Selanjutnya, hanya penulis yang berhak untuk menyediakan karya tersebut kepada publik melalui sarana kabel atau nirkabel. Hak eksploitasi ini berlaku untuk penyediaan sistem AI melalui antarmuka daring.
- Hak adaptasi: Karya hanya dapat diadaptasi dengan persetujuan penulis. Pengecualian adalah adaptasi untuk penggunaan yang dimaksudkan dan sehubungan dengan dekompilasi. Penggunaan bebas juga dikecualikan. Hal ini berlaku jika karya tersebut hanya berfungsi sebagai sumber inspirasi untuk pembuatan karya baru yang individual. Karya asli mungkin tidak lagi dapat dikenali dengan jelas dalam karya baru tersebut.

Selain itu, pencipta menikmati hak moral seperti hak yang mutlak untuk menjadi penulis atau hak yang dapat diabaikan untuk atribusi penulis.

Penulis berhak atas hak-hak berikut terhadap pelanggaran hak-haknya:

- Upaya hukum berupa perintah penghentian tanpa memandang kesalahan (dalam praktiknya, tuntutan utama, yang juga dapat ditegakkan melalui perintah penghentian sementara)

- Tuntutan untuk penghapusan (misalnya, penghancuran salinan ilegal)
- Tuntutan tanpa kesalahan untuk remunerasi yang sesuai
- Tuntutan ganti rugi (termasuk tuntutan berdasarkan kesalahan sebesar dua kali lipat dari kompensasi yang sesuai sebagai ganti rugi yang telah ditetapkan)
- Penyerahan keuntungan dan tuntutan akuntansi
- Tuntutan untuk publikasi putusan

Pemberian Hak

Jika penulis ingin mengkomersialkan karyanya, diperlukan lisensi hak. Hukum hak cipta membedakan antara izin dan hak untuk menggunakan suatu karya:

Izin untuk menggunakan suatu karya memberikan hak penggunaan non-eksklusif kepada pihak ketiga. Sebaliknya, hak untuk menggunakan suatu karya memberikan hak eksklusif kepada pihak ketiga yang berlaku terhadap siapa pun. Pihak ketiga bahkan dapat menegakkan hak eksploitasi yang dilisensikan terhadap penulis itu sendiri. Oleh karena itu, hak untuk menggunakan karya adalah hak yang lebih kuat.

Dalam kedua kasus tersebut, cakupan lisensi dapat disesuaikan secara bebas. Lisensi dapat dibatasi dalam hal waktu, wilayah, atau pokok bahasan. Perlu juga diperhatikan bahwa, menurut yurisprudensi, pemberian hak penggunaan untuk jenis eksploitasi di masa mendatang yang belum diketahui umumnya tidak diizinkan tanpa persetujuan sebelumnya. Pada saat kontrak dibuat, pemberi lisensi tidak dapat memperkirakan hal tersebut. Jika lisensi juga diberikan untuk jenis penggunaan di masa mendatang yang saat ini belum diketahui, pemberi lisensi berhak atas biaya tambahan. Ini adalah topik terkini yang berkaitan dengan AI.

Kasus khusus berlaku untuk program komputer yang dibuat oleh seorang karyawan dalam menjalankan tugas resminya. Berdasarkan hukum Austria, "hak istimewa pemberi kerja" berlaku di sini, yang memberikan hak tak terbatas kepada pemberi kerja untuk menggunakan karya tersebut. Tujuan dari ketentuan ini adalah agar pemberi kerja menanggung biaya yang terkait dengan pemrograman program komputer dan dengan demikian berhak atas hak eksploitasi eksklusif. Selain itu, pemberi kerja berhak atas hak moral, khususnya hak untuk atribusi penulis.

Perangkat Lunak Sumber Terbuka

Dalam pengembangan perangkat lunak, perangkat lunak sumber terbuka memainkan peran utama. Perangkat lunak sumber terbuka memungkinkan pengembangan lebih lanjut yang cepat dan hemat sumber daya, sehingga mendorong inovasi. Namun, perangkat lunak sumber terbuka bukanlah milik umum. Perangkat lunak ini tunduk pada ketentuan lisensinya sendiri. Lisensi tersebut biasanya memberikan izin penggunaan perangkat lunak secara gratis, termasuk kode sumbernya. Namun, sebagai imbalannya, beberapa lisensi mewajibkan pemegang lisensi dalam berbagai tingkatan. Kewajiban yang paling relevan berkaitan dengan kewajiban untuk mempublikasikan:

- **Lisensi Copyleft** Di bawah ketentuan lisensi ini, pemrograman harus didistribusikan di bawah lisensi yang sama, terlepas dari adaptasi apa pun. Oleh karena itu, hak dan kewajiban yang sama yang diterima dan dipatuhi oleh pemegang lisensi juga harus diberikan atau dialihkan kepada pihak ketiga (termasuk pelanggan akhir). Selain itu,

kode sumber biasanya harus dipublikasikan atau setidaknya diungkapkan kepada pengguna perangkat lunak (yang diproses).

- **Lisensi Non-copyleft** Dengan ketentuan lisensi ini, terdapat lebih sedikit pembatasan pada distribusi perangkat lunak lebih lanjut. Secara khusus, pengembangan lebih lanjut tidak harus didistribusikan di bawah lisensi bebas. Oleh karena itu, pemegang lisensi juga dapat menuntut biaya untuk komersialisasi perangkat lunak atau merahasiakan kode sumber.

Tantangan terbesar adalah menggabungkan beberapa lisensi perangkat lunak sumber terbuka dalam satu pengembangan. Lisensi tersebut harus kompatibel satu sama lain dan tidak boleh saling bertentangan sehingga ketentuan lisensi masing-masing dapat dipatuhi. Sebelum sistem AI dibangun di atas perangkat lunak sumber terbuka, audit sumber terbuka sebelumnya direkomendasikan untuk mengevaluasi kompatibilitas dan kemungkinan pemenuhan kewajiban yang sesuai.

Perlindungan Paten dan Model Utilitas

Paten dan model utilitas melindungi penemuan teknis. Pemiliknya menikmati hak eksklusif untuk jangka waktu tertentu dan dapat melarang orang lain menggunakan inovasi tersebut.

Untuk mendapatkan perlindungan paten, penemuan tersebut harus:

- memiliki efek teknis,
- baru (tidak ada inovasi atau publikasi sebelumnya),
- inventif (tidak jelas bagi orang yang ahli di bidang ini) dan
- dapat diterapkan secara komersial.

Sebaliknya, model utilitas (“paten kecil”) hanya perlu:

- berdasarkan langkah inventif,
- baru (dengan mempertimbangkan masa tenggang enam bulan untuk pra-publikasi sendiri) dan
- dapat diterapkan secara komersial.

Antara lain, metode matematika dan program untuk pengolahan data tidak memenuhi syarat untuk perlindungan. Pengecualian ini relevan untuk penilaian perlindungan paten atau model utilitas untuk sistem AI:

Program komputer dikecualikan dari perlindungan, jika program tersebut hanya terdiri dari instruksi kontrol untuk pengoperasian komputer (misalnya dalam bentuk algoritma). Bentuk pemrograman ini sebagai instruksi semata termasuk dalam pengecualian hukum. Namun, jika merupakan penemuan yang diimplementasikan komputer yang eksekusi instruksi programnya memiliki efek teknis lebih lanjut, perangkat lunak juga dapat memenuhi syarat untuk perlindungan sebagai paten atau model utilitas. Namun, teknis dan langkah inventif yang diperlukan juga harus ada, yang seringkali lebih sulit dicapai dalam praktik dengan perangkat lunak AI. Sebelum suatu inovasi dipublikasikan, ada baiknya untuk memeriksa perlindungan paten atau model utilitas. Hal ini meningkatkan nilai aset IP dan karenanya juga nilai perusahaan.

Perlindungan Rahasia Dagang

Sistem AI, proses yang mendasarinya, derivasi, struktur basis data, fungsionalitas, dan pengetahuan untuk pengoperasian dan pengembangan lebih lanjut juga dapat dilindungi sebagai rahasia dagang. Untuk tujuan ini, informasi harus

- bersifat rahasia,
- bernilai komersial dan
- tunduk pada langkah-langkah kerahasiaan yang sesuai.

Informasi bersifat rahasia jika tidak dapat diakses secara umum baik secara keseluruhan maupun dalam komposisi spesifik komponennya. Oleh karena itu, informasi tersebut tidak boleh dapat ditemukan tanpa upaya yang besar.

Nilai komersial diasumsikan jika informasi tersebut memiliki nilai komersial atau menyebabkan kerugian ekonomi bagi pemiliknya jika diungkapkan.

Contoh

Dokumentasi yang menyertai sistem AI dapat dikategorikan sebagai rahasia dagang terlepas dari perlindungan hak cipta, jika pengetahuan tertulis ini penting untuk pengoperasian dan pengembangan lebih lanjut dari sistem AI, menyangkut area yang belum pernah dieksplorasi sebelumnya, dan banyak pesaing di pasar tertarik untuk menjual pemrograman AI ini termasuk dokumentasinya. Dalam hal ini, akan ada nilai komersial.

Tindakan kerahasiaan yang tepat mencakup tindakan organisasi, teknis, dan kontraktual yang memadai. Tindakan spesifik bergantung pada keadaan kasus yang bersangkutan. Pada prinsipnya, klasifikasi dokumen menurut tingkat kerahasiaan, pembatasan akses menurut prinsip “kebutuhan untuk mengetahui”, pencatatan akses, enkripsi konten, kesepakatan kewajiban kerahasiaan dengan karyawan dan pihak ketiga yang terlibat, dan pelatihan rutin adalah tindakan yang mungkin dilakukan.

5.3 KEPATUHAN HKI DALAM PENGGUNAAN AI

Pemeriksaan mendalam terhadap masalah kepatuhan HKI dari suatu sistem AI sangat penting. Hal ini juga diilustrasikan oleh sengketa hukum saat ini terhadap penyedia model bahasa besar. Beberapa penerbit dan penulis mengklaim pelanggaran hak cipta berdasarkan Undang-Undang Hak Cipta Milenium Digital AS, khususnya komersialisasi HKI pihak ketiga dan distribusi karya yang dilindungi tanpa persetujuan penulis.

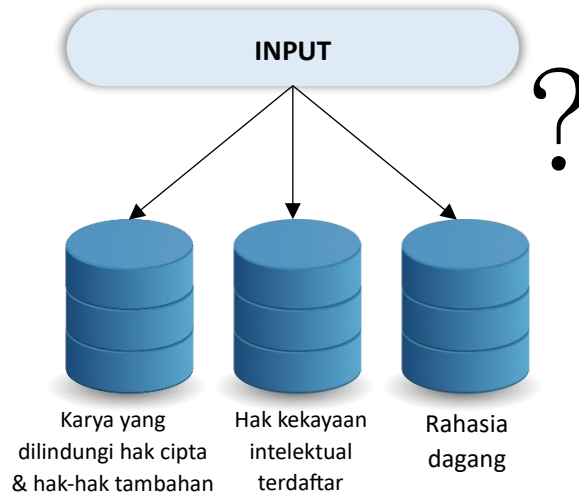
Oleh karena itu, pemeriksaan kepatuhan HKI harus berfokus pada aspek-aspek berikut:

- Apakah penggunaan materi yang dilindungi HKI di sisi input untuk pembuatan korpus AI atau untuk pelatihan AI sah secara hukum?
- Persyaratan Undang-Undang AI mana yang harus diimplementasikan di sisi input desain AI untuk melindungi hak HKI pihak ketiga, terutama saat membuat teks, gambar, dan video?
- Apakah hasil yang dihasilkan AI di sisi output menikmati perlindungan HKI, dan siapa yang dapat menggunakannya dan sejauh mana?

Masukan AI

Data Masukan yang Dilindungi Hak Kekayaan Intelektual

Masukan AI dapat terdiri dari berbagai jenis data. Dalam proses perancangan AI, perlu dinilai apakah konten yang dilindungi hak kekayaan intelektual juga perlu dikumpulkan dari aktivitas pengguna dan perintah mereka, diduplikasi dalam korpus AI, dan dianalisis:



Gambar 5.2 Contoh Sumber Data Masukan

Dalam hal ini, batasan hukum berikut harus dipertimbangkan:

- **Perlindungan hak cipta**

Jika karya yang dilindungi hak cipta digunakan untuk masukan, karya tersebut umumnya akan direproduksi sesuai dengan hukum hak cipta selama penyusunan korpus AI atau kumpulan data pelatihan. Hal ini memerlukan justifikasi yang tepat, yang dapat didasarkan pada hak penggunaan bebas yang diberikan secara hukum atau lisensi yang diberikan secara kontraktual.

Salah satu justifikasi yang mungkin adalah penggunaan bebas untuk penambahan teks dan data. Siapa pun dapat mereproduksi suatu karya untuk lembaga penelitian, untuk lembaga warisan budaya, atau untuk penggunaan mereka sendiri guna mengevaluasi teks dan data digital secara otomatis untuk mendapatkan informasi. Untuk sektor swasta, penggunaan pribadi bebas relevan, yang juga mencakup penggunaan komersial. Prasyaratnya adalah pengguna memiliki akses yang sah (misalnya, konten sumber terbuka; hak akses yang diberikan secara kontraktual) ke karya tersebut dan tidak ada reservasi penggunaan yang dinyatakan. Namun, penggunaan bebas ini tidak tidak terbatas: (i) eksploitasi oleh pihak ketiga tidak boleh menyebabkan kerugian lebih dari minimal bagi penulis. Hal ini melindungi posisi ekonominya. (ii) Lebih lanjut, penggunaan bebas tidak termasuk modifikasi apa pun selain yang diperlukan untuk evaluasi otomatis dan pengambilan informasi. (iii) Terakhir, reproduksi hanya dapat disimpan selama diperlukan untuk mencapai tujuan analisis data dan pengambilan informasi. Prinsip-prinsip ini harus diperhitungkan dalam desain AI. Tergantung pada desain spesifiknya, penggunaan materi yang dilindungi hak cipta dapat dibenarkan berdasarkan ketentuan penambahan teks dan data.

Sebagai alternatif penggunaan penambangan teks dan data, penggunaan bebas suatu karya juga dapat didasarkan pada hak reproduksi yang hanya bersifat “sementara” dan insidental. Namun, reproduksi tersebut harus (i) hanya bersifat sementara, (ii) merupakan bagian integral dan penting dari suatu proses teknis, (iii) memiliki tujuan tunggal untuk transmisi karya dalam jaringan antara pihak ketiga melalui perantara atau penggunaan yang sah, (iv) tidak memiliki makna independen dan (v) tidak boleh menyebabkan modifikasi apa pun pada salinan. Dalam kasus AI generatif, memenuhi semua persyaratan ini lebih menantang dalam praktiknya karena reproduksi biasanya tidak mudah hilang atau menyertai.

Jika tidak ada penggunaan bebas suatu karya yang berlaku, eksploitasi hanya dapat dilakukan berdasarkan lisensi hak kontraktual yang sesuai oleh penulis. Lingkup lisensi dan interpretasinya sangat penting dalam hal ini.

- **Hak cipta tambahan**

Selain itu, hak cipta tambahan dari basis data harus dipertimbangkan. Hak ini dapat dilanggar oleh scraping. Akses individual yang relatif kecil diperbolehkan, tetapi ekstraksi sistematis tidak. Menurut yurisprudensi, akses yang dilakukan selama scraping harus dipertimbangkan secara keseluruhan dan dengan demikian dijumlahkan. Risiko ini harus dimitigasi dalam desain.

- **Hak milik terdaftar**

Jika, misalnya, merek dagang, gambar paten, aplikasi model utilitas, atau desain digunakan sebagai materi pelatihan, penggunaan (i)legal di sisi input juga terutama muncul dari perspektif hak cipta. Hukum ini hanya memberikan hak tertentu kepada pemiliknya yang ditujukan untuk penggunaan komersial oleh pihak ketiga, seperti penggunaan tanda yang dilindungi yang menyerupai merek dagang untuk barang dan jasa yang identik atau serupa. Namun, efek dari hak milik terdaftar dapat berdampak pada output. Jika AI menghasilkan tanda yang serupa atau menduplikasinya dan kemudian digunakan oleh pengguna untuk tujuan bisnis dalam konteks yang serupa, penggunaan spesifik tersebut dapat merupakan pelanggaran hak merek dagang, paten, model utilitas, atau desain pihak ketiga.

- **Perlindungan rahasia dagang**

Pengungkapan rahasia dagang dan bisnis dalam korpus AI, yang biasanya dipicu oleh perintah pengguna, sangat penting. Dalam kasus solusi AI akses terbuka dan gratis, kepentingan kerahasiaan dalam informasi ini dapat hilang karena kelompok pengguna yang tidak terbatas memiliki akses dan tidak ada lagi langkah-langkah kerahasiaan yang tepat. Pada beberapa bulan pertama popularitas ChatGPT, banyak perusahaan bahkan tidak menyadari potensi pengungkapan petunjuk dan hasil pengguna melalui sistem AI, yang menyebabkan hilangnya banyak pengetahuan.

Kemungkinan pengungkapan dan konsekuensi hilangnya perlindungan kerahasiaan perdagangan dan bisnis harus dinilai pada fase desain ketika mempertimbangkan adopsi instruksi pengguna dan hasil yang dihasilkan dalam input AI dan, jika perlu, diatasi dengan desain teknologi yang tepat dan kebijakan pengguna yang jelas.

Persyaratan Undang-Undang AI untuk Sistem AI

Undang-Undang AI mengatur kewajiban untuk melindungi hak kekayaan intelektual pihak ketiga dalam berbagai ketentuan, seperti yang disebutkan di atas. Tentu saja, ini juga berkaitan dengan input dan dengan demikian terutama dengan pengembangan, pengujian, dan pelatihan sistem AI. Persyaratan khusus untuk melindungi hak kekayaan intelektual pihak ketiga tidak didefinisikan secara tepat dalam Undang-Undang AI. Hanya ketentuan dalam Pasal 53 ayat 1 yang mengatur hal ini. Pasal 1 lit c Undang-Undang AI agak lebih spesifik, yang menurutnya penyedia model AI Tujuan Umum wajib menerapkan strategi untuk mematuhi hak cipta dan, khususnya, untuk mengidentifikasi dan mematuhi reservasi penggunaan untuk penambahan teks dan data, termasuk melalui teknologi mutakhir. Menurut pendapat saya, strategi tersebut harus mencakup sumber data, aliran data, hasil pemeriksaan tindakan eksploitasi dan pernyataan tentang izin serta langkah-langkah perlindungan untuk mencegah pelanggaran hak cipta. Sehubungan dengan keterlacakan sumber yang digunakan, metode generasi augmentasi pengambilan (RAG) sering dibahas. Pertimbangan teknis tersebut juga harus dimasukkan dalam kebijakan perlindungan hak cipta.

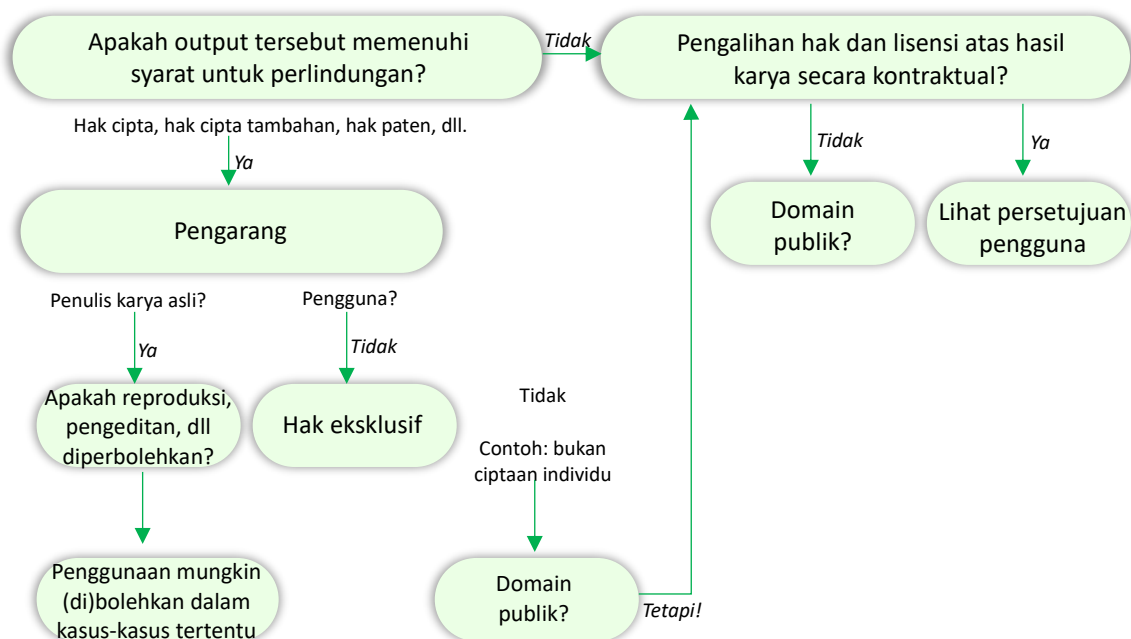
Keluaran AI

Pertanyaan tentang klasifikasi IP dari keluaran terutama berperan untuk konten yang dihasilkan AI seperti teks, gambar, dan video. Dari perspektif pengguna, ada kebutuhan akan penetapan hak yang jelas untuk menentukan kemungkinan penggunaan. Hal ini bergantung pada berbagai aspek. Poin-poin penting dijelaskan di bawah ini menggunakan contoh alat AI standar:

- Langkah pertama adalah mempertanyakan apakah konten yang dihasilkan AI memenuhi persyaratan perlindungan sebagai karya berhak cipta, penemuan, atau model utilitas yang dijelaskan pada bagian 5.1. Jika demikian, penulis harus diidentifikasi.
- Penulis dapat berupa pencipta karya asli yang menjadi inspirasi AI atau yang diadopsi kinerjanya, atau pengguna. AI tidak dapat menjadi penulis karena kurangnya kepribadian hukum alami. Namun, pengguna hanya dapat mengklaim suatu karya sebagai miliknya sendiri, jika karya tersebut benar-benar berasal dari ciptaan manusia pribadinya. Namun, dalam konteks AI, pengguna biasanya tidak mengetahui tindakan mana yang menghasilkan hasil mana. Huruf, frasa, atau bagian gambar mana yang merupakan hasil logis selanjutnya dari instruksi tertentu adalah kotak hitam bagi pengguna. Pada umumnya, derivasi hasil tidak berada di tangan pengguna. Namun, hal ini tidak harus mengarah pada penolakan perlindungan. Dalam praktiknya, upaya dilakukan untuk menentukan hal ini berdasarkan tingkat kesulitan perintah: Apakah kondisi kerangka kerja yang ditetapkan oleh pengguna begitu individual dan kreatif sehingga hasil yang dihasilkan AI dapat dikaitkan dengannya?
- Dalam kasus hasil yang dihasilkan, pertanyaan yang sangat penting harus diajukan mengenai apakah konten tersebut diadopsi tanpa perubahan dan dengan demikian direproduksi atau diedit. Dalam kasus terakhir, harus dibedakan antara pengeditan yang memerlukan persetujuan dan penggunaan bebas. Jika AI hanya melakukan

perubahan kecil dan karakter individual dari aslinya dipertahankan, ini dianggap sebagai adaptasi yang memerlukan persetujuan. Ini memerlukan lisensi dari penulis. Jika, sebaliknya, versi asli tampak kurang menonjol dibandingkan versi yang diedit dan terlihat jelas kurang menonjol, maka versi asli dianggap sebagai ciptaan baru – yaitu karya baru. Dalam hal ini, hak penggunaan eksklusif menjadi milik pengguna.

- Di satu sisi, masalah reproduksi konten pihak ketiga tanpa perubahan dan pemrosesannya harus diperhitungkan dalam desain AI untuk meminimalkan pelanggaran hak cipta langsung. Di sisi lain, penanganan konten yang dihasilkan merupakan topik literasi AI dan harus menjadi bagian wajib dari pelatihan karyawan, seperti dalam lokakarya dan panduan AI yang menyertainya.
- Jika pengguna tidak menciptakan karya intelektual, dan hasilnya juga bukan karya asli, maka tidak ada karya yang dilindungi hak cipta. Namun, ruang lingkup penggunaan konten yang dihasilkan dapat diatur secara independen oleh penyedia melalui syarat dan ketentuannya. Hampir semua penyedia sistem AI generatif menggunakan opsi ini. Pada umumnya, mereka tidak memberikan hak eksklusif kepada pengguna karena mereka tidak dapat mengesampingkan kemungkinan pengguna lain menerima hasil yang persis sama atau seringkali tidak ingin memberikan hak lebih karena alasan pengembangan alat lebih lanjut.



Gambar 5.3 Memeriksa (Ketidak)diperbolehkan Penggunaan Output

Jika ternyata pengguna bukanlah pencipta hasil AI tersebut, pengeditan menyeluruh sangatlah penting. Perancangan ulang hasil tersebut mungkin diperbolehkan sebagai penggunaan bebas, seperti yang disebutkan di atas. Kreasi baru tersebut kemudian berasal dari pengguna itu sendiri, sehingga mereka juga dapat memanfaatkan perubahan tersebut secara eksklusif.

Dalam kasus solusi AI individual, penilaian kompleks ini dapat dihilangkan dengan perlindungan kontraktual yang sesuai. Dalam hal ini, hak atas hasil yang dihasilkan dapat diberikan secara kontraktual kepada pelanggan.

5.4 DAFTAR PERIKSA

Kepatuhan IP menyangkut klasifikasi komponen masing-masing dan keseluruhan sistem AI sebagai aset IP, serta implementasi spesifik pada sisi input dan output. Daftar pemeriksaan berikut merangkum poin-poin penting sekali lagi:

Desain AI

- Apakah sistem AI saya atau komponennya dilindungi oleh hukum IP?
- Sumber data apa yang digunakan untuk membuat input (korpus AI atau kumpulan data pelatihan AI)?
- Bagaimana input AI dibentuk dari perspektif teknis? (Pengambilan data? Reproduksi?)
- Apakah sumber data yang digunakan sesuai dengan hukum?
- Apakah sistem AI memungkinkan rahasia dagang bocor? Dapatkah ini dicegah secara teknis atau organisasi?
- Apakah strategi kepatuhan hak cipta telah diterapkan? Apakah hak cipta pihak ketiga dilindungi sesuai dengan Undang-Undang AI?

Pengembangan dan Pengujian AI

- Apakah parameter yang didefinisikan dalam desain AI diimplementasikan sesuai dengan ketentuan, dan apakah penggunaan yang sesuai dengan hukum dan mitigasi risiko pelanggaran hak pihak ketiga juga dapat dicapai di lingkungan pengujian?

Operasi

- Apakah lisensi hak atas konten yang dihasilkan AI didefinisikan secara kontraktual dan jelas?
- Apakah pelatihan karyawan telah diadakan dan pedoman AI telah dikeluarkan mengenai penggunaan sistem AI yang sesuai dengan hukum?
- Apakah penyesuaian lebih lanjut pada sistem AI, desain atau parameterisasi, konfigurasi, dan koneksi antarmuka apa pun diperlukan karena kesalahan yang terjadi?

5.5 TABEL REFERENSI PERUNDANG-UNDANGAN

Bab ini didasarkan pada kerangka hukum Austria, tetapi standar Jerman yang relevan dirujuk di bawah ini tanpa klaim kebenaran apa pun.

Konteks	Hukum Austria	Hukum Jerman
Perlindungan program komputer sebagai karya linguistik	§ 40a para. 1 UrhG,A	§§ 69a ff UrhG
Perlindungan basis data	§ 40f UrhG,A	§§ 87a ff UrhG
Perlindungan basis data sederhana	§§ Bagian 76c ff UrhG,A	§ 55a UrhG
Hak eksploitasi	§§ 14 ff UrhG,A	§§ 7 ff UrhG

Hak reproduksi	§ 15 UrhG,A	§ 7 UrhG
Duplikasi sementara atau yang menyertainya	§ 41a UrhG,A	§ 44a UrhG
Penambahan teks dan data	§ 42 jam UrhG,A	§ 44b UrhG
Penggunaan yang dimaksudkan	§ 40d UrhG,A	§ 69d UrhG
Dekompilasi	§ 40e UrhG,A	§ 69e UrhG
Hak distribusi	§ 16 UrhG,A	§ 17 UrhG
Hak untuk menyediakan	§ 18a UrhG,A	§ 19a UrhG
Pelanggaran hak cipta	§§ 81 ff UrhG,A	§§ 97 ff UrhG
Hak istimewa pemberi kerja	§ 40b UrhG,A	§ 69b UrhG
Hak moral	§§ 20 dan 21 UrhG,A	§§ 12 ff UrhG
Kurangnya perlindungan untuk metode matematika dan program untuk program pengolahan data	§ 1 para. 3 PatG,A, GMG	§ 1 PatG, GebrMG
Rahasia dagang	§§ 26 dan seterusnya UWG,A	GeschGehG

BAB 6

HUKUM KONTRAK AI DAN TI

6.1 PENDAHULUAN

Rantai nilai digital mengalami perubahan konstan. Rantai nilai ini semakin global, semakin kompleks, dan memengaruhi semakin banyak bidang kehidupan. Selain berbagai potensi transformasi, AI juga membawa kompleksitas baru. Muncul pertanyaan seputar standar keamanan produk, potensi diskriminasi, dan kepercayaan. Untuk memastikan perlindungan kesehatan, keselamatan, dan hak-hak dasar, Undang-Undang AI mempertimbangkan saling **ketergantungan global** dan, sesuai dengan Pasal 2 ayat 1 Undang-Undang AI, mencakup semua **operator di sepanjang rantai pasokan**.

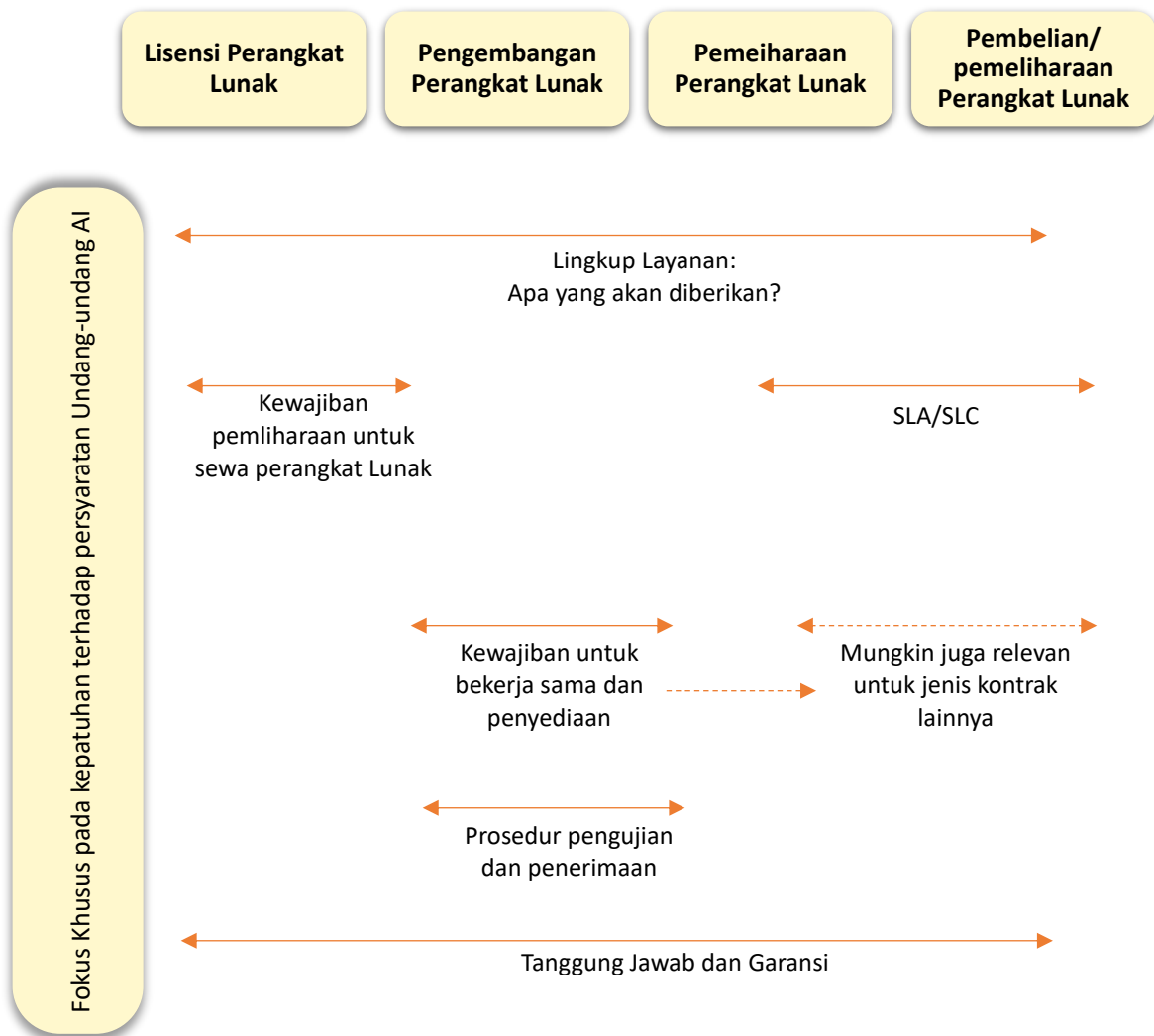
- Penyedia berarti setiap orang, terlepas dari tempat usahanya, yang memasarkan sistem AI atau menggunakannya di Uni Eropa
- Penyebar sistem AI yang berbasis di Uni Eropa atau berlokasi di Uni Eropa
- Penyedia dan penyebar sistem AI yang berbasis atau berdomisili di negara ketiga jika hasil AI digunakan di Uni Eropa
- Importir dan distributor sistem AI
- Produsen produk yang memasarkan sistem AI atau mengoperasikannya bersama produk mereka dengan nama atau merek mereka sendiri
- Perwakilan resmi penyedia yang tidak berkedudukan di Uni Eropa

Tergantung pada peran dan klasifikasi sistem AI masing-masing, para pelaku ini memiliki kewajiban yang berbeda. Namun, dalam beberapa kasus, penyedia atau pengembang akan mengembangkan dan memelihara sistem AI sepenuhnya sendiri. Sebaliknya, mereka juga akan mengandalkan keahlian pihak ketiga dan membeli perangkat lunak/perangkat keras (komponen) atau layanan pemeliharaan dan dukungan. Alasan untuk ini dapat bervariasi, seperti penghematan biaya, peningkatan efisiensi, keahlian, pengalihan tanggung jawab, dan perluasan cakupan tanggung jawab, terutama dalam kasus teknologi baru.

Saat pengadaan layanan TI, persyaratan baru **Undang-Undang AI untuk memastikan kepatuhan hukum sekarang juga harus diperhitungkan dalam kontrak TI**. Pelanggan harus menilai di mana masuk akal untuk mewajibkan penyedia layanan untuk mematuhi kewajiban khusus berdasarkan Undang-Undang AI (misalnya, informasi tambahan, dukungan dalam memenuhi kewajiban mereka sendiri, dan lain-lain.). Setiap peraturan yang berlaku langsung bagi pelanggan kemudian harus terikat pada penyedia layanan. Hal ini dimaksudkan untuk memastikan bahwa pihak yang bersangkutan yang tunduk pada kewajiban khusus dalam rantai nilai dapat menggunakan sistem AI sesuai dengan Undang-Undang AI. Hal ini sangat relevan bagi pihak yang menerapkan AI untuk kasus penggunaan tertentu di bawah pengawasan mereka dan secara teratur bergantung pada penyedia layanan. Karena alasan ini, bagian berikut secara singkat menguraikan isu-isu baru yang dipicu oleh Undang-Undang AI dalam kontrak TI dengan menggunakan **contoh pihak yang menerapkan sebagai pelanggan**. Poin-

poin peraturan yang perlu mendapat perhatian khusus saat menyusun kontrak bergantung pada layanan spesifik dan jenis kontrak. Kami memberikan gambaran umum tentang (i) Lisensi perangkat lunak standar, (ii) pengembangan perangkat lunak yang disesuaikan, (iii) pemeliharaan perangkat lunak, dan (iv) pembelian/pemeliharaan perangkat keras.

Pertanyaan tentang ruang lingkup kinerja muncul untuk semua jenis kontrak. Pertanyaan-pertanyaan tersebut dibahas dalam konteks masing-masing, sementara garansi dan tanggung jawab dibahas secara umum di bagian 6.6.



Gambar 6.1 Representasi Visual dari Titik Fokus Kontrak TI yang Paling Relevan

6.2 LISENSI PERANGKAT LUNAK STANDAR

Perangkat lunak standar saat ini terutama tersedia melalui model pembelian atau sewa.

Pembelian perangkat lunak ditandai dengan fitur-fitur berikut:

- Pembayaran satu kali
- Lisensi untuk penggunaan dalam jangka waktu yang tidak terbatas
- Penyediaan perangkat lunak sesuai dengan kesepakatan

- Pengakhiran kontrak melalui pemenuhan (hubungan utang target)

Dalam konteks AI, muncul pertanyaan – tidak hanya untuk lisensi perangkat lunak, tetapi juga untuk semua jenis kontrak lainnya – khususnya mengenai pokok bahasan layanan dan spesifikasinya. Kesepakatanlah yang menentukan di sini, yaitu karakteristik yang ditetapkan dan biasanya diasumsikan sesuai dengan § 922 Kitab Undang-Undang Hukum Perdata Austria (ABGB). Karakteristik bersyarat adalah karakteristik kinerja yang disepakati secara eksplisit. Di sisi lain, apa yang biasanya diasumsikan termasuk didasarkan pada harapan objektif, yang harus diinterpretasikan dalam setiap kasus individual, dengan mempertimbangkan persepsi publik dan sifat transaksi.

Layanan yang disepakati secara kontraktual harus diberikan. Pelanggan bermaksud untuk menentukan layanannya seakurat mungkin; penyedia, di sisi lain, ingin mendefinisikan layanan yang termasuk dan di luar cakupan agar dapat membuat penawaran yang realistis. Layanan yang ditentukan secara eksplisit dapat mewakili properti yang dibutuhkan. Namun, tidak setiap tugas dapat dijelaskan. Oleh karena itu, cakupan layanan juga dapat sebagian terbuka untuk interpretasi. Karakteristik yang biasanya diasumsikan memainkan peran penting dalam interpretasi. Namun, hal ini masih dapat diperdebatkan. Misalnya, apakah stabilitas, kompatibilitas, keramahan pengguna, waktu respons, kemampuan perluasan, atau pemeliharaan tertentu biasanya diasumsikan termasuk meskipun tidak dinyatakan secara eksplisit? Persepsi publik tentang sistem AI masih terus berkembang. Sebagai contoh, saat ini sedang dibahas bahwa keselamatan operasional dan lalu lintas sistem AI dalam arti Undang-Undang AI dan dengan demikian kepatuhan terhadap kewajiban baru peraturan tersebut memang merupakan karakteristik yang diasumsikan dari suatu produk.

Lagipula, tujuan Undang-Undang AI adalah untuk mengatasi risiko terkait dan memungkinkan penggunaan yang aman. Namun, ada juga argumen yang bertentangan berikut ini: Namun, risiko spesifik dan kewajiban implementasi bergantung pada klasifikasi sistem AI dan oleh karena itu juga sebagian pada penggunaan spesifik di lingkungan pengimplementasi. Yang terakhir khususnya seringkali sulit dinilai oleh penyedia layanan sebelumnya. Ini berlaku khususnya untuk solusi standar yang disediakan yang ditujukan untuk berbagai aplikasi. Oleh karena itu, kasus ini harus dinilai secara berbeda dari penawaran penyedia untuk sistem AI yang dapat digunakan untuk tujuan tertentu. Dalam hal ini, penyedia mengetahui kasus penggunaan dan pelanggan dapat mengharapkan bahwa persyaratan keselamatan yang diperlukan untuk pengoperasian telah diperhitungkan. Namun, setiap penafian dari penyedia juga harus dipertimbangkan selama proses desain.

Contoh

Suatu penyedia mengiklankan sistem AI untuk penyaringan lamaran pekerjaan, pengambilan keputusan otomatis untuk perekrutan dan seleksi pelamar kerja. Sistem AI ini jelas ditujukan untuk penggunaan sebagai AI berisiko tinggi sesuai dengan Lampiran III Z 4 huruf a UU AI. Dengan demikian, penyedia, importir, atau distributor memberi sinyal bahwa produknya dapat digunakan di pasar yang bersangkutan. Menurut pendapat saya, ini menunjukkan kepatuhan yang secara objektif dapat diharapkan terhadap keselamatan operasional dan lalu lintas perangkat lunak yang mendasar dan umum.

Tips Praktis

Materi pokok dan spesifikasi sistem AI harus dijelaskan dengan cermat untuk menghindari sengketa hukum dan investasi yang gagal. Hal ini harus dilakukan pada tingkat berikut:

- **Persyaratan kuantitatif** (misalnya, penyediaan model AI, algoritma, seluruh sistem AI, penyediaan jaringan saraf dengan ukuran tertentu, penyediaan fungsionalitas tambahan, penyediaan lingkungan pengujian, pembuatan manual pengguna dan dokumentasi, pelaksanaan penilaian kesesuaian untuk AI berisiko tinggi, dan lain-lain.).
- **Persyaratan kualitatif** (misalnya, persyaratan teknis, organisasi, dan hukum, seperti kepatuhan terhadap Undang-Undang AI, kepatuhan terhadap standar pasar atau penyediaan layanan mutakhir, ketersediaan keahlian AI di antara personel yang dikerahkan dan subkontraktor mana pun; pelatihan dengan kumpulan data yang seimbang untuk menghindari bias, penandaan CE sesuai dengan Pasal 48 Undang-Undang AI)

Sewa perangkat lunak umumnya dicirikan oleh fitur-fitur berikut:

- Imbalan berulang;
- Penggunaan terbatas atau tidak terbatas;
- Lisensi perangkat lunak sesuai dengan cakupan yang disepakati;
- Kewajiban pemeliharaan penyedia (misalnya perbaikan bug, pembaruan) untuk perangkat lunak sebagai layanan;
- Pengakhiran kontrak (kewajiban berkelanjutan).

Berdasarkan hukum Austria, selain tantangan yang disebutkan di atas untuk spesifikasi layanan, cakupan kewajiban pemeliharaan juga berperan dalam model perangkat lunak sebagai layanan/sewa. Kecuali disepakati lain, penyedia bertanggung jawab untuk memelihara perangkat lunak. Oleh karena itu, ia menjamin bahwa sistem AI tidak hanya memiliki properti yang disepakati pada saat penyerahan, tetapi juga berkewajiban untuk melakukan pemeliharaan berkelanjutan sesuai kontrak selama masa sewa. Namun, kewajiban pemeliharaan biasanya ditentukan lebih rinci dalam kontrak.

Contoh

Sistem AI berisiko tinggi harus sekuat mungkin terhadap kesalahan, malfungsi, atau inkonsistensi dalam sistem atau lingkungan tempat sistem dioperasikan sesuai dengan Pasal 15 ayat 4 UU AI. Dalam konteks ini, tindakan teknis dan organisasi harus diambil. Dari perspektif pelanggan, oleh karena itu disarankan tidak hanya untuk menyetujui kepatuhan terhadap kewajiban ini, tetapi juga untuk memberikan contoh tindakan teknis dan organisasi yang diharapkan untuk pemecahan masalah. Ini termasuk, misalnya, penyediaan pembaruan keamanan untuk mempertahankan status kepatuhan kontrak.

6.3 PENGEMBANGAN PERANGKAT LUNAK

Elemen inti dari kontrak **pengembangan perangkat lunak** meliputi:

- Pengembangan individual dengan mempertimbangkan kebutuhan pelanggan;

- Biasanya komitmen untuk mewujudkan pengembangan;
- Umumnya, hak eksklusif atas perangkat lunak individual;
- Pengakhiran kontrak melalui pemenuhan (biasanya penerimaan yang berhasil; hubungan hutang target).

Jika sistem AI dikembangkan secara individual, para pihak setuju untuk mengimplementasikan perangkat lunak yang secara khusus disesuaikan dengan pelanggan. Dari perspektif pengembang sebagai pelanggan, perjanjian tersebut harus disusun sebagai **kontrak kerja untuk disewa**. Hal ini juga sesuai dengan klasifikasi Mahkamah Agung Austria. Kontrak layanan harus dibedakan dari kontrak kerja. Dalam hal penyediaan layanan, hanya upaya semata dan bukan keberhasilan yang dipertaruhkan. Tentu saja, ini melemahkan posisi pelanggan dan tidak tepat mengingat pembiayaan pengembangan individual oleh pelanggan. Menurut pendapat saya, aturan yang berbeda berlaku jika para pihak secara sadar menjalin kemitraan penelitian dan dalam kasus pengembangan individual sistem AI berteknologi tinggi yang jauh melampaui keadaan terkini dan pencapaian tujuannya bergantung pada beberapa faktor yang tidak jelas.

Juga untuk pengembangan perangkat lunak, masalah yang dijelaskan pada poin 6.1 juga muncul sehubungan dengan **deskripsi layanan**. Aspek spesifik lainnya adalah **kewajiban pelanggan untuk bekerja sama**. Realisasi proyek biasanya juga bergantung pada layanan dukungan dari pihak pelanggan. Ini harus disepakati secara terpisah. **Kewajiban umum untuk bekerja sama** adalah, misalnya:

- Pembuatan dan pemeliharaan kondisi kerangka kerja tertentu seperti perangkat keras, persyaratan khusus untuk infrastruktur TI (koneksi, komputer, kapasitas, dan lain-lain.);
- Akses dan hak akses karyawan penyedia;
- Penyediaan sumber daya manusia untuk koordinasi berkelanjutan;
- Uji penerimaan.

Saat pengadaan sistem AI, kewajiban kerja sama berikut mungkin relevan, misalnya:

- Informasi tentang tujuan penggunaan agar dapat mengklasifikasikan perangkat lunak sesuai dengan Undang-Undang AI dan menerapkan persyaratan yang diperlukan untuk produksi perangkat lunak
- Untuk AI berisiko tinggi:
- Penyediaan kumpulan data pelatihan, validasi, dan pengujian sesuai dengan Pasal 10 Undang-Undang AI;
- Dukungan dalam melakukan pengujian sesuai dengan Pasal 10 Undang-Undang AI;
- Informasi tentang sistem tata kelola data/AI dan manajemen risiko yang ada untuk menghubungkan kewajiban berdasarkan Pasal 9 Undang-Undang AI dengan kerangka kerja yang ada;
- Melakukan penilaian dampak hak asasi manusia awal sesuai dengan Pasal 27 Undang-Undang AI agar dapat melakukan perubahan yang diperlukan pada desain perangkat lunak tepat waktu.

Untuk sistem AI tertentu:

- Penyediaan data kepemilikan jika sistem AI juga akan berinteraksi dengan manusia berdasarkan sumber informasi lain.

Terakhir, pengembangan sistem AI juga mengubah poin uji teknis dan persyaratan ulang dalam **prosedur penerimaan**. Dalam prosedur pengujian penyedia, yang biasanya dilakukan sebelum prosedur penerimaan, penyedia harus memastikan kepatuhan terhadap persyaratan **pengujian khusus** Undang-Undang AI:

- Kepatuhan terhadap kewajiban khusus untuk pengujian dalam kondisi dunia nyata sebagaimana dimaksud dalam Pasal 2 ayat 8 Undang-Undang AI bersamaan dengan Pasal 3 no. 57 Undang-Undang AI, seperti memperoleh persetujuan pengguna sesuai dengan Pasal 60 Undang-Undang AI;
- Pengujian sistem AI berisiko tinggi untuk mematuhi langkah-langkah manajemen risiko yang sesuai sebagaimana dimaksud dalam Pasal 9 ayat 6 Undang-Undang AI;
- Pengujian berdasarkan parameter yang telah ditentukan sebelumnya dan ambang batas probabilitas sebagaimana dimaksud dalam Pasal 9 ayat 8 Undang-Undang AI yang sesuai untuk tujuan yang dimaksudkan dari sistem AI berisiko tinggi;
- Pengujian dengan kumpulan data pelatihan, validasi, dan pengujian, dengan mempertimbangkan persyaratan ulang Pasal 10 ayat 6 Undang-Undang AI. 2 et seqq. UU AI;
- Melakukan uji serangan untuk menentukan risiko sistem (misalnya untuk model AI tujuan umum dengan risiko sistemik sesuai dengan Pasal 55 UU AI).

6.4 PEMELIHARAAN PERANGKAT LUNAK

Dalam kontrak pemeliharaan perangkat lunak, para pihak menyepakati **kesiapan operasional** perangkat lunak standar atau yang disesuaikan yang disediakan. Lingkup pemeliharaan spesifik ditentukan oleh perjanjian. Terdapat banyak ruang untuk bermanuver di sini, dan berbagai layanan ditawarkan di pasar – secara individual atau kombinasi – seperti:

- Pemecahan masalah (koreksi kesalahan);
- Koreksi kesalahan preventif melalui perbaikan bug (pemeliharaan);
- Penyediaan pembaruan;
- Penyediaan peningkatan;
- Penyediaan hotline dukungan;
- Pencadangan.

Mirip dengan pertimbangan dalam 6.4, **lingkup pemeliharaan** juga harus ditentukan dalam kontrak. Perjanjian layanan biasanya ditentukan melalui **perjanjian tingkat layanan** (SLA) secara lebih rinci. SLA berisi target yang dapat diukur secara objektif yang harus dicapai oleh penyedia. Ini seringkali berupa komitmen ketersediaan dan kualitas. Kepatuhan terhadap SLA harus dipantau dan dilaporkan. Selain itu, harus secara eksplisit disebutkan siapa yang memenuhi kewajiban pemantauan dan pelaporan ini. Jika SLA tidak terpenuhi, **kredit tingkat layanan** (SLC) dapat disepakati sebagai penalti (penalti kontraktual).

Dalam SLA, peraturan khusus AI berikut ini khususnya harus diperhatikan:

- Jika semua sistem AI digunakan, staf harus memiliki literasi AI sesuai dengan Pasal 4 UU AI. Persyaratan ini harus disepakati dalam kualitas personel yang ditugaskan.
- AI berisiko tinggi
 - Menurut Pasal 13 ayat 3 huruf e UU AI, AI berisiko tinggi memerlukan semua tindakan pemeliharaan dan perawatan yang diperlukan, termasuk frekuensinya, untuk memastikan berfungsinya sistem AI ini dengan baik, termasuk terkait pembaruan perangkat lunak. Oleh karena itu, hal ini harus diperhitungkan ketika menentukan ketersediaan, waktu respons, kesalahan, pemecahan masalah dan waktu respons, pembaruan dan peningkatan dalam SLA.
 - Langkah-langkah pemeliharaan dan perawatan yang diperlukan mencakup, khususnya, kewajiban yang tercantum dalam Pasal 9 dan seterusnya UU AI, seperti pemantauan berkala, penilaian risiko, peninjauan langkah-langkah mitigasi dan pengendalian, kewajiban pemberitahuan, pengujian, pembersihan, pembaruan, pengayaan dan agregasi data, identifikasi kesenjangan atau kekurangan data, deteksi dan koreksi distorsi dalam kumpulan data, dokumentasi teknis dan kewajiban pencatatan, pengawasan manusia, dan lain-lain.
- Sistem AI dengan tujuan umum
 - Pada model AI tujuan umum, misalnya, kepatuhan terhadap peraturan transparansi, peningkatan model yang berkelanjutan untuk mencegah gangguan terhadap hak pihak ketiga (khususnya hak cipta) dan dokumentasi teknis sesuai dengan Pasal 53 UU AI adalah hal yang relevan.
 - Untuk model AI tujuan umum dengan risiko sistemik, penilaian model tambahan, pengujian untuk mengidentifikasi dan menghilangkan risiko sistemik, dokumentasi berkelanjutan dan pemenuhan kewajiban pelaporan jika terjadi insiden serius harus dipertimbangkan secara kontraktual sesuai dengan Pasal 55 UU AI.
 - Untuk detail lebih lanjut mengenai kewajiban khusus saat menggunakan AI tujuan umum, lihat bagian 3.7.
- Sistem AI tertentu
 - Kewajiban Undang-Undang AI saat mengoperasikan sistem AI tertentu terutama terbatas pada kepatuhan terhadap peraturan transparansi dan memastikan bahwa hak dan kebebasan pihak ketiga dilindungi sesuai dengan Pasal 50 Undang-Undang AI.

Contoh-contoh tersebut memperjelas bahwa kontrak pemeliharaan juga harus dinilai ulang di masa mendatang dan disesuaikan dengan kesalahan khusus AI.

6.5 PERANGKAT LUNAK SUMBER TERBUKA

Kedaulatan atas kode pemrograman, yaitu infrastruktur digital, penting untuk masyarakat yang bebas. Infrastruktur digital yang independen diperlukan untuk dapat membentuk digitalisasi itu sendiri. Kontrol demokratis yang sejati atas kode dan perangkat keras terkait merupakan bagian dari kedaulatan digital dan, menurut Lessig, berjalan seiring dengan perangkat lunak bebas dan terbuka (sumber terbuka). Bagian ini memberikan gambaran umum tentang definisi perangkat lunak sumber terbuka, kasus penggunaan,

masalah hukum, dan relevansinya bagi Uni Eropa, termasuk ketentuan hukum dalam Undang-Undang AI.

AI Sumber Terbuka – Membuka Jalan Menuju Masa Depan?

Zuckerberg langkah selanjutnya untuk menetapkan AI sumber terbuka sebagai standar industri. Untuk tujuan ini, Meta menerbitkan Llama 3.1 405B (menurut *Zuckerberg*, model AI sumber terbuka tingkat terdepan pertama) dan model Llama 3.1 70B dan 8B yang telah ditingkatkan. Contoh lainnya termasuk BLOOM (*BigScience Large Open-Science Open-Access Multilingual Language Model*), yang dikembangkan di bawah kepemimpinan perusahaan AI Hugging Face, MPT-7B, yang diperkenalkan oleh MosAIcML Foundations, Falcon 2, generasi terbaru model bahasa skala besar sumber terbuka dari Technology Innovation Institute (TII) di Abu Dhabi, dan Vicuna-13B. Lebih dari 84% perusahaan menyatakan bahwa perangkat lunak sumber terbuka digunakan di area penting atau kritis bisnis.

Keunggulan Open Source dari Perspektif Pengembang

- **Melatih dan menyempurnakan model Anda sendiri:** Perusahaan memiliki berbagai macam kebutuhan. Idealnya, kebutuhan ini dapat dipenuhi dengan model berbagai ukuran yang dilatih atau disempurnakan dengan kumpulan data tertentu. Model open source seperti Llama dapat dilatih dengan data Anda sendiri dan dikurangi ukurannya sesuai kebutuhan.
- **Tidak bergantung pada penyedia tertutup (“vendor”):** Dengan vendor terkemuka di pasar yang menyediakan model AI tertutup, terdapat risiko ketergantungan tertentu. Open source dapat memungkinkan ekosistem perusahaan yang luas dengan toolChain yang kompatibel. Perusahaan dapat menjadi bergantung jika mereka:
 - bergantung pada model:
 - yang tidak dapat mereka jalankan dan kendalikan sendiri;
 - yang dapat diubah oleh penyedia kapan saja,
 - yang ketentuan penggunaannya dapat diubah oleh penyedia, atau
 - di mana penyediaan bahkan dihentikan sepenuhnya.
 - terikat pada satu cloud yang memiliki hak eksklusif atas suatu model.
 - Salah satu contohnya adalah Microsoft Azure Open AI, di mana, berbeda dengan OpenAI tanpa konteks Azure, keamanan akses ke data dipastikan oleh model otorisasi tersimpan (RBAC). Namun, filter konten yang dapat dimodifikasi (dan karenanya dapat dikendalikan) dan/atau pemantauan penyalahgunaan yang dapat dimodifikasi untuk layanan Azure OpenAI hanya tersedia untuk pelanggan dan mitra terkelola yang bekerja dengan tim akun Microsoft dan tunduk pada persyaratan tambahan. Hanya pelanggan yang memenuhi persyaratan ini yang dapat mengajukan permohonan untuk ini.
- **Perlindungan data (pribadi dan non-pribadi):** Salah satu peluang paling mencolok yang terkait dengan digitalisasi dan pengembangan teknologi baru adalah big data dan analitik big data. Ini adalah istilah umum untuk berbagai perkembangan yang berkaitan dengan data, yang dibagi menjadi kategori-kategori berikut:
 - volume (cakupan, volume data),
 - kecepatan (kecepatan di mana volume data dihasilkan dan ditransfer),

- variasi (rentang jenis dan sumber data) dan
- kebenaran (keaslian data).

Berkaitan dengan hal ini adalah *kapasitas pengolahan data* (juga dikenal sebagai analitik big data) – termasuk metode dan alat yang digunakan – yang telah mengambil dimensi signifikan dan mewakili sebagian besar nilai perusahaan di banyak industri. Hal ini membuat perlindungan data perusahaan menjadi semakin penting.

Model sumber terbuka memungkinkan model dijalankan di mana saja dan (lebih lanjut) dikembangkan secara transparan. Perusahaan sering bekerja dengan data rahasia yang ingin mereka jaga keamanannya. Kepercayaan pelanggan dan keamanan data rahasia (data pribadi dan non-pribadi seperti rahasia dagang) adalah aset terbesar perusahaan.

- Efisiensi teknis (biaya): Pengembang sering kali dapat menjalankan model sumber terbuka pada infrastruktur mereka sendiri dengan lebih murah, bahkan gratis. Kisaran biayanya antara 0,2 dan 7,5 USD per 1 juta token. Misalnya, Llama 3.1 405B dapat dijalankan pada infrastruktur sendiri dengan biaya sekitar 50% dari biaya penggunaan model tertutup seperti GPT-4o.
- Ekosistem Berkelanjutan: Model sumber terbuka digunakan untuk membangun infrastruktur perusahaan sendiri dan menanamkan sistem AI di dalamnya. Penciptaan arsitektur jangka panjang akan berkelanjutan dan oleh karena itu sumber terbuka akan menjadi bagian integral dari solusi ini (tentang keberlanjutan, lihat juga).

Definisi Sumber Terbuka dan Dasar Hukum

Solusi Perangkat Lunak Sumber Terbuka (OSS) menawarkan alternatif untuk perangkat lunak berbayar. Penggunaan OSS semakin mapan di industri perangkat lunak. Dengan digitalisasi kehidupan sehari-hari, penggunaan OSS juga meningkat. Definisi pertama OSS berasal dari Free Software Foundation pada akhir tahun 1990-an. Mereka mendefinisikan OSS sebagai kebebasan pengguna untuk menjalankan, menyalin, mendistribusikan, mempelajari, memodifikasi, dan meningkatkan perangkat lunak. Definisi Open Source Initiative menyatakan bahwa OSS bukan hanya akses ke kode sumber dan mencantumkan sub-item lebih lanjut.

Syarat distribusi harus memenuhi kriteria tertentu:

1. **Distribusi gratis:** Lisensi tidak boleh membatasi penjualan atau distribusi perangkat lunak.
2. **Kode sumber:** Program harus berisi kode sumber dan mengizinkan distribusinya dalam bentuk sumber dan kompilasi.
3. **Hak pengeditan/karya turunan tanpa batasan:** Lisensi harus mengizinkan modifikasi dan karya turunan serta mengizinkan distribusinya dengan ketentuan yang sama seperti perangkat lunak aslinya.
4. **Integritas kode sumber penulis:** Lisensi hanya boleh membatasi kode sumber dalam bentuk yang dimodifikasi jika distribusi file patch diizinkan.
5. **Tidak ada diskriminasi pribadi atau kelompok**
6. **Tidak ada diskriminasi** bidang aktivitas
7. **Distribusi lisensi:** Hak yang terkait dengan program harus berlaku untuk semua orang yang menerima distribusi program tersebut.

8. **Tidak ada lisensi khusus produk:** Hak tidak boleh bergantung pada program yang merupakan bagian dari distribusi perangkat lunak tertentu.
9. **Tidak ada pembatasan** perangkat lunak lain
10. **Netralitas teknologi lisensi:** Tidak ada ketentuan lisensi yang boleh didasarkan pada teknologi atau jenis antarmuka tertentu.

Definisi Perangkat Lunak Sumber Terbuka

Perangkat lunak yang dilisensikan di bawah lisensi OSS memiliki karakteristik berikut:

1. Akses publik ke kode sumber: Dengan perangkat lunak komersial, kode sumber tidak dapat diakses. Sebaliknya, dengan kode sumber yang dapat diakses secara bebas, pengguna dan programmer berkolaborasi pada OSS dan mengembangkannya lebih lanjut. Kode sumber tersedia secara gratis. Namun, OSS juga dapat digunakan secara komersial. Karena perbedaan dalam ketentuan lisensi, perangkat lunak tidak selalu cocok untuk penggunaan komersial. Program harus berisi kode sumber dan mengizinkan distribusinya dalam bentuk sumber dan kompilasi.
2. Perangkat lunak **dapat dimodifikasi** oleh siapa saja;
3. **Gratis;**
4. **Tersedia untuk diunduh** di Internet langsung dari situs web penulis, editor, atau produsen. Namun, OSS juga dapat diperoleh dari dealer, yang disebut distributor. Tergantung pada lisensi masing-masing, kewajiban lebih lanjut dapat dikenakan pada pengguna atau pemegang lisensi.

Pemegang lisensi OS diberikan izin penggunaan karya (§ 24 ayat 1 öUrhG (UU Kekayaan Intelektual Austria), § 31 dtUrhG (UU Kekayaan Intelektual Jerman)), hak untuk mengedit (§ 5 öUrhG (UU Kekayaan Intelektual Austria), § 3 dtUrhG (UU Kekayaan Intelektual Jerman)), hak reproduksi (§ 15 öUrhG (UU Kekayaan Intelektual Austria), § 16 dtUrhG (UU Kekayaan Intelektual Jerman)) dan hak distribusi (§ 16 öUrhG (UU Kekayaan Intelektual Austria), § 17 dtUrhG (UU Kekayaan Intelektual Jerman)), di mana pemegang lisensi harus mematuhi kewajiban yang ditetapkan dalam lisensi tersebut.

Kepatuhan Hukum Sumber Terbuka

OSS dapat menimbulkan kesulitan hukum berikut:

1. Setiap orang yang ikut mengembangkan OSS mengembangkannya berdasarkan lisensi sumber terbuka. Hal ini dapat mengakibatkan **banyaknya penulis bersama** (beberapa programmer). Tidak mungkin untuk menyepakati hak penggunaan untuk kasus individual.
2. Terdapat **berbagai jenis perjanjian lisensi OSS** di mana produk OSS didistribusikan. Lisensi permisif, lisensi copyleft lemah, dan lisensi copyleft kuat. Dalam hal apa pun, perhatian harus diberikan pada jenis lisensi, karena ini menimbulkan hak dan kewajiban yang berbeda, yang dapat menyebabkan pelanggaran kontrak jika terjadi ketidakpatuhan.

Tabel 6.1 Gambaran Umum Jenis Perjanjian Lisensi OSS

Lisensi Permisif	Lisensi Copyleft Lemah	Lisensi Copyleft Strong
Lisensi ini memberikan kebebasan yang luas kepada pengguna untuk menggunakan, memodifikasi, dan mendistribusikan perangkat lunak dengan pembatasan minimal dan hanya memerlukan kewajiban minimal: misalnya, penyertaan pemberitahuan hak cipta asli dan ketentuan lisensi di semua salinan atau bagian substansial dari perangkat lunak dan dokumentasi.	Lisensi copyleft lemah menyeimbangkan antara lisensi permisif dan lisensi kuat. Lisensi ini memungkinkan kode untuk digunakan, dimodifikasi, dan didistribusikan secara bebas, tetapi dengan syarat-syarat tertentu sehingga karya turunan di bawah lisensi yang sama tetap bersifat open source. Syarat-syaratnya kurang ketat dibandingkan lisensi copyleft ketat dan memungkinkan penggunaan hak milik dalam keadaan tertentu.	Lisensi copyleft yang kuat memastikan bahwa semua karya yang berasal dari perangkat lunak tersebut juga didistribusikan di bawah ketentuan lisensi yang sama . Perubahan pada perangkat lunak dan perangkat lunak apa pun yang memuatnya harus didistribusikan di bawah lisensi yang sama. Lisensi copyleft yang kuat ditujukan untuk proyek-proyek yang ingin menjamin kebebasan perangkat lunak dan mencegah <i>fork berpemilik*</i> .
Lisensi berikut termasuk dalam kategori Lisensi Permisif : Lisensi MIT yang digunakan oleh Facebook; Lisensi BSD yang digunakan oleh Google; Lisensi Permisif Universal	Lisensi berikut termasuk dalam kategori Lisensi Copyleft Lemah : Lisensi Publik Mozilla (MPL); Lisensi Pengembangan dan Distribusi Umum (CDDL); Lisensi Apache 2.0, yang digunakan oleh AWS; Lisensi Publik Microsoft	Lisensi berikut termasuk dalam kategori Lisensi Copyleft Kuat : Lisensi Publik Umum GNU (GPL), yang digunakan untuk mendistribusikan sistem operasi Linux atau perangkat lunak OpenOffice.org, dianggap sebagai lisensi OSS yang paling banyak digunakan dan mengandung copyleft yang kuat . Kategori ini juga mencakup: Lisensi Publik Umum Affero (AGPL) dan Kernel Linux, yang dilisensikan di bawah GPL Lisensi Publik Eclipse (EPL-1.0) Lisensi Publik Uni Eropa Lisensi Perangkat Lunak Bebas Jerman Lisensi Perangkat Lunak Terbuka
Lisensi MIT : Pemegang lisensi hanya perlu mempertahankan pemberitahuan hak cipta yang ada (= teks lisensi). Lisensi ini juga cocok untuk perangkat	Lisensi Apache : Bagian yang dimodifikasi harus ditandai sebagai demikian, dan ketentuan lisensi serta pemberitahuan hak cipta harus	Lisensi GPL : Lisensi ini mengandung copyleft yang kuat dalam versi 2.0 dan 3.0; ini agak lebih lemah dalam LGPL (“Lesser”).

lunak sumber tertutup di mana kode sumber tidak diungkapkan. Lisensi BSD: Pemberitahuan hak cipta, lisensi, dan klausul tanggung jawab harus dipertahankan (klausul). Pemegang hak atau (ko-)penulis tidak boleh disebutkan untuk tujuan periklanan (klausul).	dipertahankan atau disertakan. Tergantung pada seberapa “agresif” efek copyleft dirumuskan, perbedaan dibuat antara tiga kategori yang diilustrasikan di sini.	Pemegang lisensi biasanya diwajibkan untuk menyediakan kode sumber kepada publik. Secara eksplisit tidak boleh dikenakan biaya lisensi.

* Fork Proprietary = suatu proses di mana pengembang mengambil salinan kode sumber dari suatu paket perangkat lunak dan memulai pengembangan independen untuk menciptakan perangkat lunak yang berbeda dan terpisah, tersedia di.

Tidak semua lisensi termasuk dalam kategori ini. Misalnya, Perjanjian Lisensi Komunitas LLAMA adalah *“lisensi terbatas non-eksklusif, di seluruh dunia, tidak dapat dialihkan, dan bebas royalti.”* Namun, *lisensi ini juga memiliki beberapa batasan sedangkan Perjanjian Lisensi Komunitas LLAMA memiliki ketentuan yang lebih spesifik.*

1. Jika klausul “copyleft” yang kuat telah disepakati, **tautan ke perangkat lunak** berpeluang dapat merupakan pengembangan lebih lanjut yang diperluas oleh lisensi sumber terbuka. Jika OSS dikembangkan dan dipublikasikan lebih lanjut, kode sumber (baru) harus tersedia untuk umum. Konsep domain publik sudah dapat diwujudkan dalam penyediaan di dalam suatu perusahaan atau otoritas.
2. **Implementasi teknis dan kompatibilitas lisensi** (lihat) harus diperiksa ketika menggunakan OSS dalam perangkat lunak komersial, karena jika tidak, lisensi dapat dilanggar atau “melekat” pada perangkat lunak yang didasarkan padanya (“viral” atau “efek imunisasi”):
 - Dalam salah satu keputusan pertama di dunia tentang keefektifan lisensi sumber terbuka, Pengadilan Regional Munich menangani lisensi GNU GPL yang paling terkenal dan umum pada saat itu. Bertentangan dengan pendapat bahwa model lisensi yang berasal dari hukum Amerika tidak dapat ditransfer ke hubungan hukum Eropa dan Jerman, pengadilan menemukan bahwa lisensi tersebut pada dasarnya sah menurut hukum Jerman. Sementara itu, pandangan ini telah dikonfirmasi beberapa kali oleh pengadilan dan, misalnya, kemungkinan klaim ganti rugi jika terjadi pelanggaran lisensi OS telah ditetapkan.
 - Wiebe mencatat dalam hal ini bahwa tidak ada kerugian besar bagi pengguna yang dapat diasumsikan menurut hukum Austria. Keabsahan kondisi tersebut berasal dari §§ 696, 704 öABGB (Kitab Undang-Undang Perdata Austria).
 - Setiap perangkat lunak yang berasal dari atau berdasarkan program yang dilindungi GPL harus tersedia untuk pihak ketiga tanpa royalti dalam kode sumber jika dipublikasikan atau didistribusikan secara keseluruhan sesuai dengan ketentuan GPL. Dengan demikian, GPL berbeda secara mendasar dari hukum hak

cipta Austria dan Jerman. Namun, jika bagian-bagian program yang terdiri dari kode GPL dan kode non-GPL dapat dianggap sebagai program independen, bagian non-GPL ini dapat didistribusikan secara komersial secara independen. Masalah demarkasi yang relevan sangat kompleks dan sulit; pemeriksaan teknis dan hukum yang tepat direkomendasikan dalam setiap kasus individual.

3. Pelanggaran lisensi sumber terbuka dapat dianggap sebagai **pelanggaran hak cipta**. Konsekuensi hukum yang mungkin terjadi adalah: Klaim untuk perintah penghentian, klaim untuk penghapusan, klaim untuk kompensasi yang wajar, ganti rugi; penuntutan pidana; publikasi putusan. Pengguna perangkat lunak dapat dituntut bahkan jika mereka tidak mengetahui penggunaan perangkat lunak yang melanggar hukum. Saat membeli, memesan, atau berinvestasi dalam perangkat lunak, oleh karena itu harus diperiksa apakah perangkat lunak tersebut mematuhi lisensi OS (“uji tuntas sumber terbuka”, OSS), atau pemasok harus diwajibkan untuk menciptakan keadaan yang sesuai dengan OS. Jika perusahaan perangkat lunak atau produk perangkat lunak individual diakuisisi, masuk akal untuk memasukkan klausul yang sesuai mengenai OSS dalam kontrak.
4. Kewajiban hukum karakteristik yang sering menyertai OSS adalah:
 - Penyerahan teks lisensi, publikasi kode sumber, catatan penulis; penafian, larangan pembatasan OSS, kewajiban untuk mentransfer lisensi OSS kepada pengguna akhir.

Strategi Perangkat Lunak Sumber Terbuka Komisi Eropa

Pada tanggal 21 Oktober 2020, Komisi Eropa mengadopsi strategi perangkat lunak sumber terbuka barunya untuk periode 2020 hingga 2023. Di bawah prinsip panduan “Berpikir Terbuka”, strategi ini bertujuan untuk memanfaatkan kekuatan transformatif dan inovatif dari perangkat lunak sumber terbuka dan memperkuat penggunaan kolaboratif dan penggunaan kembali solusi perangkat lunak dan keahlian di seluruh Eropa. Komisi berkomitmen untuk mengintensifkan penggunaan perangkat lunak sumber terbuka tidak hanya di sektor TI, tetapi juga di bidang-bidang penting strategis lainnya: dengan mendirikan laboratorium inovasi sumber terbuka, mengurangi beban administratif penerbitan perangkat lunak sumber terbuka dan mempromosikan keterampilan dan bakat di bidang perangkat lunak sumber terbuka. Sumber terbuka diakui sebagai katalis perubahan. Poin-poin utama strategi tersebut adalah:

- menekankan pentingnya perangkat lunak sumber terbuka untuk otonomi digital Eropa dan langkah-langkah untuk mempromosikan penggunaan dan penggunaan kembali perangkat lunak sumber terbuka
- Mempromosikan sumber terbuka sebagai sarana untuk mencapai otonomi digital dan kendali atas teknologi
- Implementasi strategi digital

Pengecualian untuk Sumber Terbuka dalam Undang-Undang AI

Peraturan AI tidak berlaku untuk sistem AI yang *dilisensikan di bawah lisensi sumber terbuka dan gratis* (“OSS”), kecuali jika diklasifikasikan sebagai sistem AI berisiko tinggi atau ditempatkan di pasar atau dioperasikan sebagai sistem AI yang termasuk dalam Pasal 5 atau 50 (Pasal 2 ayat 12 Undang-Undang AI, Pertimbangan 89 Undang-Undang AI, lihat juga).

Komponen AI sumber terbuka dan gratis meliputi perangkat lunak dan data, termasuk model dan model AI tujuan umum, alat, layanan atau prosedur dari sistem AI (Pertimbangan 103 Undang-Undang AI).

Dalam praktiknya, kesalahpahaman dapat muncul bahwa perangkat lunak sumber terbuka telah sepenuhnya dikecualikan dari ruang lingkup Undang-Undang AI, atau pengecualian yang berlawanan, khususnya yang tercantum dalam Pasal 50 Undang-Undang AI, diabaikan. Oleh karena itu, pengecualian tersebut harus diperlakukan dengan hati-hati karena alasan berikut:

1. Tidak mustahil bahwa OSS dapat digunakan untuk pengembangan sistem AI tertentu (Pasal 50 Undang-Undang AI). Di sini, tidak hanya penerapan Undang-Undang AI yang harus diperiksa, tetapi juga kondisi kerangka hukum di luar persyaratan peraturan Undang-Undang AI harus diklarifikasi.
2. Bahkan jika pihak yang menyediakan OSS (penyedia) itu sendiri tidak tunduk pada peraturan, karena itu adalah OSS yang tidak terlibat dalam praktik terlarang (Pasal 5 Undang-Undang AI) dan tidak menggunakannya dalam sistem AI berisiko tinggi atau sistem AI tertentu, pihak yang menggunakan OSS untuk mengembangkan dan mengoperasikan sistem AI independen tidak tercakup oleh pengecualian tersebut.

Model AI Sumber Terbuka dan Serbaguna

UU AI memberikan pengecualian bagi penyedia model AI serbaguna yang disediakan di bawah lisensi sumber terbuka dan gratis yang *memungkinkan akses, penggunaan, modifikasi, dan distribusi model, dan yang parameternya, termasuk bobot, informasi arsitektur model, dan informasi penggunaan model, tersedia untuk umum*. Kewajiban berdasarkan Pasal 50 ayat 1 huruf a dan b UU AI tidak berlaku dalam hal ini. Pengecualian sebaliknya berlaku untuk model AI serbaguna dengan risiko sistemik (Pasal 50 ayat 2 UU AI; Pertimbangan 104 UU AI).

Bagi pihak ketiga yang menyediakan alat, layanan, proses, atau komponen (selain model AI serbaguna) untuk umum di bawah lisensi sumber terbuka dan gratis, Pasal 50 ayat 4 UU AI tidak berlaku. Akibatnya, mereka tidak mencatat informasi, kemampuan, akses teknis, dan dukungan lainnya sesuai dengan standar umum yang diakui dalam perjanjian tertulis, yang diperlukan agar penyedia sistem AI berisiko tinggi dapat sepenuhnya mematuhi kewajiban yang ditetapkan dalam Peraturan ini (lihat Pasal 25 ayat 4 UU AI tentang “Tanggung Jawab di sepanjang rantai nilai AI”).

Prospek

Terakhir, perlu dicatat bahwa Komisi Eropa bertanggung jawab untuk menyusun pedoman sesuai dengan Pasal 96 UU AI, yang dimaksudkan untuk membahas praktik terlarang (Pasal 5 UU AI), sistem AI berisiko tinggi (Pasal 6 UU AI), dan sistem AI tertentu (Pasal 50 UU AI) serta kewajiban terkait secara lebih rinci.

Oleh karena itu, masih perlu dilihat kapan dan sejauh mana Pasal 96 UU AI akan diimplementasikan agar dapat menilai secara pasti pembatasan sesuai dengan Pasal 2 ayat 12 UU AI. Pada saat yang sama, terdapat masalah bahwa tenggat waktu Pasal 113 UU AI berlaku

untuk implementasi Pasal 96 UU AI dan oleh karena itu implementasi harus dilakukan paling lambat tanggal 2 Februari 2026.

Untuk menghindari periode implementasi yang singkat setelah publikasi pedoman, perusahaan harus mempertimbangkan sejauh mana perangkat lunak sumber terbuka merupakan bagian dari strategi perusahaan dan AI mereka dan melakukan peninjauan hukum terhadap setiap proyek pengembangan.

6.6 PEMBELIAN DAN PEMELIHARAAN PERANGKAT KERAS

Pembelian perangkat keras sangat relevan di area tertentu, seperti di industri dengan **komponen robotika dan sensor**. Pengadaan biasanya disusun sebagai perjanjian pembelian klasik. Pembeli berkewajiban membayar harga pembelian, sedangkan pemasok berkewajiban untuk mentransfer kepemilikan tanpa beban, termasuk hak-hak lain yang diperlukan atas perangkat lunak yang dipasok.

Pengadaan perangkat keras dengan komponen AI berfokus pada topik-topik berikut: Persyaratan berdasarkan Undang-Undang AI juga berlaku untuk pengadaan perangkat keras. Terakhir, definisi AI juga mencakup perangkat lunak yang tertanam dalam perangkat keras. Ini berarti bahwa sistem AI yang sebagian besar berisiko tinggi juga tunduk pada kewajiban dalam hal **akurasi, ketahanan teknis, dan keamanan siber** di seluruh siklus hidup produk (Pasal 15 Undang-Undang AI), **persyaratan untuk penandaan CE, penilaian kesesuaian, dan kepatuhan terhadap standar** (misalnya ISO, DIN, Norma Ö, dan standar lainnya). Penyedia layanan wajib memenuhi persyaratan (UU AI) ini sebagai bagian dari **spesifikasi pokok layanan**.

Mengenai pemeliharaan, pertimbangan yang tercantum dalam bagian 6.3 berlaku secara mutatis mutandis. Selain itu, pelanggan juga harus mengatur secara kontraktual penyediaan suku cadang dan pelaksanaan kewajiban perbaikan agar tidak membahayakan pengoperasian sistem AI yang sedang berjalan.

6.7 INFORMASI UMUM TENTANG TANGGUNG JAWAB

Untuk penyusunan kontrak TI, ketentuan tanggung jawab berikut ini relevan:

- Garansi;
- Kompensasi atas kerusakan;
- Denda dan ganti rugi terlepas dari kesalahan.

Garansi

Penyedia layanan bertanggung jawab atas setiap cacat layanan yang diberikan. Suatu cacat dianggap terjadi jika layanan menyimpang dari spesifikasi yang disepakati pada saat penyerahan. Ini termasuk karakteristik yang ditetapkan dan biasanya diasumsikan (lihat bagian 6.1 tentang karakteristik yang ditetapkan dan biasanya diasumsikan). Jika properti-properti ini tidak ada, pelanggan berhak atas klaim garansi (perbaikan, penggantian, pengurangan harga, dan pembatalan kontrak).

Masa garansi menurut undang-undang adalah **dua tahun sejak penyerahan produk**, tetapi seringkali dibatasi di sektor B2B. Dalam enam bulan pertama sejak penyerahan, secara

hukum diasumsikan bahwa cacat tersebut sudah ada pada saat penyerahan. Aturan asumsi ini juga sering dikecualikan.

Selain itu, kewajiban untuk memberitahukan cacat disepakati dalam hubungan B2B. Pembeli harus memeriksa layanan dalam jangka waktu yang wajar dan memberitahukan setiap cacat, jika tidak, klaim akan hangus. Namun, kewajiban untuk memberitahukan cacat biasanya dikecualikan dan prosedur penerimaan disepakati.

Tips Praktis

Klaim garansi umumnya memainkan peran sekunder dalam kontrak perangkat lunak TI. Hal ini disebabkan oleh berbagai keadaan:

- Di satu sisi, sulit untuk membuktikan bahwa cacat telah ada pada saat penyerahan (dengan mempertimbangkan bahwa tidak ada perangkat lunak yang 100% bebas kesalahan). Akhirnya, aturan asumsi yang disebutkan di atas umumnya dikecualikan.
- Di sisi lain, prosedur penerimaan untuk kontrak pengembangan perangkat lunak sangat penting. Prosedur pengujian dan penerimaan dimaksudkan untuk mengidentifikasi dan memperbaiki kesalahan yang mencegah penerimaan. Selain itu, garansi semakin terpinggirkan jika pemeliharaan perangkat lunak terkait erat dengan transfer dan perbaikan bug direncanakan sebagai bagian dari periode berjalan ini.

Situasinya berbeda ketika membeli perangkat keras, terutama barang standar. Garansi sangat penting di sini.

Kompensasi atas Kerugian

Selain itu, penyedia layanan bertanggung jawab atas kerugian yang disebabkan oleh **kesalahan** (tanggung jawab kontraktual atau perdata) atau **tanggung jawab mutlak** (misalnya, Undang-Undang Tanggung Jawab Produk di Jerman dan Austria, Undang-Undang Tanggung Jawab Kereta Api dan Kendaraan Bermotor Austria). Ini adalah salah satu masalah regulasi terpenting dalam pengadaan dan penggunaan AI. Menurut ketentuan hukum Austria saat ini, penyedia layanan bertanggung jawab

- dalam hal kesalahan sesuai dengan §§ 1203 dst. ABGB (Kitab Undang-Undang Perdata Austria) dengan mempertimbangkan tanggung jawab ahli sesuai dengan § 1299 ABGB (Kitab Undang-Undang Perdata Austria) atas kerugian positif yang disebabkan secara lalai dan sengaja (termasuk kehilangan keuntungan)
- sebagai (kuasi-)produsen atau importir untuk kerusakan properti dan cedera pribadi berdasarkan PHG (Undang-Undang Tanggung Jawab Produk Austria), tergantung pada kesalahan, jika ini disebabkan oleh produk yang cacat. disebabkan.

Di masa mendatang, peraturan tanggung jawab akan disesuaikan dengan perkembangan terkini dengan **Arahan tentang Tanggung Jawab AI** dan **amandemen Arahan Tanggung Jawab Produk**. Untuk pertama kalinya, mereka akan menciptakan kerangka hukum yang harmonis untuk kerusakan yang disebabkan oleh AI. Fokusnya adalah pada perlindungan konsumen dan memungkinkan penegakan klaim ganti rugi secara de facto. Sebagai penggugat, pihak yang dirugikan menanggung beban pembuktian penuh. Tentu saja, dalam praktiknya mereka menghadapi kesulitan dalam memberikan bukti ketika mereka harus mengklaim dan membuktikan bahwa mereka telah menderita kerugian akibat penggunaan AI.

Oleh karena itu, ini adalah pertanyaan tentang hubungan sebab akibat. Pembuktian yang lebih mudah dan hak informasi yang luas sekarang harus mengubah ini dan memastikan kompensasi yang efektif. Selain itu, definisi produk dalam hukum tanggung jawab produk juga akan diperluas ke perangkat lunak di masa mendatang dan cacat produk akan dijelaskan dengan cara baru.

Namun, dalam praktik kontrak B2B, **pengecualian dan pembatasan tanggung jawab** adalah hal yang umum. Tanggung jawab di Austria dapat dibatasi

- berdasarkan jenis kerusakan (misalnya, untuk kerusakan yang tidak lazim, jenis kerusakan tertentu),
- jumlahnya (misalnya, batasan jumlah sebagai persentase, dalam euro atau berdasarkan nilai pesanan) atau
- kesalahan (misalnya, pengecualian untuk kelalaian ringan). Namun, tanggung jawab tidak dapat dikecualikan untuk
- kesengajaan,
- kelalaian berat yang terang-terangan,
- Kerusakan pada jiwa, anggota tubuh dan kesehatan dan
- Klaim berdasarkan Undang-Undang Tanggung Jawab Produk.

Tips Praktis

Risiko potensial yang terkait dengan penggunaan sistem AI harus tercakup secara memadai oleh ketentuan ganti rugi kontraktual dari perspektif pelanggan. Ini termasuk setidaknya tanggung jawab atas kerusakan dan kehilangan data, denda berdasarkan Undang-Undang AI atau sanksi serupa yang berlaku berdasarkan GDPR atau ketentuan lainnya, dan pelanggaran hak pihak ketiga saat menggunakan AI.

Perjanjian Sanksi dan Ganti Rugi serta Perjanjian Bebas Tanggung Jawab

Karena para pihak sering menghadapi kesulitan dalam memberikan bukti ketika menegakkan klaim ganti rugi (lihat juga penjelasan di atas dalam lingkungan AI), sanksi tanpa kesalahan (sanksi kontraktual) populer untuk dimasukkan dalam kontrak TI sebagai ganti rugi yang telah ditentukan dan perjanjian ganti rugi (perjanjian ganti rugi).

Kasus penggunaan umum adalah:

- Sanksi untuk:
 - keterlambatan;
 - kegagalan penerimaan;
 - pelanggaran data dan pelanggaran kewajiban kerahasiaan;
 - pelanggaran kewajiban kontraktual yang material, seperti kepatuhan terhadap ketentuan hukum;
 - pelanggaran SLA.
- Kerusakan dan klaim ganti rugi:
 - Pelanggaran hak pihak ketiga oleh perangkat lunak, khususnya hak kekayaan intelektual;
 - Pelanggaran terhadap sertifikasi, norma, dan standar yang disepakati,
 - Pelanggaran terhadap pembatasan penggunaan.

Dalam kontrak TI untuk sistem AI, risiko spesifik dalam klausul penalti dan ganti rugi juga dapat dipertimbangkan, misalnya sebagai berikut:

- Penalti atas pelanggaran kewajiban kontraktual dan hukum untuk mematuhi persyaratan Undang-Undang AI (analog dengan pelanggaran perlindungan data atau pelanggaran hukum lainnya);
- Ganti rugi dan pembebasan tanggung jawab jika terjadi pelanggaran hak pihak ketiga oleh model AI dan/atau sistem AI;
- Ganti rugi dan pembebasan tanggung jawab jika terjadi pelanggaran terhadap pembuatan dan implementasi strategi kepatuhan hak cipta AI tujuan umum;
- Ganti rugi dan pembebasan tanggung jawab jika terjadi pelanggaran hak dan kebebasan mendasar melalui pengembangan, pengujian, dan pengoperasian sistem AI, termasuk biaya nasihat hukum dan pembelaan yang wajar.

Regulasi AI baru dengan Undang-Undang AI juga akan berdampak signifikan pada tanggung jawab dan peraturan kewajiban dalam kontrak TI.

Bab ini ditulis berdasarkan kerangka hukum Austria, tetapi standar Jerman yang relevan dirujuk di bawah ini tanpa klaim kebenaran apa pun.

Konteks	Hukum Austria	Hukum Jerman
Penetapan tanggung jawab atas pernyataan iklan publik	§ 922 Abs. 2 ABGB,A (Kode Sipil Austria)	§ 434 BGB (Kitab Undang-Undang Perdata Jerman)
Lingkup kewajiban pemeliharaan	§ 1096 ABGB,A (Kode Sipil Austria)	§ 535 BGB, § 538 BGB (Kitab Undang-Undang Perdata Jerman)
Bebas dari cacat layanan yang diberikan	§§ 922 dst. ABGB,A (Kode Sipil Austria)	§ 434 dst. BGB (Kitab Undang-Undang Perdata Jerman)
Kewajiban untuk memberi tahu tentang cacat	§ 377 UGB (Kode Perusahaan Austria)	§ 377 HGB (Kitab Undang-Undang Perusahaan Jerman)
Kesalahan	§§ 1203 dst. ABGB,A (Kode Sipil Austria)	§ 823 BGB (Kitab Undang-Undang Perdata Jerman)
Penetapan tanggung jawab atas pihak pembantu	§ 1313a ABGB,A. (Kode Sipil Austria)	§ 278 BGB (Kitab Undang-Undang Perdata Jerman)
Tanggung jawab tambahan	§ 1315 ABGB,A. (Kode Sipil Austria)	§ 831 BGB (Kitab Undang-Undang Perdata Jerman)
Tanggung jawab ahli	§ 1299 ABGB,A (Kode Sipil Austria)	§ 839a BGB (Kitab Undang-Undang Perdata Jerman)
Definisi produk	§ 4 PHG,A (Undang-Undang Kewajiban Produk Austria)	§ 2 PHG (Undang-Undang Tanggung Jawab Produk Jerman)

BAB 7

SEKTOR SWASTA

7.1 AI – DARI PRASANGKA KE DISKRIMINASI

AI sering digambarkan sebagai alat yang dapat digunakan dengan perspektif netral dan objektif untuk berbagai tujuan, baik untuk memberi manfaat maupun merugikan. Pendekatan ini menyiratkan bahwa AI itu sendiri tidak baik atau buruk, tetapi efeknya bergantung pada niat pengguna. Dengan mengasumsikan bahwa sistem tersebut objektif dan netral, prasangka yang dapat menyebabkan diskriminasi disembunyikan, dan ini dapat menyebabkan reproduksi dan penguatan prasangka yang ada:

- **Reproduksi prasangka sosial:** Sistem AI belajar dari data yang dihasilkan dan dipilih oleh manusia. Jika data ini bias atau mencerminkan ketidaksetaraan sosial, AI dapat mereproduksi bias ini dalam keputusan dan rekomendasinya. *Hal ini dapat dilihat dalam teknologi pengenalan wajah, misalnya, di mana beberapa sistem berkinerja berbeda untuk orang dengan warna kulit yang berbeda karena penggunaan data gambar warna kulit terang yang dominan selama pelatihan.*
- **Penguatan ketidaksetaraan yang ada:** Penanaman bias secara tidak sadar dalam sistem AI dapat memperkuat ketidaksetaraan sosial dan ekonomi yang ada. *Misalnya, alat perekrutan berbasis AI yang didasarkan pada data historis mungkin cenderung lebih menyukai kandidat yang sesuai dengan profil tipikal karyawan pria yang sukses di masa lalu, yang berpotensi merugikan perempuan.*

Istilah-istilah kunci dalam konteks ini adalah:

- **Pembelajaran mesin** adalah cabang kecerdasan buatan yang menggunakan algoritma untuk memberi komputer kemampuan untuk belajar dari data dan membuat keputusan atau prediksi tanpa diprogram secara eksplisit. Hal ini didasarkan pada gagasan bahwa sistem dapat mengenali pola dan struktur dalam sejumlah besar data untuk mengembangkan solusi secara mandiri.
- **Objektivitas** mengacu pada kemampuan untuk membuat penilaian atau keputusan yang bebas dari bias pribadi dan pengaruh subjektif, berdasarkan kriteria berbasis fakta.
- **Netralitas** berarti tidakberpihakan dan tidak adanya perlakuan istimewa atau bias terhadap semua pihak dalam suatu isu atau konflik.
- **Bias** dipertimbangkan dalam bab ini dari perspektif hukum dan sosial-politik dan mengacu pada bias atau keberpihakan dalam pengambilan keputusan seseorang, lembaga, atau sistem AI, yang dapat menyebabkan perlakuan tidak adil atau diskriminasi berdasarkan karakteristik seperti asal, jenis kelamin, usia, atau agama. Dalam konteks sistem AI, istilah bias mengacu pada distorsi sistematis dalam data atau algoritma yang menyebabkan prasangka dalam keputusan atau prediksi AI. Distorsi ini dapat berasal dari data pelatihan, keputusan desain algoritma, atau asumsi implisit

pengembang dan seringkali mengakibatkan perlakuan tidak adil atau diskriminatif terhadap kelompok atau individu tertentu. Catatan: Istilah “bias” yang dijelaskan di sini harus dibedakan dari istilah teknis “bias” dalam statistik, yang mengacu pada distorsi sistematis yang menyebabkan penyimpangan nilai estimasi dari nilai sebenarnya dan tidak akan dijelaskan lebih lanjut di sini.

- **Bias Otomatisasi** mengacu pada kecenderungan orang untuk mempertanyakan keputusan dan penilaian yang dibuat atau disarankan oleh sistem atau teknologi otomatis dan untuk lebih menyukai keputusan tersebut, bahkan jika keputusan manusia yang lebih baik atau setara tersedia.
- **Diskriminasi** adalah segala bentuk kerugian yang tidak beralasan atau perlakuan tidak setara terhadap individu atau kelompok berdasarkan berbagai karakteristik yang terlihat atau tidak terlihat. Karakteristik yang terlihat meliputi, misalnya, usia, etnis, atau disabilitas.
- **Hak yang sama (Kesetaraan)** berarti kesetaraan formal dan hukum antara individu dan kelompok.
- **Kesetaraan (Keadilan)** berarti bahwa setiap orang memiliki kesempatan yang sama, terlepas dari asal mereka, jenis kelamin, atau usia mereka. Hal ini juga memerlukan langkah-langkah yang ditargetkan untuk mempromosikan dan mendukung orang-orang dari latar belakang yang tidak setara sedemikian rupa sehingga kesetaraan sejati dapat terwujud.

Salah satu tujuan AI yang dapat dipercaya adalah agar sistem AI menjadi “adil”. Keadilan adalah konsep yang kompleks, biasanya didefinisikan sebagai kualitas (seseorang adil) atau keadaan (sesuatu adil) dari diperlakukan secara adil. Tetapi apa yang dianggap adil dan apa yang tidak adil dapat berarti hal yang berbeda bagi orang yang berbeda dalam konteks yang berbeda. Oleh karena itu, tidak ada satu metrik untuk mengukur keadilan dalam pembelajaran mesin, tetapi *setidaknya ada 21 cara untuk mendefinisikan keadilan menurut Arvind Narayanan*.

Matriks Konfusi adalah alat yang digunakan untuk mengukur kinerja sistem AI. Matriks ini memungkinkan untuk menghitung beberapa metrik kinerja penting dan dengan demikian mengevaluasi akurasi model klasifikasi, seperti Akurasi, Presisi, Recall atau Sensitivitas dan skor F1, yang merupakan rata-rata harmonik dari Presisi dan Recall. Ini juga membantu untuk memahami bagaimana kinerja model di berbagai kelas.

Dalam konteks pembelajaran mesin, istilah kotak hitam mengacu pada model atau sistem yang fungsi internalnya tidak 100% dapat dijelaskan dan dipahami. Hal ini sangat bermasalah terutama dalam hal keterlacakan keputusan, identifikasi bias, atau memastikan keadilan. Model kotak hitam sering ditemukan dalam sistem pembelajaran mesin yang kompleks seperti jaringan saraf dalam (deep neural networks), di mana jumlah dan jenis lapisan pemrosesannya menyulitkan untuk memahami secara tepat bagaimana data masukan menghasilkan hasil tertentu.

Proksi adalah variabel pengganti yang tidak berhubungan langsung dengan karakteristik sensitif, tetapi masih dapat digunakan untuk secara tidak langsung menyimpulkan karakteristik ini. Misalnya, kode pos dapat berfungsi sebagai proksi untuk etnis atau status

sosial ekonomi. Sistem AI dapat menggunakan proksi ini untuk mengenali pola yang mengarah pada keputusan diskriminatif, bahkan jika karakteristik sensitif itu sendiri tidak ada dalam data.

Pembuatan profil menurut Pasal 4 ayat 4 GDPR berarti setiap bentuk pemrosesan otomatis data pribadi yang terdiri dari penggunaan data pribadi untuk mengevaluasi aspek pribadi tertentu yang berkaitan dengan seseorang, khususnya untuk menganalisis atau memprediksi aspek yang berkaitan dengan kinerja orang tersebut di tempat kerja, situasi ekonomi, kesehatan, preferensi pribadi, minat, keandalan, perilaku, lokasi, atau pergerakan (lihat Bab 4).

Teknologi adalah pengganda, artinya teknologi dapat memengaruhi kehidupan jutaan orang, baik secara positif maupun negatif. Dalam konteks sistem AI yang sudah digunakan untuk membuat keputusan yang mengubah hidup, sistem ini secara tidak sengaja dapat menjadi penguat prasangka dan diskriminasi. Meskipun beberapa aplikasi sengaja digunakan untuk membahayakan orang dan masyarakat, seperti sistem senjata otonom atau gambar deep fake yang dirancang untuk memengaruhi opini publik, dan aplikasi lain dikembangkan secara sembarangan, seperti perangkat lunak yang dirancang untuk mendeteksi orientasi seksual, sebagian besar sistem AI dikembangkan dan digunakan dengan niat baik.

Namun demikian, ada risiko bahwa sistem tersebut dapat menimbulkan bias yang tidak disengaja untuk mendiskriminasi individu, tetapi terlebih lagi, seluruh kelompok orang sekaligus. Bias bawah sadar ini, juga dikenal sebagai bias tidak sadar, adalah keyakinan internal atau stereotip yang memengaruhi pemahaman, tindakan, dan keputusan kita dengan cara yang biasanya tidak kita sadari. Sebagian besar proses berpikir manusia terjadi di alam bawah sadar.

Hal ini membentuk persepsi dan tindakan kita tanpa kita sadari dan dapat ditransfer ke perkembangan teknologi. Inilah bagian dari masalahnya, ketika sistem AI dikembangkan oleh kelompok yang kurang beragam seperti pria kulit putih muda stereotip dari Silicon Valley, sistem ini dapat secara tidak sengaja bias dan mengabaikan atau mendiskriminasi seluruh populasi, yang telah terjadi berkali-kali di masa lalu, seperti pada aplikasi kesehatan atau algoritma pinjaman. Meskipun para pengembang berusaha untuk bertindak netral, titik buta kognitif mereka masih dapat dimasukkan ke dalam teknologi dan berpotensi menyebabkan kerugian.

Contoh bias dalam sistem AI:

- Alat rekrutmen AI Amazon yang lebih mengutamakan kandidat laki-laki
- Algoritma pengenalan wajah dengan akurasi lebih rendah untuk orang berkulit gelap
- Alat penerjemahan otomatis yang memperkuat stereotip gender
- Aplikasi kesehatan yang lebih baik mengenali penyakit kulit pada orang berkulit terang
- Proses pinjaman yang merugikan minoritas
- Kendaraan otonom yang kurang mampu mengenali orang kulit berwarna
- Alat aplikasi berbasis AI yang merugikan perempuan
- Algoritma pencarian yang mempromosikan stereotip rasial
- Sistem pemantauan AI yang lebih sering memantau minoritas
- Algoritma dalam perawatan kesehatan yang merugikan pasien Afrika-Amerika

Oleh karena itu, tim pengembangan interdisipliner dan beragam memainkan peran penting dalam deteksi dini dan penyadaran bias dalam pengembangan AI. Misalnya, tim yang terdiri dari berbagai budaya dan gender mungkin lebih cocok untuk mengenali bias gender atau budaya dalam asisten bahasa. Namun, ini saja tidak cukup. Bias perlu diidentifikasi, dipahami, dan dihilangkan secara menyeluruh – idealnya sejak awal, sementara pemantauan dan penyesuaian terus-menerus diperlukan sepanjang siklus hidup AI. Tim yang beragam dan pengujian yang cermat sangat penting, begitu pula pemahaman tentang dinamika sosial yang dapat memengaruhi AI. Tantangannya adalah **mengenali, memahami, dan pada akhirnya menghilangkan bias**.

- Bias dalam sistem AI terutama dapat diidentifikasi melalui pengujian dan validasi yang ditargetkan, serta dengan mengukur kinerja sistem AI menggunakan metrik seperti Matriks Kebingungan. Pengukuran yang tepat dapat mengungkapkan apakah suatu sistem secara sistematis menguntungkan atau merugikan kelompok tertentu. Hal ini memungkinkan untuk mengidentifikasi ketidakadilan dan mengambil langkah-langkah untuk meningkatkan keadilan. Penilaian dampak hak-hak dasar dapat membantu mengidentifikasi dan mengurangi risiko diskriminasi sebelum terjadi.
- Untuk memahami dari mana bias dalam sistem AI berasal, pemeriksaan kritis terhadap peran AI dalam masyarakat kita sangat penting. Untuk memastikan bahwa kemajuan teknologi bermanfaat bagi semua anggota masyarakat, alih-alih memperkuat prasangka dan diskriminasi, perlu untuk memandang AI sebagai sistem sosio-teknologis yang kompleks dan meningkatkan kesadaran luas tentang kompleksitas dan isu-isu mendesak yang terletak di persimpangan AI, etika, dan keadilan sosial. Analisis kritis tentang peran AI dalam masyarakat dapat mengungkapkan bagaimana bias masyarakat memengaruhi teknologi.
- Kecerdasan buatan tidak dapat menyelesaikan masalah sosial kita yang berakar dalam, tetapi dapat membantu kita mengenalinya ketika seluruh kelompok secara sistematis dirugikan atau didiskriminasi dalam skala besar. Menghilangkan bias dalam sistem AI adalah tugas yang menantang yang tidak memiliki solusi universal yang sederhana. Patut dipertanyakan apakah akan mungkin untuk sepenuhnya menghilangkan semua bias dalam sistem AI, karena hal ini harus selalu dipertimbangkan dalam konteks budaya masing-masing dan keadaan sosial dan politik pada zamannya. Namun demikian, jika kita ingin menggunakan sistem AI untuk mengambil keputusan di bidang-bidang sensitif yang berpotensi menyebabkan diskriminasi, kita harus memastikan bahwa bias dalam sistem AI dihilangkan sejauh mungkin dan menciptakan mekanisme teknis dan hukum untuk memastikan keadilan dalam penggunaan AI.

Contoh

Seseorang melamar pekerjaan yang tampaknya sangat cocok, tetapi ditolak. Alasan penolakan: sistem AI yang digunakan oleh perusahaan telah memutuskan bahwa pelamar tidak cocok untuk posisi tersebut. Ketika sistem AI digunakan di area di mana diskriminasi mungkin terjadi, penting untuk mempertanyakan data dan kriteria apa yang menjadi dasar keputusan sistem AI untuk menilai apakah keputusan tersebut adil. Pembeneran penolakan

semata-mata dengan merujuk pada keputusan AI harus dianggap tidak cukup di sini. Ada juga risiko bahwa AI akan mencerminkan bias sistemik yang terkandung dalam data pelatihan. Oleh karena itu, sangat penting bahwa keputusan yang dibuat oleh sistem AI dalam proses perekrutan dapat dipahami dan dapat diperdebatkan oleh pelamar.

Hal ini menyoroiti masalah lain dengan keputusan yang didukung AI berdasarkan pembelajaran mesin, pembelajaran mendalam, dan jaringan saraf, bidang AI yang telah membuat kemajuan besar berkat big data dan peningkatan daya komputasi. Sistem kompleks ini seringkali buram, yang mengarah pada istilah "kotak hitam" dan menguraikan masalah keterlacakan. Kurangnya kemampuan untuk menjelaskan membuat sulit untuk memahami bagaimana sistem AI sampai pada kesimpulan dan hasilnya, dan oleh karena itu terkait erat dengan masalah keadilan dan akuntabilitas. Argumen yang sering dikemukakan adalah bahwa tidak semua orang tahu bagaimana cara kerja mobil, namun orang tetap akan mengendarainya. Menurut penulis, argumen ini tidak valid dalam konteks ini karena, di satu sisi, mereka yang membangun kendaraan tahu bagaimana cara kerjanya dan mobil tidak membuat keputusan tentang kita, kecuali jika kita berbicara tentang mobil otonom, di mana masalah pengambilan keputusan muncul kembali.

Secara kiasan, masalah kotak hitam menggambarkan fakta bahwa kita tidak dapat begitu saja memasuki algoritma untuk mengidentifikasi dan menghilangkan sumber pengambilan keputusan dan prasangka dalam sistem AI. Sebaliknya, bias dan potensi diskriminasi harus diidentifikasi menggunakan metode pengujian dan pengukuran yang memadai. Diskriminasi baru terungkap paling lambat selama operasi, misalnya ketika terlihat jelas bahwa perempuan secara sistematis tidak diundang ke wawancara kerja. Jika ditemukan selama pengujian atau penerapan bahwa sistem AI bias, maka muncul pertanyaan tentang koreksi algoritma. Solusi yang jelas adalah dengan menganonimkan data pelatihan sehingga tidak mungkin lagi untuk mengidentifikasi jenis kelamin pelamar.

Namun, ini menunjukkan bahwa sekadar menganonimkan data tidak selalu cukup untuk melatih sistem AI, karena sistem AI secara independen mengenali pola dan membangun korelasi yang dapat menyebabkan hasil diskriminatif – bahkan tanpa informasi eksplisit tentang jenis kelamin. Misalnya, AI dapat secara tidak langsung menyimpulkan atribut sensitif seperti jenis kelamin atau etnis melalui variabel yang tampaknya netral (periode perawatan, periode kosong dalam CV, kata-kata yang cenderung digunakan oleh perempuan), yang disebut proksi. Contoh penting lainnya adalah tempat tinggal atau kode pos yang tampaknya netral sebagai variabel proksi, yang sering kali dapat digunakan oleh sistem AI sebagai "proksi" untuk keadaan sosial-ekonomi atau kelompok etnis, dan memainkan peran terutama dalam pemberian kredit, serta dalam kepolisian prediktif.

Meskipun sistem otomatis menjanjikan efisiensi dan objektivitas, penggunaannya mengandung risiko bahwa orang akan mengikuti rekomendasi AI tanpa kritis, bahkan jika rekomendasi tersebut mungkin salah.

Akhirnya, harus diakui bahwa setiap klasifikasi yang kita buat berada dalam konteks politik, sosial, dan budaya dari era, wilayah, atau negara tempat kita berada. Hal ini terwujud dalam penggunaan teknologi pengawasan: Sementara di beberapa negara kamera digunakan

untuk memantau kepatuhan terhadap aturan berpakaian seperti pemakaian jilbab yang benar, negara lain di mana hal ini dilarang mungkin menggunakan teknologi serupa untuk memastikan bahwa tidak ada jilbab yang dikenakan. Atau pertimbangan untuk mengembangkan sistem untuk mengenali jenis kelamin, gender, atau orientasi seksual seseorang dapat memiliki konsekuensi yang luas, termasuk hukuman mati. Contoh-contoh tersebut memperjelaskan bahwa orientasi sistem AI sangat berakar pada norma dan nilai yang berlaku, dan bahwa teknologi AI tidak dapat dilihat secara terpisah dari kerangka sosial dan hukum tempat teknologi tersebut dikembangkan dan digunakan.

Hak atas Kesetaraan dan Non-diskriminasi

Hak untuk tidak didiskriminasi berakar pada gagasan bahwa semua orang sama di hadapan hukum dan oleh karena itu harus diperlakukan sama. Namun, prinsip non-diskriminasi melangkah lebih jauh: prinsip ini mengakui bahwa orang berbeda dalam individualitas mereka dan bahwa kesetaraan di hadapan hukum tidak selalu berarti memperlakukan semua orang secara identik. Untuk mencapai kesetaraan sejati, kita harus melampaui perlakuan sama yang sederhana dan mengakui kondisi dan tantangan berbeda yang dihadapi orang.

Sesuai dengan Pasal 1 Deklarasi Universal Hak Asasi Manusia, semua manusia dilahirkan bebas dan setara dalam martabat dan hak. Pasal 2 menyatakan bahwa setiap orang “berhak atas hak dan kebebasan yang ditetapkan dalam Deklarasi ini tanpa perbedaan apa pun, seperti ras, warna kulit, jenis kelamin, bahasa, agama, pendapat politik atau lainnya, asal kebangsaan atau sosial, harta benda, kelahiran atau status lainnya”.

Di Eropa, kita menemukan klausul non-diskriminasi terutama dalam Pasal 14 Konvensi Eropa tentang Hak Asasi Manusia (ECHR) yang melarang segala bentuk diskriminasi berdasarkan jenis kelamin, ras, warna kulit, bahasa, agama, pendapat politik atau lainnya, asal kebangsaan atau sosial, keterkaitan dengan minoritas nasional, kepemilikan, kelahiran atau status lainnya.

Piagam Hak Fundamental Uni Eropa memuat seluruh bab – Bab III, Pasal 20–26 Piagam – tentang prinsip-prinsip kesetaraan. Diskriminasi berdasarkan jenis kelamin, ras, warna kulit, asal etnis atau sosial, karakteristik genetik, bahasa, agama atau kepercayaan, pendapat politik atau lainnya, keanggotaan minoritas nasional, kepemilikan, disabilitas, usia, atau orientasi seksual dinyatakan melanggar hukum. Lebih lanjut, Piagam tersebut juga mencakup pengakuan keragaman budaya, agama, dan bahasa, kesetaraan antara pria dan wanita, perlindungan hak-hak anak dan lansia, serta langkah-langkah untuk integrasi dan hak-hak penyandang disabilitas.

Hak atas kesetaraan dan non-diskriminasi menikmati perlindungan yang luas di luar Perjanjian Uni Eropa, berdasarkan Pasal 19 Perjanjian Uni Eropa, yang memberikan kemungkinan untuk mengambil langkah-langkah yang tepat untuk memerangi diskriminasi berdasarkan jenis kelamin, ras atau asal etnis, agama atau kepercayaan, disabilitas, usia, atau orientasi seksual. Arahan-arahan ini mewajibkan Negara Anggota untuk menerapkan undang-undang dan kebijakan untuk memerangi diskriminasi.

Dalam menerapkan kerangka hukum Uni Eropa, undang-undang nasional telah diberlakukan dan badan-badan khusus telah dibentuk di semua Negara Anggota Uni Eropa untuk membantu korban diskriminasi, menegakkan pengaduan mereka, melakukan laporan dan survei independen, dan merumuskan rekomendasi untuk memerangi diskriminasi. Beberapa badan ini juga berwenang untuk mengambil keputusan dalam kasus diskriminasi dan dengan demikian bertindak sebagai badan kuasi-yudisial.

Pasal 3 Undang-Undang Dasar Republik Federal Jerman menetapkan dalam paragraf 1: *“Semua orang sama di hadapan hukum.”* Paragraf 3 menetapkan bahwa tidak seorang pun boleh *“dirugikan atau diistimewakan karena jenis kelamin, asal, ras, bahasa, tanah Air dan asal, keyakinan, pandangan agama atau politik”*. Tidak seorang pun boleh dirugikan karena disabilitasnya. Lebih lanjut, menurut paragraf 2, laki-laki dan perempuan memiliki hak yang sama. Dalam pengertian ini, negara mempromosikan *“implementasi efektif hak-hak yang sama bagi perempuan dan laki-laki dan berupaya untuk menghilangkan kerugian yang ada”*.

Dalam hukum konstitusi Austria, prinsip ini diabadikan dalam Pasal 7 B-VG (Hukum Konstitusi Federal Austria) dalam prinsip kesetaraan dan menyatakan bahwa semua warga negara federal sama di hadapan hukum dan bahwa *“hak istimewa berdasarkan kelahiran, jenis kelamin, status, kelas, dan keyakinan”* dikecualikan. Undang-Undang Dasar menegaskan hal ini dalam Pasal 2: *“Semua warga negara sama di hadapan hukum.”* Pasal 14 ECHR (Konvensi Eropa tentang Hak Asasi Manusia) melampaui warga negara dan menjelaskan larangan diskriminasi sebagai berikut: *“Penikmatan hak dan kebebasan yang ditetapkan dalam Konvensi ini harus dijamin tanpa diskriminasi berdasarkan alasan apa pun seperti jenis kelamin, ras, warna kulit, bahasa, agama, pendapat politik atau lainnya, asal kebangsaan atau sosial, keterkaitan dengan minoritas nasional, kepemilikan, kelahiran atau status lainnya.”* Prinsip kesetaraan mengandung larangan terhadap diferensiasi yang tidak objektif, yang berarti bahwa yang sama harus diperlakukan sama dan yang tidak sama harus diperlakukan tidak sama.

Untuk menerapkan Pasal 14 ECHR yang disebutkan di atas, harus ada campur tangan terhadap hak yang dilindungi oleh ECHR. Menurut ECHR, perbedaan perlakuan adalah sah jika dibenarkan oleh tujuan yang sah dan tunduk pada proporsionalitas antara sarana yang digunakan dan tujuan yang dikejar. Protokol Tambahan ke-12 untuk Pasal 14 ECHR, yang berisi larangan diskriminasi yang komprehensif, belum diratifikasi oleh Jerman maupun Austria.

Prinsip kesetaraan adalah hak fundamental dan oleh karena itu terutama ditujukan terhadap negara dan tidak memiliki validitas umum dalam hubungan hukum antara individu swasta atau antara individu swasta dan perusahaan. Merupakan tugas negara untuk memberlakukan undang-undang untuk memperluas cakupan perlindungan hak-hak fundamental ke hubungan hukum antara orang perseorangan dan badan hukum dan untuk memberlakukan perlakuan yang sama atau larangan diskriminasi untuk hubungan tertentu. Prinsip perlakuan yang sama dengan demikian melarang dalam pekerjaan Hukum melarang pengusaha melakukan diskriminasi terhadap karyawan individu tanpa alasan objektif. § 1 ayat 5 Undang-Undang Perlindungan Data Austria secara tegas mengikat operator swasta bahwa

badan hukum swasta dapat menegaskan hak fundamental atas perlindungan data dalam proses perdata

Ini berarti perlakuan tidak setara harus

- dibenarkan secara objektif oleh tujuan yang sah dan
- dana harus sesuai dan diperlukan.

Pengecualian terhadap prinsip non-diskriminasi harus dibenarkan oleh tujuan yang sah dan dapat berupa cara yang tepat untuk mencapai tujuan tersebut. Ini dapat berupa, misalnya, persyaratan pekerjaan yang nyata dan menentukan atau tindakan positif yang diimplementasikan untuk mencapai kesetaraan kesempatan yang lebih besar. Kampanye pekerjaan diluncurkan untuk penyandang disabilitas yang tidak terbuka untuk orang yang menganggur tanpa disabilitas karena pengangguran di antara penyandang disabilitas sangat tinggi.

Perjanjian Perserikatan Bangsa-Bangsa tentang perlindungan terhadap diskriminasi:

- Konvensi Internasional tentang Penghapusan Semua Bentuk Diskriminasi Rasial (CERD)
- Konvensi tentang Penghapusan Semua Bentuk Diskriminasi terhadap Perempuan (CEDAW)
- Konvensi PBB tentang Hak-Hak Penyandang Disabilitas (CRPD)

Semua perjanjian ini berisi larangan diskriminasi, tetapi menunjukkan daftar dasar perlindungan yang berbeda.

Bagaimana Prasangka Masuk ke dalam AI

Bagian ini menjelaskan bagaimana bias masuk ke dalam sistem AI. Untuk tujuan ini, karya standar *A Framework for Understanding Sources of Harm throughout the Machine Learning Life Cycle* oleh Harini Suresh dan John V. Guttag sangat berharga dalam menjelaskan bagaimana bias dapat masuk ke dalam sistem AI dan membentuk dasar yang ideal untuk bagian ini, yang sebagian besar didasarkan pada karya ilmiah ini.

Kecerdasan buatan, dalam bentuk pembelajaran mesin, semakin banyak digunakan di bidang yang relevan dengan pengambilan keputusan yang berdampak langsung pada kehidupan manusia. Ini bekerja dengan melatih model berdasarkan kumpulan data yang ada untuk membuat prediksi atau keputusan untuk data baru yang tidak diketahui. Dalam proses pengumpulan data, pemodelan, dan aplikasi, berbagai masalah dapat muncul yang memiliki konsekuensi berbahaya. Potensi sistem AI untuk melakukan diskriminasi telah dijelaskan di atas. Contoh lain dari AS adalah perangkat lunak COMPAS, yang digunakan untuk menilai risiko terdakwa untuk memprediksi kemungkinan terdakwa melakukan pelanggaran lagi atau tidak. Menurut *ProPublica*, perangkat lunak ini secara keliru mengklasifikasikan terdakwa Afrika-Amerika sebagai memiliki risiko lebih tinggi untuk melakukan pelanggaran kembali.

Ketika diskriminasi oleh sistem AI terjadi, reaksi pertama biasanya adalah menganggap bahwa data tersebut bias atau berprasangka. Meskipun banyak bias memang mungkin tertanam dalam proses pembuatan data, sangat penting untuk memahami bahwa tidak semua masalah harus dikaitkan semata-mata dengan data. Proses pembelajaran mesin melibatkan berbagai keputusan dan praktik mulai dari pemilihan model matematika hingga antarmuka

pengguna yang digunakan dalam implementasi. Setiap langkah dalam proses ini membawa risiko menyebabkan hasil yang tidak diinginkan.

Harini Suresh dan John V. Gutttag memberikan contoh berikut:

- Seorang peneliti medis ingin mengembangkan model untuk meningkatkan deteksi serangan jantung. Dia melatih model tersebut dengan catatan medis dari kelompok pasien tertentu di sebuah rumah sakit, termasuk informasi tentang apakah dan kapan orang-orang ini mengalami serangan jantung. Ia menemukan bahwa model tersebut cenderung lebih jarang mengidentifikasi serangan jantung pada wanita dengan benar, menunjukkan bahwa model tersebut mungkin belum mampu mempelajari gejala pada wanita secara memadai karena kurangnya data yang relevan. Dengan mengintegrasikan data tambahan yang mewakili wanita dengan pengalaman serangan jantung ke dalam dataset dan melatih ulang model, ia dapat meningkatkan akurasi untuk pasien wanita.
- Pada saat yang sama, seorang kolega yang bertanggung jawab untuk merekrut teknisi laboratorium baru sedang mencoba mengembangkan algoritma untuk memprediksi kesesuaian pelamar wanita dan pria berdasarkan CV mereka dan peringkat yang diberikan secara manual. Ia menemukan bahwa model tersebut secara signifikan kurang mungkin mengidentifikasi wanita sebagai kandidat yang cocok daripada pria. Terlepas dari upaya untuk memperluas dataset dengan menambahkan lebih banyak contoh wanita, perilaku diskriminatif sistem AI tetap ada.

Alasan perbedaan efek tersebut terletak pada penyebab yang berbeda: Pada contoh pertama, kurangnya data tentang perempuan berarti bahwa penambahan data lebih bermanfaat, sedangkan pada contoh kedua, prediksi diskriminatif disebabkan oleh penggunaan peringkat manusia sebagai indikator kualitas dan perluasan dataset saja tidak memperbaiki situasi.

Contoh-contoh ini menggambarkan bahwa distorsi atau prasangka terjadi pada berbagai titik dalam siklus hidup pembelajaran mesin dan oleh karena itu dapat menyebabkan diskriminasi dan konsekuensi negatif lainnya. Selain potensi diskriminasi oleh sistem AI, sistem AI juga sering salah merepresentasikan kelompok tertentu, seperti model bahasa yang memperkuat dan menyebarkan stereotip.

Sebagian besar sistem AI didasarkan pada pembelajaran mesin. Untuk memahami bagaimana bias dimasukkan ke dalam sistem, yang dapat menyebabkan hasil yang tidak adil, langkah-langkah individual dari pembelajaran mesin dipertimbangkan:

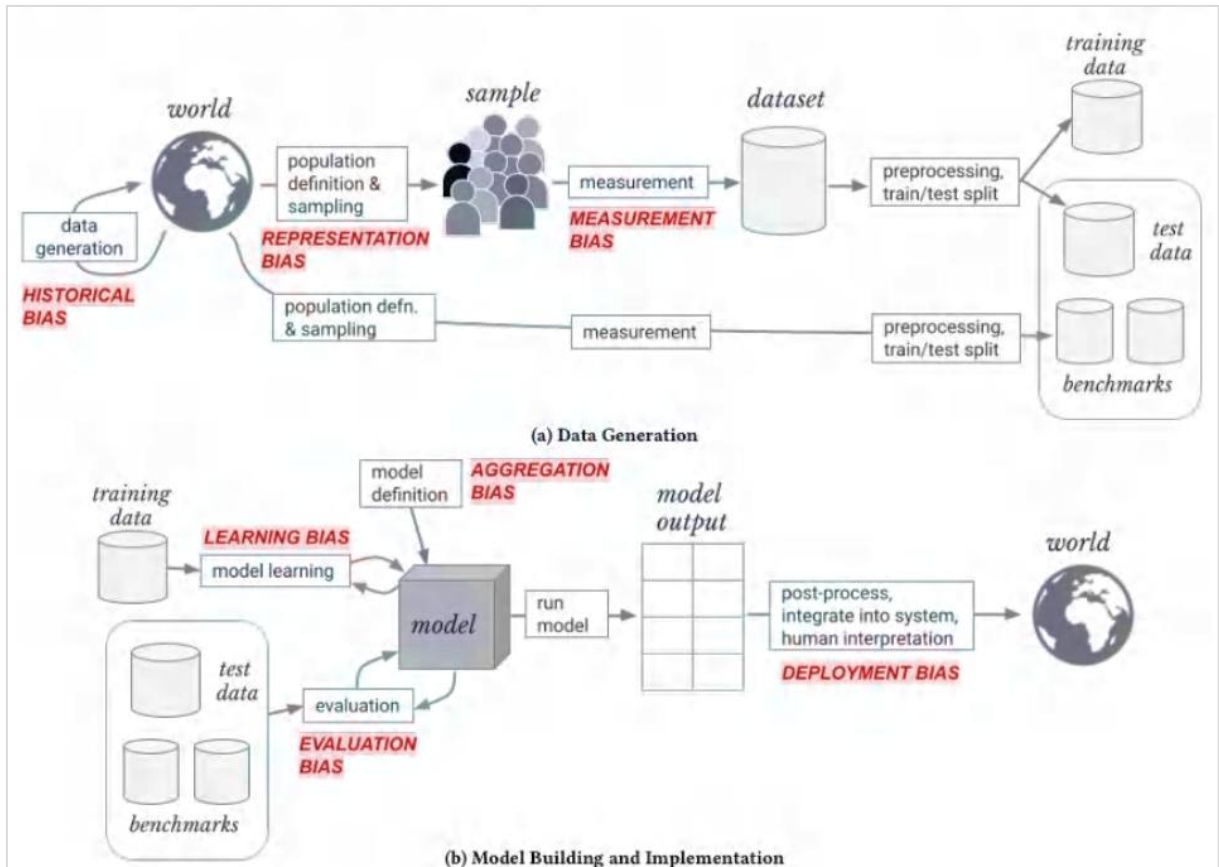
- Pengumpulan data: Proses dimulai dengan mendefinisikan kelompok sasaran dan mengumpulkan data yang diperlukan untuk model. Saat mengembangkan sistem penilaian kredit, pemilihan kelompok sasaran harus mencerminkan ketidaksetaraan sosial-ekonomi yang sudah ada sebelumnya, misalnya, jika pengumpulan data mengecualikan orang-orang di kelompok pendapatan rendah atau area geografis tertentu, ini dapat menyebabkan bias historis.
- Pemrosesan dan persiapan data: Pada fase ini, data dibersihkan, dinormalisasi, dan dikonversi ke dalam format yang dapat diproses oleh algoritma. Hal ini dapat menyebabkan bias pengukuran, seperti ketika cara variabel diukur atau dikategorikan

secara sistematis merugikan kelompok tertentu. Misalnya, jika "riwayat kredit" digunakan sebagai proksi untuk "kelayakan kredit", perbedaan sistemik dalam akses ke kredit antara kelompok sosial yang berbeda mungkin tidak diperhitungkan (secara historis, lebih sedikit orang dari latar belakang imigran yang mengajukan kredit daripada orang Amerika).

- Pengembangan model: Pada langkah ini, algoritma dilatih untuk mengenali pola dalam data dan membuat prediksi. Bias pembelajaran dapat terjadi jika pemilihan fitur, data pelatihan, atau jenis algoritma pembelajaran secara sistematis lebih mengutamakan pola tertentu daripada yang lain. Contohnya adalah sistem pengenalan wajah yang berkinerja lebih buruk pada wanita dan orang kulit berwarna karena dataset pelatihan yang didominasi oleh pria kulit putih.
- Evaluasi model: Di sini kinerja model dinilai berdasarkan data pengujian. Bias evaluasi terjadi ketika data pengujian tidak mewakili keragaman kasus penggunaan di dunia nyata. Algoritma yang diuji pada kumpulan data yang kurang beragam mungkin mencapai skor akurasi tinggi, tetapi tetap tidak adil di dunia nyata karena kumpulan data pengujian dikumpulkan terutama dari data kelompok yang bias secara demografis, seperti pelamar UKM.
- Penyisipan model: Bahkan jika model telah lulus semua pengujian, diskriminasi dapat terjadi dalam penggunaan sebenarnya. Hal ini mungkin terjadi jika lingkungan penerapan atau interaksi pengguna dengan model tidak sepenuhnya sesuai dengan kondisi di mana model tersebut dikembangkan dan diuji. Contohnya adalah algoritma perekrutan yang digunakan dalam lingkungan di mana kualifikasi atau pengalaman tertentu secara sistematis diremehkan.

Untuk meminimalkan potensi diskriminasi, penting untuk melihat secara kritis seluruh siklus hidup pembelajaran mesin dan secara proaktif menerapkan strategi untuk mengidentifikasi dan mengurangi bias. Ini termasuk menggabungkan pengetahuan ahli, memilih kumpulan data yang representatif, menerapkan praktik AI yang dapat dipercaya, dan terus meninjau serta menyesuaikan model berdasarkan umpan balik dunia nyata.

Hal ini diikuti dengan deskripsi tentang bias apa saja yang dapat masuk ke dalam sistem AI:



Gambar 7.1 Penggabungan Bias ke dalam Sistem AI

Bagaimana Undang-Undang AI Menangani Diskriminasi

Algoritma dapat menjadi diskriminatif jika menyebabkan kerugian yang tidak beralasan bagi individu. Hal ini berlaku khususnya untuk kasus-kasus di mana orang dirugikan berdasarkan karakteristik yang layak dilindungi seperti usia, jenis kelamin, etnis, agama, orientasi seksual, atau disabilitas. Perlindungan terhadap diskriminasi oleh sistem AI adalah salah satu tujuan utama Undang-Undang AI, yang bertujuan untuk memastikan tingkat perlindungan yang tinggi bagi hak-hak dasar dan keselamatan warga negara sekaligus menciptakan lingkungan yang mendorong inovasi dan pengembangan sistem AI.

Undang-Undang AI menangani masalah diskriminasi terutama dengan menetapkan aturan dan persyaratan untuk sistem AI berisiko tinggi untuk memastikan bahwa sistem ini menghormati hak-hak dasar, termasuk non-diskriminasi:

- **Persyaratan untuk sistem AI berisiko tinggi:** Undang-Undang AI mendefinisikan persyaratan tertentu untuk sistem AI yang diklasifikasikan sebagai berisiko tinggi untuk memastikan kepatuhannya terhadap hak-hak dasar. Persyaratan ini mencakup akurasi, kekokohan dan keamanan sistem, verifikasi dan validasi kualitas data, serta transparansi sistem AI.
- **Praktik AI yang Dilarang:** Undang-Undang AI melarang praktik-praktik tertentu yang dapat merupakan pelanggaran serius terhadap hak-hak fundamental, seperti praktik manipulatif yang dapat mengubah perilaku individu sedemikian rupa sehingga mengganggu kebebasan memilih mereka, atau sistem yang mengklasifikasikan

karakteristik sensitif seperti jenis kelamin, ras, atau orientasi seksual berdasarkan data biometrik.

Aturan-aturan ini dirancang untuk meminimalkan risiko diskriminasi oleh sistem AI dan untuk memastikan bahwa pengembangan dan penggunaan AI sejalan dengan hak-hak fundamental dan nilai-nilai Uni Eropa.

Pertimbangan ke-70 UU AI Uni Eropa secara eksplisit didedikasikan untuk topik diskriminasi: *“Untuk melindungi hak orang lain dari diskriminasi yang mungkin diakibatkan oleh bias dalam sistem AI, penyedia layanan, secara khusus, sejauh yang benar-benar diperlukan untuk tujuan memastikan deteksi dan koreksi bias terkait dengan sistem AI berisiko tinggi, dengan tetap memperhatikan perlindungan yang memadai untuk hak dan kebebasan mendasar individu dan mengikuti penerapan semua ketentuan yang berlaku yang ditetapkan dalam Peraturan ini selain ketentuan yang ditetapkan dalam Peraturan (EU) 2016/679 dan (EU) 2018/1725 dan Direktif (EU) 2016/680, juga dapat memproses kategori khusus data pribadi, sebagai masalah kepentingan publik yang substansial dalam arti Pasal 9(2), no. (g) Peraturan (EU) 2016/679 dan Pasal 10(2), no. (g) Peraturan (EU) 2018/1725.”*

Pasal 70 UU AI mengatur tentang pemrosesan kategori khusus data pribadi oleh penyedia sistem AI berisiko tinggi untuk tujuan mendeteksi dan mengoreksi bias (Bias). Hal ini dimaksudkan untuk melindungi hak orang lain atas perlindungan terhadap diskriminasi yang dapat diakibatkan oleh bias tersebut. Pemrosesan data tersebut diizinkan sebagai pengecualian dan sejauh yang benar-benar diperlukan untuk memastikan deteksi dan koreksi bias. Perlindungan yang memadai harus diterapkan untuk melindungi hak dan kebebasan mendasar individu dan semua ketentuan yang ditetapkan dalam Peraturan harus dipatuhi, selain ketentuan GDPR (EU) 2016/679, Peraturan (EU) 2018/1725 dan Direktif (EU) 2016/680. Pemrosesan ini diklasifikasikan sebagai masalah kepentingan publik yang substansial sesuai dengan Pasal 9 ayat 2 huruf g GDPR dan Pasal 10 ayat 1725. Pasal 2 huruf g Peraturan (EU) 2018/1725, yang merupakan dasar hukum untuk pemrosesan data.

Dalam konteks ini, Pasal 22 GDPR juga relevan, yang melindungi subjek data dari proses pengambilan keputusan yang sepenuhnya otomatis tanpa keterlibatan manusia jika keputusan individu otomatis memiliki konsekuensi hukum bagi subjek data (seperti kesimpulan atau pengakhiran kontrak) atau secara signifikan memengaruhi subjek data dengan cara lain. Subjek data berhak untuk meminta peninjauan manusia atas keputusan tersebut, untuk menyampaikan sudut pandang mereka sendiri dan untuk menantang keputusan tersebut (lihat Bab 4).

Pasal 86 UU AI melengkapi dan menentukan **hak untuk mendapatkan penjelasan tentang proses pengambilan keputusan dalam kasus individu** bagi orang-orang dalam konteks sistem AI berisiko tinggi dengan memberikan hak kepada subjek data untuk menerima penjelasan tentang peran sistem AI dalam proses pengambilan keputusan dan elemen terpenting dari keputusan yang diambil. Hal ini berlaku untuk keputusan yang didasarkan pada data yang diproses oleh sistem AI berisiko tinggi sesuai dengan Lampiran III UU AI, dengan pengecualian infrastruktur kritis (Lampiran III no. 2), dan yang memiliki efek hukum atau secara

signifikan memengaruhi subjek data. Sistem AI berikut menurut Lampiran III memiliki potensi khusus untuk mendiskriminasi individu atau kelompok individu:

- Biometrik, karena sistem pengenalan wajah saat ini memberikan hasil yang bervariasi untuk warna kulit yang berbeda dan memiliki tingkat kesalahan yang tinggi untuk wanita berkulit gelap.
- Pendidikan dan pelatihan kejuruan (no. 3), misalnya sistem AI yang memutuskan akses atau penerimaan ke lembaga pendidikan atau dimaksudkan untuk digunakan untuk penilaian hasil pembelajaran.
- Ketenagakerjaan, manajemen personalia dan akses ke wirausaha (nomor 4),
- misalnya sistem AI yang mengotomatiskan proses seleksi dengan menempatkan iklan pekerjaan yang ditargetkan dan menyaring serta mengevaluasi pelamar.
- Aksesibilitas dan penggunaan layanan dan manfaat swasta dan publik dasar (no. 5),
- misalnya Sistem AI yang menilai apakah individu berhak atas layanan bantuan dan dukungan publik dasar, termasuk layanan kesehatan, dan apakah manfaat dan layanan tersebut harus diberikan, dibatasi, ditarik, atau diminta kembali.
- Sistem AI yang melakukan pengecekan kredit dan penilaian skor kredit individu atau menghitung penilaian risiko dan penetapan harga untuk asuransi kesehatan dan jiwa.
- dan lain-lain.

Baik Pasal 22 GDPR maupun Pasal 86 UU AI memastikan transparansi dan keadilan proses pengambilan keputusan otomatis dan memberikan hak kepada subjek data untuk membela diri terhadap keputusan tersebut. Sementara Pasal 22 GDPR menetapkan hak umum untuk tidak tunduk pada keputusan yang hanya didasarkan pada pemrosesan otomatis, Pasal 86 UU AI memberikan hak khusus untuk penjelasan atas keputusan yang dibuat oleh sistem AI tertentu untuk lebih meningkatkan pemahaman dan verifikasi keputusan tersebut.

Oleh karena itu, Mahkamah Eropa (ECJ) juga telah memutuskan bahwa "keputusan otomatis" dalam arti GDPR juga ada jika nilai probabilitas dihitung secara otomatis dan keputusan seseorang sangat bergantung pada nilai probabilitas ini. Secara khusus, sengketa hukum ini menyangkut penolakan bank untuk memberikan pinjaman kepada penggugat berdasarkan perhitungan kelayakan kredit penggugat (skor kredit) oleh lembaga referensi kredit Jerman, Schufa. Menurut keputusan Mahkamah Eropa (ECJ), keputusan otomatis juga ada jika keputusan akhir diambil oleh seseorang, asalkan keputusan orang tersebut bergantung "secara signifikan" pada perhitungan otomatis yang dilakukan sebelumnya. Dengan kata lain, setiap persiapan otomatis dari keputusan manusia selanjutnya dianggap sebagai keputusan otomatis dalam arti Pasal 22 GDPR. Keputusan ECJ ini secara signifikan memperluas ruang lingkup penerapan GDPR pada keputusan otomatis.

Hal ini berarti bahwa ketika mengembangkan dan menggunakan sistem AI tertentu yang memproses data pribadi, baik persyaratan Undang-Undang AI maupun GDPR harus dipenuhi oleh penyedia dan pengembang sistem tersebut.

Bisakah Kita Memperbaiki Bias dalam AI?

Menghilangkan bias dalam sistem AI merupakan tantangan multifaset yang tidak memiliki solusi sederhana. Prasangka dapat masuk ke dalam sistem AI melalui data, algoritma,

dan proses pengambilan keputusan manusia, dan selanjutnya menyebabkan diskriminasi terhadap individu atau seluruh kelompok. Oleh karena itu, penting untuk memerangi bias dalam sistem AI dan dampaknya menggunakan berbagai strategi, yang sebagian besar telah dijelaskan di atas:

- Tim yang beragam: Inklusi perspektif yang beragam dalam proses pengembangan dapat membantu menggabungkan sebanyak mungkin sudut pandang, pengalaman yang berbeda, latar belakang budaya, dan pengetahuan spesialis ke dalam pengembangan dan mengidentifikasi titik buta pada tahap awal. Hal ini mengurangi bias sistematis dan prasangka yang tidak disengaja dalam algoritma dan meningkatkan pembuatan sistem AI yang lebih adil dan lebih representatif terhadap keragaman pengguna.
- Penilaian dampak hak fundamental: Tujuan dari penilaian dampak hak fundamental adalah untuk menganalisis dan mengevaluasi potensi dampak sistem AI yang direncanakan terhadap hak fundamental sebelum dikembangkan. Hal ini dimaksudkan untuk meminimalkan risiko terhadap hak-hak fundamental dan secara proaktif mengambil langkah-langkah untuk memastikan perlindungan hak-hak fundamental serta untuk memahami, secara aktif mengatasi, dan mengurangi dampaknya pada berbagai kelompok dan orang.
- Pengembangan atau penggunaan sesuai dengan Pedoman Etika AI yang terpercaya.
- Kumpulan data uji dan validasi: Kumpulan data uji dan validasi yang baik sangat penting untuk pengembangan AI guna memastikan akurasi, keadilan, dan ketahanan. Kumpulan data ini memungkinkan pengembang untuk mengevaluasi kinerja AI dalam berbagai kondisi. Pemilihan dan diversifikasi kumpulan data ini secara cermat membantu mengidentifikasi dan meminimalkan bias dan prasangka.
- Pengukuran keadilan: Karena sistem AI memiliki potensi diskriminasi yang tinggi, penting untuk mengukur keadilan sistem kritis. Dalam praktiknya, berbagai metrik dan pendekatan, seperti Matriks Kebingungan, digunakan untuk mengevaluasi keadilan dan bias dalam sistem AI. Masing-masing metrik ini berfokus pada aspek keadilan yang berbeda dan membantu mengidentifikasi serta mengatasi bias dalam model mereka. Menurut “21 definisi keadilan dan politiknya” oleh Arvind Narayanan, terdapat setidaknya 21 cara matematis untuk mengukur keadilan.
- Pemantauan siklus hidup: Pemantauan dan adaptasi berkelanjutan terhadap sistem AI sangat penting untuk menanggulangi diskriminasi dalam jangka panjang dan memastikan keadilan.
- Pembuatan Kode Etik:

AI dapat membantu menampakkan prasangka manusia, tetapi tidak dapat menyelesaikannya. Teknologi mencerminkan data dan keputusan yang dibuat oleh manusia. Oleh karena itu, solusi efektif untuk mengatasi bias dan ketidaksetaraan hanya dimungkinkan melalui pendekatan terpadu yang menggabungkan perspektif teknologi, etika, dan sosial.

7.2 AI DI SEKTOR KEUANGAN

Komisi Eropa menekankan “*Masa depan sistem keuangan kita adalah digital*”, dalam strateginya untuk keuangan digital di Uni Eropa. Selain solusi cloud dan blockChain, big data dan AI sangat penting. Bagaimanapun, sejumlah besar data adalah dasar dari semua analitik. AI dapat digunakan untuk mengoptimalkan derivasi dari input data. Hal ini memungkinkan produk dan inovasi baru. Mulai dari algoritma perdagangan otomatis dan deteksi penipuan hingga nasihat keuangan yang dipersonalisasi, pinjaman, manajemen risiko dan pengaduan – kasus penggunaannya tidak terbatas dan telah digunakan di sektor yang sangat diatur selama bertahun-tahun. Namun, potensinya masih jauh dari habis dan kemajuan serta manfaat yang pesat masih menanti kita. Namun, teknologi ini juga menimbulkan **tantangan** khusus di sektor ini. Di sektor keuangan yang sangat diatur, misalnya, muncul pertanyaan mengenai (i) penerimaan peraturan dan manajemen risiko dan (ii) implementasi AI yang sesuai dengan hukum.

Pertanyaan pertama sangat menarik karena keputusan yang dibuat dengan berbagai sistem dan model AI hanya dapat dipahami sampai batas tertentu. Oleh karena itu, **pertama-tama harus diperiksa apakah AI dapat digunakan sama sekali dari perspektif regulasi. Tata kelola** memainkan peran kunci di sini. Otoritas pengawas saat ini mengharapkan setiap kurangnya keterlacakan, diskriminasi tersembunyi, penyalahgunaan, atau pelanggaran hak cipta dihindari melalui tata kelola yang cermat.

Implementasi yang sesuai dengan hukum itu kompleks karena berbagai **peraturan perundang-undangan khusus sektor** (undang-undang, peraturan, dan arahan nasional) termasuk rekomendasi dan perintah formal dan informal dari otoritas (pengawas) dan pengadilan yang berwenang harus dipatuhi di sektor TI (misalnya Peraturan CRR, Arahan CRD, Peraturan Infrastruktur Pasar, Arahan Pasar dan Instrumen Keuangan, Peraturan Penyalahgunaan Pasar, Arahan Keamanan Jaringan dan Informasi, Peraturan tentang Stabilitas Operasional Sistem Digital di Sektor Keuangan, Pedoman EBA tentang Risiko TIK dan Keamanan EBA/GL/2019/04, dan lain-lain.). Jika AI digunakan sesuai dengan makna Undang-Undang AI, maka persyaratan semua peraturan khusus sektor juga harus diimplementasikan. Oleh karena itu, pemahaman mendalam tentang berbagai peraturan dan interaksinya satu sama lain diperlukan untuk mengimplementasikan AI secara efisien.)

Aspek-aspek relevansi UU AI terhadap sektor keuangan dibahas di bawah ini:

- Pengecualian terhadap ruang lingkup penerapan
- Praktik AI yang dilarang
- Sistem AI berisiko tinggi
- Model AI Tujuan Umum
- Sistem AI tertentu
- Kompetensi otoritas

Pengecualian terhadap Ruang Lingkup Penerapan

Pasal 2 UU AI mengatur ruang lingkup penerapan dan pengecualian eksplisit. Pengecualian berikut ini sangat relevan untuk sektor keuangan:

- **Kegiatan penelitian, pengujian, dan pengembangan di luar kondisi dunia nyata.**

Menurut Pasal 2 ayat 8 UU AI, peraturan tersebut tidak berlaku untuk kegiatan penelitian, pengujian, dan pengembangan yang berorientasi pada produk pada sistem AI atau model AI sebelum dipasarkan atau digunakan, **kecuali pengujian dilakukan dalam kondisi dunia nyata.**

“Pengujian dalam kondisi dunia nyata” berarti pengujian sementara sistem AI untuk tujuan yang dimaksudkan, yang dilakukan dalam kondisi dunia nyata di luar laboratorium atau lingkungan simulasi lainnya untuk mengumpulkan data yang andal dan kuat serta untuk menilai dan memverifikasi kesesuaian sistem AI. Untuk pengujian sistem AI berisiko tinggi dalam kondisi kehidupan nyata, terdapat peraturan khusus dalam Pasal 60 dan seterusnya dari Undang-Undang AI (misalnya, rencana pengujian, persetujuan oleh otoritas pengawasan pasar, durasi maksimum enam bulan, persetujuan berdasarkan informasi, perlindungan, dan lain-lain.).

Perbedaan antara pengujian dalam kondisi dunia nyata dan non-nyata bukanlah hal yang sepele. Dalam kebanyakan kasus, tujuan pengembangan dan validasi dalam lingkungan pengujian pada akhirnya adalah untuk memperoleh hasil yang andal dan tangguh untuk penggunaan produktif. Oleh karena itu, seringkali ada minat yang besar untuk mensimulasikan kondisi dunia nyata sedekat mungkin. Namun, kondisi dan oleh karena itu juga hasil dari lingkungan pengujian dan pengembangan seringkali berbeda dari kondisi di lingkungan produksi. Pilot yang sukses di lingkungan terlindungi dapat menyebabkan kinerja yang berbeda atau lebih buruk di sistem produksi. Dengan latar belakang ini, saya percaya bahwa hanya lingkungan simulasi yang dapat menjadi kriteria penentu untuk pengujian dalam kondisi dunia nyata atau tidak nyata.

Contoh

Sebuah bank sedang mengembangkan sistem AI untuk mendeteksi transaksi curang. Untuk tujuan ini, bank tersebut menggunakan infrastruktur pengujian tertutup yang disimulasikan dan data sintetis (fiktif). Menurut pendapat saya, ada banyak argumen yang mendukung lingkungan pengujian yang tidak nyata, sehingga pengecualian berlaku dan penggunaan ini belum tunduk pada Undang-Undang AI.

Kasusnya berbeda jika lembaga kredit menguji sistem AI dalam lingkungan produksi tertutup dengan data nyata. Dalam hal ini, kewajiban berdasarkan Pasal 60 dan seterusnya Undang-Undang AI harus dipatuhi.

- **Lisensi sumber terbuka gratis**

Menurut Pasal 2 ayat 12 UU AI, sistem AI yang disediakan di bawah lisensi sumber terbuka gratis tidak tercakup dalam UU tersebut. Ini tidak berlaku untuk sistem AI yang dilarang, sistem AI tertentu termasuk sistem AI tujuan umum) Pengecualian ini tidak berlaku untuk risiko sistematis, sistem pengenalan emosi, atau sistem kategorisasi biometrik yang disebutkan dalam Pasal 50.

Perangkat lunak, data, dan model yang disediakan sebagai sumber terbuka, memungkinkan untuk dibagikan secara terbuka dan pengguna dapat mengakses, menggunakan, memodifikasi, dan mendistribusikannya secara gratis, tidak diatur

dalam Regulasi AI. Hal ini mempertimbangkan gagasan untuk mendorong pertumbuhan dan inovasi. Namun, ketentuan pengecualian ini harus diperlakukan dengan hati-hati. Menurut Pertimbangan 102 dan seterusnya UU AI, ini tidak termasuk komponen AI yang disediakan dengan harga atau dimonetisasi dengan cara lain.

Contoh

Penyedia layanan perangkat lunak menawarkan sistem AI untuk segmentasi pasar dan optimasi aktivitas penjualan untuk sektor keuangan yang diatur. Perangkat lunaknya didasarkan pada perangkat lunak berpaten dan komponen pembelajaran mesin sumber terbuka terintegrasi. Karena penyediaan komponen AI sumber terbuka gratis dengan biaya tertentu, sistem AI atau bagian-bagiannya tidak termasuk dalam pengecualian Pasal 2 ayat 12 UU AI.

Sistem AI yang Dilarang

Setiap sistem AI dalam lingkup Undang-Undang AI harus diperiksa terhadap daftar larangan dalam Pasal 5 Undang-Undang AI. Beberapa larangan mungkin berlaku di sektor keuangan dan oleh karena itu praktik-praktik berikut khususnya harus dinilai secara kritis:

▪ Pengaruh bawah sadar, teknik manipulatif atau menipu

Pasal 5 ayat 1 huruf a UU AI melarang sistem AI yang menggunakan teknik pengaruh bawah sadar di luar kesadaran seseorang atau teknik manipulatif/menipu secara sengaja,

- untuk secara signifikan mengubah perilaku orang (kelompok),
- dengan secara signifikan mengganggu kemampuan mereka untuk membuat keputusan yang tepat,
- menyebabkan mereka membuat keputusan yang seharusnya tidak mereka buat, dan
- yang menyebabkan atau kemungkinan besar akan menyebabkan kerugian besar bagi orang tersebut.

Larangan ini melengkapi ketentuan Arahan UCP, GDPR, dan persyaratan khusus sektor di sektor keuangan.

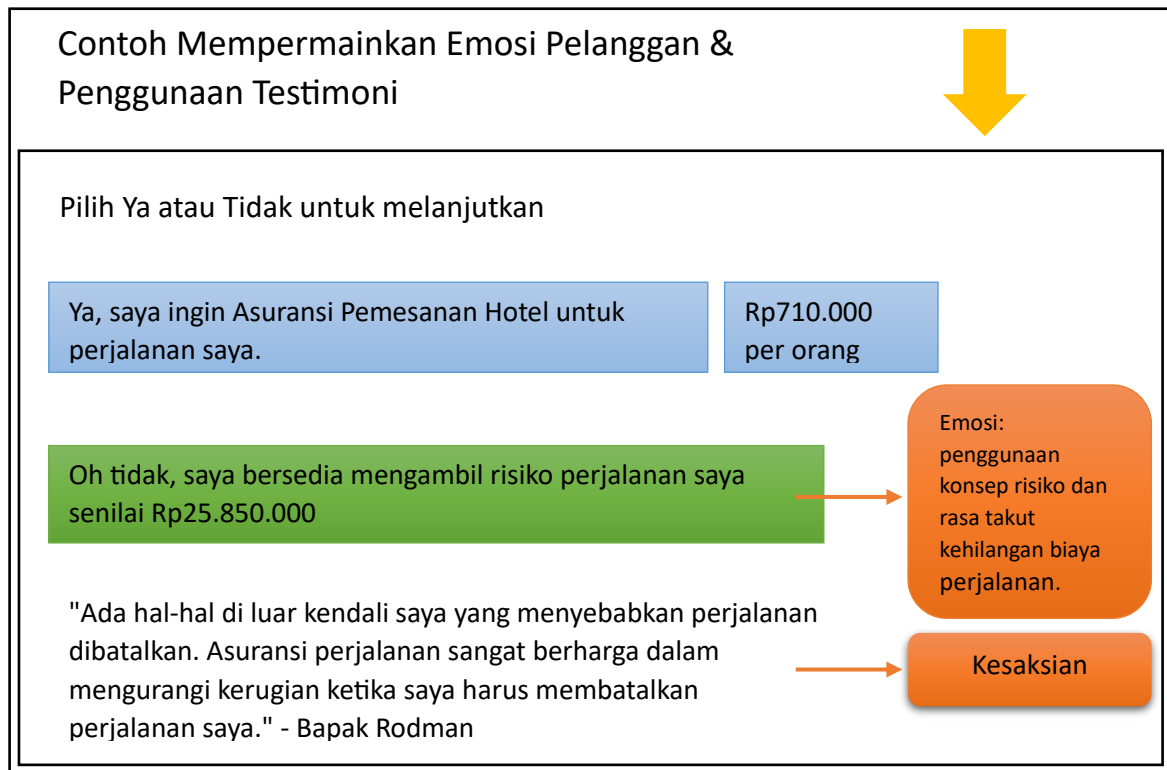
Contoh

Pengaruh emosional yang ditargetkan terhadap konsumen untuk memaksa mereka membuat keputusan tertentu dapat dianggap sebagai teknik manipulatif. Contohnya termasuk pola gelap (dark patterns).

Seperti yang ditunjukkan EIOPA, ini terjadi, misalnya, jika konsumen dibuat percaya bahwa mereka menyetujui risiko keuangan tertentu tanpa asuransi yang memadai. Jika AI digunakan untuk tujuan ini, praktik ini dapat dilarang berdasarkan Pasal 5 UU AI.

Desain antarmuka pengguna yang manipulatif juga dapat memengaruhi orang (kelompok) di bawah ambang batas persepsi sadar. Misalnya, presentasi dan desain tombol yang relevan dengan keputusan yang berbeda pada aplikasi perdagangan sudah tidak dapat diterima karena persyaratan peraturan jika opsi tombol yang setara lebih buruk atau hampir tidak terlihat dan dengan demikian secara tidak jujur mendorong pengguna ke arah tindakan tertentu. Jika sistem AI digunakan untuk tujuan ini, ini juga merupakan pelanggaran terhadap Peraturan AI. Indikasi lebih lanjut dari teknik manipulatif dapat berupa, misalnya, tindakan

paksaan atau penawaran palsu, penyampaian urgensi, opsi yang telah dipilih sebelumnya atau peringkat yang tidak akurat.



▪ **Eksplotasi kerentanan atau kebutuhan perlindungan individu (kelompok) karena karakteristik tertentu dengan potensi bahaya yang signifikan**

Pasal 5 ayat 1 huruf b UU AI melarang sistem AI yang menciptakan kerentanan atau kerentanan seseorang (kelompok).

- karena usia, disabilitas, situasi sosial atau ekonomi tertentu
- dengan tujuan atau efek memengaruhi perilaku mereka,
- yang (mungkin) akan menyebabkan kerugian yang cukup besar.

Larangan ini melengkapi teknik manipulatif dan menipu sejauh tidak memerlukan metodologi khusus dan sudah menghukum upaya mempengaruhi kekuasaan pengambilan keputusan individu yang layak dilindungi.

▪ **Evaluasi dan klasifikasi sosial terhadap orang**

UU AI juga melarang sistem AI untuk mengevaluasi atau mengklasifikasikan individu dalam jangka waktu tertentu berdasarkan perilaku sosial mereka atau karakteristik pribadi atau sifat kepribadian yang diketahui, disimpulkan, atau diprediksi jika penilaian sosial tersebut menyebabkan:

- kerugian atau diskriminasi dalam konteks sosial yang tidak terkait dengan pengumpulan data awal;
- tidak dapat dibenarkan atau tidak proporsional sehubungan dengan perilaku sosial mereka atau cakupannya.

Oleh karena itu, larangan tersebut mencakup penilaian sosial tetapi tidak terbatas pada sektor publik.

Contoh

Jika lembaga keuangan menggunakan AI untuk menilai kelayakan kredit seorang pemohon berdasarkan perilaku sosial mereka (misalnya, parkir yang salah, ekstrovert, berisik, dan lain-lain.), maka pelarangan mungkin dapat dibenarkan.

▪ **Pengenalan Emosi di Tempat Kerja**

Menurut Pasal 5 ayat 1 huruf f UU AI, penggunaan sistem AI untuk pengenalan emosi, antara lain, pada orang di tempat kerja tidak diperbolehkan. Pengecualian hanya ada jika sistem AI diperkenalkan untuk alasan medis atau keselamatan (misalnya, deteksi kelelahan pilot dan risiko keselamatan terkait bagi semua penumpang).

Contoh

Dengan persetujuan peserta panggilan, lembaga keuangan merekam panggilan yang dilakukan melalui saluran layanan pelanggan, mentranskripsikannya karena kewajiban dokumentasi hukum, dan juga menganalisisnya untuk tujuan pelatihan. Jika, dalam proses ini, karyawan saluran layanan pelanggan direkam dan emosi mereka dideteksi dengan bantuan AI (misalnya, senang, sedih, lelah, jengkel, tidak termotivasi, dan lain-lain.), ini merupakan penggunaan tanpa izin sesuai dengan Pasal 5 UU AI.

Di sisi lain, evaluasi klasik kuesioner kepuasan karyawan tidak termasuk pengenalan emosi yang tidak diperbolehkan. Dalam kasus ini, otomatisasi biasanya hanya ditujukan pada evaluasi keseluruhan, bukan pada evaluasi kuesioner individual yang sedang diprofilkan. Selain itu, survei karyawan biasanya bersifat anonim.

▪ **Kategorisasi Biometrik**

Terakhir, di sektor keuangan, perhatian harus diberikan pada larangan penggunaan sistem AI untuk kategorisasi biometrik. Pasal 5 ayat 1 huruf g UU AI melarang identifikasi atau inferensi ras, opini politik, keanggotaan serikat pekerja, keyakinan agama atau filosofis, kehidupan seks atau orientasi seksual seseorang berdasarkan kategorisasi menggunakan data biometrik. Pengecualian terbatas hanya ada di bidang penegakan hukum.

Contoh

Jika paspor terlampir (yang berisi data biometrik) digunakan dalam proses pembukaan rekening dengan tujuan untuk menyimpulkan keyakinan rasial atau ideologis, ini merupakan penggunaan AI yang tidak diperbolehkan sesuai dengan Pasal 5 UU AI.

Sistem AI Berisiko Tinggi

Di bidang keuangan dan asuransi, katalog sistem AI berisiko tinggi juga sangat penting. Apa yang memenuhi syarat sebagai AI berisiko tinggi didefinisikan dalam Pasal 6 dan seterusnya UU AI, Lampiran I dan III UU AI. Selain contoh-contoh penting dari penilaian kredit dan evaluasi kredit, sejumlah aplikasi berisiko tinggi dari katalog dalam Lampiran III UU AI dimungkinkan di sektor ini.

Klasifikasi

▪ **Biometrik**

Menurut Pasal 6 ayat 2 UU AI bersamaan dengan No. 1 Lampiran III UU AI, aplikasi biometrik berikut dianggap berisiko tinggi:

- Sistem identifikasi jarak jauh biometrik, kecuali sistem untuk memverifikasi keaslian seseorang;
- Sistem AI yang ditujukan untuk digunakan dalam kategorisasi biometrik berdasarkan atribut atau karakteristik sensitif atau terlindungi berdasarkan inferensi tentang atribut atau karakteristik tersebut;
- Sistem AI yang ditujukan untuk digunakan dalam pengenalan emosi.

Contoh

Penggunaan solusi otentikasi biometrik dengan pengenalan wajah saat membuka rekening bank secara online atau untuk pengecekan login ke rekening bank pribadi bukanlah sistem AI berisiko tinggi menurut Pasal 1 Lampiran III UU AI. Identifikasi biometrik melalui pengenalan wajah pada akhirnya diperlukan untuk memverifikasi bahwa orang tersebut adalah siapa yang mereka klaim. Hal ini juga berlaku untuk pemindai pembuluh darah yang didukung AI yang hanya mengizinkan orang yang berwenang mengakses ruang server. Menurut Pertimbangan 54 UU AI, aplikasi yang tujuan utamanya adalah untuk mengkonfirmasi identitas seseorang untuk mendapatkan akses ke suatu layanan, membuka kunci perangkat, atau mendapatkan akses aman ke suatu tempat harus dikecualikan dari area berisiko tinggi.

▪ **Infrastruktur Kritis**

Menurut Pasal 6 ayat 2 UU AI bersamaan dengan poin 2 Lampiran III UU AI, sistem AI untuk pengelolaan dan pengoperasian infrastruktur digital kritis dianggap sebagai AI berisiko tinggi. “Infrastruktur digital kritis” adalah area yang tercantum dalam poin 8 Lampiran Arahana Ketahanan Infrastruktur Kritis:

- Penyebar node Internet
- Penyedia layanan DNS (kecuali penyebar server nama root)
- Pendaftar nama TLD
- Penyedia layanan komputasi awan
- Penyedia layanan pusat data
- Penyebar jaringan pengiriman konten
- Penyedia layanan kepercayaan
- Penyedia jaringan komunikasi elektronik publik
- Penyedia jaringan komunikasi elektronik, sejauh layanan mereka dapat diakses publik

Sistem AI mendeteksi komponen keselamatan yang digunakan untuk melindungi integritas fisik infrastruktur kritis atau kesehatan dan keselamatan manusia dan properti. Kegagalan dan malfungsi komponen tersebut pada akhirnya dapat menyebabkan risiko langsung (Pertimbangan 50 UU AI).

Contoh

Suatu grup perbankan memiliki anak perusahaan yang menyediakan layanan TI internal di seluruh grup. Grup tersebut mengoperasikan pusat data untuk semua perusahaan operasional. Pusat data tersebut menggunakan sistem AI untuk keamanan kontrol akses. Oleh karena itu, sistem tersebut memenuhi fungsi keamanan dan kegagalan atau malfungsi sistem

AI juga membahayakan kesehatan dan keselamatan orang atau properti. Akses juga dimungkinkan bagi pihak ketiga. Sistem AI ini harus diklasifikasikan sebagai berisiko tinggi sesuai dengan poin 2 Lampiran III (lihat Pertimbangan 55 UU AI).

▪ **Manajemen Ketenagakerjaan dan Personalia**

Selain itu, sistem AI dalam manajemen ketenagakerjaan dan personalia diklasifikasikan sebagai AI berisiko tinggi sesuai dengan Pasal 4 Lampiran III UU AI jika sistem tersebut:

- digunakan untuk perekrutan atau seleksi individu, khususnya untuk menempatkan iklan lowongan kerja yang ditargetkan, untuk menyaring atau memfilter lamaran dan untuk mengevaluasi pelamar;
- digunakan untuk pengambilan keputusan yang memengaruhi ketentuan ketenagakerjaan, promosi dan pemutusan hubungan kerja, untuk menugaskan tugas berdasarkan perilaku individu atau karakteristik atau sifat pribadi, atau untuk memantau dan mengevaluasi kinerja.

Aplikasi ini dapat berdampak signifikan pada individu, privasi mereka, hak-hak karyawan mereka dan hak-hak mendasar mereka atas perlindungan data dan oleh karena itu tunduk pada peraturan yang lebih ketat. Pembatasan ini juga relevan dan harus dipatuhi di sektor keuangan – seperti halnya di semua sektor lainnya.

Contoh

Karena persyaratan khusus sektor, sistem manajemen risiko dan dokumentasi yang cermat diperlukan di banyak bidang. Dalam proses ini, data karyawan juga dapat diproses (misalnya melalui file log untuk memastikan sistem TI yang aman). Jika data tentang karyawan tertentu dari berbagai sumber ini juga digunakan untuk membuat keputusan tentang hubungan kerja, ini umumnya merupakan aplikasi AI berisiko tinggi.

▪ **Akses dan penggunaan layanan dan manfaat dasar swasta dan publik**

Peraturan terpenting untuk sektor keuangan adalah nomor 5 huruf b dan huruf c Lampiran III UU AI:

▪ **Penilaian kredit dan peringkat kredit**

Oleh karena itu, sistem AI yang akan digunakan untuk menilai **kelayakan kredit dan peringkat kredit** individu diklasifikasikan sebagai AI berisiko tinggi. Sistem ini mampu menolak akses individu terhadap sumber daya keuangan atau layanan penting lainnya, seperti perumahan, listrik, dan layanan telekomunikasi (lihat Pertimbangan 58 Peraturan AI). Selain itu, ada risiko tinggi bahwa sistem AI tersebut dapat menyebabkan diskriminasi terhadap individu atau kelompok dan melanggengkan distorsi historis. Karena alasan ini, legislator Uni Eropa telah memilih regulasi yang lebih ketat untuk aplikasi ini.

Namun, ada pengecualian eksplisit untuk penggunaan sistem tersebut untuk **mendeteksi penipuan keuangan**. Sistem ini seharusnya tidak termasuk AI berisiko tinggi. Selain itu, Pertimbangan-pertimbangan tersebut juga tidak ingin mengkualifikasikan sistem AI yang ditujukan untuk tujuan pengawasan guna menghitung persyaratan modal lembaga kredit dan perusahaan asuransi sebagai AI berisiko tinggi (lihat Pertimbangan 58). Menurut pendapat saya, hal terakhir ini tidak

mungkin dilakukan berdasarkan undang-undang karena katalog tersebut hanya menyebutkan penipuan keuangan, tetapi tidak menyebutkan perhitungan persyaratan modal yang diperlukan untuk tujuan pengawasan. Hal ini hanya tampak mungkin dengan **menyangkal status berisiko tinggi sesuai dengan Pasal 6 ayat 3 UU AI** jika tidak dilakukan pembuatan profil.

Contoh

Penilaian kelayakan kredit lembaga kredit dalam rangka pengecekan pemberian pinjaman umumnya termasuk dalam poin 5 huruf b Lampiran III UU AI. Dalam praktiknya, penilaian kredit tidak hanya dilakukan untuk mendeteksi penipuan keuangan, tetapi juga untuk menilai solvabilitas pelanggan. Apakah penilaian kredit berbasis AI terhadap perusahaan terbatas termasuk dalam aplikasi berisiko tinggi masih dipertanyakan. Menurut pendapat saya, berdasarkan redaksi, klasifikasi risiko hanya terbatas pada penilaian "orang perseorangan", bukan badan hukum. Oleh karena itu, menurut pendapat saya, penggunaan AI semacam itu seharusnya tidak diklasifikasikan sebagai berisiko tinggi.

- **Penilaian risiko dan penetapan harga polis asuransi jiwa**

UU AI No. 5 huruf c Lampiran III juga dapat memiliki ruang lingkup penerapan di sektor keuangan. Ketentuan ini mencakup sistem AI yang digunakan untuk **penilaian risiko dan penetapan harga** terkait dengan individu dalam kasus **asuransi jiwa dan kesehatan**. Hal ini menimbulkan risiko tinggi karena penilaian dan penetapan harga yang didukung AI dapat berdampak signifikan pada mata pencaharian masyarakat, yang dapat menyebabkan pengucilan dan diskriminasi finansial.

Contoh

Suatu sistem AI menghitung kondisi polis asuransi jiwa berdasarkan karakteristik individu, khususnya harapan hidup berdasarkan jenis kelamin, gaya hidup, kondisi kesehatan, pendapatan, polis asuransi yang ada, dan lain-lain. Terlepas dari kekhawatiran perlindungan datanya, aplikasi ini dalam hal apa pun harus diklasifikasikan sebagai aplikasi berisiko tinggi sesuai dengan poin 5 huruf c Lampiran III.

Penolakan terhadap Properti Berisiko Tinggi

Karakteristik berisiko tinggi menurut Lampiran III UU AI dapat ditolak sesuai dengan Pasal 6 ayat 3 UU AI jika sistem AI tidak memprofilkan orang perseorangan. Untuk tujuan ini, tidak boleh ada risiko signifikan terhadap kesehatan, keselamatan, atau hak-hak dasar orang perseorangan karena, antara lain, sistem AI tidak memengaruhi hasil pengambilan keputusan secara signifikan. Untuk tujuan ini, salah satu syarat yang ditentukan dalam Pasal 6 ayat 3 UU AI harus dipenuhi.

Contoh

Suatu sistem AI dirancang untuk memproses lamaran yang masuk ke iklan lowongan kerja masing-masing tanpa meninjau atau mengevaluasi isinya. Bentuk kategorisasi ini mewakili **tugas prosedural yang didefinisikan secara sempit** sesuai dengan Pasal 6 ayat 3 huruf a (lihat Pertimbangan 53 UU AI). Hal ini dapat meningkatkan risiko diskriminasi atau distorsi dan memungkinkan keputusan perekrutan yang sepenuhnya manusiawi. Jika hanya dilakukan kategorisasi dan tidak ada pembuatan profil, karakteristik risiko tinggi tersebut dapat

disangkal. Penilaian risiko polis asuransi jiwa yang didukung AI hanya digunakan setelah peninjauan kondisi dan pemrosesan aplikasi yang telah selesai sebelumnya **untuk mengidentifikasi pola pengambilan keputusan atau penyimpangan dari keputusan sebelumnya**. Ini berarti bahwa sistem AI tidak lagi mengandung risiko kerugian finansial atau pengucilan yang diasumsikan dan dapat disangkal sesuai dengan Pasal 6 ayat 2 huruf c UU AI.

Lembaga kredit memperoleh hal-hal berikut untuk peringkat kredit individu pemohon pinjaman untuk berbagai tujuan dari lembaga referensi kredit dan penilaian yang dilakukan oleh lembaga referensi kredit. Sistem ini menganalisis data tersebut dengan dukungan AI menggunakan berbagai kriteria lain (misalnya, pengalaman sendiri dari hubungan pelanggan yang ada, keakuratan atau ketidakkonsistenan informasi yang diberikan, pendapatan rumah tangga, dana sendiri, dan lain-lain.) untuk mendapatkan gambaran yang lebih baik. Dalam hal ini, penilaian lembaga kredit hanyalah salah satu dari banyak **langkah persiapan** dan bukan satu-satunya atau yang utama relevan dengan keputusan. Proses ini memenuhi syarat Pasal 6 ayat 3 huruf d. Namun, jika **pembuatan profil** dilakukan selama penggunaan AI, penolakan sebagai sistem AI berisiko tinggi dikecualikan (lihat Pasal 6 ayat 2 paragraf terakhir UU AI).

Klasifikasi risiko harus didokumentasikan dengan jelas untuk menunjukkan kepatuhan terhadap UU AI.

Interaksi antara Peraturan Keuangan dan UU AI

Jika suatu sistem AI diklasifikasikan sebagai berisiko tinggi, persyaratan yang tercantum dalam Pasal 8 dan seterusnya UU AI harus dipenuhi oleh setiap operator dalam rantai nilai. UU AI memberikan penyederhanaan bagi lembaga keuangan sejauh implementasi beberapa kewajiban dianggap telah dipenuhi atau dapat disederhanakan jika peraturan khusus sektor memberikan persyaratan serupa. Kapan lembaga keuangan dapat merujuk pada **peraturan dan implementasi** yang ada diatur secara eksplisit dalam UU AI, khususnya pada bagian-bagian berikut:

- Persyaratan untuk **sistem manajemen mutu** sesuai dengan Pasal 17 UU AI berlaku untuk penyedia yang merupakan lembaga keuangan dan tunduk pada tata kelola perusahaan internal sesuai dengan peraturan jasa keuangan dianggap telah memenuhi persyaratan jika mereka mematuhi persyaratan peraturan. Ini tidak termasuk kewajiban berdasarkan Pasal 17 ayat. 1. Pasal g UU AI (sistem manajemen risiko), pasal h (pembentukan, implementasi, dan pemeliharaan sistem untuk memantau sistem AI setelah dipasarkan), dan pasal i (pemberitahuan insiden serius) dikecualikan.
- Penyedia yang merupakan lembaga keuangan dan sesuai dengan peraturan perundang-undangan jasa keuangan, memelihara **dokumentasi teknis** sesuai dengan Pasal 18 UU AI sebagai bagian dari dokumentasi sesuai dengan peraturan khusus di sektor keuangan.
- Lembaga keuangan sebagai penyedia atau penyebar dapat menggunakan **log yang dihasilkan secara otomatis** oleh sistem AI berisiko tinggi mereka sesuai dengan Pasal 19 UU AI dan Pasal 26 ayat 6 UU AI sebagai bagian dari dokumentasi dalam arti ketentuan khusus di sektor jasa keuangan.

- Lembaga keuangan sebagai penyebar dapat memenuhi **kewajiban pemantauan** mereka yang ditetapkan dalam Pasal 26 ayat 5 subayat 1 UU AI dengan mematuhi ketentuan tentang aturan, prosedur, atau mekanisme tata kelola perusahaan internal sesuai dengan ketentuan peraturan yang relevan.

Selain itu, Pasal... Pasal 27 ayat 1 UU AI menetapkan bahwa penilaian dampak hak asasi manusia juga diperlukan ketika menggunakan AI berisiko tinggi, khususnya untuk (i) pemberian skor kredit dan penilaian kelayakan kredit dan (ii) penilaian risiko dan penetapan harga polis asuransi (kesehatan dan) jiwa. Hal ini sangat relevan untuk sektor keuangan. Untuk detail tentang penilaian dampak hak asasi manusia, lihat bagian 3.4.

Sistem/Model AI Tujuan Umum

Sistem atau model AI Tujuan Umum yang terintegrasi ke dalam sistem AI juga dapat digunakan di sektor keuangan.

Contoh

Model AI Tujuan Umum dapat digunakan untuk chatbot berbasis teks atau suara, optimasi proses, otomatisasi, atau manajemen pengaduan, misalnya.

Di bidang AI Tujuan Umum, perhatian khusus harus diberikan pada klasifikasi terpisah: AI Tujuan Umum sederhana atau dengan risiko sistematis. Untuk detail tentang klasifikasi sistem dan model AI Tujuan Umum dan kewajiban terkait, lihat bagian 3.7.

Sistem AI Tertentu

Jika perusahaan yang diatur hanya menggunakan sistem AI untuk interaksi langsung dengan orang-orang (tanpa model AI Tujuan Umum), ini dianggap sebagai sistem AI tertentu. Orang-orang yang berinteraksi dengan sistem harus diinformasikan tentang interaksi manusia-mesin, jika tidak sudah jelas bagi orang yang cukup terinformasi dan rasional dengan mempertimbangkan keadaan kasus individu. Untuk chatbot di sektor keuangan, menurut pendapat saya, tidak selalu dapat diasumsikan bahwa sistem yang didukung mesin dapat dikenali dengan jelas karena kontak pribadi secara teratur diasumsikan di sini karena sensitivitas pertanyaan. Untuk detail tentang kewajiban dan batasan transparansi terkait, lihat bagian 3.6.

Kompetensi Otoritas

UU AI mengatur satu atau lebih otoritas untuk pengawasan pasar. Ini dapat digabungkan dengan badan pemberi pemberitahuan. Lembaga mana yang akan ditunjuk sebagai otoritas pengawasan pasar belum jelas (per 19.5.2024) di Jerman dan Austria. UU AI menyerahkan hal ini kepada negara-negara anggota. Namun, untuk sektor keuangan, Pasal 74 ayat 6 UU AI menetapkan bahwa otoritas yang ditunjuk berdasarkan peraturan keuangan nasional bertanggung jawab atas pengawasan pasar terhadap kepatuhan terhadap ketentuan untuk sistem AI berisiko tinggi oleh lembaga keuangan yang diawasi, dengan syarat sistem AI tersebut terkait langsung dengan penyediaan layanan keuangan ini. Di Austria, ini adalah Otoritas Pasar Keuangan (FMA) dan di Jerman adalah Otoritas Pengawasan Keuangan Federal (BaFin). Namun, tanggung jawab yang berbeda dari otoritas dimungkinkan menurut Pasal 74 ayat 7 UU AI, dengan syarat koordinasi antara otoritas terkait dipastikan. Lihat juga bagian 3.9 untuk struktur otoritas dan tugas serta wewenangnya.

Terlepas dari pengawasan pasar berdasarkan Undang-Undang AI, kompetensi yang ada berdasarkan peraturan lain tetap berlaku. Oleh karena itu, pelanggaran Undang-Undang AI juga dapat merupakan pelanggaran terhadap hukum atau peraturan lain dan membuka proses hukum paralel. Hal ini harus diperhitungkan sehubungan dengan potensi risiko saat menggunakan sistem AI dari perspektif tata kelola dan kepatuhan di area yang diatur.

7.3 AI DALAM INDUSTRI ASURANSI

Industri asuransi di Austria memainkan peran sentral dalam melindungi dari risiko dan memastikan stabilitas keuangan penduduk. Ini adalah sistem kompleks yang dicirikan oleh peraturan negara dan menawarkan berbagai macam produk asuransi. Industri asuransi Austria diatur oleh jaringan hukum dan peraturan yang kompleks yang dirancang untuk memastikan bahwa kontrak asuransi transparan, adil, dan mudah dipahami oleh konsumen. Dasar hukum utamanya adalah:

- Undang-Undang Kontrak Asuransi Austria (VVG): VVG adalah hukum utama untuk semua kontrak asuransi di Austria. Undang-undang ini mengatur hak dan kewajiban pemegang polis dan perusahaan asuransi, penyimpulan kontrak, kewajiban untuk membayar manfaat, dan opsi penghentian.
- Kitab Undang-Undang Perdata Austria (ABGB): ABGB berisi ketentuan umum tentang kontrak dan berfungsi sebagai dasar hukum tambahan untuk VVG.
- Undang-Undang Pengawasan Pasar Keuangan Austria (FMAG): FMAG mengatur pengawasan pasar keuangan, termasuk sektor asuransi. Otoritas Pasar Keuangan (FMA) memantau kepatuhan perusahaan asuransi terhadap ketentuan hukum.

Salah satu perkembangan terbaru dalam asuransi adalah integrasi kecerdasan buatan (AI) ke dalam industri asuransi, yang akan merevolusi cara penilaian risiko, perancangan produk, dan pelayanan pelanggan. Jumlah data yang sangat besar yang dihasilkan oleh perusahaan asuransi menyediakan lahan subur untuk penggunaan algoritma AI yang dapat mengenali pola, membuat prediksi, dan mengotomatiskan proses.

AI dapat digunakan di bidang-bidang berikut:

- Penilaian dan prioritas risiko:
 - **Penilaian risiko yang lebih tepat:** Model AI dapat menggunakan data yang luas untuk menganalisis peristiwa historis dan memprediksi risiko di masa depan dengan lebih akurat.
 - **Tarif yang dipersonalisasi:** Dengan menganalisis profil pelanggan individu, produk asuransi yang disesuaikan dapat ditawarkan.
 - **Deteksi penipuan:** Deteksi anomali dan analisis pola membantu mengidentifikasi aktivitas penipuan pada tahap awal.
- **Layanan pelanggan:**
 - **Chatbot dan asisten virtual:** Chatbot yang didukung AI mengambil alih tugas layanan pelanggan rutin dan tersedia sepanjang waktu.
 - **Saran yang dipersonalisasi:** Algoritma AI dapat lebih memahami kebutuhan pelanggan dan memberikan rekomendasi individual.

- **Pemrosesan klaim yang lebih cepat:** Otomatisasi pemberitahuan dan pemrosesan klaim mempercepat proses secara signifikan, misalnya omni:us.
- **Optimalisasi proses:**
 - **Otomatisasi:** Tugas berulang seperti pemrosesan data dan pemeriksaan dokumen dapat diotomatisasi, mengurangi biaya dan meningkatkan efisiensi.
 - **Analisis prediktif:** AI memungkinkan untuk memprediksi peristiwa di masa mendatang dan dengan demikian mengambil tindakan proaktif.

Kecerdasan buatan akan secara permanen mengubah industri asuransi. Perusahaan asuransi yang berinvestasi dalam teknologi AI pada tahap awal dapat memperoleh keunggulan kompetitif dan melayani pelanggan mereka dengan lebih baik.

Contoh aplikasi spesifik berikut ini dihasilkan dari topik yang tercantum:

- **Penyelesaian klaim:** Analisis gambar berbasis AI untuk penilaian kerusakan kendaraan atau bangunan yang cepat dan tepat.
- **Penilaian kredit:** Model AI untuk menilai kelayakan kredit calon pelanggan.
- **Pengembangan produk:** Pengembangan produk asuransi baru berdasarkan data riset pasar yang didukung AI.
- **Loyalitas pelanggan:** Kampanye pemasaran dan penawaran yang dipersonalisasi untuk meningkatkan kepuasan pelanggan, misalnya dengan deepassist.

Tantangan untuk bidang aplikasi ini adalah kualitas data sangat penting untuk akurasi model AI. Selain itu, hasil model AI harus mudah dipahami dan dijelaskan.

Terlepas dari tantangan ini, penggunaan AI dalam industri asuransi menawarkan banyak keuntungan:

- **Peningkatan efisiensi:** otomatisasi proses dan pengurangan aktivitas manual.
- **Pengurangan biaya:** optimalisasi sumber daya dan penghindaran kesalahan.
- **Peningkatan kepuasan pelanggan:** penawaran yang dipersonalisasi dan layanan yang lebih cepat.
- **Model bisnis baru:** pengembangan produk dan layanan inovatif. Tergantung pada sistem AI yang digunakan, perlu dilakukan klasifikasi dalam Undang-Undang AI yang berlaku.

Penilaian Risiko dan Penjaminan Dinamis dalam Asuransi Kesehatan

Contoh

Pelamar dipandu melalui dialog digital interaktif. Jumlah pertanyaan yang diajukan sama dengan yang dibutuhkan dan keputusan penjaminan dibuat segera. Big data dan analitik data memungkinkan untuk mengoptimalkan proses pertanyaan dan menilai risiko berdasarkan beberapa ratus juta tahun asuransi, jauh lebih banyak daripada yang tersedia bagi penilai risiko. Kondisi yang sudah ada sebelumnya pada pelamar dicatat menggunakan alat khusus untuk pencatatan diagnostik yang peka konteks. Penilaian risiko kemudian dilakukan berdasarkan data kesehatan yang tercatat menggunakan sistem penilaian risiko berbasis bukti.

Peran yang relevan

Penyedia adalah perusahaan yang mengembangkan dan menjual sistem AI, dan pengimplementasikan adalah perusahaan yang menggunakan sistem AI dalam bisnisnya.

Klasifikasi sebagai AI berisiko tinggi

Sistem AI tersebut diklasifikasikan sebagai AI berisiko tinggi karena tercantum dalam Lampiran III no. 5 huruf c UU AI, jika sistem AI tersebut dimaksudkan untuk digunakan untuk penilaian risiko dan penetapan harga terkait dengan orang perseorangan dalam kasus asuransi jiwa dan kesehatan. Sistem ini dikategorikan sebagai sistem AI berisiko tinggi sesuai dengan Pasal 6 ayat 2 UU AI. Kewajibannya dapat ditemukan secara rinci di bagian 3.3.2.4.

Klasifikasi sebagai sistem AI berisiko tinggi berarti bahwa persyaratan berikut ini secara khusus harus dipenuhi:

- Sistem manajemen risiko harus dibentuk, diterapkan, didokumentasikan, dan dipelihara sesuai dengan Pasal 9 UU AI.
- Menurut Pasal... 10. UU AI, jika teknik yang digunakan dalam pelatihan model AI dengan data, yang dikembangkan dengan kumpulan data pelatihan, validasi, dan pengujian, harus memenuhi kriteria kualitas yang ditentukan dalam paragraf 2 hingga 5 jika kumpulan data tersebut digunakan.
- Sesuai dengan Pasal 11 UU AI, dokumentasi teknis sistem AI berisiko tinggi harus disiapkan sebelum sistem ini dipasarkan atau dioperasikan dan harus selalu diperbarui.
- Teknologi sistem AI berisiko tinggi harus memungkinkan perekaman peristiwa secara otomatis (selanjutnya disebut sebagai “pencatatan”) sesuai dengan Pasal 12 UU AI selama siklus hidup sistem.
- Sesuai dengan Pasal 13 UU AI, sistem AI berisiko tinggi harus dirancang dan dikembangkan sedemikian rupa sehingga pengoperasiannya cukup transparan untuk memungkinkan pengimplementasian menafsirkan dan menggunakan keluaran sistem dengan tepat.
- Sistem AI berisiko tinggi harus dirancang dan dikembangkan sedemikian rupa sehingga dapat diawasi secara efektif oleh orang perseorangan sesuai dengan Pasal 14 UU AI selama masa penggunaannya, termasuk dengan alat antarmuka manusia-mesin yang sesuai.
- Sesuai dengan Pasal 15 UU AI, sistem AI berisiko tinggi harus dirancang dan dikembangkan untuk mencapai tingkat akurasi, ketahanan, dan keamanan siber yang memadai dan berfungsi secara konsisten dalam hal ini sepanjang siklus hidupnya.

Selain itu, penyedia sistem AI berisiko tinggi khususnya harus mematuhi persyaratan berikut sesuai dengan Pasal 16 UU AI, yaitu:

- a) memastikan bahwa sistem AI berisiko tinggi mereka memenuhi persyaratan yang ditetapkan dalam paragraf 2;
- b) menunjukkan pada sistem AI berisiko tinggi atau, jika ini tidak memungkinkan, pada kemasannya atau dalam dokumentasi yang menyertainya, nama, nama dagang terdaftar atau merek dagang terdaftar dan alamat kontak mereka;
- c) memiliki sistem manajemen mutu yang sesuai dengan Pasal 17 UU AI;
- d) menyimpan dokumentasi yang disebutkan dalam Pasal 18 UU AI;
- e) menyimpan log yang dihasilkan secara otomatis oleh sistem AI berisiko tinggi mereka sesuai dengan Pasal 19 UU AI jika log tersebut berada di bawah kendali mereka;

- f) memastikan bahwa sistem AI berisiko tinggi tersebut menjalani prosedur penilaian kesesuaian yang relevan sesuai dengan Pasal 43 UU AI sebelum dipasarkan atau dioperasikan;
- g) menerbitkan Deklarasi Kesesuaian UE sesuai dengan Pasal 47 UU AI;
- h) menempelkan tanda CE pada sistem AI berisiko tinggi atau, jika ini tidak memungkinkan, pada kemasannya atau dalam dokumentasi yang menyertainya untuk menunjukkan kesesuaian dengan Peraturan ini sesuai dengan Pasal 48 UU AI;
- i) mematuhi kewajiban pendaftaran yang ditetapkan dalam Pasal 49 ayat 1 UU AI;
- j) mengambil tindakan korektif yang diperlukan dan memberikan informasi yang dibutuhkan berdasarkan Pasal 20 UU AI;
- k) menunjukkan, berdasarkan permintaan yang beralasan dari otoritas kompeten nasional, bahwa sistem AI berisiko tinggi mematuhi persyaratan yang ditetapkan dalam paragraf 2;
- l) memastikan bahwa sistem AI berisiko tinggi memenuhi persyaratan aksesibilitas sesuai dengan Arahan (EU) 2016/2102 dan (EU) 2019/882.

Keputusan tentang orang

Menurut Pasal 86 UU AI, orang-orang yang terkena dampak keputusan yang diambil oleh pengimplementasi berdasarkan keluaran sistem AI berisiko tinggi yang tercantum dalam Lampiran III UU AI, dengan pengecualian sistem yang tercantum dalam nomor 2 Lampiran tersebut, dan yang memiliki efek hukum atau secara signifikan memengaruhi mereka sedemikian rupa sehingga mereka menganggapnya merugikan kesehatan, keselamatan, atau hak-hak fundamental mereka, berhak untuk menerima penjelasan yang jelas dan bermakna dari pengimplementasi tentang peran sistem AI dalam proses pengambilan keputusan dan tentang elemen utama keputusan yang diambil.

Dalam kasus yang dimaksud, tidak ada keputusan langsung yang dibuat tentang kesehatan (misalnya, penentuan metode pengobatan tertentu), tetapi keputusan dibuat tentang kemungkinan kesimpulan polis asuransi kesehatan atau persyaratannya. Interpretasi luas dari Mahkamah Eropa dapat mengarah pada penerapan Pasal 86 UU AI.

Bagaimanapun, Pasal 22 GDPR berlaku karena keputusan otomatis dibuat berdasarkan kasus per kasus. Oleh karena itu, persyaratan dan langkah-langkah yang tercantum dalam Pasal 22 ayat 2 GDPR harus dipatuhi (lihat juga Bab 4, Perlindungan data).

7.4 AI DAN PELAPORAN PELANGGARAN

Arahan Pelapor Pelanggaran Uni Eropa 2019/1937 (singkatnya Arahan Pelapor Pelanggaran) telah berlaku di semua negara anggota sejak Desember 2023 (akhir masa transisi) untuk organisasi dengan lebih dari 50 karyawan dan administrasi publik. Arahan ini dimaksudkan untuk meningkatkan kondisi bagi pelapor pelanggaran di seluruh Uni Eropa dan menawarkan mereka lebih banyak keamanan (Pasal 1 Arahan Pelapor Pelanggaran). Undang-undang tersebut menetapkan saluran pelaporan yang aman baik di dalam organisasi maupun kepada badan eksternal untuk menjamin anonimitas dan keamanan pelapor pelanggaran saat

menyampaikan laporan. Undang-undang tersebut juga menetapkan sanksi untuk mencegah pembalasan terhadap pelapor pelanggaran.

Bab ini membahas dampak ketentuan Undang-Undang AI terhadap kepatuhan terhadap hukum perlindungan pelapor pelanggaran masing-masing Negara Anggota karena setiap Negara Anggota harus mentransposisikan Arahan Uni Eropa ini ke dalam hukum lokal. Hukum ini sekarang memainkan peran sentral dalam organisasi karena menawarkan perlindungan kepada orang-orang yang melaporkan pelanggaran terhadap ketentuan hukum tertentu. Cakupan penerapannya lebih luas di beberapa negara daripada di negara lain. Direktif Uni Eropa sendiri hanya menetapkan cakupan minimum sepuluh kategori (lihat tabel).

Saluran pelaporan internal sesuai dengan direktif Uni Eropa pada dasarnya mendorong budaya keterbukaan dan rasa tanggung jawab dalam organisasi, yang sangat penting untuk kepatuhan dan pemantauan peraturan yang efektif. Dalam ekonomi modern, kepatuhan lebih dari sekadar mematuhi persyaratan hukum. Hal ini telah menjadi bagian integral dari tata kelola perusahaan dan manajemen risiko.

Undang-Undang AI Uni Eropa sekarang akan menjadi cakupan material lebih lanjut dari Direktif Pelapor Pelanggaran untuk memastikan bahwa pengembangan, implementasi, dan pengoperasian kecerdasan buatan dilakukan secara bertanggung jawab dan sesuai dengan hukum dan standar etika yang berlaku di perusahaan.

Pasal 87 UU AI – Pelaporan Pelanggaran dan Perlindungan Pelapor

Arahan Pelapor berlaku untuk pelaporan pelanggaran Peraturan ini dan perlindungan bagi orang yang melaporkan pelanggaran tersebut. Undang-undang perlindungan pelapor pelanggaran di setiap Negara Anggota Uni Eropa mengambil langkah penting menuju penguatan transparansi dan integritas dalam bisnis dan sektor publik dengan mendorong dan melindungi para pelapor pelanggaran.

Tabel berikut memberikan gambaran umum tentang persyaratan (minimum) dari Arahan Pelapor Pelanggaran:

Kategori/Pasal	Isi Arahan (UE) 2019/1937
Tujuan Arahan (Pasal 1 Arahan Pelapor Pelanggaran)	Arahan Pelapor Pelanggaran UE bertujuan untuk melindungi orang-orang yang melaporkan pelanggaran hukum UE. Arahan ini dimaksudkan untuk memastikan bahwa pelapor pelanggaran dapat melaporkan tanpa takut akan pembalasan.
Lingkup materi (Pasal 2 Arahan Pelapor Pelanggaran)	Direktif ini berlaku untuk laporan internal dan eksternal serta pengungkapan publik yang berkaitan dengan pelanggaran yang memengaruhi kepentingan keuangan Uni Eropa atau bidang lain seperti: ▪ Pengadaan publik ▪ Layanan keuangan ▪ Produk keuangan dan pasar keuangan, pencegahan pencucian uang dan pendanaan terorisme

	▪ Keamanan dan kesesuaian produk ▪ Keselamatan jalan ▪ Perlindungan lingkungan ▪ Perlindungan radiasi ▪ Keamanan pangan dan pakan, kesehatan hewan dan kesejahteraan hewan ▪ Kesehatan masyarakat ▪ Perlindungan data ▪ Negara-negara anggota dapat memperluas cakupan materiil!
Langkah-langkah perlindungan (Pasal 6 dan 19 Arahan Pelapor Pelanggaran)	Pelapor pelanggaran yang bertindak sesuai hukum dilindungi dari pemecatan, penurunan pangkat, dan bentuk pembalasan lainnya. Tindakan terlarang lainnya meliputi: ▪ Pemindahan tugas atau perubahan tempat kerja ▪ Pengurangan gaji ▪ Perubahan jam kerja ▪ Penolakan untuk berpartisipasi dalam pelatihan lanjutan ▪ Penilaian kinerja negatif atau pemberian referensi buruk ▪ Tindakan disiplin, paksaan, intimidasi ▪ Perundungan atau pengucilan ▪ Diskriminasi ▪ Perlindungan ini juga mencakup orang-orang terkait dan pihak ketiga yang mendukung.
Pembentukan saluran pelaporan internal (Pasal 7–9 Arahan tentang Pelapor Pelanggaran)	Badan hukum swasta dengan lebih dari 50 karyawan atau dengan omset tahunan lebih dari 10 juta euro wajib membuat saluran pelaporan internal. Saluran ini harus melindungi kerahasiaan pelapor dan memungkinkan mereka untuk tetap anonim. Selain itu, badan hukum di sektor publik dengan > 50 karyawan: ▪ Kantor administrasi negara ▪ Administrasi dan departemen regional ▪ Badan hukum publik lainnya ▪ Kotamadya dengan > 10.000 penduduk atau > 50 karyawan
Prosedur pelaporan (Pasal 9 Arahan Pelapor Pelanggaran)	Laporan harus dapat disampaikan dalam bentuk tertulis atau lisan, atau keduanya. Selain itu, pertemuan tatap

	muka harus dimungkinkan dalam jangka waktu yang wajar atas permintaan pelapor.
Kewajiban untuk menanggapi (Pasal 9 Arahan Pelapor Pelanggaran)	Organisasi harus menanggapi laporan dalam batas waktu yang ditentukan. Konfirmasi penerimaan harus dikirim dalam waktu tujuh hari dan deskripsi tindakan tindak lanjut dalam waktu tiga bulan.
Laporan eksternal dan pengungkapan publik (Pasal 10–15 Arahan Pelapor Pelanggaran)	Jika saluran pelaporan internal tidak ada atau tidak berfungsi, atau jika laporan internal tidak mungkin memberikan solusi (misalnya, jika ada ancaman langsung terhadap kepentingan publik atau risiko pembalasan), pelapor dapat beralih ke otoritas eksternal. Jika tidak ada tanggapan, pelapor dapat mempublikasikan informasi tersebut.

Pelapor pelanggaran hanya dilindungi (Pasal 6 Arahan Pelapor Pelanggaran) jika mereka memiliki alasan yang wajar untuk percaya bahwa informasi yang dilaporkan tentang pelanggaran itu benar pada saat pelaporan dan bahwa informasi ini termasuk dalam ruang lingkup Arahan tersebut. Menurut Pasal 23 Arahan Pelapor Pelanggaran, Negara Anggota harus memberlakukan sanksi yang efektif, proporsional, dan bersifat mencegah terhadap orang atau badan hukum yang:

- Menghalangi atau mencoba menghalangi laporan
- Melakukan pembalasan terhadap pelapor pelanggaran
- Memulai proses hukum yang jahat terhadap pelapor pelanggaran
- Melanggar kewajiban untuk menjaga kerahasiaan identitas pelapor pelanggaran

Apa yang Perlu Dilakukan?

Jika suatu perusahaan telah menerapkan saluran pelaporan internal, maka sekarang harus diperiksa apakah cakupan penerapan Undang-Undang AI yang diperluas sudah termasuk dalam kategori dan deskripsi sistem pelaporan pelanggaran atau harus dilengkapi:

1. Penambahan kategori saluran pelaporan internal
2. Melengkapi deskripsi saluran pelaporan internal (misalnya, teks bantuan, deskripsi fakta, contoh potensi pelanggaran, dan lain-lain.)
3. Penunjukan seseorang yang bertanggung jawab untuk memproses potensi pemberitahuan berdasarkan Undang-Undang AI
4. Perluasan alur kerja/proses yang telah ditentukan di perusahaan
5. Perluasan kebijakan pelaporan pelanggaran internal
6. Perluasan pelatihan dan materi pelatihan
7. Perluasan deskripsi kepatuhan internal (misalnya, teks dan contoh di intranet, dokumen orientasi, teks dalam kontrak kerja atau perjanjian kerja, dan lain-lain.)
8. Perluasan pelaporan untuk memasukkan kategori Undang-Undang AI

Perlu dicatat bahwa cakupan penerapan materiil dapat berbeda dari satu Negara Anggota ke Negara Anggota lainnya. Selain itu, penggunaan AI juga dapat termasuk dalam cakupan Arahan

Pelaporan Pelanggaran melalui cara-cara tidak langsung, misalnya jika data pribadi diproses oleh AI.

Pelapor Pelanggaran untuk Kategori AI

Seorang pelapor pelanggaran yang melaporkan kesalahan atau perilaku tidak etis terkait penggunaan AI dalam suatu organisasi dilindungi oleh Arahan Uni Eropa 2019/1937. Laporan tersebut dapat menyangkut pengembangan dan implementasi sistem AI serta penggunaan dan dampaknya.

Dengan meningkatnya penggunaan AI di perusahaan dan kemampuan sistem AI, risiko bahwa teknologi tersebut tidak memenuhi semua persyaratan hukum atau disalahgunakan juga meningkat. Hal ini pada gilirannya meningkatkan kebutuhan akan pelapor pelanggaran untuk menarik perhatian pada perilaku yang berpotensi berbahaya atau ilegal.

Contoh Laporan Pelapor Pelanggaran dalam Konteks Undang-Undang AI

Andra bekerja di departemen SDM sebuah perusahaan menengah yang sedang memperkenalkan sistem berbasis AI baru untuk mengevaluasi lamaran pekerjaan. Sistem ini dirancang untuk meningkatkan efisiensi proses rekrutmen dan membantu mengidentifikasi talenta terbaik. Selama bekerja dengan sistem tersebut, Andra memperhatikan bahwa meskipun sistem tersebut mengidentifikasi banyak kandidat yang berkualitas, sistem tersebut melewatkan sejumlah besar pelamar dengan resume atau jalur karier yang tidak konvensional yang berpotensi membawa keterampilan dan perspektif berharga bagi organisasi.

Andra menyadari bahwa mengabaikan kandidat-kandidat ini dapat melemahkan kekuatan inovatif dan keragaman perusahaan dalam jangka panjang. Khawatir tentang potensi masalah tersebut, Andra pertama-tama menghubungi tim proyek yang bertanggung jawab untuk mengimplementasikan sistem AI. Dia menyarankan untuk mengadaptasi model tersebut sehingga dapat mengevaluasi jalur karier yang tidak konvensional dengan lebih baik. Namun, tim proyek enggan menerima saran Andra, karena khawatir penyesuaian tambahan dapat melebihi anggaran proyek dan menunda jadwal.

Setelah kekhawatirannya tidak ditanggapi oleh tim proyek, Andra memutuskan untuk melaporkan masalah tersebut melalui saluran pelaporan pelanggaran internal. Dalam laporannya, ia menekankan tidak hanya kekhawatiran jangka pendek terkait keuangan dan waktu, tetapi juga manfaat jangka panjang dari pelacakan bakat yang lebih komprehensif bagi perusahaan.

Manajemen menanggapi saran Andra dengan serius dan mengakui pentingnya strategis dari sarannya. Mereka menugaskan tim ilmuwan data dan spesialis SDM untuk merevisi sistem AI sesuai dengan saran tersebut. Penyesuaian tersebut menghasilkan sistem penilaian yang lebih baik yang dapat mengenali dan memasukkan lebih banyak variasi bakat, sehingga meningkatkan kualitas dan keragaman karyawan baru.

Perusahaan mendapat manfaat yang sangat besar dari pendekatan proaktif Andra: kualitas dan keragaman karyawan baru meningkat dan perusahaan dipandang sebagai pemberi kerja yang progresif dan menarik. Inisiatif Andra menunjukkan bagaimana pelaporan pelanggaran tidak hanya berfungsi untuk mengungkap keluhan, tetapi juga untuk mendorong perubahan konstruktif di dalam perusahaan dan memastikan keberhasilan jangka panjangnya.

Ada beberapa alasan mengapa pelaporan pelanggaran (whistleblowing) dapat menjadi lebih penting di bidang AI:

- Meningkatnya jumlah persyaratan regulasi untuk sistem AI. Tidak hanya di Eropa, tetapi juga di AS dan Asia, semakin banyak undang-undang dan peraturan yang harus dipatuhi perusahaan.
- Dengan meningkatnya penggunaan AI, kontrol regulasi atas penggunaannya juga meningkat. Otoritas pengatur seperti Securities and Exchange Commission (SEC) dan Departemen Kehakiman AS (DOJ) telah menetapkan program untuk memantau dan menegakkan peraturan terkait AI. Undang-Undang AI juga akan menetapkan otoritas pengawas nasional di Uni Eropa.
- Di Eropa, otoritas perlindungan data nasional juga semakin memperhatikan penggunaan data yang sesuai dengan GDPR saat melatih AI dan dalam penggunaan produktif.
- Dengan implementasi teknologi AI, nilai-nilai yang berasal dari data yang dihasilkan dalam proses masa lalu juga didigitalisasi. Hal ini meningkatkan persyaratan untuk keputusan etis yang perlu dibuat selama proyek AI. Namun, tidak semua orang yang terlibat dalam proyek tersebut menyadari bahwa mereka hanya dapat memengaruhi hasil AI di masa depan dengan memilih data yang tepat. Kelalaian dalam konteks ini dapat menyebabkan proyek gagal dan dapat memicu laporan internal.

Ketika karyawan tahu bahwa mereka dapat dengan aman menunjukkan tantangan dalam proyek AI tanpa takut akan pembalasan, mereka merasa termotivasi untuk berbicara secara terbuka tentang masalah dan peluang untuk perbaikan. Hal ini dapat mengarah pada komunikasi internal yang lebih baik dan pendekatan yang lebih proaktif terhadap masalah kepatuhan, sehingga menyelamatkan perusahaan dari denda.

Informasi rahasia juga dapat memberikan wawasan berharga tentang kerentanan dan risiko dalam sistem AI yang ada yang mungkin tidak terdeteksi. Informasi ini sangat penting untuk mengubah proses sebelum dapat menyebabkan kerugian atau meningkatkan efisiensi dan keamanan aplikasi AI secara keseluruhan.

Contoh Laporan Pelapor Pelanggaran untuk AI Berisiko Tinggi

Saya ingin menarik perhatian Anda pada masalah etika serius yang muncul dalam penggunaan sistem AI kami untuk diagnosis medis. Sistem Diagnosis AI v2.3 saat ini digunakan di beberapa rumah sakit untuk membantu diagnosis penyakit. Meskipun sistem ini secara resmi memenuhi persyaratan Undang-Undang AI, saya menemukan bahwa sistem ini secara sistematis mendiskriminasi kelompok pasien tertentu.

Diagnostic AI v2.3 menunjukkan akurasi yang jauh lebih rendah dalam mendiagnosis penyakit pada pasien dari etnis tertentu. Hal ini menyebabkan diagnosis yang salah atau penundaan pengobatan, yang dapat memiliki konsekuensi kesehatan yang serius bagi pasien-pasien ini. Sistem AI tidak memberikan transparansi yang cukup tentang proses pengambilan keputusan, dan dokter serta staf medis tidak menerima informasi yang jelas tentang bagaimana diagnosis tertentu dibuat. Hal ini menyulitkan untuk mengenali kesalahan dan mempertanyakan atau memperbaiki hasilnya. Mohon selidiki masalah ini dan perbaiki.

Dengan menciptakan lingkungan yang mendukung pelaporan pelanggaran, perusahaan tidak hanya dapat lebih baik mematuhi standar hukum dan etika, tetapi juga memperkuat daya saing dan daya inovasi mereka sendiri.

Bidang Penerapan AI dalam Implementasi Arahan Pelaporan Pelanggaran

Salah satu kasus penggunaan AI tertentu adalah platform pelaporan pelanggaran yang didukung AI yang menawarkan solusi inovatif kepada perusahaan untuk menangani keluhan secara lebih efisien dan merespons laporan dengan lebih cepat. Dengan menggabungkan berbagai tindakan dan teknik otomatis, perusahaan dapat memperkuat program kepatuhan dan etika mereka serta mempromosikan budaya perusahaan yang transparan dan dapat dipercaya.

Definisi Tugas

Implementasi platform pelaporan pelanggaran di mana beberapa tugas penting diambil alih oleh AI untuk meminimalkan tindakan manual yang memakan waktu. Sistem pelaporan internal ini harus mampu memenuhi semua persyaratan hukum dan membantu pelapor pelanggaran merasa aman dan mengatasi masalah secara internal terlebih dahulu sebelum memberi tahu badan eksternal.

Tantangan dalam Proses Pelaporan Pelanggaran

Platform pelaporan pelanggaran tradisional sering dihadapkan dengan sejumlah besar laporan yang perlu ditinjau secara manual. Hal ini dapat menyebabkan penundaan dan penilaian yang tidak konsisten. Ada juga risiko bahwa kerahasiaan pelapor pelanggaran tidak cukup terlindungi, terutama jika manajer dituduh atau nama karyawan muncul dalam laporan. Selain itu, laporan sering diterima pada saat karyawan tidak online (di luar jam sibuk) dan oleh karena itu tidak dapat merespons dengan cepat terhadap komunikasi dengan pelapor pelanggaran.

Oleh karena itu, sistem yang didukung AI harus membantu mengatasi tantangan berikut:

- Menilai relevansi dan keakuratan laporan yang masuk sesuai dengan persyaratan hukum sebelum pelapor pelanggaran secara resmi mengirimkan laporan dan memberi tahu pelapor pelanggaran bahwa perlindungan hukum hanya berlaku untuk sejumlah kriteria terbatas.
- Mengevaluasi kualitas laporan dalam hal cakupan dan detail konten serta memberikan informasi tentang informasi apa yang masih diperlukan untuk memulai analisis secara efisien.
- Mengusulkan tindakan yang tepat dan pertanyaan lanjutan berdasarkan kasus-kasus yang telah dianalisis sebelumnya.
- Mengidentifikasi apakah nama-nama petugas pelapor pelanggaran disertakan dalam laporan dan tidak memberikan akses kepada mereka terhadap laporan-laporan tersebut untuk memastikan pemrosesan yang independen.
- Mengidentifikasi apakah para eksekutif dari lingkaran atas dituduh dan hanya menugaskan laporan-laporan ini kepada petugas tertentu.

Tantangan dalam Proyek AI

Proyek pelaporan pelanggaran berbasis AI menghadirkan sejumlah tantangan khusus, terutama terkait pelatihan model AI dan pengumpulan data yang cukup dan representatif untuk pemrosesan kasus. Beberapa tantangan utama adalah:

- **Jumlah pesan yang cukup:** Sejumlah besar data diperlukan untuk melatih model AI, seringkali beberapa ribu. Dalam konteks pelaporan pelanggaran, sulit untuk mengumpulkan jumlah dan variasi kasus yang cukup untuk melatih model yang kuat. Banyak perusahaan mungkin hanya memiliki beberapa kasus yang terdokumentasi, dan ini seringkali bersifat rahasia, yang semakin membatasi akses ke data ini.
- **Kualitas data:** Kualitas data yang tersedia untuk pelatihan sangat penting untuk keberhasilan proyek. Data yang hilang, tidak lengkap, atau tidak konsisten dapat berdampak negatif pada kinerja model. Namun, laporan yang diproses di masa lalu seringkali tidak didokumentasikan secara standar.
- **Pemetaan berbagai kasus:** Model AI harus mampu mengenali dan memproses berbagai skenario pelaporan pelanggaran. Ini termasuk berbagai jenis pelanggaran (misalnya, penyimpangan keuangan, pelanggaran etika, pelanggaran lingkungan). Jika pelatihan didasarkan pada sejumlah kasus yang terbatas, model mungkin kesulitan untuk merespons dengan tepat terhadap kasus baru atau langka.
- **Bias dan keadilan:** Ada risiko bahwa data pelatihan mungkin mengandung bias atau distorsi sistematis lainnya yang memengaruhi prediksi model. Jika jenis perilaku buruk tertentu atau kelompok orang tertentu terlalu banyak atau terlalu sedikit terwakili dalam data, hal ini dapat menyebabkan kinerja yang tidak seimbang.
- **Persyaratan perlindungan data dan kerahasiaan laporan:** Karena laporan whistleblowing sering kali berisi informasi pribadi atau sangat sensitif, merupakan tantangan untuk menggunakan data ini untuk pelatihan model AI tanpa melanggar GDPR atau peraturan perlindungan data lainnya, misalnya karena mantan whistleblower tidak ingin memberikan persetujuan mereka untuk pelatihan AI. Teknik anonimisasi dapat membantu, tetapi perlu diterapkan dengan hati-hati untuk memastikan bahwa data tersebut masih berguna untuk pelatihan.
- **Kompleksitas model:** Kompleksitas model AI untuk aplikasi pelaporan pelanggaran dapat menjadi tantangan, karena model-model ini harus mampu mengenali tidak hanya pola-pola sederhana tetapi juga hubungan dan anomali kompleks yang dapat mengindikasikan pelanggaran.
- **Kompetensi tim proyek:** Proyek AI dilakukan secara berbeda dari proyek perangkat lunak berbasis aturan karena fokusnya sangat tertuju pada pengetahuan domain dan kesesuaian data. Hal ini harus tercermin dalam tim proyek, dan mereka yang terlibat harus memiliki tingkat pengetahuan minimum tentang teknik AI, manajemen data, etika, dan persyaratan hukum.

Pemilihan dan kuantitas data khususnya akan menimbulkan tantangan saat mengimplementasikan proyek.

Keunggulan Aplikasi Pelaporan Pelanggaran Berbasis AI

Namun, memproses informasi dengan dukungan AI memiliki sejumlah keunggulan yang perlu dipertimbangkan dan ditimbang dengan lebih cermat:

- Peningkatan efisiensi: Evaluasi dan prioritas pemberitahuan secara otomatis mengurangi upaya manual dan mempercepat proses respons.
- Peningkatan kualitas dalam pemrosesan laporan: Penilaian laporan yang konsisten dan objektif melalui analisis yang didukung AI (AI in the Loop).
- Perlindungan orang: Anonimitas dan kerahasiaan orang yang disebutkan dalam laporan yang diajukan dapat ditingkatkan.
- Pengambilan keputusan yang lebih baik: Rekomendasi tindakan dan prioritas yang beralasan mendukung tim kepatuhan dalam pemrosesan laporan yang efektif.
- Pencegahan konflik: Mencegah petugas mengakses pesan di mana mereka sendiri disebutkan dan penugasan pesan sensitif yang ditargetkan.

Bahkan di perusahaan yang hanya menerima beberapa laporan per tahun, penggunaan solusi pelapor pelanggaran berbasis AI yang telah dilatih sebelumnya akan menguntungkan, karena orang perlu terus dilatih dalam penanganan informasi yang dilaporkan dengan benar sehingga semua persyaratan hukum terpenuhi secara andal selama analisis. Sistem AI dapat membimbing orang di sini sehingga tidak terjadi kesalahan.

Penilaian Risiko untuk Kelompok Sasaran

Orang-orang berikut termasuk di antara mereka yang terpengaruh oleh sistem pelaporan pelanggaran dan harus dipertimbangkan dalam proyek AI sehubungan dengan risiko spesifik:

- **Pelapor pelanggaran:** Dengan diperkenalkannya sistem AI, harus dipastikan bahwa nama dan informasi apa pun yang merujuk pada orang tersebut diperlakukan secara rahasia.
- **Orang yang disebutkan dalam laporan:** Dengan diperkenalkannya sistem AI, harus dipastikan bahwa nama, referensi informasi yang mengarah pada orang tersebut dan status mereka dalam laporan (misalnya saksi atau pelaku potensial) diperlakukan secara rahasia dan juga tidak digunakan untuk pelatihan AI lebih lanjut.
- **Tim kepatuhan:** Kinerja orang-orang yang bertanggung jawab atas pemrosesan tidak boleh digunakan untuk mengukur atau menilai kinerja.

Prosedur Kasus Penggunaan Pelaporan Pelanggaran

Proses dan fungsi berikut dapat didukung oleh platform pelaporan pelanggaran berbasis AI yang bekerja sama dengan tim kepatuhan:

1. Seseorang mengirimkan laporan yang menunjukkan kemungkinan pelanggaran di departemen tertentu.
 - Jika laporan dikirimkan atas nama, AI dapat mengenali nama tersebut dan menganonimkannya untuk analisis internal.
2. AI menganalisis pemberitahuan dan menilai apakah relevan sesuai dengan persyaratan hukum dan apakah isi pemberitahuan tersebut cukup untuk memulai analisis secara efisien.

- Jika laporan tidak memenuhi salah satu kriteria hukum, pelapor akan diberitahu, karena perlindungan hukum tidak dijamin dalam kasus ini. Ia kemudian dapat menarik laporan tersebut.
 - Jika konten penting tidak termasuk dalam laporan, AI secara otomatis meminta informasi lebih lanjut dari orang yang memberikan informasi tersebut.
 - Informasi kunci diidentifikasi dalam pemberitahuan dan diberikan untuk penyimpanan dalam manajemen kasus. Ini dapat mencakup, misalnya, hal-hal berikut: Nama-nama pelaku potensial, nama departemen, lokasi, tanggal, total, dan lain-lain.
3. Sistem memberi tahu orang yang tepat di tim kepatuhan untuk memproses laporan tersebut.
 - Ini memastikan bahwa karyawan yang namanya disebutkan dalam laporan tidak memiliki akses ke laporan tersebut.
 - AI hanya dapat menetapkan laporan yang berkaitan dengan manajer tingkat atas kepada administrator tertentu.
 - Kategori pelaporan yang berbeda dapat ditugaskan kepada orang yang berbeda di tim kepatuhan.
 4. Sistem AI menghasilkan rekomendasi untuk investigasi internal sehingga tim kepatuhan dapat mengambil tindakan segera.
 - Berdasarkan investigasi yang telah dilakukan di masa lalu, AI mengusulkan prosedur audit yang tepat untuk klarifikasi.
 5. AI dapat mendukung komunikasi antara staf kepatuhan dan pelapor dengan mengevaluasi isi laporan dan secara otomatis menghasilkan pertanyaan lanjutan.
- Oleh karena itu, sistem AI dapat mendukung orang dalam memproses berbagai tugas, terutama dalam hal menetapkan, menyusun, dan mengelompokkan informasi dengan benar, serta merespons laporan dengan cepat saat pelapor sedang online.

Penggunaan Teknik Digital dalam Kasus Pelaporan Pelanggaran

Teknik AI berikut dapat digunakan dalam proyek AI ini:

Referensi	Fungsi	Fungsi Non-AI	Fungsionalitas AI	Teknik AI	Fitur Keamanan TI	Kelompok Orang yang Terdampak
1	Portal penerimaan dan anonimisasi	Portal web aman untuk pengajuan laporan (anonim)	Anonimisasi data pribadi untuk perlindungan identitas	Pengenalan Entitas Bernama (NER), penyamaran nama menggunakan tempat penampung	Enkripsi, anonimisasi data	Indikator
2	Analisis konten	Tinjauan dan ekstraksi informasi yang relevan	Analisis dan ekstraksi informasi relevan dari teks pesan	Pemrosesan Bahasa Alami (NLP), Pengenalan Entitas Bernama (NER)		Tim Kepatuhan
2	Penilaian relevansi dan akurasi	Penilaian manual atas relevansi dan	Penilaian otomatis relevansi dan	Pembelajaran mesin, sistem berbasis aturan	Pemilihan data	Tim Kepatuhan

		keakuratan hukum	akurasi sesuai dengan persyaratan hukum		pelatihan yang baik	
2	Evaluasi kualitas pesan	Analisis manual atas tingkat detail dan konsistensi pesan	Evaluasi kualitas laporan dalam hal cakupan dan detail konten	Pemrosesan Bahasa Alami (NLP), pengenalan pola		Tim Kepatuhan
3	Deteksi konflik dan kerahasiaan	Pemeriksaan manual untuk konflik dan kerahasiaan	Pengenalan nama orang tertentu dalam pesan dan pencegahan akses mereka, penugasan pesan sensitif	Pengenalan Entitas Bernama (NER), sistem berbasis aturan	Mekanisme kontrol akses, pemeriksaan kerahasiaan	Tim Kepatuhan
4	Rekomendasi tindakan dan tindak lanjut	Pembuatan manual rekomendasi tindakan dan pertanyaan lainnya	Pembuatan otomatis rekomendasi tindakan dan pertanyaan spesifik untuk tindak lanjut	Pohon keputusan, sistem berbasis aturan		Tim Kepatuhan
5	Sistem komunikasi dan pemberitahuan	Pemantauan dan pemberitahuan secara real-time kepada pengambil keputusan yang relevan	Pemberitahuan otomatis dan pemantauan serta analisis konten pesan secara real-time	Pemrosesan Bahasa Alami (NLP), Sistem Pemberitahuan Otomatis	Enkripsi	Tim Kepatuhan, pelapor pelanggaran

Konsep ini dimaksudkan sebagai proposal dan hanya mewakili dasar untuk proyek AI. Namun, fungsi-fungsi tersebut juga dapat diimplementasikan menggunakan teknologi lain.

Pengembangan dan Implementasi Lebih Lanjut

Fase-fase berikut harus terus diimplementasikan dalam proyek AI setelah AI dikembangkan:

- **Fase percontohan:** Pengenalan sistem AI di area-area terpilih di perusahaan untuk memvalidasi dan menyempurnakan fungsionalitasnya. Kriteria harus ditentukan terlebih dahulu.
- **Penskalaan:** Setelah fase percontohan yang sukses (sesuai dengan kriteria yang ditentukan), perluasan ke seluruh perusahaan.
- **Peningkatan berkelanjutan:** Pemantauan AI secara berkala (peninjauan hasil dan penilaian akurasi oleh pengguna domain) dan adaptasi model dan sistem AI berdasarkan umpan balik dan temuan baru.

Kasus penggunaan ini menggambarkan bagaimana AI dapat diintegrasikan ke dalam platform pelaporan pelanggaran untuk meningkatkan kualitas dan efisiensi pemrosesan laporan dan dengan demikian memperkuat integritas dan etika perusahaan. Jelas juga bahwa pemrosesan bersama oleh AI dan manusia memberikan manfaat terbesar dan meminimalkan risiko.

7.5 EVOLUSI AI DALAM HUBUNGAN KERJA

Hukum ketenagakerjaan Austria mengatur hubungan antara pengusaha dan karyawan. Hukum ini mencakup berbagai topik, mulai dari pembentukan hubungan kerja hingga pengakhirannya. Sumber hukum ketenagakerjaan terpenting di Austria adalah:

- **Undang-undang:** Undang-undang terpenting dalam hukum ketenagakerjaan Austria adalah **Undang-Undang Karyawan (Ange-stelltenengesetz – AngG)**. Selain itu, ada sejumlah undang-undang lain yang relevan dengan hukum ketenagakerjaan, misalnya Kitab Undang-Undang **Perdata Austria (Allgemeines Bürgerliches Ge-setzbruch – ABGB)**, Kitab Undang-Undang Industri (**Gewerbeordnung – GewO**), dan lain-lain.
- **Perjanjian kolektif:** Perjanjian kolektif adalah kontrak antara perwakilan karyawan (serikat pekerja) dan perwakilan pengusaha yang berlaku untuk industri atau profesi tertentu. Perjanjian ini biasanya menetapkan upah, jam kerja, dan kondisi kerja lainnya.
- **Perjanjian kerja:** Perjanjian perusahaan adalah kontrak antara pemberi kerja dan dewan pekerja perusahaan. Perjanjian ini mengatur hal-hal khusus perusahaan, misalnya jam kerja, cuti, dan waktu istirahat.
- **Kontrak kerja individu:** Kontrak kerja individu adalah kontrak antara pemberi kerja dan karyawan individu. Kontrak ini mengatur kondisi kerja individu karyawan, misalnya gaji, jam kerja, dan tugas.

Topik terpenting dalam hukum ketenagakerjaan adalah:

- **Kontrak kerja:** Kontrak kerja mengatur kondisi dasar hubungan kerja, misalnya jenis pekerjaan, upah, jam kerja, dan cuti.
- **Waktu kerja:** Waktu kerja adalah waktu di mana karyawan wajib bekerja. Waktu kerja maksimum menurut undang-undang di Austria adalah empat puluh jam per minggu.
- **Upah:** Upah adalah imbalan atas pekerjaan karyawan. Biasanya disepakati dalam euro per jam atau per bulan.
- **Cuti:** Karyawan berhak atas cuti berbayar. Cuti minimum yang diatur undang-undang di Austria adalah 25 hari per tahun.
- **Pemutusan hubungan kerja:** Hubungan kerja dapat diakhiri oleh salah satu pihak. Masa pemberitahuan diatur oleh hukum.
- **Perlindungan karyawan:** Perlindungan karyawan mencakup serangkaian peraturan yang dirancang untuk melindungi kesehatan dan keselamatan karyawan di tempat kerja.

Di Austria, pemberi kerja harus mematuhi ketentuan hukum tertentu saat mencari karyawan baru untuk memastikan bahwa prosesnya adil dan tidak diskriminatif.

Prinsip umum:

- **Perlakuan setara:** Semua pelamar, tanpa memandang jenis kelamin, ras, agama, usia, disabilitas, orientasi seksual, atau etnis, berhak atas perlakuan yang setara.
- **Larangan diskriminasi:** Diskriminasi langsung dan tidak langsung dalam iklan lowongan kerja, dalam proses lamaran, dan selama hubungan kerja dilarang.
- **Transparansi:** Iklan lowongan kerja harus secara jelas menjelaskan persyaratan bagi pelamar dan kondisi kerja yang ditawarkan.
- **Perlindungan data:** Data pribadi pelamar harus dilindungi sesuai dengan peraturan perlindungan data.

Persyaratan khusus:

- **Kewajiban pelaporan:** Perusahaan dengan lebih dari dua puluh karyawan wajib melaporkan lowongan pekerjaan kepada Layanan Ketenagakerjaan Publik Austria (AMS).
- **Aplikasi ramah disabilitas:** Lamaran dari penyandang disabilitas harus dipertimbangkan secara setara. Perusahaan wajib mengambil langkah-langkah yang sesuai untuk mempermudah proses lamaran bagi penyandang disabilitas.
- **Hukum ketenagakerjaan warga negara asing:** Saat mempekerjakan karyawan asing, ketentuan hukum ketenagakerjaan dan tempat tinggal harus dipatuhi.

Platform aplikasi menggunakan AI untuk secara otomatis menyaring CV untuk posisi yang diiklankan. **Penguraian CV** (mengurai = menganalisis) sudah menjadi bidang aplikasi umum untuk kecerdasan buatan. Teknologi ini menganalisis dokumen lamaran dan mengekstrak informasi yang relevan seperti kualifikasi dan pengalaman profesional. Data ini kemudian tersedia dalam format standar seperti basis data untuk pemrosesan dan analisis lebih lanjut.

Sistem ATS (Applicant Tracking Systems) membantu perusahaan untuk mengelola proses aplikasi, mempublikasikan lowongan pekerjaan, dan mengelola calon kandidat. Penguraian CV dan sistem ATS sering bekerja bersama. Contoh sistem ATS tersebut adalah Oracle Taleo atau Greenhouse. Perusahaan juga dapat menggunakan AI atau platform tertentu untuk menguji dan menilai keterampilan yang dibutuhkan dari pelamar. Codility dan HackerRank digunakan oleh perusahaan besar khususnya untuk memeriksa keterampilan teknis.

AI dapat digunakan dalam berbagai tingkatan. Ini berkisar dari pembuatan iklan lowongan pekerjaan secara lengkap hingga analisis video yang didukung AI.

Menulis Iklan Lowongan Kerja dengan AI

Contoh

Penggunaan langsung alat LLM umum (misalnya Google Gemini, ChatGPT) untuk mendapatkan hasil dari AI melalui perintah (input). Pada prinsipnya, semua tugas teks dapat diselesaikan dengan AI.

Identifikasi alternatif judul pekerjaan:

Judul pekerjaan yang tepat adalah faktor kunci keberhasilan iklan lowongan kerja. Alat seperti Google Trends dapat digunakan untuk memeriksa seberapa sering berbagai varian dicari. Ini memungkinkan Anda untuk membuat keputusan berbasis data yang mendukung judul pekerjaan yang paling sering digunakan oleh kandidat. Ada dua pilihan untuk

mengidentifikasi judul pekerjaan yang sesuai atau alternatif: Anda sudah memiliki judul pekerjaan dan ingin menerima saran alternatif dari AI berdasarkan judul tersebut. Atau Anda memiliki garis besar kualifikasi yang Anda cari dan tugas yang direncanakan dan pertama-tama mencari judul yang pada dasarnya sesuai dengan posisi tersebut.

Contoh permintaan untuk menggunakan ChatGPT atau Google Gemini untuk mencari alternatif yang sesuai:

“Mohon bantu saya mengidentifikasi judul pekerjaan alternatif untuk pencarian. Alternatif tersebut, di satu sisi, harus menunjukkan kemungkinan penunjukan yang berbeda dan, di sisi lain, dirancang untuk memiliki volume pencarian pencari kerja yang tinggi. Judul harus dekat dengan istilah sumber tanpa terlalu banyak menafsirkan peran tersebut. Ini adalah perusahaan di [INDUSTRI; opsional], yang dapat disertakan dalam judul, tetapi bukan keharusan.”

Buat dan optimalkan deskripsi perusahaan:

Bagian penting dari setiap iklan lowongan kerja adalah deskripsi diri perusahaan. Ini harus menunjukkan apa yang membuat perusahaan menonjol sebagai pemberi kerja. AI dapat membantu dalam penyusunan kata, tetapi juga dalam pengoptimalan teks.

Tentukan persyaratan dan tugas terkait pekerjaan:

Di sini Anda menentukan dengan tepat apa yang Anda cari dan tugas apa yang harus dilakukan oleh calon karyawan di perusahaan. Contoh perintah untuk mendapatkan hasil yang bermanfaat menggunakan ChatGPT atau Google Gemini:

“Buat daftar tugas dan persyaratan untuk iklan lowongan pekerjaan untuk pencarian [posisi]. Gunakan bahasa Jerman yang formal dan tidak diskriminatif. Posisi ini khususnya akan digunakan di [spesialisasi] – yaitu [tugas spesifik, jika dapat disebutkan]. [Bidang tanggung jawab penting lainnya] adalah bidang tanggung jawab yang penting.”

Campuran saluran untuk publikasi iklan lowongan pekerjaan:

Setelah iklan lowongan pekerjaan dibuat, saatnya untuk menyampaikannya kepada kandidat yang tepat melalui saluran yang tepat. Untuk melakukan ini, Anda dapat menggunakan alat AI generatif untuk mencari saluran yang sesuai untuk publikasi. Misalnya, Google Gemini dapat digunakan sebagai alat pencarian ulang.

Contoh perintah:

“Saya membutuhkan campuran saluran yang sesuai untuk mempublikasikan iklan lowongan pekerjaan saya untuk pencarian [posisi] di [lokasi]. Buat daftar portal pekerjaan, media industri, dan saluran media sosial yang sesuai yang dapat saya gunakan untuk mengiklankan pekerjaan saya.”

Peran yang relevan

Penyebarnya ChatGPT dalam arti Undang-Undang AI adalah perusahaan OpenAI, yang berdedikasi pada penelitian AI.

Klasifikasi sebagai AI berisiko tinggi

Tidak, tidak ada AI berisiko tinggi.

Titik kontak dengan AI terlarang

Tidak, tidak ada titik kontak dengan AI terlarang.

Kewajiban Transparansi

Aturan transparansi pada prinsipnya berlaku sesuai dengan Pasal 50 Undang-Undang AI. Jika, misalnya, konten gambar, video, atau audio dibuat atau dimodifikasi oleh AI, fakta ini harus diungkapkan. Ini juga berlaku jika AI membuat atau memodifikasi teks yang disebarluaskan untuk tujuan informasi publik.

Dukungan AI untuk Seleksi Pelamar Melalui Analisis Video

Contoh

Pelamar yang melamar pekerjaan diminta untuk merekam video berdurasi satu menit selain CV tradisional mereka. Dalam video ini, pelamar menjawab pertanyaan: "Mengapa Anda ingin bekerja untuk XY?" Video-video ini direkam dan kemudian dievaluasi oleh alat AI.

Kecerdasan buatan menciptakan profil kepribadian. Model Big 5 menggambarkan kepribadian seseorang berdasarkan lima dimensi: keterbukaan, kesadaran, ekstrover, keramahan, dan neurotisme. Model ini mengklasifikasikan kandidat berdasarkan lima dimensi kepribadian yang berbeda ini, yang diakui secara universal dan lintas budaya. Bersama dengan profil kepribadian, profil komunikasi pelamar juga disediakan. Dengan menggabungkan profil-profil tersebut, perusahaan menerima profil objektif dari semua pelamar, yang dapat mempercepat seluruh proses pra-seleksi secara signifikan.

Peran yang relevan

Dalam kasus penggunaan ini, semua peran dapat relevan, tergantung pada konstelasi.

Klasifikasi sebagai AI berisiko tinggi

Ya, karena Lampiran III no. 4 huruf a UU AI mendefinisikan sistem AI yang dimaksudkan untuk digunakan untuk perekrutan atau seleksi orang, khususnya untuk menempatkan iklan pekerjaan yang ditargetkan, untuk menyaring atau memfilter lamaran dan untuk mengevaluasi pelamar, sebagai sistem AI berisiko tinggi sesuai dengan Pasal 6 ayat 2 UU AI.

Klasifikasi sebagai sistem AI berisiko tinggi berarti bahwa persyaratan berikut ini harus dipenuhi secara khusus:

- Sistem manajemen risiko harus dibentuk, diterapkan, didokumentasikan, dan dipelihara sesuai dengan Pasal 9 UU AI.
- Menurut Pasal 10 UU AI, jika teknik yang digunakan untuk melatih model AI dengan data (kumpulan data pelatihan, validasi, dan pengujian) harus memenuhi kriteria kualitas yang ditentukan dalam paragraf 2 hingga 5.
- Menurut Pasal 11 UU AI, dokumentasi teknis sistem AI berisiko tinggi harus disiapkan sebelum sistem ini dipasarkan atau dioperasikan dan harus selalu diperbarui.
- Teknologi sistem AI berisiko tinggi harus memungkinkan perekaman peristiwa secara otomatis (selanjutnya disebut sebagai "pencatatan") sesuai dengan Pasal 12 UU AI selama siklus hidup sistem.
- Sesuai dengan Pasal 13 UU AI, sistem AI berisiko tinggi harus dirancang dan dikembangkan sedemikian rupa sehingga pengoperasiannya cukup transparan untuk memungkinkan pengimplementasian menafsirkan dan menggunakan keluaran sistem dengan tepat.

- Sistem AI berisiko tinggi harus dirancang dan dikembangkan sedemikian rupa sehingga dapat diawasi secara efektif oleh orang perseorangan sesuai dengan Pasal 14 UU AI selama masa penggunaannya, termasuk dengan alat antarmuka manusia-mesin yang sesuai.
- Sesuai dengan Pasal 15 UU AI, sistem AI berisiko tinggi harus dirancang dan dikembangkan untuk mencapai tingkat akurasi, ketahanan, dan keamanan siber yang memadai dan berfungsi secara konsisten dalam hal ini sepanjang siklus hidupnya.

Keputusan tentang orang perseorangan

Menurut Pasal 86 UU AI, orang yang terkena dampak keputusan yang diambil oleh pengimplementasikan berdasarkan keluaran sistem AI berisiko tinggi yang tercantum dalam Lampiran III, dengan pengecualian sistem yang tercantum dalam nomor 10, 2 dari Lampiran tersebut, dan yang memiliki efek hukum atau secara signifikan mempengaruhi mereka dengan cara yang mereka anggap merugikan kesehatan, keselamatan, atau hak-hak fundamental mereka, berhak untuk menerima penjelasan yang jelas dan bermakna dari pihak yang menerapkan tentang peran sistem AI dalam proses pengambilan keputusan dan tentang elemen-elemen utama dari keputusan yang diambil.

AI dalam kasus penggunaan yang dimaksud dapat mengganggu hak-hak fundamental, khususnya jika bertindak secara diskriminatif. Hak atas perlindungan data pribadi, kebebasan untuk memilih pekerjaan, dan hak untuk bekerja atau perlindungan terhadap diskriminasi dapat terganggu.

Namun, Pasal 22 GDPR berlaku karena keputusan otomatis dibuat berdasarkan kasus per kasus. Oleh karena itu, persyaratan dan langkah-langkah yang tercantum dalam Pasal 22 ayat 2 GDPR harus dipatuhi.

Kewajiban Penyedia

Selain itu, **penyedia** sistem AI berisiko tinggi khususnya harus mematuhi persyaratan berikut sesuai dengan Pasal 16 UU AI, yaitu:

- a) memastikan bahwa sistem AI berisiko tinggi mereka memenuhi persyaratan yang ditetapkan dalam Bagian 2;
- b) mencantumkan pada sistem AI berisiko tinggi atau, jika tidak memungkinkan, pada kemasannya atau dalam dokumentasi yang menyertainya, nama, nama dagang terdaftar atau merek dagang terdaftar dan alamat kontak mereka;
- c) memiliki sistem manajemen mutu yang sesuai dengan Pasal 17 UU AI;
- d) menyimpan dokumentasi yang disebutkan dalam Pasal 18 UU AI;
- e) menyimpan log yang dihasilkan secara otomatis oleh sistem AI berisiko tinggi mereka sesuai dengan Pasal 19 UU AI jika log tersebut berada di bawah kendali mereka;
- f) memastikan bahwa sistem AI berisiko tinggi tersebut menjalani prosedur penilaian kesesuaian yang relevan sesuai dengan Pasal 43 UU AI sebelum dipasarkan atau dioperasikan;
- g) menerbitkan Deklarasi Kesesuaian UE sesuai dengan Pasal 47 UU AI;

- h) menempelkan tanda CE pada sistem AI berisiko tinggi atau, jika tidak memungkinkan, pada kemasannya atau dalam dokumentasi yang menyertainya untuk menunjukkan kesesuaian dengan Peraturan ini sesuai dengan Pasal 48 UU AI;
- i) mematuhi kewajiban pendaftaran yang ditetapkan dalam Pasal 49 ayat 1 UU AI;
- j) mengambil tindakan korektif yang diperlukan dan memberikan informasi yang dipersyaratkan berdasarkan Pasal 20 UU AI;
- k) menunjukkan, atas permintaan yang beralasan dari otoritas kompeten nasional, bahwa sistem AI berisiko tinggi tersebut sesuai dengan persyaratan yang ditetapkan dalam Bagian 2 UU AI;
- l) memastikan bahwa sistem AI berisiko tinggi tersebut memenuhi persyaratan aksesibilitas sesuai dengan Direktif (UE) 2016/2102 dan (UE) 2019/882.

7.6 AI DALAM PENDIDIKAN

Kecerdasan buatan (AI) dalam pendidikan merupakan antarmuka interdisipliner antara ilmu komputer, pedagogi, psikologi, ilmu sosial, dan ilmu pendidikan. Penelitian dan pengembangan yang sedang berlangsung di bidang ini menunjukkan bagaimana sistem pendidikan di seluruh dunia berkembang dan beradaptasi dengan kebutuhan masyarakat yang semakin digital. Tujuannya adalah untuk mengoptimalkan dan mempersonalisasi proses pengajaran dan pembelajaran melalui penggunaan sistem cerdas untuk meningkatkan hasil pendidikan. Teknologi ini bertujuan untuk secara fundamental mengubah sektor pendidikan dengan memungkinkan otomatisasi, kustomisasi, dan peningkatan efisiensi. Selain implementasi, lembaga pendidikan mengambil peran fasilitator. Peran tersebut mencakup pengajaran dan transfer keterampilan AI sehingga peserta didik dan guru memperoleh keterampilan dan kompetensi digital yang diperlukan untuk dapat berpartisipasi aktif dalam ekonomi, masyarakat, dan proses demokrasi di masa depan (Pertimbangan 56 UU AI).

Sistem AI digunakan dalam berbagai aplikasi. Bidang aplikasi mencakup penilaian ujian otomatis, platform pembelajaran adaptif yang menawarkan kurikulum dan jalur pembelajaran yang dipersonalisasi, dan analitik prediktif untuk memprediksi perilaku belajar dan risiko putus sekolah. Studi internasional awal menunjukkan bahwa lingkungan pembelajaran imersif menggunakan teknologi seperti realitas virtual (VR), realitas tertambah (AR), dan realitas campuran (MR) untuk membenamkan peserta didik dalam dunia realistik, interaktif, dan tiga dimensi. Lebih lanjut, sistem pemantauan yang didukung AI digunakan untuk mendeteksi upaya kecurangan selama ujian. Selain itu, ChatGPT, chatbot AI berbasis teks, membuka berbagai kemungkinan bagi guru dan siswa. Pembuatan GPT sendiri memungkinkan pengembangan skenario, misalnya untuk sesi konseling. Ini juga menawarkan opsi untuk menerima jawaban atas literatur ujian tergantung pada tingkat pembelajaran. Sistem AI untuk tujuan umum seperti ChatGPT diperlakukan secara terpisah dalam Undang-Undang AI dan tunduk pada persyaratan khusus (lihat bagian 3.7 GPAI). Ini termasuk, antara lain, kewajiban transparansi sistem (Pasal 50 Undang-Undang AI). Beragamnya teknologi dan kemungkinan aplikasi memungkinkan guru untuk menanggapi kebutuhan individu peserta didik dan menyesuaikan pelajaran sesuai dengan kebutuhan tersebut.

Lembaga pendidikan di semua tingkatan, dari sekolah dasar hingga lembaga pendidikan tinggi, serta lembaga pendidikan orang dewasa dan kejuruan, semakin mengintegrasikan teknologi AI untuk mengatasi kebutuhan belajar individu peserta didik, menyederhanakan proses administrasi, dan meningkatkan kualitas pengajaran dalam hal inovasi dan digitalisasi. Penggunaan AI memungkinkan guru dan dosen untuk membuat keputusan yang tepat berdasarkan analisis berbasis data, sehingga lingkungan belajar menjadi lebih interaktif dan efektif. Namun, implementasi AI dalam pendidikan tidak lepas dari tantangan dan risiko. Penggunaan teknologi ini secara etis sangat penting untuk mencegah diskriminasi dan pelanggaran data. Selain kebijakan dan pedoman internal lembaga pendidikan, Undang-Undang AI menyediakan kerangka kerja penting untuk memastikan penggunaan AI yang aman dan etis dalam pendidikan. Secara khusus, klasifikasi sistem AI tertentu sebagai berisiko tinggi atau dilarang memerlukan pemeriksaan Undang-Undang AI. Meskipun demikian, bahkan sistem AI dengan “risiko terbatas” (Pasal 50 UU AI) tetap mengandung risiko tertentu yang dapat diminimalkan melalui kewajiban transparansi. Untuk sistem AI dengan “risiko minimal”, tidak ada kewajiban lebih lanjut yang berlaku bagi pengembang, selain memastikan literasi AI pengguna. Pendekatan berbasis risiko dengan demikian menetapkan kondisi kerangka kerja penting untuk memastikan bahwa peraturan tersebut efektif dan mengikat (Pertimbangan 26 UU AI) sehingga penggunaan AI dalam pendidikan bersifat inovatif dan aman. Aspek-aspek berikut dibahas di bawah ini:

- Peran dalam UU AI
- Literasi AI
- Sistem AI dengan risiko “terbatas” dalam pendidikan
- Sistem AI berisiko tinggi dalam pendidikan
- Sistem AI yang dilarang dalam pendidikan

Peran dalam Undang-Undang AI

Undang-Undang AI bertujuan untuk mempromosikan penggunaan kecerdasan buatan yang aman dan etis. Pengenalan peran yang didefinisikan secara jelas sangat penting untuk menetapkan tanggung jawab dan memastikan kepatuhan. Hal ini seharusnya mencegah penyalahgunaan dan memastikan bahwa teknologi AI digunakan secara efektif dan (etis) bertanggung jawab.

Penyedia (Pasal 3 ayat 3 Undang-Undang AI): Perusahaan dan pengembang yang mengembangkan atau menyediakan sistem AI untuk sektor pendidikan harus memastikan bahwa sistem tersebut mematuhi persyaratan peraturan dan juga mengungkapkan apakah sistem tersebut, misalnya, merupakan AI berisiko tinggi.

Pelaksana (Pasal 3 ayat 4 Undang-Undang AI): Lembaga pendidikan seperti sekolah, perguruan tinggi, dan universitas, tetapi juga individu yang menerapkan atau menggunakan sistem AI, yaitu bertanggung jawab atas integrasi dan pengoperasian AI. Pelaksana mentransfer kompetensi, otorisasi, dan pelatihan yang diperlukan kepada individu. Mereka juga memberikan dukungan dan pengawasan manusia yang diperlukan. Oleh karena itu, lembaga pendidikan tidak hanya bertanggung jawab untuk mengintegrasikan AI ke dalam kurikulum, tetapi juga harus memastikan bahwa sistem yang digunakan memenuhi

persyaratan peraturan. Mereka juga harus menyediakan sumber daya, pelatihan, dan infrastruktur untuk memastikan penggunaan yang bertanggung jawab dan mengembangkan keterampilan yang diperlukan di kalangan guru (lihat juga Lampiran IV UU AI).

Pengguna, misalnya, adalah guru yang menggunakan sistem AI dalam pendidikan sehari-hari dan dianggap sebagai mediator antara teknologi dan siswa, tetapi juga menggunakan AI untuk mendukung pengajaran mereka. Namun, pengguna di lembaga pendidikan juga dapat berupa departemen TI. Pengguna harus memiliki keterampilan literasi AI yang diperlukan (Lampiran IV UU AI) dan harus, misalnya, menyadari klasifikasi risiko tinggi dan mematuhi UU AI.

Otoritas Pengawasan Pasar (Pasal 3 ayat 26 UU AI): adalah otoritas nasional yang melaksanakan kegiatan dan mengambil tindakan yang diatur dalam UU AI;

Otoritas pengatur: Lembaga yang memantau kepatuhan terhadap UU AI, memastikan kepatuhan terhadap persyaratan hukum dan memberikan sanksi atas pelanggaran.

Literasi AI (Pasal 4 UU AI)

Penggunaan sistem AI dalam pendidikan atau pelatihan sangat penting untuk mempromosikan pendidikan dan pelatihan digital dan kejuruan berkualitas tinggi (Pertimbangan 56 UU AI). Hal ini memungkinkan peserta didik dan guru untuk memperoleh dan meneruskan keterampilan digital, literasi media, dan pemikiran kritis yang diperlukan. Penyedia, penyebar, dan subjek data (Pertimbangan 20 UU AI) harus dilengkapi dengan keterampilan dan kompetensi yang diperlukan untuk membuat keputusan yang tepat tentang sistem AI. **Hak-hak fundamental, kesehatan, dan keselamatan** juga harus dijaga untuk memungkinkan kontrol demokratis. Oleh karena itu, promosi literasi AI merupakan prasyarat penting untuk memastikan bahwa warga negara dapat terus berpartisipasi aktif dalam ekonomi, masyarakat, dan proses demokrasi di masa depan (Pertimbangan 20 UU AI). Definisi literasi AI menurut UU AI (Pasal 3 no. 56 UU AI) adalah sebagai berikut:

“Literasi AI berarti keterampilan, pengetahuan, dan pemahaman yang memungkinkan penyedia, penyebar, dan pihak yang terdampak, dengan mempertimbangkan hak dan kewajiban masing-masing dalam konteks Peraturan ini, untuk melakukan penyebaran sistem AI yang terinformasi, serta untuk memperoleh kesadaran tentang peluang dan risiko AI dan kemungkinan bahaya yang dapat ditimbulkannya.”

Selain penyedia, penyebar sistem AI juga wajib menunjukkan tingkat literasi AI yang memadai (Pasal 4 UU AI bersamaan dengan Pasal 3 no. 56 UU AI). Lingkup kewajiban penyebar berbeda tergantung pada klasifikasi risiko sistem AI, yaitu sistem AI berisiko tinggi memiliki kewajiban paling banyak dan sistem AI dengan risiko minimal memiliki kewajiban paling sedikit. Namun, semua tingkat risiko memiliki keterampilan literasi AI yang diperlukan (Pasal 4 UU AI) sebagai kewajiban bersama. Hal ini menggambarkan relevansi literasi AI. Selain aplikasi praktis, penting juga untuk menangani dan memahami pengolahan data, termasuk **masalah privasi, pemahaman etika, pemahaman tentang bias dan diskriminasi dalam sistem** dan dalam aplikasi. Desain dan penggunaan yang cermat menjadi dasar penggunaan AI dalam pendidikan untuk menghindari dampak negatif (lihat juga bagian 3.2 Literasi AI). Pelatihan dan pendidikan lanjutan secara berkala diperlukan untuk memperluas pengetahuan guru tentang

AI dan meningkatkan keterampilan didaktik mereka. Dianjurkan untuk mengintegrasikan aplikasi praktis dari alat dan platform pembelajaran berbasis AI ke dalam pelajaran. Hal ini mendorong penggunaan teknologi dan mempersiapkan peserta didik untuk tantangan di masa depan. Pengembangan kurikulum, pelatihan, dan aplikasi praktis yang tepat merupakan langkah penting untuk mempromosikan keterampilan AI komprehensif yang memenuhi persyaratan pendidikan digital modern.

Sistem AI dengan Risiko “Terbatas” (Pasal 50 UU AI) dalam Pendidikan

Untuk sistem AI dengan risiko terbatas sesuai dengan Pasal 50 UU AI (lihat bagian 3.6), **kewajiban transparansi** terhadap aktor hilir (Pasal 50 ayat 3 UU AI, Pasal 50 ayat 4 UU AI) juga harus diperhitungkan selain kompetensi AI (Pasal 4 UU AI). Menurut Pasal 50 UU AI, kewajiban transparansi dapat meminimalkan risiko terbatas. Informasi tentang penggunaan sistem AI harus diberikan secara jelas dan tidak ambigu paling lambat pada saat penggunaan pertama atau kontak pertama. Persyaratan aksesibilitas saat ini harus diperhitungkan (lihat Pasal 50 ayat 5 UU AI). Berikut adalah contoh sistem AI dengan risiko “terbatas” di sektor pendidikan.

Contoh I: Chatbot

Chatbot dapat digunakan untuk tugas-tugas administratif seperti menjawab pertanyaan umum atau membuat janji temu. Sistem ini meningkatkan efisiensi dan mengurangi beban administratif di lembaga pendidikan. Namun, pengguna harus diberitahu bahwa mereka berkomunikasi dengan chatbot dan bukan dengan orang sungguhan, tetapi dengan AI (kewajiban transparansi sesuai dengan Pasal 50 UU AI). Selain kewajiban transparansi ini, hak-hak Uni Eropa dan nasional tetap berlaku yang mengatur, misalnya, penggunaan dan pemrosesan data pribadi sesuai dengan GDPR.

Contoh II: Pembuatan gambar dan video

Jika konten pembelajaran visual dibuat atau didukung oleh AI, kewajiban transparansi sesuai dengan Pasal 50 UU AI juga berlaku di sini. Peserta didik harus diberitahu bahwa konten tersebut dibuat atau dimanipulasi oleh AI.

Pengecualian terhadap kewajiban transparansi muncul jika ada editor yang bertanggung jawab atas isi dan bentuk teks yang dihasilkan dan dimanipulasi oleh AI. Proses peninjauan dan persetujuan memastikan bahwa konten tersebut benar dan berkualitas tinggi, yang menghilangkan kewajiban transparansi khusus tersebut.

Contoh III: Lingkungan Pembelajaran Adaptif

Sistem pembelajaran matematika adaptif menggunakan AI untuk menganalisis kemajuan belajar siswa guna menawarkan jalur pembelajaran yang dipersonalisasi. Sistem menyesuaikan kesulitan tugas berdasarkan kinerja individu dan perilaku belajar untuk memastikan keberhasilan belajar yang optimal. Namun, sistem AI tidak menilai kinerja. Saat menggunakan atau mendaftar untuk pertama kalinya, peserta didik harus diberitahu bahwa sistem menggunakan AI untuk mengadaptasi konten pembelajaran.

Sistem pembelajaran adaptif membawa risiko juga digunakan untuk penilaian. Akibatnya, ada kemungkinan sistem AI akan diklasifikasikan sebagai sistem AI berisiko tinggi. Misalnya, jika (1) sistem membuat keputusan otomatis tentang apakah peserta didik dapat melanjutkan ke kursus atau kelas berikutnya. (2) Sistem secara otomatis memberikan

sertifikasi dan penilaian yang dapat memengaruhi jalur pendidikan dan karier peserta didik selanjutnya. Kemungkinan sistem AI berisiko tinggi dalam pendidikan diuraikan di bawah ini.

Sistem AI Berisiko Tinggi dalam Pendidikan

Sistem AI yang digunakan dalam pendidikan dan pelatihan juga dapat mengontrol akses ke lembaga dan program pendidikan, menilai hasil pembelajaran, mengevaluasi pencapaian pendidikan, dan memungkinkan pemantauan peserta didik selama ujian, di antara hal-hal lainnya. Sistem ini berpotensi memengaruhi secara signifikan jalannya kehidupan pendidikan dan profesional seseorang. Oleh karena itu, sistem ini juga diklasifikasikan sebagai sistem AI berisiko tinggi (Pertimbangan 56 UU AI). Sistem AI berisiko tinggi dalam pendidikan dapat memiliki efek yang sangat invasif jika tidak dirancang dan digunakan dengan benar. Sistem ini dapat melanggar hak atas pendidikan dan pelatihan serta hak untuk tidak diskriminasi. Sistem ini membawa risiko melanggar pola diskriminasi historis, khususnya terhadap perempuan, kelompok usia tertentu, penyandang disabilitas, atau orang dengan asal etnis atau orientasi seksual tertentu (Pertimbangan 56 UU AI). Sistem AI berisiko tinggi didefinisikan dalam UU AI sebagai kategori terpisah dengan kewajiban khusus bagi pengembangnya. Berbeda dengan sistem AI dengan risiko “terbatas”, kewajiban transparansi saja tidak cukup untuk sistem AI berisiko tinggi. Dalam hal ini, UU AI mengatur kewajiban komprehensif selama penggunaan.

Lampiran III No. 3 UU AI, Pasal 6 ayat 2 subayat 3 UU AI mengklasifikasikan sistem AI berisiko tinggi dalam bidang pendidikan dan pelatihan. Definisi ini diilustrasikan di bawah ini menggunakan contoh praktis untuk memberikan pemahaman yang lebih baik tentang klasifikasi dan implikasinya.

- a) *Sistem AI yang dimaksudkan untuk digunakan untuk menentukan akses atau penerimaan atau untuk mengalokasikan individu ke lembaga di semua tingkatan pendidikan dan pelatihan (Lampiran III/3, UU AI, Pasal 6 ayat 2 subayat 3).*

Contoh I untuk a) Sistem persetujuan otomatis

Sistem AI mengevaluasi aplikasi untuk tempat di universitas berdasarkan nilai sekolah, hasil tes standar, dan kegiatan ekstrakurikuler. Sistem ini menentukan akses atau penerimaan individu ke lembaga pendidikan dan dengan demikian secara langsung memengaruhi prospek pendidikan dan karier mereka.

Contoh II untuk a) Pemberian beasiswa otomatis

Sistem AI mengevaluasi aplikasi beasiswa berdasarkan nilai sekolah, nilai tes standar, dan kegiatan ekstrakurikuler. Sistem ini menentukan akses atau penerimaan individu ke lembaga pendidikan dan dengan demikian secara langsung memengaruhi prospek pendidikan dan karier mereka.

Kedua sistem AI (contoh I & II) akan diklasifikasikan sebagai sistem AI berisiko tinggi sesuai dengan Lampiran III/, Bagian a) UU AI. Menurut klasifikasi tersebut, tidak ada keputusan otomatis berbasis AI yang dapat dibuat terkait akses atau penerimaan individu ke lembaga pendidikan.

- b) *Sistem AI yang dimaksudkan untuk digunakan untuk penilaian hasil pembelajaran, termasuk di mana hasil ini digunakan untuk memandu proses pembelajaran individu di*

lembaga atau program di semua tingkatan pendidikan dan pelatihan (Lampiran III/3 Peraturan AI, Pasal 6 ayat 2 subayat 3 UU AI).

Contoh I untuk b) Penilaian otomatis ujian dan/atau pengumpulan tugas

Sistem AI mengevaluasi ujian tertulis dan esAI, menganalisis jawaban, dan memberikan nilai yang digunakan peserta didik untuk penilaian. Sistem ini digunakan untuk menilai hasil belajar dan dengan demikian secara langsung memengaruhi proses pembelajaran dan kinerja akademik siswa. Menurut Lampiran III/3, b) Undang-Undang AI, oleh karena itu akan diklasifikasikan sebagai sistem AI berisiko tinggi.

Contoh II untuk b) Lingkungan pembelajaran imersif

Sistem VR yang didukung AI untuk pelatihan. Untuk menciptakan situasi realistis bagi siswa (misalnya, kedokteran), sistem VR yang didukung AI digunakan dalam pelatihan. AI mengevaluasi kinerja siswa secara real-time, memberikan umpan balik, dan menyesuaikan kesulitan tugas dengan kemajuan peserta didik. Sistem ini digunakan untuk menilai hasil belajar dan secara langsung memengaruhi proses pembelajaran dan penilaian kinerja.

Oleh karena itu, sistem AI ini dapat memengaruhi karier (profesional) orang tersebut dan akan diklasifikasikan sebagai sistem AI berisiko tinggi sesuai dengan Lampiran III/3 UU AI, Pasal 6 ayat 2 huruf b UU AI.

- c) Sistem AI yang dimaksudkan untuk digunakan untuk tujuan menilai tingkat pendidikan yang sesuai yang akan diterima seseorang atau yang akan mereka akses di dalam atau di lembaga-lembaga di semua tingkatan pendidikan dan pelatihan (Lampiran III/3 UU AI, Pasal 6 ayat 2 subayat 3 UU AI);

Contoh I untuk c) Identifikasi kebutuhan dukungan

Sistem AI menganalisis kemajuan belajar dan perilaku peserta didik untuk mengidentifikasi kebutuhan dukungan individu dan menyarankan program. Dengan demikian, sistem tersebut menilai tingkat pendidikan yang sesuai dan memengaruhi langkah-langkah dukungan yang diterima seseorang. Menurut Lampiran III UU AI, Pasal 6 ayat 2 huruf c UU AI, sistem tersebut akan diklasifikasikan sebagai sistem berisiko tinggi.

- d) *Sistem AI yang dimaksudkan untuk digunakan untuk memantau dan mendeteksi perilaku terlarang siswa selama ujian di atau dalam lembaga pendidikan dan pelatihan di semua tingkatan (Lampiran III UU AI, Pasal 6 ayat 2 no. 3 UU AI);*

Contoh I untuk d) Pemindai plagiarisme yang didukung AI

Sistem AI menganalisis karya yang diserahkan untuk plagiarisme dengan memeriksa kemiripan teks dan kecocokan dengan sumber yang ada. Sistem ini digunakan untuk memantau dan mendeteksi perilaku terlarang (plagiarisme) dalam ujian dan tugas, sehingga memengaruhi penilaian. Menurut Lampiran III UU AI, Pasal 6 ayat 2 huruf d UU AI, ini diklasifikasikan sebagai sistem AI berisiko tinggi.

Contoh II hingga d) Pemantauan dan deteksi perilaku terlarang selama ujian

Sistem AI digunakan selama ujian daring, di mana semua siswa menyalakan kamera, untuk mendeteksi perilaku terlarang seperti berbicara, mencontek, dan lainnya. Sistem ini memantau dan mendeteksi potensi perilaku curang selama ujian dan dengan demikian

memengaruhi penilaian. Menurut Lampiran III UU AI, Pasal 6 ayat 2 huruf d UU AI, ini diklasifikasikan sebagai sistem AI berisiko tinggi.

Kasus penggunaan juga dapat menggabungkan berbagai bagian, seperti analisis prediktif untuk risiko putus sekolah. Sistem AI menganalisis data perilaku dan kinerja untuk mengidentifikasi peserta didik yang berisiko putus sekolah/universitas/pendidikan dan menawarkan intervensi. Sistem AI berisiko tinggi menurut Lampiran III UU AI, no. 3. b) dan c) UU AI menilai hasil belajar dan pencapaian pendidikan dan dapat memulai tindakan yang memengaruhi jalur pendidikan individu.

Singkatnya, penggunaan AI dalam pendidikan, khususnya dalam penilaian hasil belajar, menghadirkan tantangan dan peluang yang signifikan. Meskipun sistem AI dapat memberikan umpan balik real-time yang berharga dan secara dinamis menyesuaikan konten pembelajaran, penilaian akhir kinerja harus selalu tetap berada di tangan instruktur manusia. Pelatih dan guru harus dapat melihat rekomendasi yang dihasilkan oleh AI dan menyesuaikannya sesuai kebutuhan. Evaluasi berbasis AI tidak boleh berdampak langsung pada evaluasi kinerja resmi untuk menjaga keadilan dan transparansi proses pendidikan. Sangat penting bahwa AI tidak menjadi satu-satunya otoritas untuk penilaian dan evaluasi yang memengaruhi karier profesional atau akademis siswa. Untuk menghindari dikategorikan sebagai sistem AI berisiko tinggi, sangat penting untuk mendefinisikan peran AI secara jelas dan memastikan pengawasan manusia. Ini adalah satu-satunya cara untuk memastikan bahwa manfaat AI dimanfaatkan tanpa membahayakan hak dan peluang siswa.

Namun, jika terdapat AI berisiko tinggi dan tidak ada pengecualian yang berlaku (Pasal 6 ayat 3 UU AI), maka kewajiban berikut bagi pengembang sistem AI berisiko tinggi akan berlaku:

Tabel 7.1 Kewajiban Pengembang Sistem AI Berisiko Tinggi

Kewajiban Pengimplementasikan berdasarkan Regulasi AI	Sistem AI berisiko tinggi
Literasi AI	Seni. 4 UU AI
Transparansi terhadap pemain hilir	Seni. 26 ayat. 1 UU AI
Penggunaan sistem AI sesuai dengan petunjuk penggunaan	Seni. 26 ayat. 1, 3, 4 UU AI
Pengawasan manusia	Seni. 26 ayat. 2 UU AI
Pemantauan sistem AI	Seni. 26 ayat. 5 UU AI
Pelaporan insiden serius	Seni. 26 ayat. 5 UU AI, Pasal. 73 UU AI
Penyimpanan log yang dihasilkan	Seni. 26 ayat. 6 UU AI
Jika relevan, penilaian dampak perlindungan data	Seni. 26 ayat. 9 UU AI
Kerja sama dengan otoritas nasional yang berwenang	Seni. 26 ayat. 12 UU AI
Hak untuk mendapatkan penjelasan tentang proses pengambilan keputusan dalam kasus individual	Seni. 86 ayat. 1 UU AI
Kewajiban untuk memberi tahu badan perwakilan karyawan jika pemberi kerja menggunakan sistem AI berisiko tinggi di tempat kerja	Seni. 26 ayat. 7 UU AI

Kewajiban untuk mendaftar jika lembaga Uni Eropa, badan Uni Eropa, dan badan Uni Eropa lainnya	Seni. 26 ayat. 8 UU AI, Pasal. 49 UU AI
Otorisasi yang diperlukan dari otoritas yudisial atau administratif jika digunakan untuk identifikasi biometrik jarak jauh selanjutnya	Seni. 26 ayat. 10 UU AI
Penyusunan penilaian dampak hak-hak fundamental jika, antara lain, lembaga publik atau swasta menyediakan layanan publik.	Seni. 27 UU AI

Sistem AI yang Dilarang dalam Pendidikan

Meskipun sistem AI berisiko tinggi dapat diterapkan melalui langkah-langkah yang tepat, ada sistem AI tertentu yang penggunaannya dalam pendidikan sepenuhnya dilarang. Bab selanjutnya akan memberikan contoh sistem AI yang dilarang tersebut dan menjelaskan mengapa sistem tersebut diklasifikasikan sebagai terlarang untuk memastikan integritas dan keamanan sistem pendidikan.

Contoh I: Pengenalan Emosi

Sistem AI menganalisis emosi peserta didik secara real-time selama pelajaran. Dosen ingin menggunakan hasilnya untuk menilai partisipasi peserta didik. Penggunaan AI untuk menyimpulkan emosi orang sungguhan di lembaga pendidikan dilarang, kecuali untuk alasan medis atau keselamatan (Pasal 5 ayat 1 huruf f UU AI).

Bahkan jika penilaian tersebut dihilangkan, ini tetap merupakan praktik yang dilarang. Jadi, meskipun guru ingin menggunakan hasilnya untuk menyesuaikan gaya mengajar mereka, misalnya, itu tetap merupakan praktik yang dilarang, seperti yang ingin digarisbawahi sekali lagi oleh contoh berikut.

Contoh II: Pengenalan Emosi

Sistem AI memantau peserta didik selama ujian untuk mendeteksi tanda-tanda stres atau kecemasan guna memberikan dukungan tepat waktu. Pengambilan emosi dari individu (selama ujian) merupakan praktik terlarang berdasarkan Pasal 5 ayat 1 huruf f UU AI, kecuali ada alasan medis atau keselamatan.

Jika terdapat sistem AI terlarang sesuai dengan Pasal 5 UU AI, pengujian harus diselesaikan dan sistem AI tersebut tidak boleh dioperasikan atau dipasarkan.

7.7 AI DALAM PERAWATAN KESEHATAN

Sistem (bantuan) kecerdasan buatan dalam perawatan kesehatan semakin banyak digunakan. Bahkan telah terjadi **ledakan nyata dalam sistem AI dan penelitian** serta pengembangan AI, terutama dalam beberapa tahun terakhir di bidang kedokteran, dan potensi revolusinya sangat jelas.

Menemukan sistem AI di **rumah sakit** Selain penggunaannya dalam administrasi, sistem AI juga digunakan secara langsung terkait dengan perawatan pasien, khususnya untuk diagnostik, individualisasi perawatan, dalam robot bantuan bedah, untuk analisis sejumlah besar data dalam kedokteran perawatan intensif dan untuk triase. Pasien sendiri juga

menggunakan perangkat atau aplikasi yang didukung AI untuk (memantau sendiri) nilai-nilai tertentu dalam penyakit kronis.

AI di bidang diagnostik saat ini memberikan **dukungan** terbesar di sektor rumah sakit, misalnya di bidang radiologi, di mana gambar dievaluasi oleh sistem AI dalam waktu yang sangat singkat, atau/dan di departemen lain, di mana analisis dan interpretasi data kesehatan seperti sampel darah dari berbagai penyakit, seperti Alzheimer, leukemia, dan kanker usus besar dideteksi. Hal ini memungkinkan diagnosis lebih awal dan oleh karena itu biasanya menciptakan pilihan pengobatan yang kurang rumit dan kurang invasif.

Khususnya dalam deteksi kanker kulit, AI telah terbukti mencapai akurasi diagnostik yang hampir sama dengan dokter berpengalaman, dan algoritma tersebut terkadang bahkan jauh lebih unggul daripada dokter (asisten) yang tidak berpengalaman. Sistem AI tertentu tidak hanya mencapai hasil yang (setidaknya) setara dengan praktisi berpengalaman, tetapi juga mencapai tujuan diagnostik jauh lebih cepat.

Oleh karena itu, dapat dipahami bahwa pertanyaan tentang kemungkinan hak integrasi AI dalam konteks diagnostik diangkat dalam debat hukum. Inilah sebabnya mengapa rumah sakit sudah semakin banyak mengintegrasikan sistem AI dan akan terus melakukannya di masa mendatang.

Oleh karena itu, AI diagnostik kulit diasumsikan sebagai kasus penggunaan, di mana langkah-langkah untuk Undang-Undang AI pada prinsipnya juga berlaku untuk sistem diagnostik lain dan sistem yang disebutkan di atas di rumah sakit.

Contoh: Diagnosis Penyakit Kulit dengan AI

Sistem yang didukung AI untuk diagnosis penyakit kulit sedang diimplementasikan di sebuah rumah sakit yang menggunakan data citra medis (khususnya citra perubahan kulit) dan data pasien (misalnya hasil laboratorium, riwayat penyakit sebelumnya). Ini adalah perangkat medis yang menggunakan pembelajaran mesin untuk mengenali pola yang menunjukkan penyakit kulit tertentu. Hasilnya digunakan oleh dokter kulit untuk mendukung diagnosis dan pengambilan keputusan, khususnya dalam kasus kanker kulit (Pertimbangan 12 Undang-Undang AI, Pasal 3 ayat 1 Undang-Undang AI). Deteksi dini karenanya lebih mungkin terjadi, yang mengoptimalkan hasil pengobatan dan perawatan pasien secara individual. Prosedurnya terutama sebagai berikut.

1. **Pencatatan data:** Pasien diperiksa dan data citra medis serta informasi kesehatan yang relevan dicatat.
2. **Analisis data:** Sistem AI menganalisis data yang dikumpulkan secara real-time. Sistem ini membandingkan informasi tersebut dengan basis data ekstensif tentang pola dan perkembangan penyakit.
3. **Saran diagnosis:** Berdasarkan analisis, sistem AI memberikan rekomendasi kepada dokter untuk kemungkinan diagnosis dan menunjukkan temuan abnormal.
4. **Tinjauan medis:** Dokter meninjau saran sistem AI, mempertimbangkan pengalaman klinis mereka, dan melakukan tes lebih lanjut jika perlu.
5. **Rencana perawatan:** Setelah diagnosis dikonfirmasi oleh dokter, rencana perawatan individual disusun untuk pasien.

Penerapan Undang-Undang AI

Karena sistem ini menggunakan pembelajaran mesin, maka sistem ini termasuk dalam Undang-Undang AI (Pasal 2 ayat 1 Undang-Undang AI, Pasal 3 no. 1 Undang-Undang AI).

Penyebar dalam arti Undang-Undang AI – rumah sakit dan dokter

Rumah sakit dianggap sebagai penyebar dalam arti Undang-Undang AI (Pasal 3 no. 4 Undang-Undang AI), karena merupakan badan hukum yang menggunakan sistem AI di bawah tanggung jawabnya sendiri. Hal ini juga berlaku bagi para **dokter** yang menggunakan sistem AI sebagai individu yang tidak menggunakan sistem AI sebagai bagian dari aktivitas pribadi mereka, melainkan sebagai aktivitas profesional.

Para pengimplementasikan memiliki berbagai kewajiban berdasarkan Undang-Undang AI, tergantung pada klasifikasi kategori risiko dari sistem AI yang digunakan.

Klasifikasi AI Berisiko Tinggi dalam Makna Undang-Undang AI

Meskipun Uni Eropa menggunakan Undang-Undang AI untuk mempromosikan sistem – termasuk yang terkait dengan kesehatan – di pasar internal melalui inovasi, pemasaran, dan pembangunan kepercayaan, Uni Eropa juga menyadari risiko khusus yang terkait dengan hal ini, terutama di bidang ini. Namun, sistem diagnostik (bantuan) cerdas tidak dilarang secara langsung, tetapi diizinkan pada prinsipnya. Namun, perhatian khusus harus diberikan untuk memastikan tingkat perlindungan kesehatan dan keselamatan yang tinggi (Pasal 1 Undang-Undang AI). Oleh karena itu, sistem diagnostik AI secara teratur diklasifikasikan sebagai AI berisiko tinggi, bukan hanya karena digunakan di bidang infrastruktur kritis – perawatan kesehatan.

Bagaimanapun, AI diagnostik kanker kulit harus dikategorikan sebagai sistem AI berisiko tinggi, karena merupakan **perangkat medis** dalam arti Peraturan Perangkat Medis (EU) 2017/745 (singkatnya MDR), yang secara eksplisit dirujuk dalam Lampiran Undang-Undang AI (Pertimbangan 50 Undang-Undang AI; Pasal 6 ayat 1 huruf a Undang-Undang AI; Lampiran I no. 11 Undang-Undang AI).

Algoritma AI untuk mendukung diagnostik kanker kulit adalah perangkat medis dalam arti MDR, karena merupakan perangkat lunak yang, menurut produsen, ditujukan untuk penggunaan manusia dan dimaksudkan sendiri atau dalam kombinasi untuk memenuhi tujuan medis, khususnya diagnosis, tetapi juga untuk prediksi, prognosis, dan pengobatan penyakit (Pasal 2 Z 1 MDR) dan tunduk pada **penilaian kesesuaian** dalam arti Peraturan Perangkat Medis dan dengan demikian telah disertifikasi (Pasal 6 ayat 1 huruf b Peraturan Perangkat Medis, Pasal 52 ayat 6 Peraturan Perangkat Medis). Bukan pihak yang memasang, yaitu bukan rumah sakit, tetapi **penyedia** yang harus memastikan bahwa produk tersebut sesuai dengan persyaratan yang berlaku dalam MDR (Pasal 8 ayat 2 UU AI).

Persyaratan dan Kewajiban Pihak yang Memasang di Rumah Sakit Menurut UU AI

UU AI menetapkan sejumlah persyaratan dan kewajiban pada kategori AI berisiko tinggi bagi pihak yang memasang dan dengan demikian juga bagi rumah sakit dan staf manajemen serta komite-komitennya.

Memperoleh dan memahami informasi tentang transparansi

Untuk tujuan ini, manajemen atau dewan manajemen rumah sakit harus – penyedia sebaiknya – jika penyedia sistem belum melakukannya atau belum melakukannya secara lengkap – memastikan bahwa semua informasi yang tersedia tentang transparansi diperoleh.

Informasi ini, seperti tingkat akurasi diagnosis, keadaan yang diketahui dan dapat diprediksi yang memengaruhi akurasi usulan diagnostik, kesalahan penerapan yang dapat diprediksi yang dapat menyebabkan risiko terhadap kesehatan atau hak-hak fundamental khususnya, serta data yang diungkapkan untuk tujuan ini yang digunakan dalam proses pengembangan dan, misalnya, pekerjaan pemeliharaan dan perawatan (Pasal 13 UU AI), tidak hanya harus dibaca tetapi juga dipahami oleh karyawan departemen terkait, terutama departemen kepatuhan, agar dapat diimplementasikan dengan benar.

Jika terdapat ketidakpastian atau ambiguitas, tanyakan kepada penyedia layanan atau ikuti kursus pelatihan yang ditawarkan oleh penyedia layanan agar tidak menanggung risiko tanggung jawab (perdata dan/atau pidana) jika terjadi kerusakan kesehatan yang terkait dengan AI karena kegagalan untuk bertindak sesuai dengan kewajiban.

Tetapkan langkah-langkah sesuai dengan petunjuk penggunaan

Sesuai dengan petunjuk penggunaan terlampir dan informasi dari penyedia yang disebutkan di atas, langkah-langkah teknis dan organisasi yang sesuai harus diambil untuk menggunakan sistem di bangsal dermatologi dan klinik rawat jalan yang relevan (Pasal 26 UU AI).

Manajemen data

Saat data tambahan, yaitu data pasien, dimasukkan, hal ini tunduk pada kendali pengimplementasikan. Data ini harus sesuai dengan tujuan sistem AI berisiko tinggi dan cukup representatif (Pasal 26 ayat 4 UU AI). Selain itu, ketentuan GDPR harus dipatuhi.

Pantau sistem dan laporkan kesalahan

Rumah sakit harus memantau pengoperasian sistem diagnostik AI menggunakan petunjuk penggunaan dengan bantuan IT, dokter yang menggunakan sistem, dan, jika perlu, staf perawat (Pasal 26 ayat 5 UU AI).

Berkas log yang secara otomatis dihasilkan oleh sistem AI harus disimpan setidaknya selama enam bulan sesuai dengan UU AI, kecuali jika hukum nasional menetapkan lain (Pasal 26 ayat 6 UU AI). Apabila terjadi risiko terhadap kesehatan, keselamatan, atau hak-hak dasar (Pasal 26 ayat 5 UU AI dan Pasal 79 ayat 1 UU AI) atau insiden serius, seperti kesalahan diagnosis (yang mungkin tidak dapat diprediksi) (lihat juga Pasal 73 UU AI), hal ini juga harus dikirimkan kepada penyedia atau distributor (mungkin importir) dan, jika kedua pihak lainnya tidak dapat dihubungi, kepada otoritas pengawasan pasar yang berwenang tanpa penundaan.

Dalam hal terjadi risiko atau kesalahan sistem yang serius, sistem harus segera dihentikan (untuk sementara waktu).

Manajemen Risiko

Untuk menghindari risiko sebaik mungkin, sistem manajemen risiko di rumah sakit atau kelompok rumah sakit (Pasal 9 UU AI) harus dibentuk oleh departemen kepatuhan – yang harus diisi oleh dokter, pengacara, teknisi, dan, idealnya, ahli etika. Ini berarti bahwa AI harus ditinjau secara terus-menerus dan teratur, dan jika perlu, diperbarui untuk menghilangkan

risiko yang dapat diprediksi yang dapat memengaruhi kesehatan, keselamatan, atau hak-hak mendasar pasien. Hal ini karena pihak yang menerapkan, khususnya, masih dapat mengidentifikasi risiko selama penggunaan yang tepat yang belum (dapat) diprediksi pada fase pengembangan (Pertimbangan 93 UU AI).

Manajemen risiko – di mana, menurut UU AI, pengetahuan teknis, pengalaman, dan tingkat pendidikan yang dapat diharapkan dari pihak yang menerapkan harus diperhitungkan dengan tepat (Pasal 9 ayat 5 UU AI) – mencakup khususnya identifikasi, analisis, dan penilaian tidak hanya risiko yang diketahui tetapi juga **risiko atau penyalahgunaan yang dapat diprediksi** secara wajar yang dapat memengaruhi kesehatan, keselamatan, atau hak-hak mendasar ketika digunakan untuk tujuan yang dimaksudkan (Pasal 9 ayat 2 UU AI). Harus diperhitungkan apakah sistem tersebut kemungkinan akan berdampak buruk pada orang di bawah usia 18 tahun, yaitu pasien muda, atau, jika sesuai, kelompok rentan, di mana pasien pada umumnya diklasifikasikan sebagai rentan, terutama jika mereka penyandang disabilitas (Pasal 9 ayat 9 UU AI).

Langkah-langkah tersebut harus menghilangkan atau mengurangi risiko sejauh mungkin; risiko residual harus dinilai dapat diterima. Langkah-langkah **mitigasi dan pengendalian yang tepat** harus ditentukan untuk mengelola risiko yang tidak dapat dikesampingkan (Pasal 9 ayat 5 UU AI).

Berdasarkan penilaian ini, langkah-langkah harus diambil untuk mengelola risiko dan dirancang sedemikian rupa sehingga risiko residual dan risiko residual keseluruhan dianggap dapat diterima.

Untuk dapat melakukan hal ini, tidak hanya informasi yang harus dipahami dan diimplementasikan, tetapi penyedia layanan juga harus **dilatih** untuk pada akhirnya menerapkan langkah-langkah mitigasi dan pengendalian risiko yang tepat.

Pengawasan Manusia

Selain itu, pengawasan manusia terhadap sistem, oleh orang-orang yang memiliki kompetensi, pelatihan, dan otorisasi yang diperlukan, oleh pengembang (Pasal 14 UU AI jo. Pasal 26 UU AI).

Pemeriksaan harus dilakukan oleh dokter yang kompeten dan berpengalaman untuk memantau AI, menafsirkan diagnosis yang disarankan AI, dan memeriksa perkembangan terkini di bidang dermatologi. Harus juga dimungkinkan untuk mengenali malfungsi atau kesalahan diagnosis. Dalam kasus penggunaan ini, dokter tersebut adalah dokter, khususnya dokter spesialis kulit.

Pengembang harus memberikan dukungan yang diperlukan kepada dokter (Pasal 26 ayat 2 UU AI) untuk memastikan bahwa karyawan sepenuhnya memahami penggunaan AI, misalnya melalui pelatihan tentang sistem, prosedurnya, data pelatihan, akurasi, dan kerentanan terhadap kesalahan, dan lain sebagainya. Selain itu, dokter harus diberi tahu dan diinformasikan tentang kemungkinan bias untuk meningkatkan kesadaran akan perlunya menghindari kepercayaan otomatis atau berlebihan pada diagnosis dan, jika berlaku, usulan pengobatan yang dihasilkan oleh sistem AI ("**bias otomatisasi**").

Karena sebagian besar dokterlah yang harus menerapkan langkah-langkah pengendalian di bidang ini, mereka juga harus dilatih dan diinformasikan dengan tepat, karena pada akhirnya dokterlah yang membuat diagnosis berdasarkan dan didukung oleh keluaran AI. Dalam melakukannya, mereka harus mengenali dan mempertimbangkan kesalahan penerapan atau alasan untuk keputusan yang menyimpang (misalnya, karena kondisi pra-eksisting spesifik pasien yang tidak termasuk dalam data pelatihan) dan membuat keputusan pengobatan lebih lanjut – dengan mempertimbangkan otonomi pasien dan etika medis. Oleh karena itu, disarankan agar rumah sakit menyediakan formulir informasi dan persetujuan yang sesuai atau agar dokter menjelaskan bahwa diagnosis awal akan dibuat dengan bantuan AI, tetapi keputusan akhir akan dibuat oleh staf medis.

Sanksi

Negara-negara Anggota masih bertanggung jawab untuk mengeluarkan ketentuan mengenai “sanksi dan tindakan penegakan hukum lainnya, yang dapat mencakup peringatan dan tindakan non-moneter” (Pasal 99 UU AI) jika terjadi pelanggaran UU AI, termasuk bagi pihak yang menerapkan sistem tersebut yang tidak dengan sungguh-sungguh mematuhi kewajibannya berdasarkan Pasal 26 UU AI (lihat di atas).

7.8 AI DALAM PERIKLANAN

Periklanan adalah bidang pekerjaan yang kreatif dan juga bidang di mana tren selalu diadaptasi pada tahap awal. Oleh karena itu, tidak mengherankan bahwa apa yang disebut "kecerdasan buatan" juga berperan di sini – khususnya dalam bentuk model generatif. Selain itu, ada evaluasi algoritmik perilaku pengguna untuk tujuan periklanan, yang telah menjadi praktik umum selama lebih dari 15 tahun dan telah dianggap bermasalah secara hukum dan etika selama waktu yang sama. Sejumlah besar informasi yang dikumpulkan selama bertahun-tahun melalui jenis analisis ini mewakili basis data yang sangat besar untuk diproses oleh sistem AI. Hal ini karena dua bidang bertemu di sini di mana sistem AI sangat cocok: Pemrosesan data massal (kata kunci: **Big Data**) dan pengenalan pola. Namun, hanya karena pemrosesan algoritmik dapat bekerja dengan baik di bidang-bidang ini bukan berarti hal itu diizinkan di mana-mana. Ada baiknya untuk melihat undang-undang lain seperti Undang-Undang Persaingan Austria (UWG), undang-undang hak cipta, dan Peraturan Perlindungan Data Umum (GDPR).

Persyaratan Hukum untuk AI dalam Periklanan

Sistem AI yang Dilarang

Evaluasi algoritmik perilaku pengguna untuk tujuan periklanan dapat dibagi menjadi dua bidang:

1. penargetan untuk menemukan kelompok sasaran, yaitu menemukan dan menargetkan kelompok atau individu, biasanya berdasarkan informasi yang dikumpulkan dan dievaluasi tentang individu, keadaan mereka, dan perilaku mereka;
2. mempengaruhi kelompok atau individu dengan menampilkan informasi dan/atau pesan iklan yang dipersonalisasi, biasanya berdasarkan penargetan atau penargetan mikro.

Manipulasi terhadap perilaku orang yang tidak mereka pilih secara sadar dilarang berdasarkan Pasal 5 ayat 1 huruf a UU AI. Menurut Pertimbangan 29 UU AI, teknik manipulatif dilarang jika memiliki efek material yang "secara material mendistorsi perilaku manusia, yang mengakibatkan kerugian signifikan, khususnya yang memiliki dampak buruk yang cukup penting terhadap kesehatan fisik, psikologis, atau kepentingan finansial". Secara khusus, dan terlepas dari apakah efeknya secara eksplisit merugikan, pengaruh subliminal yang tidak dapat dikenali oleh manusia dilarang, karena rangsangan ini berada di luar jangkauan persepsi.

Praktik-praktik berikut dilarang berdasarkan Pasal 5 UU AI: "penempatan di pasar, pengoperasian, atau penggunaan sistem AI yang menggunakan teknik subliminal di luar kesadaran seseorang atau teknik manipulatif atau menipu secara sengaja, dengan tujuan, atau efek, secara material mendistorsi perilaku seseorang atau sekelompok orang dengan secara nyata mengurangi kemampuan mereka untuk membuat keputusan yang berdasarkan informasi, sehingga menyebabkan mereka mengambil keputusan yang seharusnya tidak mereka ambil dengan cara yang menyebabkan atau kemungkinan besar menyebabkan orang tersebut, orang lain, atau sekelompok orang mengalami kerugian yang signifikan." (Pasal 5 ayat 1 huruf a UU AI).

Eksplorasi kelompok rentan juga dilarang berdasarkan UU AI. Pasal 5 A 1 huruf a UU AI. Pasal 29 Undang-Undang AI melarang sistem AI yang mengeksploitasi "kerentanan apa pun dari seseorang atau kelompok orang tertentu karena usia, disabilitas, atau situasi sosial atau ekonomi tertentu, dengan tujuan, atau efek, untuk secara material mendistorsi perilaku orang tersebut atau orang yang termasuk dalam kelompok tersebut dengan cara yang menyebabkan atau kemungkinan besar akan menyebabkan orang tersebut atau orang lain mengalami kerugian yang signifikan". Pasal 29 Undang-Undang AI menambahkan bahwa orang-orang ini lebih rentan terhadap eksploitasi, misalnya orang-orang yang hidup dalam kemiskinan ekstrem dan minoritas etnis atau agama.

Pasal 29 Undang-Undang AI juga mengklarifikasi bahwa penyedia atau penyebar sistem AI tidak boleh memiliki niat untuk menyebabkan kerugian yang signifikan. Referensi eksplisit dibuat di sini untuk praktik komersial yang tidak adil dan Direktif 2005/29/EC (Direktif UE tentang Praktik Komersial yang Tidak Adil, lihat di bawah). Namun, praktik komersial umum dan sah di bidang periklanan tidak boleh dilarang. Namun, Pasal 29 Undang-Undang AI tidak mendefinisikan apa yang dimaksud dengan "umum". Argumen bahwa metode atau sistem tertentu sudah mengakar dan digunakan oleh semua orang kemungkinan besar akan gagal dalam hal praktik terlarang.

Mengenai penargetan dan iklan politik, lihat juga Peraturan (EU) 2024/900 Parlemen Eropa dan Dewan tentang transparansi dan penargetan iklan politik, Lampiran III no 8 lit. b Undang-Undang AI dan bagian 8.3, AI dalam Pemilu dan Proses Demokrasi.

Tumpang Tindih dengan Hukum Lain

Pertimbangan 29 Undang-Undang AI merujuk pada Arahani Uni Eropa tentang Praktik Komersial yang Tidak Adil. Di dalamnya, hukum tentang perdagangan yang adil antara perusahaan dan konsumen diselaraskan sejauh mungkin di tingkat Eropa. Karena ini adalah arahan Uni Eropa, maka harus dimasukkan ke dalam hukum nasional. Di Austria dan Jerman,

hal ini dilakukan melalui hukum nasional masing-masing tentang persaingan (misalnya, UWG Austria).

Hukum persaingan dimaksudkan untuk memastikan persaingan yang adil. Hukum ini memberikan solusi hukum terhadap praktik yang akan memberikan perusahaan keuntungan yang tidak adil atas para pesaingnya. “Praktik bisnis yang tidak adil” didefinisikan sebagai praktik bisnis yang menyesatkan atau agresif.

Praktik bisnis agresif adalah praktik yang cenderung membatasi kebebasan memilih atau berperilaku seseorang melalui:

- Pelecehan,
- Pemaksaan, atau
- Pengaruh yang tidak semestinya,

dan menyebabkan orang tersebut mengambil keputusan bisnis yang seharusnya tidak diambilnya (lihat Pasal 8 Arahan Praktik Komersial yang Tidak Adil).

Praktik komersial yang **menyesatkan** sesuai dengan Pasal 7 Arahan Praktik Komersial Tidak Adil terjadi ketika pernyataan palsu dibuat atau orang disesatkan dengan cara lain tentang suatu produk atau layanan. Ini juga termasuk menyembunyikan informasi penting.

Lampiran 1 Arahan Praktik Komersial Tidak Adil berisi **daftar hitam praktik komersial** yang dianggap tidak adil dalam semua keadaan. Sehubungan dengan sistem AI, ini bisa berupa, misalnya, pemasangan tanda CE yang tidak sah, tetapi juga iklan yang disamarkan sebagai informasi. Klaim bahwa sistem AI dapat menyembuhkan penyakit, malfungsi atau kelainan bentuk, kontak yang terus-menerus dan tidak diinginkan dengan orang atau ajakan langsung kepada anak-anak juga termasuk di dalamnya.

Tidak hanya hukum persaingan yang adil yang memainkan peran penting sehubungan dengan periklanan, tetapi juga GDPR; khususnya Pasal 22 GDPR, yang mengatur **keputusan otomatis** dalam kasus individu dan **pembuatan profil**. Jika data pribadi diproses, seseorang berhak atas keputusan yang tidak dibuat secara eksklusif oleh AI, terutama jika keputusan ini memiliki efek hukum pada mereka atau secara signifikan memengaruhi mereka dengan cara yang serupa (lihat Bab 4, Perlindungan data, untuk detailnya). Singkatnya: Hanya karena sesuatu “diizinkan” berdasarkan Undang-Undang AI bukan berarti hal itu tidak dilarang berdasarkan undang-undang lain.

Perdagangan Data

Bidang lain yang menjadi fokus otoritas pada tahun 2024 adalah perdagangan data. Hal ini dipicu oleh penelitian tim investigasi dari netzpolitik.org dan Bayrischer Rundfunk, yang menemukan nama, alamat rumah dan kantor, hobi, dan pekerjaan lain dari orang-orang, termasuk orang lain di layanan sipil, dari “sampel” pedagang data dengan 3,6 miliar titik data. Otoritas Jerman khawatir, dan di AS Pentagon terlibat dalam masalah ini. Diharapkan akan ada peraturan lebih lanjut di bidang pengumpulan data, tetapi terutama dalam perdagangan data, selain undang-undang yang sudah berlaku. Di Austria, misalnya, perdagangan data sudah diatur dalam Undang-Undang Regulasi Perdagangan (Gewerbeordnung). **Lebih lanjut**, pembatasan tujuan berlaku di seluruh Eropa sesuai dengan Pasal 6 ayat 1 huruf f. b. GDPR, yang menyatakan bahwa data hanya boleh dikumpulkan untuk tujuan yang ditentukan,

eksplisit, dan sah. Pemrosesan lebih lanjut data untuk tujuan yang tidak sesuai dengan tujuan semula hanya diperbolehkan dalam batas tertentu (Pasal 6 ayat 4 GDPR).

Pada prinsipnya, setiap pemrosesan data, termasuk perdagangan data, harus memiliki **dasar hukum** untuk pemrosesan data. Ini mungkin berarti bahwa subjek data harus memberikan **persetujuan** sukarela dan terinformasi sebagai ekspresi kehendak yang tegas (Pasal 4 ayat 11 GDPR dan Pasal 7 GDPR).

Karena tampaknya tidak terlalu menjanjikan untuk melarang penggunaan kumpulan data tersebut hanya oleh perusahaan-perusahaan Eropa saja, karena data tersebut masih dapat dikumpulkan dan digunakan oleh perusahaan-perusahaan di negara ketiga, sangat mungkin bahwa iklan yang dipersonalisasi dapat dilarang sepenuhnya. Pada Oktober 2023, Dewan Perlindungan Data Eropa (EDPB) mengusulkan untuk melarang Meta memproses data pribadi untuk tujuan periklanan tanpa persetujuan eksplisit, sukarela, dan terinformasi dari subjek data. Hal ini menyebabkan Meta memperkenalkan "bayar atau oke" pada musim semi 2023, di mana Anda dapat menyetujui iklan yang dipersonalisasi atau berlangganan untuk dapat menggunakan Facebook, Instagram, dan lainnya tanpa iklan. Pada Juli 2024, model tersebut sudah ada dalam daftar pemeriksaan otoritas perlindungan konsumen Uni Eropa karena kemungkinan kurangnya transparansi dan informasi yang menyesatkan.

Personalisasi

Penargetan dan tampilan konten yang dipersonalisasi, yang telah dipraktikkan selama bertahun-tahun, berarti bahwa linimasa dan pengalaman web terlihat berbeda untuk semua individu. Namun, karena hal ini tidak hanya digunakan oleh perusahaan untuk mendorong orang membeli barang atau jasa tertentu, tetapi juga oleh pemangku kepentingan lain seperti portal berita, LSM, atau bahkan partai politik, orang memiliki persepsi yang berbeda tentang situasi faktual. Tampilan konten yang dipersonalisasi yang dikendalikan secara algoritmik **menciptakan gelembung**. Hal ini pada gilirannya berarti bahwa tidak ada lagi dasar diskusi yang seragam secara sosial, yang pada akhirnya dapat membahayakan demokrasi. Selain situasi awal ini, sistem AI sekarang digunakan untuk lebih mengoptimalkan personalisasi. Oleh karena itu, tidak mengherankan jika ada aturan ketat untuk bidang ini.

Ada baiknya untuk melihat lebih dekat standar di sini: Apakah yang kita lakukan baik hanya karena efektif? Manipulasi dan menargetkan kelompok rentan “pada saat yang tepat” bukanlah praktik yang baik secara etis dan juga dilarang berdasarkan Undang-Undang AI. Untuk informasi lebih lanjut tentang AI yang dilarang, khususnya dalam kasus iklan pemilihan, lihat kotak di atas tentang praktik AI yang dilarang berdasarkan Pasal 5 ayat 1 huruf a Undang-Undang AI dan Pasal 5 ayat 1 huruf b Undang-Undang AI dan Lampiran III Undang-Undang AI.

Konsumsi Energi dan Keberlanjutan

Selain semua aspek lainnya, Undang-Undang AI juga secara eksplisit membahas perlindungan lingkungan dari dampak buruk sistem AI. Model AI generatif khususnya mengonsumsi sumber daya yang terus meningkat dan sudah memancarkan sejumlah besar CO₂. Di sisi lain, tindakan yang bertanggung jawab secara sosial sesuai dengan kriteria ESG, yaitu lingkungan, sosial, dan tata kelola (lihat bagian 10.6 tentang keberlanjutan).

Namun keberlanjutan tidak hanya melibatkan komponen penilaian siklus hidup. Huruf “S” dalam **ESG** juga tidak boleh dilupakan, seperti yang berulang kali ditekankan oleh Undang-Undang AI. Tindakan yang bertanggung jawab secara sosial juga berarti membentuk tim yang beragam yang anggotanya mencakup sebanyak mungkin perspektif dan bidang studi. Saat ini, ini tidak hanya mencakup representasi yang setara dari orang-orang dari semua gender, tetapi juga pembagian kerja yang tangguh yang mencakup orang-orang kreatif. Mempekerjakan para kreatif tidak hanya memiliki keuntungan bahwa mereka – seperti halnya teknisi – seringkali memiliki perspektif mereka sendiri tentang masalah dan solusinya, tetapi mereka juga membawa kedalaman manusiawi yang nyata ke dalam komunikasi dengan kelompok sasaran melalui karya mereka pada teks, grafik, foto, video, dan lainnya. Sementara generator AI menarik karena hasilnya yang cepat dengan upaya minimal, seperti yang ditunjukkan oleh sebuah studi tentang **Estetika Desain**, kualitas konten yang dihasilkan kini menyebabkan kelelahan tertentu di kalangan masyarakat. Menurut sebuah studi, penyebutan “AI” dalam nama produk atau deskripsi produk menyebabkan **penurunan kepercayaan emosional** dan dengan demikian mengurangi niat pembelian. Hasilnya sama untuk berbagai kategori produk dan layanan, sehingga ada tren yang sesuai. Menggunakan kecerdasan manusia untuk membentuk komunikasi lebih berkelanjutan di banyak tingkatan, terutama dalam hal kesuksesan bisnis jangka menengah dan panjang.

Praktik Terbaik: AI Generatif dalam Kreasi

Jika tidak ada penggunaan AI yang dilarang dalam arti Undang-Undang AI, GDPR, Undang-Undang Persaingan Austria (UWG) atau hukum hak cipta dan secara etis dan berkelanjutan dapat dibenarkan untuk menggunakan model AI generatif dalam periklanan, sejumlah aturan praktik terbaik telah ditetapkan di antara para kreator yang memberikan nasihat etis dan hukum yang baik.

1. Saat menggunakan model generatif, Anda tidak boleh menggunakan nama seniman yang masih hidup atau sudah meninggal atau orang lain dalam petunjuk. Meskipun kecil kemungkinan Anda dapat membuat **plagiarisme** yang tepat dengan model generatif, dimungkinkan untuk mengungkap basis data dengan merekayasa balik model AI. Dalam keadaan tertentu, ini dapat menyebabkan **pelanggaran data** dan **pelanggaran hak cipta**. Dengan tidak menyebutkan nama dalam petunjuk, Anda memastikan bahwa pemegang hak cipta tidak memiliki alasan untuk mengambil tindakan terhadap materi yang dibuat.
2. Selain itu, kami tidak ingin meniru kolega yang gayanya kami sukai, tetapi lebih memilih mengembangkan karya kami sendiri dengan **Unique Selling Proposition (USP)** yang autentik, keunikan, dan nilai pengakuan. Meskipun materi yang dihasilkan tidak tunduk pada hak cipta, hal itu adil bagi para seniman dan karya mereka.
3. Penggunaan model generatif menarik dan menggembirakan bagi sebagian orang. Ini dapat membantu orang-orang kreatif, tetapi tidak harus demikian. Ada orang-orang kreatif yang memiliki ide sendiri dan ingin mengimplementasikannya. Dari segi Unique Selling Points (USP) saja, merupakan ide yang baik untuk membiarkan **kecerdasan** dan kreativitas **manusia** mengimplementasikan teks, gambar, dan elemen musik perusahaan. Dalam keadaan apa pun, mereka yang bertanggung jawab atas kreasi tidak boleh dipaksa

untuk menggunakan alat AI. Sebaliknya, alat AI sekarang begitu sering diintegrasikan ke dalam solusi perangkat lunak yang tersedia secara komersial oleh produsen sehingga larangan ketat tidak lagi masuk akal.

4. Konten yang dihasilkan AI harus selalu diberi **label** sebagai konten yang dihasilkan AI, meskipun Undang-Undang AI hanya mensyaratkan identifikasi AI dalam kasus-kasus seperti chatbot dalam layanan pelanggan atau deepfake (lihat Pasal 50 Undang-Undang AI). Pernyataan dasar memastikan bahwa orang-orang mengetahui apa yang mereka hadapi dan dapat menilai konten tersebut sesuai dengan konteksnya.
5. Selain itu, tergantung pada alat yang digunakan, mungkin diwajibkan secara kontraktual berdasarkan **lisensi** bahwa alat yang digunakan untuk menghasilkan konten tersebut harus disebutkan namanya. Jika penyebutan nama wajib ini diabaikan, hal ini menyebabkan pelanggaran kontrak, yang dapat berakibat mahal dalam keadaan tertentu.

7.9 PARIWISATA

Industri pariwisata mencakup berbagai layanan dan aktivitas yang bertujuan untuk memberikan pengalaman yang menyenangkan dan tak terlupakan bagi para wisatawan. Industri ini memainkan peran penting dalam perekonomian global dengan menciptakan lapangan kerja, mempromosikan pertukaran budaya, dan berkontribusi pada pembangunan regional. Industri pariwisata dapat dibagi menjadi beberapa **segmen**:

1. **Akomodasi**: Hotel, hostel, persewaan liburan, resor, penginapan dan tempat berkemah. Fasilitas-fasilitas ini menawarkan berbagai pilihan akomodasi dan kenyamanan bagi para pelancong.
2. **Transportasi**: maskapai penerbangan, kereta api, perusahaan bus, layanan penyewaan mobil, kapal pesiar, dan bentuk transportasi umum dan pribadi lainnya yang mengangkut para pelancong ke dan di dalam destinasi mereka.
3. **Katering**: Restoran, kafe, bar, dan tempat makan lainnya yang menawarkan pengalaman kuliner kepada para pelancong yang seringkali mencerminkan masakan dan budaya lokal.
4. **Aktivitas rekreasi**: Taman hiburan, pantai, acara olahraga, aktivitas luar ruangan seperti mendaki gunung, menyelam, bermain ski, dan fasilitas rekreasi lainnya yang menawarkan hiburan dan petualangan kepada pengunjung.
5. **Pengalaman budaya**: Museum, situs bersejarah, galeri seni, teater, festival, dan acara budaya lainnya yang menampilkan warisan dan tradisi suatu destinasi.
6. **Pengalaman dan acara budaya**: Museum, situs bersejarah, galeri seni, teater, festival, dan acara budaya lainnya yang menampilkan warisan dan tradisi suatu destinasi.
7. **Agen perjalanan dan penyelenggara tur**: Agen perjalanan menyediakan layanan konsultasi dan pemesanan bagi wisatawan, sementara penyelenggara tur menyusun paket perjalanan lengkap yang mencakup transportasi, akomodasi, makanan, dan aktivitas. Keduanya memainkan peran penting dalam perencanaan dan pengorganisasian perjalanan dengan menawarkan layanan yang disesuaikan dan seringkali bertindak sebagai perantara antara pelanggan dan penyedia layanan.

- 8. Informasi dan layanan pariwisata:** Pusat informasi, platform daring, dan aplikasi seluler yang menyediakan informasi kepada wisatawan tentang atraksi, aktivitas, acara lokal, dan layanan. Sumber daya ini membantu perencanaan dan pelaksanaan perjalanan dengan menyediakan informasi terkini dan bermanfaat.
- 9. Perjalanan bisnis dan MICE (Pertemuan, Insentif, Konferensi, Pameran):** Perusahaan yang menawarkan layanan untuk perjalanan bisnis dan pengorganisasian pertemuan, insentif, konferensi, dan pameran. Segmen ini mencakup perencanaan acara, pemesanan akomodasi dan transportasi, serta layanan khusus untuk pelanggan bisnis.
- 10. Pariwisata kesehatan dan kesejahteraan:** Fasilitas dan layanan yang berfokus pada kesehatan dan kesejahteraan, termasuk spa, pusat kebugaran, penawaran wisata medis, dan layanan terkait kesehatan lainnya. Fasilitas ini menawarkan program untuk meningkatkan kesehatan fisik dan mental para wisatawan.

Kasus Penggunaan: Efisiensi Operasional

Dalam industri pariwisata, efisiensi operasional dan proses yang lancar memainkan peran penting dalam memaksimalkan kualitas layanan dan meminimalkan biaya operasional. Teknologi AI berkontribusi secara signifikan terhadap optimalisasi berbagai proses operasional dengan mengotomatiskan tugas, mengelola sumber daya secara efisien, dan memungkinkan pengambilan keputusan berbasis data. Dengan menggunakan AI, perusahaan di sektor pariwisata dapat meningkatkan efisiensi mereka dengan membebaskan staf sambil memastikan kualitas layanan yang tinggi.

1. Sistem pemesanan otomatis (segmen: semua)

- **Deskripsi:** Sistem berbasis AI mengelola pemesanan secara real-time dengan memperbarui ketersediaan secara otomatis, memproses permintaan pemesanan, dan mengirimkan konfirmasi.
- **Contoh – Kasus Penggunaan AI**
 - Sistem reservasi waktu nyata yang menyinkronkan permintaan di berbagai platform (situs web, aplikasi, agen perjalanan)
 - Manajemen pemesanan secara waktu nyata
 - Pembaruan ketersediaan otomatis
 - Pemrosesan permintaan pemesanan
 - Pengiriman konfirmasi pemesanan
- **Peran yang relevan (Pasal 3 UU AI)**
 - Penyedia (Pasal 3 ayat 3 UU AI): Perusahaan yang mengembangkan sistem pemesanan
 - Penyebar (Pasal 3 ayat 4 UU AI): Hotel, penyebar tur, agen perjalanan
- **Keuntungan:** Pengurangan pemesanan ganda, peningkatan kepuasan pelanggan melalui konfirmasi cepat, optimalisasi hunian kamar
- **Tingkat risiko:**
 - AI berisiko tinggi menurut Pasal 6 UU AI: Tidak, tidak tercantum dalam Lampiran I atau III

- Apakah ada titik kontak dengan AI terlarang? Tidak, tidak ada aplikasi terlarang yang teridentifikasi
- Kewajiban transparansi menurut Pasal 6 UU AI: 50 Tindakan AI Untuk interaksi langsung dengan orang alami

2. Penetapan harga dinamis (Segmen: 1, 2, 3, 4, 5, 6)

- **Deskripsi:** Sistem menyesuaikan harga untuk kamar, penerbangan, dan lainnya. berdasarkan permintaan saat ini, musim, acara di area tersebut, dan harga pesaing secara real-time.
- **Contoh – Kasus penggunaan AI**
 - Sistem manajemen hasil yang menaikkan harga ketika permintaan tinggi atau menawarkan diskon khusus ketika tingkat pemesanan rendah
 - Penyesuaian tarif kamar berdasarkan permintaan dan musim
 - Penetapan harga dinamis untuk penerbangan tergantung pada harga pesaing dan acara
 - Promosi diskon otomatis untuk tarif pemesanan rendah
- **Peran yang relevan (Pasal 3 UU AI)**
 - Penyedia (Pasal 3 ayat 3 UU AI): Perusahaan yang mengembangkan sistem penetapan harga dinamis
 - Pengimplementasikan (Pasal 3 ayat 4 UU AI): Hotel, maskapai penerbangan, pengimplementasikan tur
- **Keuntungan:** Maksimisasi pendapatan, pemanfaatan yang lebih tinggi, penetapan harga yang kompetitif
- **Tingkat risiko:**
 - **AI berisiko tinggi menurut** Pasal 6 UU AI: Tidak, tidak tercantum dalam Lampiran I atau III
 - **Apakah ada titik kontak dengan AI terlarang?** Ya, misalnya jika sistem menggunakan teknik manipulatif atau mengeksploitasi kelompok rentan
 - **Kewajiban transparansi sesuai** dengan Pasal 6 UU AI: 50 Undang-Undang AI: Untuk interaksi langsung dengan orang perseorangan

3. Pemeliharaan Prediktif (segmen: 1, 2, 3, 4, 8, 9)

- **Deskripsi:** Sistem AI memantau kondisi fasilitas, kendaraan, dan lainnya. dan memprediksi pekerjaan pemeliharaan sebelum masalah terjadi.
- **Contoh – Kasus penggunaan AI**
 - Sensor dan algoritma AI yang mendeteksi anomali pada mesin dan memberikan rekomendasi pemeliharaan untuk mencegah kerusakan
 - Sensor dan algoritma AI yang mendeteksi anomali pada kendaraan dan memberikan rekomendasi pemeliharaan. Memprediksi dan merencanakan pekerjaan pemeliharaan
 - Sensor dan algoritma AI yang mendeteksi anomali pada peralatan kebugaran dan perangkat medis serta memberikan rekomendasi pemeliharaan
- **Peran yang relevan (Pasal 3 UU AI)**

- Penyedia (Pasal 3 ayat 3 UU AI): Perusahaan yang mengembangkan sistem pemeliharaan prediktif
 - Pengimplementasikan (Pasal 3 ayat 4 UU AI): Hotel, perusahaan transportasi, pusat kesehatan, fasilitas rekreasi
 - **Keuntungan:** Pengurangan waktu henti, penghematan biaya melalui pemeliharaan preventif, masa pakai sistem yang lebih lama
 - **Tingkat risiko:**
 - **AI berisiko tinggi menurut Pasal 6 UU AI:** Tidak, tidak tercantum dalam Lampiran I atau III
 - **Apakah ada titik kontak dengan AI terlarang?** Tidak, tidak ada aplikasi terlarang yang teridentifikasi
- 4. Manajemen kapasitas dan kontrol pengunjung (segmen: 4, 5, 7)**
- **Deskripsi:** Sistem yang didukung AI menganalisis data pengunjung secara real-time untuk mengoptimalkan kapasitas dan mengelola arus pengunjung.
 - **Contoh – Kasus penggunaan AI**
 - Sistem yang memprediksi jumlah pengunjung dan mengambil tindakan yang tepat untuk mencegah kepadatan pengunjung
 - Sistem yang memprediksi kebutuhan staf dan material berdasarkan jumlah peserta dan jadwal acara
 - **Peran yang relevan (Pasal 3 UU AI)**
 - Penyedia (Pasal 3 ayat 3 UU AI): Perusahaan yang mengembangkan sistem manajemen kapasitas
 - Pengimplementasikan (Pasal 3 ayat 4 UU AI): Tempat acara, taman hiburan, museum
 - **Keuntungan:** Menghindari kemacetan, meningkatkan keamanan dan kenyamanan bagi pengunjung, penggunaan sumber daya yang efisien
 - **Tingkat risiko:**
 - **AI berisiko tinggi menurut Pasal 6 UU AI:** Tidak, tidak tercantum dalam Lampiran I atau III
 - **Apakah ada titik kontak dengan AI yang dilarang?** Tidak, tidak ada aplikasi terlarang yang teridentifikasi
 - **Kewajiban transparansi sesuai dengan Pasal 50 UU AI** Untuk interaksi langsung dengan orang perseorangan
- 5. Sistem tiket otomatis (segmen: 4, 5)**
- **Deskripsi:** Sistem AI mengelola penjualan dan distribusi tiket, termasuk alokasi tempat duduk dan pengecekan validitas tiket.
 - **Contoh:**
 - Platform tiket online yang memproses pesanan secara real-time dan menerbitkan tiket digital
 - Alokasi tempat duduk otomatis
 - Pengecekan validitas tiket

- **Peran yang relevan (Pasal 3 UU AI)**
 - Penyedia (Pasal 3 ayat 3 UU AI): Perusahaan yang mengembangkan sistem tiket
 - Pengimplementasikan (Pasal 3 ayat 4 UU AI): Tempat acara, taman hiburan, museum
 - **Keuntungan:** Peningkatan efisiensi, pengurangan antrian, manajemen tiket yang disederhanakan
 - **Tingkat risiko:**
 - **AI berisiko tinggi sesuai dengan Pasal 6 UU AI:** Tidak, tidak tercantum dalam Lampiran I atau III
 - **Apakah ada titik kontak dengan AI terlarang?** Tidak, tidak ada aplikasi terlarang yang teridentifikasi.
 - Kewajiban transparansi sesuai dengan Pasal 50 UU AI untuk interaksi langsung dengan orang perseorangan
- 6. Kontrol akses otomatis (segmen: 4, 5)**
- **Deskripsi:** Sistem AI untuk verifikasi tiket dan otorisasi akses otomatis, termasuk pengenalan wajah dan data biometrik
 - **Contoh – Kasus penggunaan AI**
 - Verifikasi tiket dan otorisasi akses secara real-time
 - Penggunaan pengenalan wajah dan data biometrik untuk kontrol akses
 - Kombinasi pengenalan wajah dan pemindaian kode QR untuk mempercepat masuk
 - **Peran yang relevan (Pasal 3 UU AI)**
 - Penyedia (Pasal 3 no. 3 UU AI): Perusahaan yang mengembangkan sistem akses bersyarat
 - Pengimplementasikan (Pasal 3 no. 4 UU AI): Tempat acara, taman hiburan, museum
 - **Keuntungan:** Pemrosesan lebih cepat di pintu masuk, peningkatan keamanan, pengurangan antrian
 - **Tingkat risiko:**
 - **AI berisiko tinggi sesuai dengan Pasal 50 UU AI 6. UU AI:** Saat menggunakan metode pengenalan biometrik, Lampiran I No. 1 UU AI mungkin berlaku.
 - **Apakah ada titik kontak dengan AI yang dilarang?** Mungkin, jika melibatkan identifikasi biometrik jarak jauh secara real-time.
 - **Kewajiban transparansi sesuai dengan Pasal 50 UU AI** untuk interaksi langsung dengan orang perseorangan.
- 7. Optimalisasi rute dan manajemen lalu lintas (Segmen: 2)**
- **Deskripsi:** Sistem yang didukung AI menganalisis kondisi lalu lintas secara real-time untuk menentukan rute terbaik bagi kendaraan dan menghindari kemacetan.
 - **Contoh – Kasus penggunaan AI**
 - Analisis kondisi lalu lintas secara real-time
 - Menyarankan rute alternatif untuk menghindari kemacetan

- Mempertimbangkan data lalu lintas, kecelakaan, dan pekerjaan jalan saat merencanakan rute
- **Peran yang relevan (Pasal 3 UU AI)**
 - Penyedia (Pasal 3 no. 3 UU AI): Perusahaan yang mengembangkan sistem optimalisasi rute.
 - Pengimplementasikan (Pasal 3 no. 4 UU AI): Perusahaan transportasi.
- **Keuntungan:** Pengurangan waktu perjalanan, konsumsi bahan bakar lebih rendah, ketepatan waktu meningkat
- **Tingkat risiko:**
 - AI berisiko tinggi menurut Pasal 6 UU AI: Tidak, tidak tercantum dalam Lampiran I atau III
 - Apakah ada titik kontak dengan AI terlarang? Tidak, tidak ada aplikasi terlarang yang teridentifikasi

8. Manajemen Armada (Segmen: 2)

- **Deskripsi:** Sistem AI memantau dan mengelola armada kendaraan untuk memprediksi kebutuhan perawatan dan mengoptimalkan penggunaan kendaraan
- **Contoh – Kasus penggunaan AI**
 - Pemantauan data kendaraan secara real-time
 - Prediksi kebutuhan perawatan
 - Optimalisasi penempatan kendaraan
 - Sistem yang menganalisis data kendaraan secara real-time dan memberikan rekomendasi untuk perawatan atau suku cadang
- **Peran yang relevan (Pasal 3 UU AI)**
 - Penyedia (Pasal 3 ayat 3 UU AI): Perusahaan yang mengembangkan sistem manajemen armada
 - Penyebar (Pasal 3 ayat 4 UU AI): Perusahaan transportasi
 - Operator (Pasal 3 ayat 8 UU AI): Manajer armada, personel perawatan
- **Keuntungan:** Pengurangan waktu henti, masa pakai kendaraan yang lebih lama, efisiensi biaya
- **Tingkat risiko:**
 - **AI berisiko tinggi menurut Pasal 3 UU AI 6. Undang-Undang AI:** Tidak, karena efek utamanya bersifat operasional dan tidak ada keputusan langsung yang dibuat tentang orang
 - **Apakah ada titik kontak dengan AI yang dilarang?** Tidak, tidak ada aplikasi terlarang yang teridentifikasi

9. Sistem pemesanan otomatis (Segmen: 3)

- **Deskripsi:** Sistem yang didukung AI yang memproses pesanan secara real-time, meneruskannya ke dapur, dan memantau tingkat stok
- **Contoh – Kasus penggunaan AI**
 - Pemrosesan pesanan secara real-time
 - Penerusan pesanan otomatis ke dapur

- Pemantauan dan pengelolaan inventaris
- Menu digital dan kios swalayan yang mengirim pesanan langsung ke dapur
- **Peran yang relevan (Pasal 3 Undang-Undang AI)**
 - Penyedia (Pasal 3 ayat 3 Undang-Undang AI): Perusahaan yang mengembangkan sistem pemesanan
 - Pengimplementasikan (Pasal 3 ayat 4 Undang-Undang AI): Restoran
- **Keuntungan:** Pengurangan waktu tunggu, pemrosesan pesanan yang akurat, peningkatan kontrol inventaris
- **Tingkat risiko:**
 - **AI berisiko tinggi menurut Pasal 6 UU AI:** Tidak, tidak tercantum dalam Lampiran I atau III
 - **Apakah ada titik kontak dengan AI terlarang?** Tidak, tidak ada aplikasi terlarang yang teridentifikasi
 - **Kewajiban transparansi sesuai dengan Pasal 6 UU AI:** Tidak ada 50 Regulasi AI: Untuk interaksi langsung dengan orang perseorangan

10. Manajemen Kamar/Rumah Pintar (segmen: 1, 4, 9)

- **Deskripsi:** Kontrol otomatis pencahayaan, pemanasan/pendinginan, dan fungsi kamar lainnya berdasarkan hunian dan preferensi tamu
- **Contoh – Kasus penggunaan AI**
 - Penyesuaian suhu kamar secara otomatis
 - Kontrol pencahayaan berdasarkan kehadiran dan waktu
 - Adaptasi fungsi kamar lainnya sesuai preferensi tamu
- **Peran yang relevan (Pasal 3 UU AI)**
 - Penyedia (Pasal 3 ayat 3 UU AI): Perusahaan yang mengembangkan sistem kamar pintar
 - Pelaksana (Pasal 3 ayat 4 UU AI): Hotel, pusat kebugaran
- **Manfaat:** Penghematan energi, peningkatan pengalaman tamu melalui lingkungan yang disesuaikan
- **Tingkat risiko:**
 - **AI berisiko tinggi menurut Pasal 6 UU AI:** Tidak, tidak tercantum dalam Lampiran I atau III
 - **Apakah ada titik kontak dengan AI yang dilarang?** Tidak, tidak ada aplikasi terlarang yang teridentifikasi
 - **Kewajiban transparansi sesuai dengan Pasal. 50 Regulasi AI:** Untuk interaksi langsung dengan orang perseorangan

11. Penjadwalan Otomatis (Segmen: 9)

- **Deskripsi:** Sistem berbasis AI yang mengelola dan mengoptimalkan janji temu untuk perawatan dan layanan secara real-time
- **Contoh – Kasus penggunaan AI**
 - Sistem yang secara otomatis menemukan waktu yang tersedia untuk perawatan kesehatan dan menerima pemesanan

- Mengelola janji temu secara real-time
- Optimalisasi pemanfaatan sumber daya melalui alokasi janji temu otomatis
- Menghindari pemesanan ganda dan janji temu yang terlewat
- **Peran yang relevan (Pasal 3 UU AI)**
 - Penyedia (Pasal 3 ayat 3 UU AI): Perusahaan yang mengembangkan sistem penjadwalan
 - Pengimplementasikan (Pasal 3 ayat 4 UU AI): Pusat kesehatan, fasilitas kebugaran
- **Keuntungan:** Menghindari pemesanan ganda dan janji temu yang terlewat, penggunaan sumber daya yang optimal
- **Tingkat risiko:**
 - **AI berisiko tinggi menurut Pasal 3 UU AI 6. UU AI:** Tidak, tidak tercantum dalam Lampiran I atau III
 - **Apakah ada titik kontak dengan AI terlarang?** Tidak, tidak ada aplikasi terlarang yang teridentifikasi
 - **Kewajiban transparansi sesuai dengan Pasal 50 UU AI:** Untuk interaksi langsung dengan orang perseorangan

Kasus Penggunaan: Pengalaman Tamu

Pengalaman tamu yang luar biasa adalah inti dari industri pariwisata. Dengan bantuan teknologi AI, kebutuhan dan preferensi tamu individu dapat dipahami dan dipenuhi dengan lebih baik. Sistem berbasis AI menawarkan rekomendasi yang dipersonalisasi, memungkinkan proses layanan yang lancar dan cepat, serta menciptakan pengalaman yang mendalam. Teknologi ini membantu membawa pengalaman tamu ke tingkat yang baru dengan menyediakan penawaran yang disesuaikan dan bantuan segera. Penggunaan AI tidak hanya meningkatkan kepuasan tamu, tetapi juga loyalitas dan kemungkinan mereka untuk kembali.

1. Rekomendasi yang dipersonalisasi (Segmen: semua)

- **Deskripsi:** Sistem berbasis AI memberikan rekomendasi yang dipersonalisasi untuk atraksi lokal, restoran, dan aktivitas berdasarkan data tamu.
- **Contoh – kasus penggunaan AI**
 - Aplikasi atau layar interaktif di lobi yang memberikan saran wisata yang dipersonalisasi berdasarkan pemesanan dan preferensi sebelumnya
 - Menu digital yang memberikan saran yang dipersonalisasi berdasarkan pesanan dan preferensi sebelumnya
 - Aplikasi atau layar interaktif yang menawarkan kiat yang dipersonalisasi atau kiat acara yang disesuaikan
 - Aplikasi acara yang dipersonalisasi, dengan jadwal, pilihan parkir, kiat mengemudi
 - Platform digital yang memberikan saran perjalanan yang disesuaikan berdasarkan data wisatawan
- **Peran yang relevan (Pasal 3 UU AI)**
 - Penyedia (Pasal 3 ayat 3 UU AI): Perusahaan yang mengembangkan sistem rekomendasi

- Pelaksana (Pasal 3 ayat 4 UU AI): Hotel, penyelenggara tur, perencana acara
- **Keuntungan:** Pengalaman tamu yang lebih baik melalui rekomendasi yang disesuaikan, peningkatan kepuasan dan tingkat kunjungan kembali
- **Tingkat risiko:**
 - **AI berisiko tinggi menurut Pasal 6 UU AI:** Tidak, tidak tercantum dalam Lampiran I atau III
 - **Apakah ada titik kontak dengan AI yang dilarang?** Kemungkinan, jika teknik manipulatif digunakan
 - **Kewajiban transparansi sesuai dengan Pasal 50 UU AI:** Untuk interaksi langsung dengan orang perseorangan
 - **Bidang hukum penting lainnya:** Pasal 22 GDPR, § 160 dst. öTKG (Undang-Undang Telekomunikasi Austria), § 25 ayat 1 dtTDDG (Undang-Undang Telekomunikasi Jerman), lihat bagian 7.8 tentang periklanan

2. Asisten virtual/chatbot (segmen: semua)

- **Deskripsi:** Chatbot dan asisten suara menawarkan jawaban atas pertanyaan dan layanan sepanjang waktu.
- **Contoh – Kasus Penggunaan AI**
 - Asisten suara di kamar yang melakukan reservasi restoran, memesan layanan kamar, atau memberikan informasi tentang hotel dan area sekitarnya
 - Chatbot di situs web restoran atau di aplikasi yang menjawab pertanyaan tentang menu, jam buka, dan reservasi
 - Chatbot di telepon yang tersedia untuk menjawab pertanyaan
 - Chatbot yang dapat melakukan pemesanan, menjawab pertanyaan, dan lainnya.
- **Keuntungan:** Layanan tersedia sepanjang waktu, meringankan beban staf, Penyelesaian masalah yang cepat
- **Tingkat Risiko:**
 - **AI berisiko tinggi menurut Pasal 6 UU AI:** Tidak, tidak tercantum dalam Lampiran I atau III
 - **Apakah ada titik kontak dengan AI terlarang?** Tidak, tidak ada aplikasi terlarang yang teridentifikasi
 - **Kewajiban transparansi sesuai dengan Pasal 50 UU AI:** Untuk interaksi langsung dengan orang perseorangan

3. Proses check-in dan check-out/boarding otomatis (segmen: 1, 2)

- **Deskripsi:** Pengenalan wajah dan aplikasi seluler mempercepat dan menyederhanakan proses check-in dan check-out.
- **Contoh – Kasus penggunaan AI**
 - Kios Check-in Mandiri
 - Penyerahan bagasi otomatis
 - Gerbang keberangkatan dengan pengenalan wajah
 - Aplikasi seluler yang memungkinkan tamu mengakses kamar mereka secara langsung tanpa harus menunggu di resepsionis atau saat check-in

- **Peran yang relevan (Pasal 3 UU AI)**
 - Penyedia (Pasal 3 ayat 3 UU AI): Perusahaan yang mengembangkan sistem check-in/check-out
 - Pengimplementasikan (Pasal 3 ayat 4 UU AI): Hotel, maskapai penerbangan
 - **Keuntungan:** Penghematan waktu, peningkatan pengalaman pelanggan, pengurangan antrian
 - **Tingkat risiko:**
 - **AI berisiko tinggi menurut Pasal 6 UU AI:** lihat Lampiran I ayat 13 UU AI (Peraturan tentang Keselamatan Penerbangan), Lampiran III ayat 1 UU AI (pengenalan wajah biometrik), Lampiran III ayat 2 UU AI (infrastruktur kritis)
 - **Apakah ada titik kontak dengan AI terlarang?** Tidak, tidak ada aplikasi terlarang yang teridentifikasi.
 - **Kewajiban transparansi menurut Pasal 3 UU AI:** 50 Undang-Undang AI: Untuk interaksi langsung dengan orang perseorangan
- 4. Pengalaman interaktif dan imersif (segmen: 4, 5)**
- **Deskripsi:** Penggunaan AI dan realitas tertambah (AR) atau realitas virtual (VR) untuk menciptakan pengalaman interaktif dan imersif
 - **Contoh – Kasus penggunaan AI**
 - Aplikasi AR yang menghidupkan situs bersejarah atau pengalaman VR yang memungkinkan pengunjung untuk menghidupkan kembali peristiwa masa lalu
 - Acara & Kegiatan yang menggabungkan pengalaman nyata dengan realitas campuran (MR)
 - Menciptakan pengalaman interaktif dan imersif melalui AR dan VR
 - Penggunaan MR untuk menggabungkan pengalaman nyata dan virtual
 - Menghidupkan situs bersejarah dan peristiwa masa lalu melalui AR dan VR
 - **Peran yang relevan (Pasal 3 Undang-Undang AI)**
 - Penyedia (Pasal 3 ayat 3 Undang-Undang AI): Perusahaan yang mengembangkan teknologi AR, VR, dan MR
 - Pelaksana (Pasal 3 ayat 4 Undang-Undang AI): Museum, tempat acara
 - **Keuntungan:** Daya tarik yang lebih besar dari situs dan acara budaya, koneksi emosional yang lebih dalam dengan pengunjung, bentuk presentasi inovatif
 - **Tingkat risiko:**
 - **AI berisiko tinggi menurut Pasal 6 UU AI:** Tidak, tidak tercantum dalam Lampiran I atau III
 - **Apakah ada titik kontak dengan AI terlarang?** Tidak, tidak ada aplikasi terlarang yang teridentifikasi
 - **Kewajiban transparansi sesuai dengan Pasal. 50 Undang-Undang AI:** Untuk interaksi langsung dengan orang perseorangan
- 5. Umpan balik dan analisis waktu nyata (segmen: semua)**
- **Deskripsi:** Sistem berbasis AI untuk mengumpulkan dan menganalisis umpan balik pengunjung secara waktu nyata untuk terus meningkatkan pengalaman acara

- **Contoh – Kasus penggunaan AI:**
 - Aplikasi seluler dan pemantauan media sosial yang mengumpulkan dan menganalisis umpan balik pengunjung untuk memungkinkan penyesuaian segera
 - Pengumpulan umpan balik pengunjung secara waktu nyata
 - Analisis umpan balik yang dikumpulkan untuk meningkatkan pengalaman
 - Penyesuaian segera berdasarkan umpan balik
 - **Peran yang relevan (Pasal 3 Undang-Undang AI)**
 - Penyedia (Pasal 3 ayat 3 Undang-Undang AI): Perusahaan yang mengembangkan sistem umpan balik dan analisis
 - Pelaksana (Pasal 3 ayat 4 Undang-Undang AI): Tempat acara, museum, taman hiburan, hotel
 - **Keuntungan:** Peningkatan kemampuan adaptasi, kepuasan pengunjung yang lebih tinggi, peningkatan berkelanjutan
 - **Tingkat risiko:**
 - **AI berisiko tinggi menurut Pasal 3 Undang-Undang AI 6. Undang-Undang:** Tidak, tidak tercantum dalam Lampiran I atau III
 - **Apakah ada titik kontak dengan AI terlarang?** Tidak, tidak ada aplikasi terlarang yang teridentifikasi
 - **Kewajiban transparansi sesuai dengan Pasal 50 Undang-Undang AI:** Untuk interaksi langsung dengan orang perseorangan
- 6. Terjemahan waktu nyata (segmen: semua)**
- **Deskripsi:** Sistem yang didukung AI untuk terjemahan percakapan dan teks secara waktu nyata untuk mengatasi hambatan bahasa
 - **Contoh – Kasus penggunaan AI:**
 - Aplikasi seluler dan kios yang menawarkan terjemahan instan dalam berbagai bahasa
 - Pengumpulan umpan balik pengunjung secara waktu nyata
 - Analisis umpan balik yang dikumpulkan untuk meningkatkan pengalaman
 - Penyesuaian langsung berdasarkan umpan balik
 - Terjemahan percakapan secara waktu nyata
 - Terjemahan teks ke dalam beberapa bahasa
 - **Keuntungan:** Pengurangan hambatan bahasa, peningkatan komunikasi dengan tamu internasional
 - **Tingkat risiko:**
 - **AI berisiko tinggi menurut Pasal 6 Undang-Undang AI:** Tidak, tidak tercantum dalam Lampiran I atau III
 - **Apakah ada titik kontak dengan AI terlarang?** Tidak, tidak ada aplikasi terlarang yang teridentifikasi
 - **Kewajiban transparansi sesuai dengan Pasal 50 UU AI:** Untuk interaksi langsung dengan orang perseorangan
- 7. Program kesehatan personal (Segmen: 9)**

- **Deskripsi:** Sistem berbasis AI yang menciptakan program kesehatan dan kebugaran individual berdasarkan data tamu
- **Contoh – Kasus penggunaan AI:**
 - Sistem yang menyarankan rencana nutrisi dan program pelatihan personal berdasarkan data kesehatan dan preferensi
 - Kustomisasi program kesehatan dan kebugaran berdasarkan preferensi dan data kesehatan tamu
- **Peran yang relevan (Pasal 3 UU AI)**
 - Penyedia (Pasal 3 ayat 3 UU AI): Perusahaan yang mengembangkan program kesehatan dan kebugaran
 - Pelaksana (Pasal 3 ayat 4 UU AI): Pusat kebugaran, fasilitas kebugaran
- **Manfaat:** Peningkatan kesehatan dan kepuasan tamu melalui program yang disesuaikan
- **Tingkat risiko:**
 - **AI berisiko tinggi sesuai dengan Pasal 6 UU AI:** Tidak, tidak tercantum dalam Lampiran I atau III
 - **Apakah ada titik kontak dengan AI terlarang?** Tidak, tidak ada aplikasi terlarang yang teridentifikasi
 - **Kewajiban transparansi sesuai dengan Pasal 50 UU AI:** Untuk interaksi langsung dengan orang perseorangan
 - **Ketentuan hukum penting lainnya:** Pasal 9 GDPR

Kasus Penggunaan: Perusahaan Cerdas

Perusahaan cerdas di bidang pariwisata mengandalkan teknologi AI canggih untuk meningkatkan keberlanjutan dan efisiensi operasional. Sistem berbasis AI memantau dan mengendalikan konsumsi energi, mengoptimalkan rantai pasokan, dan memastikan keselamatan tamu dan staf. Melalui pengelolaan sumber daya yang cerdas dan pemeliharaan peralatan yang prediktif, bisnis dapat mengurangi biaya sekaligus membantu melindungi lingkungan. Pendekatan inovatif ini membantu perusahaan untuk beroperasi lebih berkelanjutan dan efisien tanpa mengorbankan kualitas layanan tamu.

1. Efisiensi energi (segmen: 1, 2, 3, 4)

- **Deskripsi:** Sistem AI memantau dan mengoptimalkan konsumsi energi secara real-time untuk mengurangi biaya dan meningkatkan keberlanjutan. Bangunan, kendaraan (pengurangan emisi)
- **Contoh – Kasus penggunaan AI:**
 - Sistem yang mengontrol pencahayaan dan pendingin udara di area publik dan kamar tamu berdasarkan data hunian
 - Sistem yang memantau konsumsi bahan bakar dan memberikan tips kepada pengemudi tentang cara mengemudi lebih efisien
 - Sistem yang memantau konsumsi energi peralatan dapur dan memberikan rekomendasi untuk optimasi
- **Peran yang relevan (Pasal 3 UU AI)**

- Penyedia (Pasal 3 ayat 3 UU AI): Perusahaan yang mengembangkan sistem efisiensi energi
- Pengimplementasikan (Pasal 3 ayat 4 UU AI): Hotel, perusahaan transportasi, restoran
- **Keuntungan:** Pengurangan biaya energi, operasi berkelanjutan, ramah lingkungan
- **Tingkat risiko:**
 - **AI berisiko tinggi menurut Pasal 6 UU AI:** Tidak, tidak tercantum dalam Lampiran I atau III
 - **Apakah ada titik kontak dengan AI yang dilarang?** Tidak, tidak ada aplikasi terlarang yang teridentifikasi

2. Manajemen Keamanan (segmen: 1, 2, 4, 5, 6)

- **Deskripsi:** Penggunaan AI untuk memantau kamera keamanan, mengidentifikasi anomali, dan mendukung personel keamanan
- **Contoh – Kasus penggunaan AI:**
 - Sistem pemantauan cerdas yang mendeteksi perilaku mencurigakan dan memperingatkan personel keamanan secara real-time
 - Sistem untuk memantau kondisi pengemudi (misalnya, deteksi kantuk), analisis data kendaraan secara real-time untuk mencegah kecelakaan
 - Sistem untuk memantau tempat wisata dan area pengunjung yang mendeteksi anomali dan memperingatkan staf keamanan
 - Sistem pemantauan tempat yang mendeteksi anomali dan memperingatkan personel keamanan
 - Dukungan untuk personel keamanan melalui alarm real-time
- **Peran yang relevan (Pasal 3 UU AI)**
 - Penyedia (Pasal 3 ayat 3 UU AI): Perusahaan yang mengembangkan sistem pemantauan
 - Pelaksana (Pasal 3 ayat 4 UU AI): Hotel, tempat acara, perusahaan transportasi
- **Keuntungan:** Peningkatan keamanan bagi tamu dan staf, waktu respons yang lebih cepat terhadap insiden keamanan
- **Tingkat risiko:**
 - **AI berisiko tinggi sesuai dengan Pasal 6 UU AI:** Lampiran I no. 1 UU AI (Biometrik)
 - **Apakah ada titik kontak dengan AI terlarang?** Ya, jika sistem biometrik digunakan untuk tujuan penegakan hukum, ini hanya diperbolehkan dalam batas tertentu.
 - **Kewajiban transparansi sesuai dengan Pasal 50 Undang-Undang AI:** Untuk interaksi langsung dengan orang perseorangan

3. Manajemen Rantai Pasokan (segmen: 1, 2, 3, 4, 5)

- **Deskripsi:** Mengoptimalkan rantai pasokan melalui peramalan dan manajemen inventaris berbasis AI untuk memastikan selalu ada stok yang cukup
- **Contoh – Kasus penggunaan AI:**
 - Sistem yang secara otomatis memicu pesanan berdasarkan pola konsumsi dan waktu pengiriman untuk menghindari hambatan

- Peramalan konsumsi dan kebutuhan stok
 - Pemicu pesanan otomatis berdasarkan pola konsumsi dan waktu pengiriman
 - Optimalisasi manajemen gudang dan rantai pasokan
 - **Peran yang relevan (Pasal 3 Undang-Undang AI)**
 - penyedia (Pasal 3 ayat 3 Undang-Undang AI): Perusahaan yang mengembangkan sistem manajemen rantai pasokan
 - Pengimplementasikan (Pasal 3 ayat 4 Undang-Undang AI): Hotel, restoran, tempat acara, perusahaan transportasi
 - **Keuntungan:** Efisiensi biaya, menghindari hambatan, perencanaan dan manajemen gudang yang lebih baik
 - **Tingkat risiko:**
 - **AI berisiko tinggi menurut Pasal 3 ayat 6 Undang-Undang AI:** Tidak, tidak tercantum dalam Lampiran I atau III
 - **Apakah ada titik kontak dengan AI yang dilarang?** Tidak, tidak ada aplikasi terlarang yang teridentifikasi
- 4. Manajemen Pemeliharaan (segmen: 1, 2, 3, 4, 5, 6)**
- **Deskripsi:** Sistem AI untuk memantau dan memprediksi kebutuhan pemeliharaan wahana dan fasilitas untuk meminimalkan waktu henti
 - **Contoh – Kasus penggunaan AI:**
 - Sensor dan algoritma AI yang memantau kondisi wahana dan fasilitas serta memberikan rekomendasi pemeliharaan
 - Prediksi kebutuhan pemeliharaan berdasarkan data sensor dan algoritma
 - Optimalisasi perencanaan pemeliharaan untuk meminimalkan waktu henti
 - **Peran yang relevan (Pasal 3 UU AI)**
 - Penyedia (Pasal 3 ayat 3 UU AI): Perusahaan yang mengembangkan sistem manajemen pemeliharaan
 - Pelaksana (Pasal 3 ayat 4 UU AI): Taman hiburan, tempat acara, perusahaan transportasi, hotel, restoran
 - Operator (Pasal 3 ayat 8 UU AI): Personil pemeliharaan, manajer fasilitas, penyedia layanan TI
 - **Keuntungan:** Pencegahan kerusakan, masa pakai sistem yang lebih lama, Peningkatan keamanan
 - **Tingkat risiko:**
 - AI berisiko tinggi menurut Pasal 6 UU AI: Tidak, tidak tercantum dalam Lampiran I atau III
 - Apakah ada titik kontak dengan AI terlarang? Tidak, tidak ada aplikasi terlarang yang teridentifikasi

Tingkat risiko:

5. Kontrol kualitas dan pemantauan kebersihan (segmen: 3, 9)

- **Deskripsi:** Sistem yang didukung AI yang memantau kualitas dan kebersihan makanan dan dapur

- **Contoh – Kasus penggunaan AI:**
 - Sensor dan algoritma AI yang mendeteksi anomali dalam kualitas makanan atau memantau kepatuhan terhadap standar kebersihan
 - **Keuntungan:** Memastikan standar kualitas dan kebersihan yang tinggi, menghindari pemborosan makanan, melindungi kesehatan tamu
 - **Tingkat risiko:**
 - **AI berisiko tinggi menurut Pasal 6 UU AI:** Tidak, tidak tercantum dalam Lampiran I atau III
 - **Apakah ada titik kontak dengan AI terlarang?** Tidak, tidak ada aplikasi terlarang yang teridentifikasi
- 6. Transportasi dan manajemen lalu lintas (segmen: 2, 4, 5)**
- **Deskripsi:** Sistem berbasis AI untuk mengoptimalkan arus lalu lintas di sekitar lokasi acara, termasuk manajemen parkir dan transportasi umum
 - **Contoh – Kasus penggunaan AI:**
 - Sistem yang menganalisis arus lalu lintas dan membuat rencana rute lalu lintas dinamis untuk meminimalkan kemacetan
 - Pembuatan rencana rute lalu lintas dinamis untuk menghindari kemacetan lalu lintas
 - Optimalisasi manajemen ruang parkir dan transportasi umum
 - **Peran yang relevan (Pasal 3 UU AI)**
 - Penyedia (Pasal 3 ayat 3 UU AI): Perusahaan yang mengembangkan sistem manajemen lalu lintas
 - Pengimplementasikan (Pasal 3 ayat 4 UU AI): Lokasi acara, taman hiburan
 - **Keuntungan:** Pengurangan masalah lalu lintas, peningkatan aksesibilitas lokasi, kepuasan peserta yang lebih tinggi
 - **Tingkat risiko:**
 - **AI berisiko tinggi menurut Pasal 6 UU AI** Tidak, tidak tercantum dalam Lampiran I atau III
 - **Apakah ada titik kontak dengan AI terlarang?** Tidak, tidak ada aplikasi terlarang yang teridentifikasi
 - **Kewajiban transparansi sesuai dengan Pasal 50 UU AI:** Untuk interaksi langsung dengan orang perseorangan

7.10 AI DALAM PENGEMUDIAN OTONOM

Istilah otonom berarti kemandirian dan swasembada dan sering digunakan dalam kaitannya dengan kendaraan otonom. Ini menyiratkan bahwa kendaraan dapat mengemudi, berakselerasi, dan mengerem secara independen di lalu lintas. Jalur menuju otonomi kendaraan dijelaskan oleh standar SAE J3016, yang didasarkan pada standar terkait. Standar tersebut mendefinisikan level 0 hingga 5, yang menggambarkan kendaraan swakemudi, dimulai dengan tanpa otomatisasi (level 0), bantuan pengemudi (level 1), otomatisasi parsial

(level 2), otomatisasi bersyarat (level 3) hingga otomatisasi tinggi (level 4) dan otomatisasi penuh (level 5).

Selain istilah otonom, istilah otomatis juga dapat ditemukan dalam literatur. Sistem otonom dan independen juga merupakan sistem otomatis. Menurut IEC60050351, arti otomatis didefinisikan sebagai “pelengkapan perangkat sehingga beroperasi sepenuhnya atau sebagian tanpa campur tangan manusia”. Hal ini juga tercermin dalam tingkat otomatisasi untuk pengemudian otomatis. Semakin tinggi tingkat otomatisasi, semakin sedikit peran manusia sebagai pengaman tambahan. Dalam konteks ini, istilah *mengemudi otomatis* berarti pelaksanaan langkah-langkah proses tanpa kendali manusia.

Gambar 7.2 menjelaskan tingkatan mengemudi otonom ini, di mana tingkat 1 berarti bantuan pengemudi seperti kontrol jelajah, tingkat 2 dianggap sebagai otomatisasi parsial, di mana kendaraan dapat mengemudi dan berakselerasi. Tingkat 3 melibatkan otomatisasi bersyarat, di mana kendaraan dapat mengemudi dan berakselerasi serta mengambil alih persepsi lingkungan sekitarnya, tetapi manusia masih harus campur tangan, misalnya pada angkutan otomatis. Pada tingkat 4 (sangat otomatis), kendaraan melakukan semua tugas mengemudi dalam kondisi tertentu, di mana intervensi manusia dimungkinkan dalam kondisi tertentu. Pada tingkat 5 (sepenuhnya otomatis), kendaraan melakukan semua tugas mengemudi yang diketahui dan dipelajari.



Gambar 7.2 Tahapan Otomasi

Kendaraan otonom tingkat 2 (otomatisasi parsial) memiliki satu atau lebih fungsi parsial yang mendukung pengemudi, misalnya kontrol jelajah otomatis atau perubahan jalur otomatis. Kendaraan otonom level 4 (sangat otomatis), di sisi lain, mampu mengemudi secara

otonom tanpa pengemudi terlibat dalam pengambilan keputusan operasional. Saat ini tidak ada kendaraan di Eropa yang diizinkan untuk mengemudi secara sangat otomatis (level 4) atau sepenuhnya otonom (level 5) tanpa operator sesuai dengan peraturan lalu lintas jalan nasional (StVO, Kode Lalu Lintas Jalan Austria).

Selain standar SAE, terdapat klasifikasi lain karena kurangnya kedalaman teknis. Ini adalah Domain Desain Operasional (ODD), yang mendefinisikan kondisi operasi spesifik di mana sistem pengemudian otomatis harus bekerja dengan benar dan aman. Oleh karena itu, ODD menentukan jenis jalan, rentang kecepatan, kondisi lingkungan (termasuk cuaca, siang/malam hari), hukum dan peraturan lalu lintas yang berlaku, dan batasan lainnya. Setiap kasus penggunaan otomasi Level 1–4 hanya dapat digunakan dalam ODD spesifiknya. Ada kemungkinan bahwa ODD dari suatu kasus penggunaan sangat terbatas, misalnya jalan terpisah atau rute tetap tunggal di jalan umum dengan kecepatan rendah.

Legislasi Austria & Internasional

Di Austria, **AutomatFahrV** (Peraturan Austria untuk Pengemudian Otomatis) diterbitkan pada tahun 2016. Dengan berlakunya amandemen kedua pada April 2022, pengembangan kerangka hukum untuk pengujian sistem otomatis semakin maju. Versi kedua peraturan tersebut menciptakan kasus penggunaan lebih lanjut untuk pengujian otomatis kendaraan.

Peraturan tersebut terdiri dari delapan kasus, lima di antaranya ditujukan untuk pengujian: kendaraan otomatis untuk mengangkut barang, untuk mengangkut penumpang, minibus otomatis, mesin kerja otomatis, dan kendaraan militer. Terdapat juga tiga kasus penggunaan lebih lanjut untuk operasi kehidupan nyata, seperti asisten parkir otomatis.

Selain kasus uji, persyaratan baru diperkenalkan untuk analisis rute dan penilaian risiko saat mendaftarkan solusi mobilitas. Salah satu poin kritik terhadap desain AutomatFahrV adalah pendekatan berbasis kasus, yang spesifik tetapi tidak dirancang untuk masyarakat umum. Karena kemajuan teknologi yang pesat di bidang ini, amandemen lebih lanjut terhadap peraturan asli diperlukan. Oleh karena itu, dapat diasumsikan bahwa undang-undang untuk mengemudi otonom akan didefinisikan dari perspektif umum di masa mendatang, serupa dengan apa yang telah terjadi di Jerman sejak tahun 2021 dengan undang-undang untuk mengemudi otonom.

Selain itu, persyaratan baru telah diperkenalkan untuk analisis rute dan penilaian risiko sehubungan dengan pengenalan kendaraan. Penilaian risiko ini mencakup analisis menyeluruh terhadap rute di area publik di bagian rute individu sepanjang 100–200 m dan saat ini membutuhkan banyak upaya bagi pengembang dan pemberi persetujuan. Di masa mendatang, pengenalan alat analisis dan penilaian rute akan sangat penting ketika produsen memasuki pasar Austria.

Peraturan Keselamatan Umum ada di tingkat internasional (Peraturan UE 2019/2144) peraturan UE ini menetapkan sistem bantuan wajib untuk semua pendaftaran pertama yang baru, seperti kontrol jelajah cerdas, asisten mundur, sistem peringatan kantuk, dan lampu rem darurat untuk mobil penumpang.

Peraturan Pelaksanaan EU 2022/1426 juga relevan di tingkat Eropa. Peraturan ini, yang mulai berlaku pada September 2022, berlaku terkait prosedur dan spesifikasi teknis yang seragam untuk persetujuan tipe sistem pengemudian otomatis kendaraan yang sepenuhnya otomatis. Istilah kendaraan yang sepenuhnya otomatis mengacu pada kendaraan yang akan digunakan dalam rentang operasi yang ditentukan (ODD yang disebutkan di atas), di mana tidak ada lagi pengemudi di dalam kendaraan. Peraturan ini saat ini mencakup seri kecil maksimal 250 unit kendaraan per tahun di suatu Negara Anggota. Peraturan pelaksanaan ini diperkenalkan untuk menilai keamanan sistem sebelum persetujuan dapat diberikan di Uni Eropa. Di Austria, saat ini belum ada perusahaan yang menggunakan persetujuan ini, karena peraturan saat ini (AutomatFahrV) untuk transportasi penumpang otomatis hanya mengizinkan pengujian.

Terakhir namun tidak kalah penting, ada UNECE-R 157, yang mulai berlaku pada Januari 2021 dan yang, terkait dengan Sistem Penjaga Jalur Otomatis (Automated Lane Keeping Systems/ALK), mengatur situasi untuk sistem level 3. Sistem ALK mengambil alih penjagaan jalur otomatis di jalan raya atau jalan yang menyerupai jalan raya hingga kecepatan 60 km/jam. Di Jerman, persetujuan tipe pertama untuk sistem ALK telah diberikan kepada Mercedes Benz.

Peraturan Perlindungan Data Umum (General Data Protection Regulation/GDPR) juga relevan dari perspektif internasional dan Eropa. Kendaraan otonom terdiri dari sejumlah besar unit kontrol dan sensor terkait yang membaca data dan meneruskannya ke pabrikan. Mercedes, misalnya, mencatat data posisi GPS, jarak tempuh, konsumsi bahan bakar, pengisian tangki, tekanan ban, dan tingkat cairan operasional di dalam kendaraan.

Dalam konteks ini, laporan aktivitas tahun 2015 tentang perlindungan data telah menyatakan bahwa tindakan pencegahan yang tidak memadai sedang dilakukan untuk memastikan bahwa tidak ada profil pergerakan pribadi yang dapat dibuat di sektor antar mobil berdasarkan data mengemudi yang dipertukarkan. Menurut GDPR, profil pergerakan juga merupakan data pribadi (lihat bab 4).

Persepsi kendaraan terhadap lingkungannya memastikan bahwa objek dan orang dikenali oleh kamera dan bahwa kendaraan bereaksi terhadapnya dengan mengerem. Metode kecerdasan buatan (AI) digunakan dalam pengembangan algoritma pengenalan orang ini. Algoritma "You look only once" (YOLO) memastikan bahwa orang dikenali secara real-time, di mana prosesnya terdiri dari jaringan saraf yang "terlatih". YOLO termasuk dalam kelompok pembelajaran mendalam berbasis grid - Ini berarti bahwa gambar dipecah menjadi raster dan fitur dicari dalam gambar raster. Identitas atau karakteristik pribadi orang tersebut tidak relevan dengan proses tersebut; objek yang dikenali hanya ditandai dengan persegi panjang.

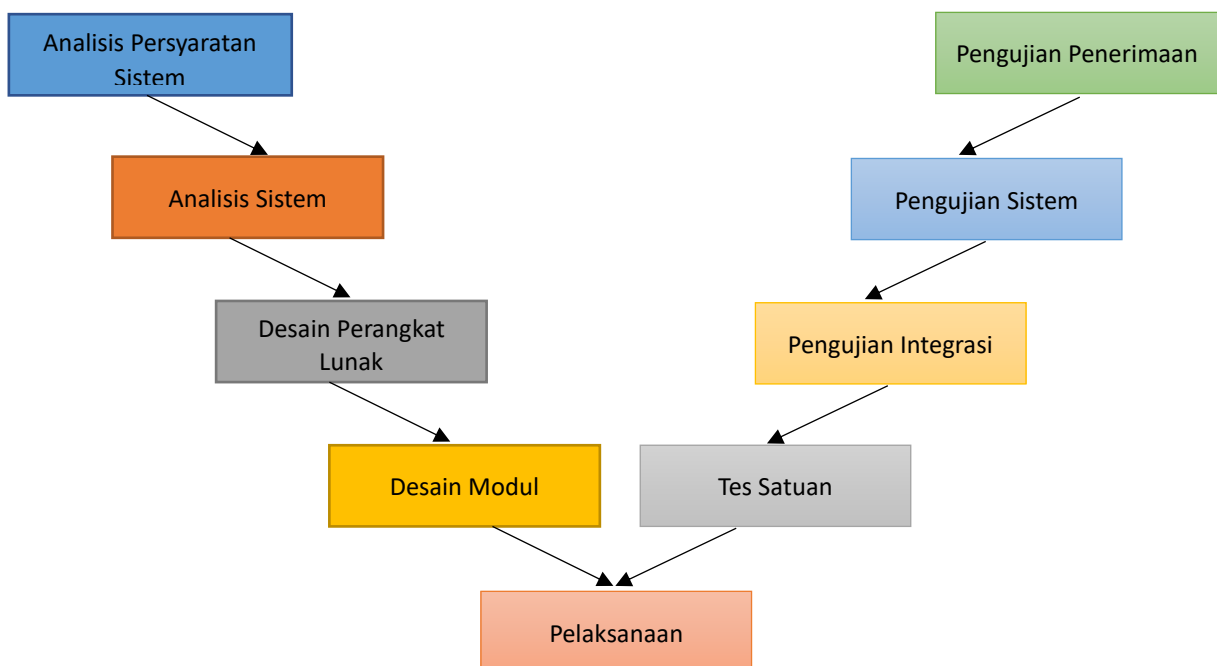
Pengembangan Fungsi Pengemudian Otonom

Dalam pengembangan pengemudian otonom, standar ISO 26262 mendefinisikan keselamatan fungsional. Di sini didefinisikan sebagai "tidak adanya risiko yang tidak wajar akibat bahaya yang dapat terjadi sebagai akibat dari perilaku sistem yang salah". Di mana perilaku yang salah adalah "kegagalan atau perilaku yang tidak disengaja dari suatu elemen dalam kaitannya dengan tujuan desainnya selama pengembangan".

Model V adalah model proses langkah demi langkah yang digunakan untuk integrasi dan pengembangan perangkat lunak dalam pengemudian otonom. Pada umumnya, tidak hanya satu fungsi yang dikembangkan, tetapi beberapa persyaratan untuk pengenalan objek didefinisikan dalam analisis persyaratan, yang kemudian diimplementasikan dalam arsitektur sistem (langkah 2) dan dalam arsitektur perangkat lunak (langkah 3). Kode perangkat lunak yang sebenarnya dapat ditemukan dalam arsitektur perangkat lunak dan dalam desain. Bagian kanan diagram mendefinisikan pengujian fungsi – tergantung pada tahap di sisi kiri, pengujian yang sesuai dilakukan di sisi kanan.

ISO 26262 juga mencakup penilaian risiko fungsi pengemudian otonom. Hal ini dilakukan dengan menggunakan analisis mode kegagalan dan dampaknya (FMEA), analisis pohon kejadian (ETA) atau analisis pohon kesalahan (FTA) yang didukung. Dalam pengembangan fungsi berbasis AI untuk pengemudian otonom, pengembangan sesuai dengan ISO 26262 merupakan metode standar untuk beralih dari persyaratan perangkat lunak ke pengujian sistem dan dengan demikian memastikan transparansi.

Pendekatan menurut ISO 26262 untuk mencapai risiko yang dapat diterima ditunjukkan pada Gambar 7.3 dengan mengacu pada diskusi serupa tentang Tingkat Integritas Keselamatan (SIL) dari IEC 61508. Risiko sementara yang tinggi (ASIL D) menyiratkan pengurangan risiko yang besar yang dibutuhkan selama pengembangan, yang menghasilkan persyaratan yang ketat untuk pengembangan suatu produk. Risiko sementara yang rendah (misalnya ASIL A), di sisi lain, menyiratkan tingkat pengurangan risiko yang rendah yang dibutuhkan, yang menghasilkan persyaratan yang kurang ketat untuk pengembangan suatu item. Risiko yang dapat diterima tidak didefinisikan secara eksplisit dalam ISO 26262, tetapi ditentukan oleh persyaratan khusus ASIL melalui spesifikasi tujuan keselamatan untuk pengembangan produk.



Gambar 7.3 Model V Pengembangan Perangkat Lunak

Undang-Undang AI dan Pengemudian Otonom

Berdasarkan model pengembangan perangkat lunak yang disajikan, dapat dilihat bahwa banyak sub-fungsi yang terlibat dalam pengembangan perangkat lunak untuk pengemudian otonom, yang membuat klasifikasi dalam kasus Undang-Undang AI menjadi tidak mudah.

Dalam konteks pengemudian otonom, pemendekan pengembangan – validasi/pengujian – dan homologasi sesuai dengan semua kondisi kerangka hukum dan kualitatif akan diperlukan. Secara khusus, dapat diamati bahwa AI akan semakin banyak digunakan dalam validasi perangkat lunak. Ini adalah satu-satunya cara untuk membuat jumlah kode perangkat lunak dapat dikelola.

Di masa depan, Undang-Undang AI akan dimulai pada tahap pengembangan dan menetapkan bahwa sistem pengenalan objek yang digunakan dalam kendaraan (semi-)otonom harus menjalani prosedur pengujian dan validasi yang ketat untuk memastikan keamanan dan keandalannya, karena diklasifikasikan sebagai aplikasi berisiko tinggi. Alasannya adalah jika fungsi pengenalan objek gagal, orang tersebut tidak dikenali dan karenanya dapat tertabrak dan terluka.

Prosedur-prosedur yang disebutkan di atas dari model V harus diintegrasikan ke dalam pengembangan sistem validasi berbasis AI untuk memungkinkan kontrol sistem yang efisien. Meskipun demikian, masih perlu untuk melibatkan manusia dalam operasi nyata dalam konteks keseluruhan validasi dan pengujian.

Bersama dengan AVL LIST, TÜV Süd telah mengembangkan prosedur untuk menguji kendaraan otonom di masa mendatang. Untuk validasi dan homologasi yang efisien, yaitu persetujuan kendaraan dan komponen kendaraan, kombinasi pengujian virtual dan nyata di bangku uji dan di lapangan uji sangat penting untuk dapat memecahkan kompleksitas dan variasi situasi. Saat ini tidak ada peraturan hukum internasional yang berlaku untuk fungsi mengemudi otomatis, tetapi ada kegiatan yang sedang berlangsung, misalnya di Perserikatan Bangsa-Bangsa.

Sehubungan dengan Undang-Undang AI, perlu juga merujuk pada Lampiran I, yang tidak mengklaim bersifat menyeluruh. Penerapan suatu undang-undang yang tercantum dalam Lampiran I mengarah pada asumsi bahwa itu adalah sistem AI berisiko tinggi. Untuk tujuan ini, sistem AI yang digunakan harus merupakan komponen keselamatan suatu produk sesuai dengan salah satu peraturan perundang-undangan yang disebutkan di atas, atau produk itu sendiri adalah sistem AI, atau sistem AI harus menjalani penilaian kesesuaian dengan peraturan perundang-undangan yang tercantum sebagai suatu produk.

Selain Undang-Undang AI, Lampiran I memuat ketentuan-ketentuan berikut yang berkaitan dengan kendaraan otonom:

- Peraturan (UE) No. 168/2013 Parlemen Eropa dan Dewan tanggal 15 Januari 2013 tentang persetujuan dan pengawasan pasar kendaraan roda dua atau tiga dan kendaraan roda empat

- Peraturan (UE) 2018/858 Parlemen Eropa dan Dewan tanggal 30 Mei 2018 tentang persetujuan dan pengawasan pasar kendaraan bermotor dan trailernya, serta sistem, komponen, dan unit teknis terpisah yang ditujukan untuk kendaraan tersebut
- Peraturan (UE) 2019/2144 Parlemen Eropa dan Dewan tanggal 27 November 2019 tentang persyaratan persetujuan tipe untuk kendaraan bermotor dan trailernya, serta untuk sistem, komponen, dan unit teknis terpisah yang ditujukan untuk kendaraan tersebut, sehubungan dengan keselamatan umum dan perlindungan penumpang dan pengguna jalan yang rentan

BAB 8

SEKTOR PUBLIK

8.1 “PENGAMBILAN KEPUTUSAN PUBLIK” DAN AI

Ketika mempertimbangkan penggunaan sistem AI di bidang pengambilan keputusan di sektor publik, penting untuk diingat **bahwa prosedur administrasi yang sepenuhnya otomatis**, misalnya dalam konteks penerbitan penilaian pajak di administrasi pajak, sudah mapan di Austria dan sesuai dengan prosedur standar. Sistem yang digunakan di sini biasanya didasarkan pada prinsip pengkodean yang jelas yang dirancang dalam bentuk perintah jika-maka dan oleh karena itu selalu memproses data dengan cara yang sama. Dalam konteks ini, yang dibicarakan adalah apa yang disebut sistem berbasis aturan, yang tidak dapat diklasifikasikan sebagai AI (lihat § 96 öBAO (Kode Fiskal Federal Austria)).

Sebaliknya, sistem AI, yang digunakan oleh pengguna sebagai **alat bantu pengambilan keputusan** atau alat pengambilan keputusan otomatis sepenuhnya, menganalisis pola dan aturan yang mendasari data untuk menerapkannya, misalnya, pada berbagai dokumen aplikasi sebagai bagian dari proses subsumsi karakteristik faktual dari dasar klaim. Semakin kompleks mekanisme pembelajaran mandiri, semakin sulit bagi pihak yang bertanggung jawab untuk memahami setiap langkah dalam proses pengambilan keputusan. Alat pengambilan keputusan tersebut tidak hanya membuka ruang lingkup penerapan Undang-Undang AI, tetapi juga diklasifikasikan sebagai berisiko tinggi menurut metodologinya, tergantung pada tujuan pemberian klaim untuk layanan yang akan diperiksa, dan tunduk pada peraturan penggunaan yang lebih ketat. Selain ketentuan yang timbul dari Undang-Undang AI, harus selalu diingat bahwa ketentuan prosedur nasional yang relevan yang sama berlaku untuk alat pengambilan keputusan otomatis seperti halnya prosedur administrasi tradisional, terlepas dari apakah itu sistem AI atau bukan. Hal ini mencakup, khususnya, hak pemohon untuk didengar, hak untuk mendapatkan pernyataan alasan atas keputusan tersebut dan **hak untuk mendapatkan perlindungan hukum yang efektif**.

Kasus Penggunaan dalam Lampiran III UU AI

Lampiran III UU AI berisi daftar kemungkinan aplikasi sistem AI yang tingkat risikonya telah diidentifikasi atau dapat diprediksi. Kasus penggunaan yang ada berkaitan khususnya dengan bidang-bidang di mana penggunaan AI dianggap sangat "sensitif" karena bidang aktivitas yang bersangkutan dan fungsi sistem yang bersangkutan. Dalam kasus-kasus ini, peningkatan persyaratan untuk kualitas data yang tinggi, dokumentasi dan ketertelusuran, transparansi, pengawasan manusia, presisi, dan ketahanan yang diatur dalam UU AI dimaksudkan untuk mengurangi risiko gangguan terhadap hak-hak fundamental atau risiko keamanan yang terkait dengan AI ini yang tidak tercakup oleh peraturan perundang-undangan lain yang ada (lihat Pertimbangan 72 dan 73 UU AI).

Aturan klasifikasi untuk sistem AI berisiko tinggi dapat ditemukan dalam Pasal 6 UU AI, di mana Pasal 6 ayat 2 dan 3 UU AI sangat relevan untuk kasus-kasus penerapan UU AI yang tercantum dalam Lampiran III UU AI. Sebagai prasyarat penting agar kasus-kasus yang tercantum dalam Lampiran III UU AI dapat diklasifikasikan sebagai sistem berisiko tinggi, Pasal 6 ayat 3 UU AI menyatakan bahwa kasus-kasus tersebut tidak menimbulkan risiko bahaya yang signifikan terhadap kesehatan, keselamatan, atau hak-hak dasar manusia dan tidak secara signifikan memengaruhi hasil pengambilan keputusan, antara lain.

Selain itu, suatu sistem dalam lingkup Lampiran III tidak dianggap berisiko tinggi sesuai dengan Pasal 6 ayat 3 UU AI jika:

- sistem AI dimaksudkan untuk melakukan tugas prosedural yang didefinisikan secara sempit (huruf a),
- sistem AI dimaksudkan untuk meningkatkan hasil yang sebelumnya dicapai oleh aktivitas manusia (huruf b),
- sistem AI dimaksudkan untuk mengenali pola keputusan atau penyimpangan dari pola keputusan sebelumnya dan tidak dimaksudkan untuk menggantikan atau memengaruhi penilaian manusia yang telah diselesaikan sebelumnya tanpa tinjauan manusia yang sesuai (huruf c),
- sistem AI dimaksudkan untuk melakukan tugas persiapan untuk penilaian yang relevan untuk tujuan kasus penggunaan yang tercantum dalam Lampiran III (huruf d).

Contoh: Alokasi Manfaat Sosial

Salah satu kasus penggunaan untuk sistem Lampiran III berisiko tinggi adalah sistem AI yang dimaksudkan untuk digunakan “oleh otoritas publik atau atas nama otoritas publik untuk menilai apakah orang perseorangan berhak atas bantuan dan layanan publik dasar, termasuk layanan kesehatan, dan apakah manfaat dan layanan tersebut akan diberikan, dibatasi, ditarik, atau diklaim kembali” (lihat Lampiran III no. 8 huruf a UU AI). Ini sudah menyiratkan bahwa ini adalah kasus di mana otoritas bertindak sebagai penyebar dalam arti Pasal 3 no. 4 UU AI.

Salah satu skenario yang mungkin untuk pemberian manfaat sosial kepada orang perseorangan oleh otoritas yang berwenang adalah pembayaran manfaat kesejahteraan sosial kepada orang-orang yang berisiko tinggi mengalami kemiskinan. Menurut dasar hukum nasional masing-masing (lihat misalnya di Jerman § 27 SGB XII. (Kode Sosial Jerman) atau § 5 SH-GG (Undang-Undang Dasar Bantuan Sosial Jerman)), siapa pun yang tidak mampu atau tidak cukup mampu untuk menutupi biaya hidup yang diperlukan dari sumber daya dan sarana mereka sendiri berhak atas manfaat. Otoritas nasional yang berwenang harus memeriksa sejauh mana sumber daya keuangan pribadi orang tersebut tersedia, khususnya pendapatan dan aset yang ada atau klaim yang belum terselesaikan terhadap pihak ketiga, dan lainnya., serta situasi kehidupan orang yang berhak menerima manfaat. Verifikasi dokumen yang diterima dan rekonsiliasi dengan otoritas lain seperti otoritas suaka, layanan ketenagakerjaan, dan lainnya. dapat dilakukan menggunakan sistem otomatis. **Proses subsumsi** untuk fakta-fakta individual yang akan diperiksa berpotensi diambil alih oleh sistem AI. Selain itu, ada hak tambahan untuk bantuan sosial (manfaat sosial minimum yang berorientasi pada kebutuhan

di Austria) jika pemohon tidak menerima manfaat dari sumber lain seperti tunjangan pengangguran.

Dengan asumsi bahwa verifikasi kelayakan untuk tunjangan sosial, seperti tunjangan sosial minimum yang berorientasi pada kebutuhan, dapat dilakukan oleh sistem otomatis, ini akan menjadi kasus di mana otoritas harus memverifikasi kelayakan seseorang untuk tunjangan sosial publik dasar, keberadaan persyaratan yang sesuai seperti tempat tinggal utama, batas pendapatan, cakupan kebutuhan perumahan, dan lainnya. Jika aplikasi tersebut sekarang digunakan oleh staf administrasi sebagai pelaksana dalam arti Pasal 3 ayat 4 UU AI untuk membuat keputusan dalam konteks prosedur administrasi yang memberikan atau menolak *hak atas bantuan dan layanan publik dasar* (Lampiran III ayat 5 huruf a UU AI) atau mendistribusikan sumber daya yang ada, ini memengaruhi ruang lingkup penerapan sistem AI berisiko tinggi dan kemudian diatur lebih ketat. Sistem yang digunakan kemudian harus memenuhi persyaratan yang ditetapkan dalam Pasal 2 dan 3 UU AI. Sesuai dengan Pasal Berdasarkan Pasal 26 UU AI, administrasi sebagai pelaksana sistem berkewajiban untuk mengambil langkah-langkah teknis dan organisasi yang tepat untuk memastikan bahwa sistem tersebut dapat digunakan sesuai dengan petunjuk penggunaan yang terlampir pada sistem (lihat Pasal 13 ayat 2 UU AI). Pelaksana harus menugaskan pengawasan manusia kepada orang-orang yang memiliki kompetensi, pelatihan, dan otorisasi yang diperlukan serta memberikan dukungan yang diperlukan (Pasal 13 UU AI; Pasal 14 ayat 2 UU AI).

Jika seseorang telah mengajukan permohonan kepada badan publik sebagai pemohon dan dirugikan secara signifikan oleh **proses pengambilan keputusan** yang sah secara hukum dalam pemberian layanan publik atau penyediaan layanan atau jika ada dampak buruk lainnya terhadap kesehatan, keselamatan, atau hak-hak dasar pemohon, Pasal 86 UU AI memberikan kewajiban transparansi. Pemohon berhak menerima penjelasan yang jelas dan bermakna dari badan publik tentang peran sistem AI dalam proses pengambilan keputusan dan tentang elemen-elemen terpenting dari keputusan yang diambil.

Transparansi harus dirancang sedemikian rupa sehingga para pengimplementasi dapat memahami bagaimana sistem AI bekerja, bagaimana fungsionalitasnya dievaluasi, dan bagaimana kekuatan dan keterbatasannya diidentifikasi (Pertimbangan 72 UU AI). Penyedia sistem tersebut dalam arti Pasal 3 ayat 3 UU AI harus mengambil langkah-langkah yang tepat untuk memungkinkan pengambilan keputusan yang transparan oleh badan publik sebagai pengimplementasi ketika memasarkan dan mengoperasikannya.

Pertanyaan apakah layanan dukungan dan layanan yang disediakan oleh otoritas publik atau badan publik lainnya dianggap berisiko tinggi dalam arti UU AI akan menjadi "signifikansi". Mungkin ada potensi masalah demarkasi dalam kasus-kasus individual ketika menyangkut pertanyaan apakah sistem AI harus dinilai sebagai berisiko tinggi.

Terlepas dari GDPR, pemohon selalu dilindungi oleh Pasal 3 ayat 3 UU AI. 22 GDPR ketika menggunakan alat pengambilan keputusan yang sepenuhnya otomatis jika alat tersebut digunakan untuk mengevaluasi aspek pribadi individu ("**pembuatan profil**"), keputusan tersebut memiliki efek hukum pada orang tersebut dan/atau secara signifikan mempengaruhinya dengan cara yang serupa (lihat juga Bab 4, Perlindungan data)

Contoh: Alokasi Tempat Taman Kanak-kanak

Sistem AI sudah digunakan di administrasi Warsawa untuk alokasi tempat taman kanak-kanak, yang didasarkan pada data yang diberikan oleh orang tua untuk menghitung sejumlah poin tertentu dan mengalokasikan anak yang bersangkutan, yang “mendaftar” untuk tempat taman kanak-kanak, ke fasilitas menggunakan algoritma.

Dengan demikian, sistem tersebut mengasumsikan fungsi alokasi dari masalah sumber daya (potensial). Dalam hal cara kerja AI, ini adalah kombinasi dari sistem berbasis pakar dan aturan, yang dikombinasikan dengan sistem untuk tujuan pengambilan keputusan algoritmik, yaitu dua pengembangan AI yang berbeda dengan tujuan untuk memfasilitasi dan sebagian besar mengotomatiskan proses pengambilan keputusan. Akibatnya, sistem ini tidak hanya digunakan di sektor swasta, tetapi juga di sektor publik dan dengan demikian meluas ke proses pengambilan keputusan di mana administrasi bertindak sebagai penyebar AI.

Salah satu contoh penggunaan sistem AI oleh lembaga publik tercakup dalam Lampiran III no. 3 huruf a UU AI dan merujuk pada sistem AI yang dimaksudkan untuk digunakan untuk menentukan akses atau penerimaan atau alokasi orang perseorangan ke lembaga di semua tingkatan pendidikan dan pelatihan dan oleh karena itu dianggap berisiko tinggi. Kewajiban yang ditetapkan dalam UU AI untuk penyedia, penyebar, dan lainnya. berlaku untuk sistem berisiko tinggi (lihat khususnya Pasal 6, 13, 26 UU AI).

8.2 AI DALAM PENUNTUTAN PIDANA

Undang-Undang AI Uni Eropa yang baru diadopsi juga memberikan aturan untuk penggunaan sistem AI di bidang hukum pidana. Latar belakang langkah-langkah yang dijelaskan lebih rinci di bawah ini adalah, antara lain, meningkatnya penggunaan AI dalam penuntutan pidana di seluruh Eropa, yang dikaitkan dengan kemungkinan campur tangan hak (fundamental). Sistem AI ini dapat digunakan untuk penilaian risiko individu dan prediksi kejahatan serta memengaruhi penuntutan pidana lebih lanjut.

Secara khusus, hal ini menyangkut penggunaan apa yang disebut sistem identifikasi jarak jauh biometrik waktu nyata, yaitu sistem yang didukung AI yang, menurut Pasal 3 Undang-Undang AI, dapat digunakan untuk mengidentifikasi orang tanpa keterlibatan aktif mereka dan, sebagai aturan, dari jarak jauh (lihat Pasal 3 ayat 41 Undang-Undang AI). Hal ini dilakukan dengan membandingkan data biometrik, yaitu data pribadi – yang berkaitan dengan karakteristik tertentu seseorang, misalnya Gambar wajah diperoleh dari “materi hidup” atau “materi yang hampir hidup” (misalnya rekaman video, lihat Pasal 17 UU AI) – dengan data biometrik orang yang disimpan dalam basis data referensi (lihat Pasal 3 ayat 41 UU AI). Fungsi sistem identifikasi jarak jauh biometrik secara real-time memungkinkan “pengumpulan data biometrik, pencocokan, dan identifikasi dilakukan tanpa penundaan (waktu) yang signifikan” (lihat Pasal 3 ayat 42 UU AI). Hal ini memungkinkan dilakukannya pekerjaan kepolisian proaktif untuk menemukan orang-orang yang berpotensi berbahaya, tersangka, atau korban.

Terlepas dari pencegahan kejahatan dan perlindungan korban yang terkait dengan sistem ini, sistem ini juga dapat menyebabkan pelanggaran hak-hak mendasar orang-orang yang menjadi sasaran sistem tersebut. Hal ini menyangkut, misalnya, martabat manusia, hak

untuk tidak didiskriminasi dan, dalam bidang hukum pidana, praduga tidak bersalah dan dengan demikian hak untuk diadili secara adil.

Selain itu, penggunaan sistem semacam itu juga dapat merugikan privasi sebagian besar penduduk dan menyebabkan perasaan diawasi terus-menerus. Dengan demikian, hal itu secara tidak langsung dapat menghambat pelaksanaan kebebasan berkumpul dan hak-hak fundamental lainnya (lihat Pertimbangan 32 UU AI). Ada juga risiko bahwa ketidakakuratan teknis dalam sistem AI dapat menyebabkan hasil yang salah dan dengan demikian menyebabkan diskriminasi, khususnya terkait usia, asal etnis, ras, jenis kelamin, atau disabilitas (lihat Pertimbangan 32 UU AI).

Oleh karena itu, tujuan mendasar untuk memastikan bahwa AI dalam konteks penegakan hukum juga sejalan dengan nilai-nilai Uni Eropa harus diperhitungkan oleh Peraturan yang sekarang telah diadopsi (lihat Pertimbangan 1, 3, 33 UU AI). Dengan demikian, proses legislatif untuk Peraturan AI bersifat konsensual, setidaknya terkait dengan larangan mendasar terhadap kepolisian prediktif yang berkaitan dengan individu. Sebaliknya, pengecualian terhadap larangan tersebut, yaitu Ketika sistem tersebut tetap dapat digunakan, hal itu menjadi poin perselisihan utama yang menyebabkan negosiasi yang panjang dan intensif. Dengan menyeimbangkan berbagai kepentingan, baru pada Desember 2023 tercapai kompromi dan peraturan akhir untuk otoritas kriminal di Uni Eropa.

Penggunaan Sistem Identifikasi Jarak Jauh Biometrik Real-time

Praktik yang Dilarang Secara Fundamental

Pasal 5 UU AI mengatur praktik terlarang yang berkaitan dengan AI dan juga menyebutkan sistem identifikasi jarak jauh biometrik real-time dari orang-orang di area yang dapat diakses publik oleh otoritas penuntut pidana. Ini termasuk sistem identifikasi langsung, tetapi juga sistem dengan "penundaan singkat terbatas" untuk mencegah penghindaran (Pasal 3 no. 42 UU AI). Ini secara eksplisit menetapkan larangan terhadap sistem AI tersebut. Meskipun sistem ini dilarang, penggunaannya tetap diizinkan dalam kondisi tertentu, asalkan diperlukan dalam kasus-kasus luar biasa.

Penggunaan yang Diizinkan dengan Syarat yang Ketat

Sistem identifikasi jarak jauh biometrik waktu nyata diizinkan berdasarkan Pasal 5 ayat 1 huruf h UU AI untuk perlindungan calon korban kejahatan dan orang hilang di satu sisi dan untuk penuntutan (pidana) terhadap orang di sisi lain. Sistem AI ini dapat digunakan jika diperlukan untuk mencari korban penculikan, perdagangan manusia, atau eksploitasi seksual tertentu dan orang hilang (pada umumnya) tidak dapat dihindari (lihat Pasal 5 ayat 1 huruf h sub-ayat i UU AI).

Selain itu, penggunaan sistem identifikasi jarak jauh biometrik waktu nyata juga diizinkan untuk pencegahan ancaman spesifik, signifikan, dan langsung terhadap kehidupan atau integritas fisik seseorang atau untuk pencegahan ancaman serangan teroris yang ada atau yang dapat diperkirakan (lihat Pasal 5 ayat 1 huruf h sub-ayat ii UU AI). Kebolehan juga diberikan untuk melacak atau mengidentifikasi orang-orang yang diyakini telah melakukan kejahatan serius dan oleh karena itu sedang dituntut atas kejahatan serius tertentu yang disebutkan secara eksplisit (lihat Pasal 5 ayat 1 huruf h sub-ayat iii UU AI).

Secara khusus, ini termasuk tindak pidana terorisme, perdagangan manusia, eksploitasi seksual anak dan pornografi anak, perdagangan ilegal narkoba dan zat psikotropika, perdagangan ilegal senjata, amunisi atau bahan peledak, pembunuhan, penganiayaan berat, perdagangan organ atau jaringan manusia, perdagangan zat nuklir atau radioaktif, penculikan, perampasan kebebasan atau penyanderaan (lihat Lampiran II UU AI). Ini mengacu pada tujuan melakukan penyelidikan kriminal, proses pidana atau pelaksanaan hukuman pidana untuk tindak pidana tersebut, dengan syarat Negara Anggota menjatuhkan hukuman penjara atau perintah penahanan untuk jangka waktu minimal setidaknya empat tahun (lihat Pasal 5 ayat 1 huruf h sub-ayat iii UU AI). Poin ini juga berubah sebelum resolusi akhir UU AI. Hukuman untuk pelanggaran yang membenarkan penggunaan sistem untuk tujuan penegakan hukum telah ditingkatkan dari tiga menjadi empat tahun sejak rancangan awal Komisi.

Bagaimana Penggunaan Diizinkan dalam Kasus-Kasus Luar Biasa

- **Khusus untuk konfirmasi identitas**

Jika salah satu pengecualian yang disebutkan di atas untuk penggunaan sistem identifikasi jarak jauh biometrik secara real-time diberikan, maka hal ini tunduk pada persyaratan lebih lanjut yang timbul dari UU AI agar benar-benar diizinkan untuk menggunakan aplikasi AI tersebut. Misalnya, penggunaan oleh otoritas penuntut pidana hanya diizinkan untuk mengkonfirmasi identitas orang tertentu yang bersangkutan dalam kasus-kasus yang disebutkan di atas (lihat Pasal 5 ayat 2 UU AI).

Selain itu, penggunaan sistem AI tersebut harus selalu dilakukan dengan mempertimbangkan dampaknya dalam kasus tertentu; Di satu sisi, berkaitan dengan tingkat keparahan, probabilitas, dan luasnya potensi kerugian jika sistem tersebut tidak digunakan, dan di sisi lain, berkaitan dengan tingkat keparahan, probabilitas, dan luasnya konsekuensi terhadap hak dan kebebasan orang yang terkena dampak jika sistem tersebut digunakan (lihat Pasal 5 ayat 2 UU AI).

Selain itu, penggunaan sistem identifikasi jarak jauh biometrik waktu nyata di ruang publik harus didasarkan pada batasan hukum di tingkat nasional dan oleh karena itu harus dibatasi seminimal mungkin dalam hal waktu, cakupan geografis dan pribadi dari orang yang bersangkutan dan dengan mempertimbangkan bukti yang tersedia (lihat Pasal 5 ayat 2 dan 3 UU AI; Pertimbangan 34 UU AI).

- **Berdasarkan otorisasi dan registrasi**

Otorisasi harus diperoleh sebelum sistem digunakan. Hal ini dikeluarkan oleh otoritas peradilan nasional atau otoritas administratif independen yang berwenang – atas permintaan otoritas penuntut pidana (lihat Pasal 5 ayat 3 UU AI, Pertimbangan 35 UU AI) – jika penilaian dampak telah dilakukan sehubungan dengan hak-hak fundamental dan sistem yang akan digunakan juga termasuk dalam basis data Uni Eropa. Hanya dalam kasus-kasus mendesak yang dibenarkan, sistem dapat digunakan tanpa registrasi, selama hal ini dilakukan segera setelahnya (Pasal 5 ayat 2 UU AI).

Dasar untuk keputusan mengizinkan penggunaan sistem oleh otoritas dalam proses penuntutan adalah bukti objektif atau indikasi yang jelas yang disampaikan kepada otoritas bahwa penggunaan sistem tersebut diperlukan dan proporsional untuk identifikasi dan

pencapaian salah satu tujuan yang disebutkan di atas dan terbatas pada apa yang benar-benar diperlukan (lihat Pasal 5 ayat 3 UU AI).

Keputusan tentang apakah akan memberikan otorisasi untuk kasus tertentu atau tidak, dalam hal apa pun mengikat bagi otoritas penegak hukum yang meminta. Namun, dalam kasus-kasus mendesak dan beralasan, penggunaan sementara tanpa izin juga dimungkinkan dalam konteks ini jika permohonan izin diajukan paling lambat 24 jam setelah penggunaan sistem dimulai (lihat Pasal 5 ayat 3 UU AI). Keputusan tidak boleh dibuat hanya berdasarkan hasil sistem identifikasi jarak jauh biometrik waktu nyata, yang mengakibatkan konsekuensi hukum negatif bagi seseorang. Jika permohonan akhirnya ditolak, setiap penggunaan sistem identifikasi jarak jauh biometrik waktu nyata yang telah dimulai dalam proses penuntutan pidana juga harus segera dihentikan dan semua data dan hasil sebelumnya harus dihapus tanpa penundaan.

▪ **Di bawah pengawasan melalui kewajiban pelaporan**

UU AI sekarang juga menyediakan jenis mekanisme pemantauan yang membuat penggunaan sistem menjadi agak terbatas. Poin kuncinya di sini adalah bahwa setiap penggunaan sistem identifikasi jarak jauh biometrik waktu nyata di area yang dapat diakses publik untuk tujuan penegakan hukum juga harus dilaporkan kepada otoritas pengawasan pasar nasional yang berwenang dan otoritas perlindungan data nasional (lihat Pasal 5 ayat 4 UU AI). Otoritas nasional yang bertanggung jawab atas pengawasan juga harus melaporkan setiap tahun kepada Komisi tentang kasus-kasus penggunaan (lihat Pasal 5 ayat 6 UU AI).

Berdasarkan data yang diberikan oleh Negara Anggota, Komisi akan menerbitkan laporan tahunan tentang penggunaan sistem identifikasi jarak jauh biometrik waktu nyata di ruang publik yang dapat diakses untuk tujuan penegakan hukum di Uni Eropa, meskipun tidak ada data operasional sensitif tentang kasus-kasus spesifik yang disertakan (lihat Pasal 5 ayat 7 UU AI).

Kewajiban Implementasi Negara-Negara Anggota

Secara retrospektif dan dengan mempertimbangkan kepentingan substantif yang saling bertentangan dalam ketentuan ini – di satu sisi, untuk mencegah campur tangan serius terhadap hak dan kebebasan mendasar melalui larangan komprehensif, dan di sisi lain untuk tetap mengizinkan pengecualian untuk penggunaan sistem identifikasi jarak jauh biometrik waktu nyata untuk kepentingan publik (lihat Pertimbangan 33 UU AI) – kini terserah kepada Negara-Negara Anggota untuk mengimplementasikan ketentuan tersebut dalam hukum nasional mereka. Mereka harus menentukan penggunaan sistem tersebut di area yang dapat diakses publik untuk tujuan penegakan hukum sehubungan dengan penerapan, pemberian, pelaksanaan, dan pengawasan, serta memberitahukan ketentuan ini kepada Komisi dalam waktu 30 hari setelah pengesahannya (lihat Pasal 5 ayat 5 UU AI).

8.3 AI DALAM PEMILU DAN PROSES DEMOKRASI

“Tahun 2024 unik (sejauh ini) dalam sejarah manusia karena lebih banyak orang akan memberikan suara dalam pemilu daripada sebelumnya. Tantangan yang diketahui terhadap integritas pemilu tahun ini termasuk serangan politik terhadap independensi badan pemilu,

lingkungan politik yang terpolarisasi, disinformasi, dan bahkan krisis kesehatan masyarakat dan bencana alam.” Menurut Anchor Change Election Cycle Tracker dan data tambahan dari Statista, pemilu akan diadakan di lebih dari 60 negara di seluruh dunia pada tahun 2024, dengan sekitar 2 miliar orang, atau sekitar seperempat dari populasi dunia, akan memberikan suara. Tahun ini disebut sebagai “tahun pemilu super” atau mungkin tahun pemilu terbesar yang pernah ada, dengan pemilu di negara-negara berpenduduk padat seperti Amerika Serikat, Meksiko, India, dan Indonesia yang sangat penting. Selain itu, warga negara dari 27 negara Uni Eropa akan memilih Parlemen Eropa baru dalam pemilihan supranasional. IDEA International menyediakan peta komprehensif dengan detail relevan tentang pemilihan umum 2024.

Diskusi yang Muncul tentang Dampak AI terhadap Demokrasi dan Proses Pemilu

Laporan IDEA International tentang persepsi demokrasi menunjukkan bahwa evolusi teknologi yang berkelanjutan secara konsisten telah memengaruhi pemilu, mulai dari pengenalan radio dan televisi hingga munculnya internet dan media sosial. Namun, kemajuan terbaru dalam kecerdasan buatan (AI) generatif mungkin memiliki dampak yang mendalam, namun belum sepenuhnya dipahami, terhadap pemilu dan integritas proses pemilu yang dirasakan. Selain itu, ada bukti bahwa kampanye disinformasi, yang berpotensi diperkuat oleh AI, memengaruhi kemampuan pemilih untuk mengevaluasi legitimasi pemilu dengan benar. Laporan IDEA mengakui pengaruh teknologi dan AI yang semakin besar terhadap demokrasi dan menyarankan pendekatan yang hati-hati terhadap penggunaan alat-alat ini. Laporan tersebut membahas bagaimana kemajuan dalam AI generatif memengaruhi persepsi kredibilitas pemilu.

- Terdapat kekhawatiran bahwa kampanye disinformasi yang didorong oleh AI dapat melemahkan kemampuan pemilih untuk menilai kredibilitas pemilihan dengan benar. Hal ini menyoroti peran ganda AI sebagai alat potensial untuk mendorong keterlibatan demokratis dan sebagai ancaman yang dapat memengaruhi pemahaman dan kepercayaan publik terhadap proses pemilihan.
- Meskipun dampak AI belum dibahas secara rinci di semua bagian laporan, dampak menyeluruh teknologi ini terhadap demokrasi sudah jelas. Laporan tersebut menunjukkan bahwa seiring teknologi semakin terintegrasi ke dalam kehidupan sehari-hari dan proses demokrasi, teknologi akan memainkan peran penting dalam membentuk persepsi publik tentang demokrasi. Integrasi ini membutuhkan regulasi dan pengawasan yang cermat untuk memastikan bahwa integrasi tersebut mendukung, bukan melemahkan, nilai-nilai demokrasi.
- Temuan menunjukkan bahwa meskipun AI dan teknologi lainnya menawarkan peluang untuk meningkatkan proses demokrasi – seperti pemilihan yang lebih mudah diakses dan efisien – teknologi tersebut juga menimbulkan tantangan yang signifikan. Tantangan tersebut meliputi memastikan keamanan proses pemilihan, melindungi dari penyalahgunaan data pribadi, dan memerangi penyebaran informasi yang salah.
- Hasil survei yang dilakukan oleh IDEA menggarisbawahi perlunya menetapkan standar untuk penggunaan AI dalam proses demokrasi. Ini termasuk mengembangkan

kerangka kerja yang dapat secara efektif menyeimbangkan manfaat AI dalam meningkatkan partisipasi dan transparansi sambil mengatasi risiko yang terkait dengan privasi, keamanan, dan potensi AI untuk digunakan dengan cara manipulatif.

Menurut Freedom House, banyak diskusi tentang AI berakar pada pertanyaan lama tentang tata kelola internet, seperti bagaimana peraturan dapat melindungi masyarakat dari operator negara dan non-negara yang berbahaya sambil mempromosikan sektor swasta yang dinamis dan inovatif. Apa kewajiban hukum yang harus dimiliki perusahaan ketika produk mereka disalahgunakan? Pelajaran yang dipetik dari diskusi selama dekade terakhir tentang pengawasan pemerintah, pentingnya partisipasi aktif oleh masyarakat sipil, dan jebakan dari pengaturan diri yang berlebihan memberikan panduan untuk menavigasi area baru ini. Mengingat peran AI dalam penindasan digital, sangat penting untuk menciptakan kerangka hukum yang dirancang dengan cermat untuk melindungi hak asasi manusia di era digital.

Laporan yang sama menggambarkan gambaran suram tentang menurunnya kebebasan internet di seluruh dunia untuk tahun ke-13 berturut-turut, menyoroti meningkatnya represi digital di negara-negara seperti Iran, Myanmar, dan Filipina. Bahkan negara-negara seperti Kosta Rika, yang pernah dipuji karena kebebasan internetnya, kini menghadapi tantangan dari kebijakan yang memanfaatkan pelecehan daring. Munculnya AI generatif menimbulkan risiko baru dan dapat memicu kampanye disinformasi. Penggunaan teknologi ini untuk memanipulasi diskusi daring telah berlipat ganda dalam sepuluh tahun terakhir dan kini memengaruhi setidaknya 47 pemerintah. Peran AI dalam sensor semakin meningkat, dengan negara-negara otoriter maju menggunakan teknologi chatbot untuk memperketat kendali mereka, dan setidaknya 21 negara menggunakan pembelajaran mesin untuk membungkam unggahan yang tidak diinginkan.

Terlepas dari potensi penindasan yang dimiliki AI, pelajaran dari sejarah tata kelola internet memberikan peta jalan untuk melindungi kebebasan internet. Dunia demokratis harus mengembangkan standar berbasis hak asasi manusia untuk AI yang memperhitungkan ancaman yang ditimbulkan oleh operator negara dan non-negara. Pendekatan ini membutuhkan kolaborasi antara pembuat kebijakan demokratis dan pakar masyarakat sipil untuk memastikan internet yang bebas dan terbuka. Kondisi penggunaan AI saat ini menggarisbawahi pentingnya kebijakan proaktif dan terinformasi untuk menjaga integritas hak asasi manusia secara daring. Meskipun kemajuan teknologi mengkhawatirkan, hal itu juga menawarkan peluang – jika dikelola dengan benar – untuk memperkuat perlindungan yang dibutuhkan untuk kebebasan internet.

Laporan Ipsos memberikan wawasan berharga tentang persepsi global mengenai dampak AI terhadap integritas informasi, khususnya dalam konteks pemilihan umum, berdasarkan analisis yang dilakukan di 29 negara di seluruh dunia. Laporan tersebut menyimpulkan bahwa ada kesadaran yang kuat di berbagai negara bahwa teknologi AI semakin memudahkan pembuatan laporan dan gambar berita palsu yang realistis. Hal ini menggarisbawahi kekhawatiran yang semakin meningkat bahwa AI dapat memperburuk masalah misinformasi dan disinformasi yang sudah menjadi masalah besar di era digital. Namun, kepercayaan dalam membedakan antara berita nyata dan berita palsu sangat

bervariasi dari satu wilayah ke wilayah lain. Sementara beberapa populasi relatif percaya diri dalam kemampuan mereka untuk membedakan kebenaran dari kebohongan, yang lain jauh kurang percaya diri. Perbedaan ini dapat memengaruhi bagaimana masyarakat yang berbeda menanggapi dan mengatur teknologi AI dalam proses pemilihan mereka. Laporan-laporan ini dan laporan lainnya menyoroti persimpangan kritis antara teknologi AI dan integritas demokrasi serta menggarisbawahi kebutuhan mendesak akan langkah-langkah proaktif untuk mengurangi risiko dan memperkuat ketahanan sistem pemilihan di seluruh dunia.

Terdapat kekhawatiran besar bahwa AI generatif dapat secara signifikan mengganggu proses pemilihan, menurut Chatham House. Teknologi ini dapat mengkloning suara, membuat video palsu, dan menghasilkan narasi persuasif yang dapat merusak keaslian pesan kampanye. Sayangnya, penggunaan AI untuk disinformasi telah meningkat, dengan AI digunakan untuk menciptakan keraguan, mencemarkan nama baik lawan, atau memengaruhi debat publik. Berikut adalah dua contoh, tetapi ada ratusan contoh serupa di seluruh dunia dalam konteks pemilihan umum:

- Sebuah iklan politik yang diterbitkan oleh Komite Nasional Republik menggambarkan skenario distopia jika Presiden Joe Biden terpilih kembali: Ledakan di Taipei saat Tiongkok menginvasi, gelombang migran menyebabkan kepanikan di AS, dan darurat militer diumumkan di San Francisco.
- Dalam sebuah video yang dihasilkan oleh kecerdasan buatan, Hillary Clinton tampak menawarkan dukungannya kepada seorang Republikan: "Saya sangat mengagumi Ron DeSantis. Dia adalah tipe pemimpin yang dibutuhkan negara kita."

Bagaimana Seharusnya AI Didefinisikan dalam Konteks Pemilu?

Dalam bidang proses pemilu, definisi AI mencakup pemahaman tentang penerapannya dalam siklus hidup pemilu, mulai dari pendaftaran dan pendidikan pemilih hingga pemungutan dan penghitungan suara yang sebenarnya serta analisis hasil pemilu.

Dalam konteks Eropa, referensi terhadap Regulasi AI sangat penting: *"Sistem AI' berarti sistem berbasis mesin yang dirancang untuk beroperasi dengan berbagai tingkat otonomi dan yang dapat menunjukkan kemampuan adaptasi setelah diterapkan, dan yang, untuk tujuan eksplisit atau implisit, menyimpulkan, dari masukan yang diterimanya, bagaimana menghasilkan keluaran seperti prediksi, konten, rekomendasi, atau keputusan yang dapat memengaruhi lingkungan fisik atau virtual."* (Lihat bagian 3.1, Pendahuluan Undang-Undang AI)

Definisi OECD tahun 2024 adalah referensi bagus lainnya: *"Sistem AI adalah sistem berbasis mesin yang, untuk tujuan eksplisit atau implisit, menyimpulkan, dari input yang diterimanya, bagaimana menghasilkan output seperti prediksi, konten, rekomendasi, atau keputusan yang dapat memengaruhi lingkungan fisik atau virtual. Sistem AI yang berbeda bervariasi dalam tingkat otonomi dan adaptabilitasnya setelah penerapan."*

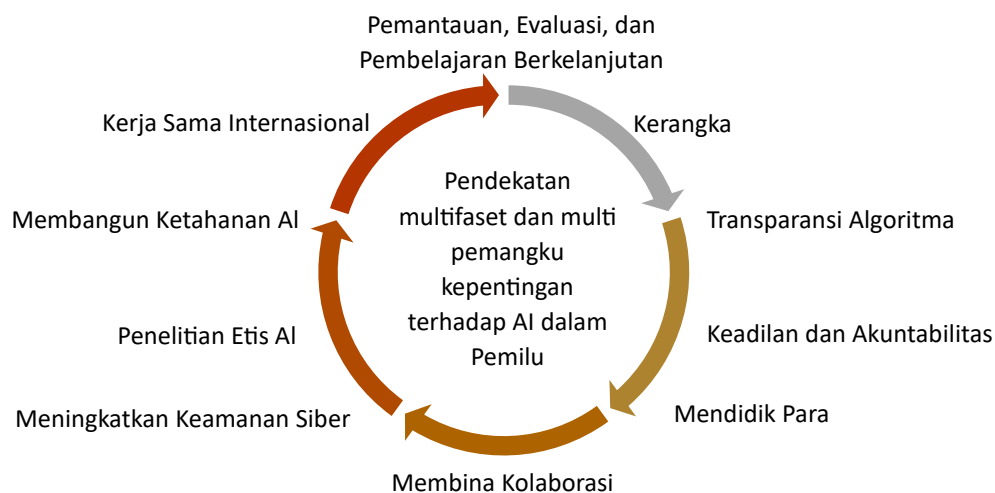
Berdasarkan definisi sistem AI yang ada, dalam konteks pemilihan yang lebih luas, sistem AI menjadi alat dinamis yang mampu belajar dan berevolusi. Misalnya, mereka dapat menganalisis data pemilih dan konstituen untuk meningkatkan penargetan pesan kampanye, memantau tren media sosial untuk mendeteksi misinformasi, atau mengoptimalkan alokasi

sumber daya pemilihan. Beroperasi dengan tingkat otonomi tertentu, sistem ini dapat belajar dari data baru dan menyesuaikan fungsinya setelah penerapan untuk meningkatkan kinerja dalam mencapai tujuan yang telah ditentukan, baik untuk meningkatkan partisipasi pemilih, memastikan keamanan dan integritas proses pemilihan, atau memberikan akses yang adil terhadap informasi pemilihan.

Memanfaatkan Peluang dan Meminimalkan Risiko melalui Penggunaan AI

Integrasi AI ke dalam konteks pemilihan umum merupakan bidang yang relatif baru. Tanpa kerangka kerja yang komprehensif, kita dapat secara bertahap membangun pedoman dan prinsip umum yang membahas penggunaan teknologi dalam proses demokrasi dan mengatasi tantangan spesifik AI dengan membangun praktik tata kelola internet, tata kelola data, dan bidang lainnya. Kurangnya kerangka kerja yang kuat dan khusus untuk AI dalam pemilihan umum saat ini menggarisbawahi perlunya tindakan mendesak dan khusus dari para pemimpin global, ahli teknologi, dan masyarakat sipil.

Berikut ini mengusulkan kerangka kerja untuk pendekatan multi-lapisan dan multi-pemangku kepentingan terhadap penggunaan AI dalam pemilihan umum.



Gambar 8.1 Pendekatan Multidimensi Dan Multipemangku Kepentingan Terhadap Penggunaan AI Dalam Pemilu

Inti dari pendekatan ini adalah kebutuhan untuk menciptakan kerangka kerja yang kuat dan tangguh yang terus beradaptasi dan dicirikan oleh pemantauan, evaluasi, dan pembelajaran berkelanjutan. Proses dinamis ini mendukung dan dipengaruhi oleh pengembangan dan penegakan kerangka hukum yang ketat yang mengatur penggunaan AI secara etis dalam pemilu. Transparansi algoritma AI sangat diperlukan. Mendidik pemilih sangat penting untuk efektivitas AI dalam pemilu. Dengan mendorong dialog dan kemitraan antara pemerintah, perusahaan sektor swasta, masyarakat sipil, dan organisasi internasional, sikap yang lebih holistik dan proaktif terhadap tantangan dan peluang AI dalam pemilu dapat muncul. Peningkatan keamanan siber merupakan prioritas berkelanjutan karena ancaman siber berkembang seiring dengan kemajuan AI. Melindungi data pemilu dan integritas pemilu dari ancaman ini adalah tugas berkelanjutan yang membutuhkan mekanisme yang waspada.

Penelitian AI yang etis harus memandu pengembangan AI dengan cara yang menjunjung tinggi nilai-nilai demokrasi dan menguji sistem ini secara ketat terhadap standar etika tertinggi. Di tingkat internasional, kolaborasi sangat penting, tidak hanya dalam berbagi praktik terbaik dan pelajaran yang didapat, tetapi juga dalam menyelaraskan standar global yang melampaui batas negara, karena pengaruh pemilu digital tidak mengenal batas. Membangun ketahanan terhadap AI berarti mengantisipasi tantangan dan ancaman di masa depan, bahkan yang belum diketahui. Dengan melalui siklus inovasi dan refleksi yang berkelanjutan ini, masyarakat demokratis dapat berupaya untuk mempertahankan integritas dan kepercayaan dalam proses pemilu mereka di era AI.

Tabel 8.1 Langkah-Langkah Membangun Kepercayaan Untuk Penggunaan AI Dalam Pemilu

Komponen	Contoh
Pengembangan kerangka peraturan	Pemerintah harus memberlakukan undang-undang dan peraturan komprehensif yang mengatur penggunaan AI dalam pemilihan. Ini termasuk mendefinisikan parameter yang jelas untuk penggunaan AI yang etis, menetapkan standar untuk transparansi dan akuntabilitas, dan memastikan bahwa alat AI tidak digunakan untuk memanipulasi perilaku pemilih atau hasil pemilihan. Selain ketentuan Undang-Undang AI (klasifikasi penggunaan AI dalam pemilihan), contoh penting yang terkait dengan AI dalam pemilihan adalah adopsi Kode Etik pada tanggal 9 April 2024 oleh semua partAI politik Eropa, yang bertujuan untuk mempromosikan kampanye pemilihan yang etis dan adil, terutama dalam konteks melindungi pemilihan dari campur tangan asing dan disinformasi. Kesepakatan ini merupakan upaya bersama oleh partAI-partAI ini untuk secara proaktif menghindari penguatan narasi yang merusak nilai-nilai Eropa dan dipimpin oleh entitas di luar Uni Eropa.
Transparansi algoritmik	Algoritma AI yang digunakan dalam proses pemilihan harus transparan sehingga memungkinkan untuk memeriksa dan memahami cara kerjanya, pengambilan keputusan, dan pengaruhnya terhadap pengguna. Transparansi ini sangat penting untuk kepercayaan dan untuk memeriksa sistem ini terhadap bias atau manipulasi. Contoh penting dari lembaga yang dapat memberikan panduan dan dukungan kepada para pemangku kepentingan yang bekerja pada AI dalam pemilihan di Eropa adalah Pusat Transparansi Algoritma Eropa (ECAT) – sebuah badan Komisi Eropa yang memainkan peran sentral dalam memastikan transparansi algoritma. Dengan memberikan dukungan teknis untuk menegakkan Undang-Undang Layanan Digital (DSA), meneliti dampak sosial dari sistem algoritmik, dan mengevaluasi algoritma platform, ECAT membantu memastikan bahwa lanskap digital menjunjung tinggi integritas demokrasi. Melalui kolaborasi dan pembangunan komunitas, lembaga ini mempromosikan metode untuk aplikasi AI yang adil dan bertanggung jawab yang sangat penting untuk menjaga transparansi dan netralitas pengambilan keputusan algoritmik dalam proses pemilihan. Upaya ECAT merupakan bagian penting dari perlindungan pemilihan dari risiko yang terkait dengan pengeditan konten dan disinformasi yang didorong oleh AI.

	Pemerintah Inggris adalah contoh yang baik, karena merupakan salah satu yang pertama memperkenalkan standar transparansi algoritmik untuk departemen pemerintah dan badan sektor publik pada bulan November 2021, bekerja sama dengan Pusat Etika dan Inovasi Data. Pada bulan Februari 2024, pemerintah mengumumkan bahwa penggunaan ATRS (Standar Pencatatan Transparansi Algoritmik) akan diwajibkan untuk semua departemen pemerintah pusat, dengan maksud untuk memperluasnya ke seluruh sektor publik seiring waktu.
Keadilan dan tanggung jawab	Harus ada mekanisme untuk meminta pertanggungjawaban pengembang dan pengguna sistem AI atas pekerjaan mereka. Ini berarti tidak hanya menetapkan standar untuk keadilan dan akurasi, tetapi juga konsekuensi yang dapat ditegakkan untuk penyalahgunaan AI. Penyedia alat AI harus mematuhi standar kualitas, privasi, dan keamanan yang tinggi untuk produk mereka. Mereka harus mengungkapkan data pelatihan eksternal yang digunakan untuk mengembangkan model AI mereka, karena data ini mungkin mengandung bias yang dapat memengaruhi hasil pemilihan. Mereka harus dapat mendemonstrasikan alat AI mereka menggunakan data pemilih negara bagian dan lokal untuk memberikan gambaran realistis tentang kinerja alat tersebut. Setelah akuisisi, otoritas pemilihan negara bagian harus mempertahankan kendali dan kepemilikan atas semua data yang diproses oleh sistem AI.
Mendidik pemilih	Meningkatkan kesadaran dan mendidik pemilih tentang peran AI dalam pemilihan dapat memungkinkan mereka untuk mengevaluasi informasi yang mereka terima secara kritis. Kampanye pendidikan pemilih dapat mencakup informasi tentang cara melawan disinformasi yang dihasilkan AI dan pentingnya pengecekan fakta. “Kampanye pendidikan pemilih yang terencana dan strategis dapat mengurangi dampak misinformasi dan disinformasi yang dihasilkan oleh alat AI”. Berikut adalah contoh inisiatif pendidikan pemilih di AS yang disebut “BEHIND THE HEADLINES.” Kampanye ini, yang berlangsung hingga Hari Pemilihan 2024, menargetkan pemilih perempuan, berkulit gelap, dan Hispanik untuk meningkatkan kesadaran tentang dampak AI dalam pemilihan dan risiko misinformasi. Kampanye ini mencakup sumber daya multibahasa, termasuk konten media sosial, webinar, dan video penjelasan, seperti video yang menunjukkan bagaimana deepfake dibuat menggunakan sulih suara yang dihasilkan AI. Tujuan utama kampanye ini adalah untuk menyoroti personalisasi pesan yang didorong oleh AI, mengungkap prevalensi konten deep fake yang menyesatkan, dan menekankan dampak misinformasi yang dihasilkan AI terhadap perilaku pemungutan suara individu.
Meningkatkan kerja sama	Menciptakan ekosistem kolaboratif yang mencakup lembaga pemerintah, perusahaan teknologi, masyarakat sipil, dan akademisi dapat memfasilitasi berbagi praktik terbaik dan pengembangan strategi yang tepat untuk mengatasi tantangan yang ditimbulkan oleh AI dalam pemilihan umum. Kesepakatan Teknologi untuk Memerangi Penggunaan AI yang Menipu dalam Pemilihan Umum 2024 adalah inisiatif kolektif oleh

	perusahaan teknologi terkemuka untuk memerangi penyebaran konten berbahaya yang dihasilkan AI yang menyesatkan pemilih. Perusahaan seperti Adobe, Google, Microsoft, Meta, dan lainnya telah berkomitmen untuk mengembangkan teknologi yang dapat mendeteksi konten audio, video, dan gambar yang dihasilkan AI yang bertujuan untuk memanipulasi penampilan dan pesan tokoh politik atau menyesatkan pemilih tentang proses pemilihan. Perjanjian tersebut berisi delapan komitmen spesifik, termasuk pengembangan alat sumber terbuka, penilaian berkelanjutan terhadap risiko yang ditimbulkan oleh teknologi tersebut, dan upaya untuk mengekang penyebaran konten yang menyesatkan di platform mereka. Selain itu, perjanjian tersebut menekankan transparansi, keterlibatan publik, dan kampanye pendidikan untuk meningkatkan literasi media dan memperkuat ketahanan masyarakat terhadap ancaman ini. Perjanjian ini dibangun berdasarkan upaya yang telah dilakukan oleh masing-masing perusahaan dan bertujuan untuk melindungi ruang digital dari bahaya AI yang menyesatkan pada periode pemilihan. Contoh menarik lainnya adalah nilai koalisi pemilihan yang dipimpin negara, yang terbukti menjadi mekanisme yang efektif untuk memerangi misinformasi. Dengan menyatukan outlet berita, organisasi pengecekan fakta, dan kelompok lokal di dalam suatu negara, koalisi ini bekerja sama untuk mengatasi kebutuhan spesifik pemilih dan memberikan dukungan dan informasi yang tepat sasaran menjelang pemilihan.
Meningkatkan keamanan siber	Penguatan keamanan siber sistem pemilu terhadap ancaman berbasis AI harus menjadi prioritas. Ini berarti melindungi infrastruktur dari peretasan dan mengamankan data dari analisis AI yang tidak sah yang dapat memengaruhi integritas pemilu. Salah satu contoh alat adalah Cybersecurity Toolkit dengan alat, layanan, dan sumber daya gratis yang disediakan oleh CISA (Cybersecurity and Infrastructure Security Agency of the United States of America).
Promosi penelitian AI yang etis	Mendukung penelitian tentang implikasi etis AI dalam pemilihan dapat memberikan wawasan yang lebih dalam tentang potensi konsekuensi penggunaannya dan memandu pengembangan teknologi yang memperkuat prinsip-prinsip demokrasi. Contoh studi tentang dampak teknologi baru pada pemilihan yang bebas dan adil ("Studi Pemilihan") dapat ditemukan dalam sumber. Meskipun tinjauan literatur berasal dari tahun 2021, tinjauan ini memberikan gambaran umum dan analisis literatur relevan yang diidentifikasi dan ditinjau dalam konteks studi tentang dampak teknologi baru pada pemilihan yang bebas dan adil. Pertanyaan penelitian berikut digunakan dalam pencarian: Bagaimana penggunaan teknologi baru seperti kecerdasan buatan dan teknologi blockChain/buku besar terdistribusi (DLT) dan teknik daring baru seperti penargetan mikro dan penyaringan algoritmik, yang bergantung pada data pemilih untuk membuat dan menyebarkan disinformasi daring dan menargetkan berbagai kategori pemilih, dapat berdampak pada hasil pemilihan dan kepercayaan publik terhadapnya? Apa saja potensi risiko dan peluang teknologi ini ketika digunakan dalam konteks pemilihan? Bagaimana risiko dapat diminimalkan dan peluang teknologi dapat dimaksimalkan untuk

	memperkuat aturan pemilihan umum yang bebas dan adil sebagai tulang punggung demokrasi?
Membangun ketahanan AI	Seiring dengan perkembangan teknologi AI, strategi untuk memerangi penyalahgunaannya juga harus ikut berkembang. Ini berarti berinvestasi pada AI yang dapat mendeteksi dan melindungi dari disinformasi serta menciptakan mekanisme respons cepat untuk melawan ancaman AI secara real-time. Pada saat yang sama, petugas pemilu, staf TI, dan pemangku kepentingan lainnya dapat lebih mampu mengidentifikasi, mengatasi, dan menetralkan ancaman siber melalui pelatihan keamanan siber yang komprehensif. Pendidikan dan pelatihan tidak hanya mempersiapkan orang untuk menghadapi ancaman langsung, tetapi juga memberikan dasar untuk ketahanan berkelanjutan terhadap tantangan AI yang terus berkembang dan memastikan bahwa sistem pemilu tetap kuat dan dapat dipercaya.
Kerja sama internasional	Kerja sama internasional sangat penting dalam konteks pemilihan umum, karena pengaruh AI melampaui batas negara, sehingga upaya bersama untuk mengurangi risikonya menjadi sangat penting. Meskipun pemilihan umum pada dasarnya merupakan urusan nasional, pemilihan umum dipengaruhi oleh ekosistem digital global di mana teknologi AI memainkan peran penting. Dalam mengatasi tantangan terkait AI dalam pemilihan umum, negara-negara dapat memperoleh manfaat dari pendekatan terpadu untuk berbagi informasi intelijen yang mencakup berbagi informasi tentang ancaman AI yang muncul dan tindakan penanggulangan yang efektif. Selain itu, standarisasi peraturan sangat penting. Dengan menyelaraskan hukum dan kebijakan tentang penggunaan AI, negara-negara dapat menciptakan kerangka kerja yang koheren yang memastikan konsistensi dan keadilan dalam proses pemilihan di seluruh dunia. Undang-Undang AI merupakan contoh terobosan dari legislasi komprehensif yang mengatur aplikasi AI dan menjadi preseden bagi wilayah lain. Fokusnya pada sistem AI berisiko tinggi, termasuk yang digunakan dalam pemilihan umum, menunjukkan pendekatan proaktif untuk menangani dampak AI terhadap demokrasi. Demikian pula, rancangan Konvensi Kerangka Kerja Dewan Eropa tentang Kecerdasan Buatan, Hak Asasi Manusia, Demokrasi dan Aturan Hukum menyediakan struktur komprehensif bagi negara-negara anggota dan berpotensi negara-negara non-anggota untuk memastikan bahwa teknologi AI dikembangkan dan digunakan dengan cara yang menghormati nilai-nilai demokrasi dan hak asasi manusia. Kerangka kerja ini dan laporan penjelasan yang menyertainya menguraikan prinsip dan pedoman yang dapat memfasilitasi regulasi yang harmonis antar negara dan mendorong lingkungan kolaboratif untuk mengatasi tantangan global AI. Kerangka kerja internasional semacam itu tidak hanya meningkatkan efektivitas upaya masing-masing negara, tetapi juga memastikan bahwa pengembangan lebih lanjut teknologi AI berlangsung dalam konteks global yang menghormati dan menjunjung tinggi integritas demokrasi. Pendekatan kolektif ini dapat menghasilkan pertahanan yang lebih kuat

	terhadap campur tangan AI dalam pemilihan umum, mempromosikan proses demokrasi yang lebih sehat di tingkat internasional.
Pemantauan, evaluasi, dan pembelajaran berkelanjutan	Seiring dengan perkembangan teknologi AI dan aplikasinya dalam pemilihan umum, strategi untuk mengatasinya juga harus berkembang. Evaluasi dan revisi kebijakan, peraturan, dan materi pendidikan secara berkala sangat penting untuk mengantisipasi ancaman baru. Alat AI harus dievaluasi secara terus-menerus selama pengembangannya, dari konsepsi hingga integrasi dan pengoperasian dalam proses pemilihan umum, dan pengadaan semua produk/layanan lain yang bergantung pada AI harus diawasi dengan cermat.

AI dan Integritas Pemilu: Analisis Hipotetis Skandal Cambridge Analytica dalam Konteks Undang-Undang AI

Deskripsi kasus: Kontroversi Cambridge Analytica telah mendominasi lanskap privasi data, kampanye politik, dan media sosial dengan cara baru. Hal ini telah mendorong pemerintah dan perusahaan untuk mengambil langkah-langkah perlindungan, menyeimbangkan perlindungan data dengan kebutuhan akan transparansi dan penelitian.

Skandal Cambridge Analytica, yang terungkap pada tahun 2018, mengungkapkan bagaimana perusahaan analitik data tersebut mengumpulkan jutaan profil Facebook pemilih AS tanpa izin. Data ini digunakan untuk membuat program perangkat lunak yang ampuh untuk memprediksi dan memengaruhi perilaku pemungutan suara, yang berdampak pada tim pemilihan Donald Trump dan kampanye Brexit. Pelapor Christopher Wylie mengungkapkan bahwa Cambridge Analytica, di bawah arahan Steve Bannon dan didanai oleh Robert Mercer, menggunakan Facebook untuk membuat profil pemilih dan menargetkan individu dengan iklan politik yang dipersonalisasi. Data tersebut dikumpulkan melalui aplikasi yang dikembangkan oleh akademisi Aleksandr Kogan, yang tidak hanya mengumpulkan data pengguna tetapi juga data dari teman-teman Facebook mereka, sehingga mengumpulkan kumpulan data yang sangat besar.

The Guardian dan New York Times mengungkapkan bahwa Facebook mengetahui tentang penyalahgunaan data pada akhir tahun 2015, tetapi gagal memperingatkan pengguna dan hanya mengambil langkah-langkah terbatas untuk melindungi data. Skandal tersebut menyebabkan kemarahan yang meluas dan mendorong tindakan legislatif di seluruh dunia, termasuk Undang-Undang Layanan Digital Uni Eropa dan Undang-Undang Pasar Digital. Facebook telah mengambil langkah-langkah untuk melindungi data pengguna, tetapi pengungkapan tersebut telah menimbulkan kekhawatiran yang signifikan tentang peran platform dalam penargetan politik dan privasi data. Skandal tersebut juga menyebabkan berbagai investigasi dan sidang oleh lembaga pemerintah di AS, Inggris, dan negara-negara lain.

Penerapan Undang-Undang AI

Praktik Cambridge Analytica, khususnya penggunaan profil psikologis dan iklan politik yang ditargetkan dapat diklasifikasikan sebagai praktik AI terlarang berdasarkan Pasal 5 ayat 1 huruf a dan mungkin Pasal 5 ayat 1 huruf b Undang-Undang AI. Teknik mereka mencakup pendekatan manipulatif yang mendistorsi perilaku pemilih dan merusak kemampuan individu

untuk membuat keputusan yang tepat, sehingga kemungkinan besar menyebabkan kerugian yang signifikan.

UU AI mengklasifikasikan sistem AI ke dalam empat kategori risiko: dilarang, risiko tinggi, risiko terbatas (kewajiban transparansi), dan risiko minimal. Mengingat sifat aktivitas Cambridge Analytica – menggunakan analitik data dan AI untuk iklan politik yang ditargetkan dan memengaruhi perilaku pemilih – sistem AI termasuk dalam kategori "risiko tinggi" menurut Lampiran III UU AI, yang secara eksplisit menyebutkan penggunaan AI dalam pemilihan:

Pasal 8 huruf b) Sistem AI yang dimaksudkan untuk digunakan untuk memengaruhi hasil pemilihan atau referendum atau perilaku pemungutan suara orang perseorangan dalam menggunakan hak pilih mereka dalam pemilihan atau referendum. Ini tidak termasuk sistem AI yang outputnya tidak secara langsung memengaruhi orang perseorangan, seperti alat yang digunakan untuk mengatur, mengoptimalkan, atau menyusun kampanye politik dari sudut pandang administratif atau logistik.

Jika metode Cambridge Analytica melibatkan manipulasi yang secara signifikan merusak otonomi pemilih atau mengeksploitasi kelompok rentan, beberapa praktik mereka dapat termasuk dalam kategori terlarang ini, seperti:

Pasal 5 ayat 1 huruf a UU AI – teknik manipulatif atau menipu: menempatkan di pasar, mengoperasikan, atau menggunakan sistem AI yang menggunakan teknik subliminal di luar kesadaran seseorang atau teknik manipulatif atau menipu yang disengaja yang dimaksudkan untuk atau memiliki efek secara signifikan memengaruhi perilaku seseorang atau sekelompok orang, secara material mengganggu kemampuan seseorang untuk membuat keputusan yang terinformasi, menyebabkan orang tersebut membuat keputusan yang seharusnya tidak akan dibuatnya, dengan cara yang menyebabkan atau kemungkinan akan menyebabkan kerugian signifikan bagi orang tersebut, orang lain, atau sekelompok orang.

Cambridge Analytica menggunakan data yang dikumpulkan oleh Facebook untuk membuat iklan politik yang ditargetkan yang dirancang untuk memengaruhi perilaku pemungutan suara dengan mengeksploitasi kerentanan psikologis. Hal ini kemungkinan besar akan termasuk dalam praktik terlarang karena teknik mereka bertujuan untuk memanipulasi perilaku pemilih tanpa persetujuan mereka yang terinformasi, yang dapat secara signifikan mengganggu kemampuan individu untuk membuat keputusan independen.

Pasal 5 ayat 1 huruf b UU AI – Eksploitasi kelompok orang yang rentan: menempatkan di pasar, mengoperasikan atau menggunakan sistem AI yang mengeksploitasi kerentanan seseorang atau kelompok orang tertentu karena usia, disabilitas, atau situasi sosial atau ekonomi tertentu, dengan tujuan atau efek untuk secara signifikan memengaruhi perilaku orang tersebut atau orang yang termasuk dalam kelompok tersebut dengan cara yang menyebabkan atau kemungkinan besar akan menyebabkan kerugian yang signifikan bagi orang tersebut atau orang lain.

Cambridge Analytica menargetkan individu berdasarkan profil psikologis untuk memengaruhi perilaku pemungutan suara mereka. Jika dapat dibuktikan bahwa

perusahaan tersebut menargetkan kelompok rentan berdasarkan situasi sosial atau ekonomi mereka, praktik ini juga akan termasuk dalam kategori terlarang ini.

Pasal 5 ayat 1 huruf b UU AI – Eksploitasi kelompok orang yang rentan: menempatkan di pasar, mengoperasikan atau menggunakan sistem AI yang mengeksploitasi kerentanan seseorang atau kelompok orang tertentu karena usia, disabilitas, atau situasi sosial atau ekonomi tertentu, dengan tujuan atau efek untuk secara signifikan memengaruhi perilaku 1 lit c Undang-Undang AI – Penilaian sosial adalah penempatan di pasar, penggunaan, atau pemanfaatan sistem AI untuk mengevaluasi atau mengklasifikasikan individu atau kelompok individu selama periode waktu tertentu berdasarkan perilaku sosial mereka atau karakteristik pribadi atau kepribadian yang diketahui, disimpulkan, atau diprediksi, di mana evaluasi sosial tersebut menghasilkan satu atau kedua hal berikut: (i) perlakuan yang merugikan atau tidak menguntungkan terhadap individu tertentu atau seluruh kelompoknya dalam konteks sosial yang tidak terkait dengan konteks di mana data tersebut awalnya dihasilkan atau dikumpulkan; (ii) perlakuan yang merugikan atau tidak menguntungkan terhadap individu tertentu atau kelompoknya yang tidak dapat dibenarkan atau tidak proporsional dengan perilaku sosial mereka atau tingkat keseriusannya.

Cambridge Analytica membuat profil psikologis terperinci dan menggunakannya untuk penargetan mikro politik. Praktik pembuatan profil mereka dapat dianggap sebagai bentuk penilaian sosial jika menghasilkan perlakuan yang tidak proporsional atau pesan politik yang ditargetkan, meskipun hal ini lebih bernuansa dan bergantung pada spesifikasi penggunaan data mereka.

Analisis di atas menunjukkan potensi pelanggaran Undang-Undang AI oleh praktik Cambridge Analytica. Skandal ini menggarisbawahi pentingnya tata kelola AI yang kuat untuk melindungi integritas pemilihan dan perlunya kewaspadaan dan regulasi berkelanjutan dalam penggunaan AI dalam proses politik. Agar Cambridge Analytica mematuhi ketentuan Undang-Undang AI, perusahaan tersebut perlu mematuhi hal-hal berikut:

- Membangun sistem manajemen risiko untuk mengidentifikasi dan mengurangi risiko yang terkait dengan sistem AI mereka.
- Memastikan kumpulan data berkualitas tinggi, memelihara kumpulan data, dan menerapkan praktik manajemen data yang baik untuk menghindari bias dan ketidakakuratan.
- Memelihara dokumentasi teknis komprehensif yang merinci desain, pengembangan, dan proses operasional sistem AI Anda.
- Memberi tahu pengguna dengan jelas ketika mereka berinteraksi dengan sistem AI atau mengonsumsi konten yang dihasilkan AI.
- Implementasi langkah-langkah untuk memastikan pengawasan manusia yang memadai terhadap pengoperasian sistem AI, termasuk rencana kontingensi jika terjadi kegagalan AI.
- Memastikan bahwa sistem AI tangguh, akurat, dan aman serta mencakup mekanisme untuk mencegah dan mengurangi risiko.

- Kepatuhan terhadap GDPR dan hukum perlindungan data terkait lainnya untuk melindungi data pribadi dan memastikan hak privasi.
- Pemantauan berkelanjutan terhadap sistem AI setelah implementasi untuk memastikan kepatuhan dan menyelesaikan risiko atau masalah yang muncul.

Lebih jauh lagi, pertimbangan etis memainkan peran penting dalam penggunaan AI dalam proses politik. Skandal ini menyoroti implikasi yang lebih luas dari penyalahgunaan AI terhadap demokrasi, termasuk terkikisnya kepercayaan publik dan potensi manipulasi perilaku pemilih. Memastikan praktik AI yang etis dan menjaga transparansi dalam aplikasi AI sangat penting untuk menjunjung tinggi nilai-nilai demokrasi dan melindungi integritas sistem pemilihan. Dengan mematuhi prinsip-prinsip ini, organisasi dapat berkontribusi pada proses pemilihan yang adil dan transparan dan dengan demikian memperkuat kepercayaan publik terhadap sistem demokrasi.

8.4 AI DI SEKTOR NIS

Pendahuluan NIS dan NIS 2

Arahan NIS berasal dari tahun 2016 dan diimplementasikan di Austria dalam NISG (Undang-Undang Federal Austria untuk Memastikan **Tingkat Keamanan yang Tinggi** untuk Sistem Jaringan dan Informasi – disingkat Undang-Undang Keamanan Sistem Jaringan dan Informasi). Arahan NIS dan NISG dimaksudkan untuk memastikan dan menyelaraskan tingkat keamanan yang lebih tinggi untuk sistem jaringan dan informasi di seluruh Uni Eropa. Perusahaan yang bersangkutan harus mengambil langkah-langkah teknis, operasional, dan organisasi yang tepat dan proporsional untuk manajemen risiko keamanan siber dan menerapkan "pendekatan semua bahaya" (lihat Pasal 21 Arahan NIS2). Jaringan dan sistem informasi tersebut meliputi:

- jaringan komunikasi elektronik sesuai dengan § 3 Z 11 öTKG (Undang-Undang Telekomunikasi Austria)
- perangkat pemrosesan digital yang terdistribusi secara spasial untuk dukungan teknis pengumpulan, pemrosesan, penyimpanan, pemeliharaan, penggunaan, transmisi, pengolahan, atau pembuangan informasi digital
- data digital yang diproses dalam jaringan komunikasi elektronik tersebut atau dalam perangkat tersebut

Pihak yang dituju oleh öNISG saat ini adalah **penyedia layanan penting** di sektor energi, transportasi udara, jalan raya dan kereta api, infrastruktur pasar keuangan, layanan kesehatan, penyediaan Air minum, dan infrastruktur digital. **Lembaga administrasi publik** tertentu juga tercakup, dan layanan ini diatur secara khusus karena memainkan peran kunci dalam kegiatan ekonomi dan sosial dan sangat penting bagi mereka. Insiden keamanan di bidang ini dapat mengganggu kinerja kegiatan ekonomi, menyebabkan kerugian finansial, dan merusak kepercayaan pengguna.

Direktif NIS mensyaratkan tingkat keamanan yang tinggi di sektor-sektor terkait, tetapi juga kerja sama antar Negara Anggota, pembentukan otoritas nasional dan tim darurat komputer, serta pelaporan insiden signifikan kepada mereka. Keamanan jaringan dan

informasi berarti tidak hanya mampu menangkal insiden keamanan, tetapi juga mencegahnya, mendeteksi dan menghilangkan kesalahan yang telah terjadi, serta memulihkan operasi normal. Ancaman harus diidentifikasi, dinilai, dan dilacak. Kesalahan harus ditangani dan kemampuan untuk bertindak dan berfungsi harus dipulihkan.

Otoritas yang berwenang adalah SCIRT Austria, yang dibentuk di Kementerian Dalam Negeri Federal.

NIS2

Namun, Direktif NIS telah digantikan oleh Direktif NIS2. Namun, Direktif NIS2 belum diimplementasikan ke dalam hukum nasional baik di Jerman maupun di Austria. Direktif ini harus diimplementasikan paling lambat pada 18 Oktober 2024, jika tidak, ada risiko tuntutan pelanggaran terhadap Uni Eropa.

Direktif NIS2, seperti NIS, seharusnya memperkuat sektor-sektor yang terdampak dalam hal mempersiapkan dan menanggapi insiden keamanan. Cakupan penerapannya diperluas untuk melindungi kegiatan sosial dan ekonomi yang penting dengan lebih baik. Langkah-langkah manajemen risiko sama pentingnya dengan kewajiban pelaporan tertentu. Sektor yang terdampak:

Sektor dengan Tingkat Kritis Tinggi	Sektor-Sektor Penting Lainnya
▪ Energi ▪ Lalu Lintas ▪ Perbankan (penerapan prioritas Peraturan DORA 2022/2554) ▪ Infrastruktur pasar keuangan (penerapan prioritas Peraturan DORA 2022/2554) ▪ Layanan Kesehatan ▪ Air Minum ▪ Air Limbah ▪ Infrastruktur Digital ▪ Manajemen Layanan TIK B2B ▪ Administrasi Publik ▪ Ruang Angkasa	▪ Layanan pos dan kurir ▪ Pengelolaan limbah ▪ Kimia ▪ Pangan ▪ Industri pengolahan/manufaktur ▪ Penyedia layanan digital ▪ Penelitian (opsional)

Perbedaan juga dibuat berdasarkan **ukuran perusahaan**, di mana jumlah karyawan, omset tahunan, dan total neraca tahunan harus diperhitungkan. Perusahaan kecil (kurang dari 50 karyawan, omset tahunan maksimum Rp.100 miliar atau total neraca tahunan maksimum Rp. 100 miliar) tidak tercakup oleh NIS2, meskipun ada pengecualian. **Kategori ukurannya** adalah:

Jumlah Karyawan Penuh Waktu/Penjualan Tahunan/Total Neraca Tahunan	Klasifikasi Perusahaan
▪ Lebih dari 50 karyawan tetap dan ▪ penjualan tahunan sama dengan atau lebih dari Rp. 100 miliar atau ▪ total neraca tahunan sama dengan/lebih dari Rp. 100 miliar	Perusahaan kecil
▪ Lebih dari 250 karyawan tetap dan ▪ omzet tahunan sama dengan/lebih dari Rp. 500 miliar atau	Perusahaan menengah

▪ total neraca tahunan sama dengan/lebih dari Rp. 430 miliar	Perusahaan besar
▪ Setara dengan/lebih dari 250 karyawan penuh waktu atau	
▪ penjualan tahunan lebih dari Rp. 500 miliar dan	
▪ total neraca tahunan lebih dari Rp. 430 miliar	

Direktif tersebut merujuk pada Rekomendasi Komisi tentang definisi UKM, yang juga memuat spesifikasi lebih lanjut mengenai perhitungan ukuran perusahaan, khususnya untuk perusahaan afiliasi, yaitu **kelompok** atau **grup perusahaan**. **Usaha kecil** pada umumnya tidak tercakup dalam NIS2, tetapi ada pengecualian, khususnya jika mereka adalah penyedia layanan kepercayaan atau bertindak sebagai penyedia layanan atau pemasok untuk perusahaan yang terdampak.

Perbedaan juga dibuat antara **perusahaan penting dan esensial**, yang menentukan apakah pemeriksaan keamanan dilakukan ex ante atau ex post jika terdapat kecurigaan yang beralasan. Fasilitas penting adalah perusahaan besar, misalnya dari sektor energi, transportasi, kesehatan, dan Air minum. Perusahaan penting adalah perusahaan menengah dari sektor-sektor ini dan perusahaan besar dan menengah dari sektor pos, limbah, kimia, makanan, layanan digital, dan lainnya. Ada pengecualian untuk infrastruktur digital, misalnya layanan komunikasi, layanan cloud, layanan pusat data, dan lainnya. Daftar lengkapnya dapat ditemukan dalam lampiran NIS2.

Direktif NIS2 memberlakukan berbagai kewajiban pada perusahaan, termasuk **langkah-langkah manajemen risiko**, keamanan rantai pasokan, dan kewajiban pelaporan. Direktif ini menetapkan sanksi berat untuk ketidakpatuhan. Badan manajemen fasilitas yang bersangkutan bertanggung jawab. Mereka harus memastikan dan mengawasi kepatuhan. Mereka bertanggung jawab jika perusahaan menderita kerugian yang disebabkan secara sengaja karena ketidakpatuhan.

Pentingnya NIS2 untuk Rantai Pasokan

NIS2 tidak hanya mensyaratkan kepatuhan perusahaan yang secara langsung berlaku untuk NIS2, tetapi juga mensyaratkan rantai pasokan untuk diamankan. "TI" semakin global, berlapis-lapis, terhubung, dan pada akhirnya semakin kompleks. Hampir tidak ada perusahaan yang masih memiliki penyedia layanan TI "satu-satunya" yang melakukan segalanya untuk mereka; sebaliknya, sejumlah besar sistem digunakan, yang pada gilirannya berasal dari sejumlah besar penyedia layanan dan pemasok. Sistem-sistem ini kemudian tidak lagi berjalan "di tempat", yaitu di server perusahaan sendiri, tetapi seringkali di cloud.

Oleh karena itu, NIS2 mensyaratkan **manajemen risiko pihak ketiga** yang ketat, yaitu... Manajemen risiko ditujukan khusus untuk penyedia layanan dan pemasok ini. Tidak hanya pemasok individual yang diperhitungkan, tetapi juga hubungan antara fasilitas individual dan penyedia layanan serta pemasok mereka. Manajemen risiko harus mempertimbangkan kerentanan pemasok dan penyedia layanan serta kualitas produk secara keseluruhan dan keamanan TI mereka, keamanan proses pengembangan mereka, dan langkah-langkah perlindungan apa yang telah diambil.

Penyedia layanan dan pemasok perusahaan NIS2 dapat menunjukkan kepatuhan terhadap persyaratan ini dengan berbagai cara, misalnya melalui sertifikasi, audit, atau

verifikasi individual. Otoritas NIS Austria merekomendasikan standar dan praktik terbaik berikut:

- ÖISHB: Kerja sama dengan pihak eksternal, evaluasi sertifikasi, hubungan pemasok
- ISO/IEC 27001: Keamanan informasi dalam hubungan pemasok
- IEC 62443 2-1: Keamanan rantai pasokan
- CIS CSC v8.0: Manajemen penyedia layanan
- Peringkat Risiko Siber KSÖ: Persyaratan untuk peringkat A atau B

NIS2 telah diperhitungkan dalam pedoman ENISA “Praktik Baik untuk Keamanan Siber Rantai Pasokan”. Oleh karena itu, panduan ini dapat berfungsi sebagai alat bantu implementasi.

Penggunaan AI di Perusahaan NIS

Penggunaan AI oleh perusahaan NIS dan NIS2 diatur dalam dua cara. **Lampiran I dan III** menetapkan arahan atau peraturan tertentu dan penggunaan sistem AI dalam infrastruktur kritis.

Penggunaan sistem AI sebagai **komponen keselamatan** sangat penting. Menurut Pasal 3 ayat 14 UU AI, komponen keselamatan suatu produk atau sistem adalah komponen produk atau sistem yang memenuhi fungsi keselamatan atau yang kegagalan atau malfungsinya membahayakan kesehatan atau keselamatan orang atau harta benda.

UU AI sendiri membenarkan klasifikasi penggunaan sistem AI dalam infrastruktur kritis dengan menyatakan bahwa malfungsi atau kegagalan dapat **membahayakan nyawa dan kesehatan banyak orang** dan menyebabkan **gangguan yang cukup besar terhadap kehidupan sosial dan ekonomi**. Komponen keselamatan adalah sistem yang digunakan untuk melindungi integritas fisik infrastruktur kritis atau kesehatan dan keselamatan orang atau harta benda, tetapi tidak penting untuk fungsi sistem tersebut. Kegagalan atau malfungsi komponen tersebut dapat menyebabkan risiko terhadap integritas fisik dan oleh karena itu risiko terhadap kesehatan dan keselamatan orang atau harta benda. Komponen yang digunakan semata-mata untuk tujuan keamanan siber tidak memenuhi syarat sebagai komponen keamanan. Contoh komponen keselamatan dalam infrastruktur kritis adalah sistem untuk memantau tekanan Air atau alarm kebakaran di pusat komputasi awan.

Lampiran I Undang-Undang AI

Sistem AI yang digunakan **sebagai komponen keselamatan** suatu perangkat, atau jika sistem AI itu sendiri adalah perangkat dan tercantum dalam Lampiran I, dianggap sebagai sistem AI berisiko tinggi. Hal yang sama berlaku untuk perangkat yang komponen keselamatannya adalah sistem AI, di mana sistem AI atau perangkat tersebut harus menjalani penilaian kesesuaian sebelum dipasarkan atau dioperasikan.

Tergantung pada sektornya, peraturan perundang-undangan Uni Eropa berikut ini khususnya mungkin relevan bagi perusahaan NIS2:

- Direktif Mesin 2006/42/EC: Berlaku untuk mesin, komponen keselamatan, rantai, tali, sabuk, dan lainnya.
- Peraturan tentang peralatan pelindung (UE) 2016/425: peralatan yang dapat dikenakan atau dipegang oleh orang sebagai perlindungan terhadap satu atau lebih risiko terhadap kesehatan atau keselamatan mereka

- Peraturan Perangkat Medis (UE) 2017/745: Perangkat medis yang ditujukan untuk penggunaan manusia dan aksesorinya, termasuk investigasi klinis terkait; misalnya perangkat, instrumen, perangkat lunak, atau implan untuk tujuan diagnosis, prognosis, paliasi, atau investigasi
- Peraturan untuk perangkat medis untuk diagnostik in vitro (EU) 2017/746: reagen, kit, instrumen, perangkat, perangkat lunak untuk pengujian in vitro
- Peraturan Penerbangan Sipil (EC) 300/2008 dan Peraturan 2018/1139: penerbangan pesawat sipil; keamanan penerbangan adalah kombinasi dari langkah-langkah dan sumber daya manusia dan material yang dirancang untuk melindungi penerbangan sipil dari tindakan campur tangan yang melanggar hukum yang membahayakan keamanan penerbangan sipil.
- Arahan tentang interoperabilitas sistem kereta api (UE) 2016/797: Ketentuan tentang komponen, antarmuka, dan prosedur interoperabilitas serta untuk koherensi keseluruhan sistem kereta api UE untuk memastikan pergerakan kereta api yang aman dan berkelanjutan

Oleh karena itu, jika perusahaan NIS2 menggunakan komponen berbasis AI yang termasuk dalam salah satu peraturan perundang-undangan di Lampiran I, perusahaan tersebut harus memastikan kepatuhan terhadap persyaratan untuk AI berisiko tinggi. Jika perusahaan tersebut menggunakan pemasok untuk tujuan ini, perusahaan tersebut juga harus memastikan kepatuhan terhadap persyaratan NIS2 mengenai keamanan rantai pasokan.

Lampiran III Undang-Undang AI

Semua sistem AI yang tercantum dalam Lampiran III dianggap sebagai sistem AI berisiko tinggi. Pengecualian berlaku jika sistem AI tidak menimbulkan risiko signifikan terhadap kesehatan, keselamatan, atau hak-hak dasar individu, termasuk pengaruh non-material terhadap hasil keputusan. Pengecualian ini berlaku jika satu atau lebih kriteria berikut terpenuhi:

- Sistem AI hanya melakukan langkah proses yang didefinisikan secara sempit;
- Sistem AI digunakan untuk meningkatkan hasil aktivitas yang sebelumnya dilakukan oleh manusia;
- Sistem AI harus mendeteksi pola pengambilan keputusan atau penyimpangan darinya dan tidak menggantikan penilaian yang sebelumnya dilakukan oleh manusia tanpa tinjauan manusia yang tepat; atau
- Sistem AI melakukan tugas persiapan untuk penilaian yang relevan untuk salah satu kasus penggunaan dari Lampiran III.

Namun, sistem AI selalu dinilai sebagai sistem berisiko tinggi jika mencakup pembuatan **profil individu**. Penyedia yang berpendapat bahwa sistem AI tersebut bukan AI berisiko tinggi harus mendokumentasikan penilaian ini sebelum sistem AI tersebut dipasarkan atau dioperasikan. Penyedia tersebut wajib mendaftar sesuai dengan Pasal 49 ayat 2 Peraturan AI dan harus dapat menunjukkannya jika diminta oleh otoritas. Komisi Uni Eropa akan mengeluarkan tindakan delegasi tentang Lampiran III atau mengadaptasinya ke Lampiran III secara keseluruhan.

Tumpang tindih utama antara NIS2 dan Undang-Undang AI menyangkut poin 2 Lampiran III, yang mendefinisikan sistem AI berisiko tinggi dalam infrastruktur kritis sebagai sistem AI yang akan digunakan sebagai komponen *keamanan untuk pengelolaan dan pengoperasian infrastruktur digital kritis, transportasi jalan, dan penyediaan Air, gas, panas, dan listrik*.

Oleh karena itu, definisi dalam Lampiran III poin 2 tidak konsisten dengan semua sektor dalam NIS2, di mana Pasal 3 poin 62 Undang-Undang AI merujuk pada Pasal 2 ayat 2. 4. Direktif CER 2022/2557 (Peraturan tentang ketahanan fasilitas kritis) berkaitan dengan definisi infrastruktur kritis. Menurut Direktif CER, layanan infrastruktur kritis esensial adalah semua layanan yang penting untuk pemeliharaan fungsi-fungsi penting masyarakat, kegiatan ekonomi penting, kesehatan dan keselamatan publik, atau pelestarian lingkungan. Negara-negara anggota harus mendefinisikan dan menentukan hal ini. Baik Jerman maupun Austria belum mengesahkan undang-undang untuk mengimplementasikan Direktif CER. Oleh karena itu, belum memungkinkan untuk membuat pernyataan akhir tentang interaksi antara Peraturan CER dan NIS2.

Oleh karena itu, menurut rumusan tersebut, hanya hal-hal berikut yang dianggap sebagai infrastruktur kritis sesuai dengan Lampiran III Undang-Undang AI:

- Infrastruktur digital, misalnya penyedia node internet, penyedia layanan cloud, penyedia layanan pusat data, penyedia jaringan komunikasi elektronik publik, penyedia layanan komunikasi elektronik yang dapat diakses publik
- Lalu lintas jalan, khususnya otoritas lalu lintas jalan, pengoperasian sistem lalu lintas cerdas
- Pasokan Air, khususnya pemasok Air minum (rumusan ini tidak mencakup pembuangan Air limbah)
- Gas, misalnya pemasok gas alam, penyedia pabrik untuk pemurnian dan pengolahan gas alam
- Panas, misalnya penyedia pemanas distrik
- Listrik, misalnya perusahaan listrik, penyedia jaringan distribusi, penyedia stasiun pengisian daya

Jika operator infrastruktur kritis dari sektor yang tercantum di sini menggunakan sistem AI sebagai komponen keselamatan, operator tersebut harus memenuhi persyaratan untuk sistem AI berisiko tinggi. **Daftar periksa** untuk penggunaan AI di perusahaan NIS2:

• Apakah terdapat sistem AI berisiko tinggi sesuai dengan Lampiran III? • Apakah sistem AI tersebut berfungsi sebagai komponen keselamatan sesuai dengan salah satu peraturan perundang-undangan dari Lampiran I?	• Pasal 6 dan seterusnya menjelaskan klasifikasi dan kewajiban bagi pengembang dan penyedia sistem AI berisiko tinggi;
• Apakah ini sistem AI lain yang memiliki kewajiban transparansi berdasarkan Undang-Undang AI?	• Pasal 52 UU AI memuat kewajiban transparansi bagi penyedia dan mengimplementasikan sistem AI tertentu dan model AI untuk tujuan umum; lihat bagian 3.6

• Apakah ini model AI untuk keperluan umum?	• Pasal 52 dan seterusnya UU AI memuat aturan untuk klasifikasi GPAI dengan risiko sistemik dan kewajiban bagi penyedia; lihat bagian 3.7.

BAB 9

ETIKA

9.1 PEDOMAN ETIKA UNTUK AI YANG DAPAT DIPERCAYA

Bab berikut membahas implikasi etis dari penggunaan AI. Alat-alat yang berguna disediakan, seperti pedoman untuk AI yang dapat dipercaya atau untuk inovasi etis. Fokus diperluas melampaui Regulasi AI dan pedoman global dipertimbangkan, serta badan, komite, dan panel yang menangani kecerdasan buatan.

Bab ini menyajikan pedoman etika untuk AI yang dapat dipercaya, yang diterbitkan pada April 2019 oleh Kelompok Pakar Tingkat Tinggi Komisi Eropa tentang Kecerdasan Buatan. Daftar evaluasi untuk AI yang dapat dipercaya, yang menyertai pedoman tersebut, juga dirujuk. Meskipun pedoman ini secara eksplisit mengecualikan diskusi hukum, pedoman ini diberi signifikansi yang lebih besar oleh Undang-Undang AI, karena merujuk pada pedoman tersebut. Terakhir, pendekatan yang serupa dengan pedoman etika ini atau mengembangkannya lebih lanjut dan oleh karena itu mungkin berharga untuk bidang aplikasi tertentu disajikan secara singkat.

Tentang Apa Ini?

Pertama-tama, poin penting: pedoman etika menganggap sistem AI sebagai sistem sosio-teknis. Ini berarti bahwa pedoman etika tidak hanya merujuk pada komponen teknis seperti model, bobot, atau kode, tetapi juga pada topik seperti pengolahan data, organisasi di sekitar sistem AI, atau proses tata kelola seperti yang berkaitan dengan pengawasan manusia. Dengan demikian, pedoman etika juga merupakan upaya untuk beralih dari sekadar daftar persyaratan (seperti persyaratan aksesibilitas WRC (Komisi Hubungan Kerja)) menuju pengembangan kompetensi evaluasi yang peka terhadap konteks sesuai dengan prinsip-prinsip etika.

Pedoman etika dari Kelompok Pakar Tingkat Tinggi tentang AI ditujukan untuk semua pemangku kepentingan yang merancang, mengembangkan, memperkenalkan, mengimplementasikan, menggunakan, atau terpengaruh oleh sistem AI. Pedoman ini dimaksudkan untuk memungkinkan implementasi prinsip-prinsip etika yang paling holistik dan praktis terkait dengan sistem AI. Para penulis pedoman menganggap etika sebagai komponen dari sistem AI yang dapat dipercaya:

(15) AI yang dapat dipercaya dicirikan oleh tiga komponen yang harus dipenuhi selama seluruh siklus hidup sistem:

- 1. Harus sesuai hukum dan karenanya mematuhi hukum yang berlaku dan semua ketentuan undang-undang;*
- 2. Harus etis dan dengan demikian menjamin kepatuhan terhadap prinsip dan nilai etika; dan*

3. *Harus tangguh, baik secara teknis maupun sosial, karena sistem AI dapat menyebabkan kerugian yang tidak disengaja meskipun didasarkan pada niat baik.*

Semua komponen ini harus dipenuhi agar sistem AI dianggap dapat dipercaya. Bagi pedoman ini, etika dan ketangguhan adalah dua prinsip yang saling terkait yang harus diimplementasikan bersama, karena: Hanya jika sistem AI melayani tujuan etis, sejalan dengan norma etika dan juga dapat menjaga janji etis ini secara teknis dan sosial, maka sistem tersebut dapat dianggap dapat dipercaya.

Pedoman etika ini berupaya untuk memberikan lebih banyak penjelasan tentang aspek kedua dan ketiga dari AI yang dapat dipercaya, karena aspek pertama – kerangka hukum – dikecualikan oleh para ahli sendiri, tetapi kemudian mengarah pada pengembangan Undang-Undang AI. Ini termasuk definisi empat prinsip etika, yang dapat diturunkan dari Piagam Hak Fundamental Uni Eropa. Dalam konteks ini, kelompok ahli secara khusus menekankan penghormatan terhadap martabat manusia, kebebasan individu, penghormatan terhadap demokrasi, keadilan dan supremasi hukum, kesetaraan, non-diskriminasi dan solidaritas, serta hak-hak sipil. Nilai-nilai ini berfungsi sebagai panduan tentang apa yang harus dilakukan dengan sistem AI (berbeda dengan apa yang dapat dilakukan dengan sistem AI).

Prinsip Etika Pedoman

Prinsip-prinsip etika merumuskan prinsip-prinsip yang harus diintegrasikan sebagai nilai-nilai formatif dalam pengembangan dan penggunaan sistem AI (lihat Tabel 9.1). Dalam praktiknya, mungkin ada ketegangan antara prinsip-prinsip ini, yang harus dipertimbangkan dan diselesaikan oleh organisasi yang berpartisipasi. Organisasi-organisasi ini juga bertanggung jawab untuk mengambil langkah-langkah yang tepat dan sesuai risiko untuk melindungi dari dampak negatif.

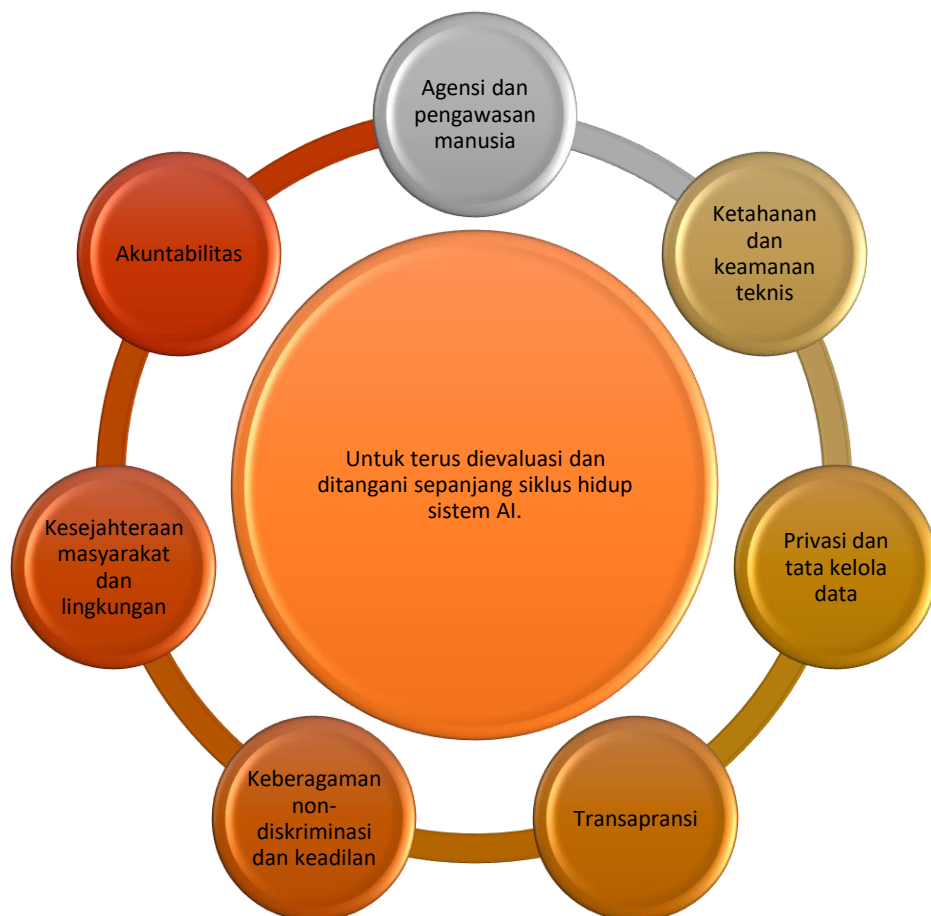
Tabel 9.1 Prinsip-Prinsip Untuk Pengembangan Dan Penggunaan Sistem AI

Prinsip etika	Keterangan
Penghormatan terhadap otonomi manusia	Sistem AI harus menerapkan langkah-langkah yang mempromosikan, memperkuat, dan melengkapi keterampilan kognitif, sosial, dan budaya manusia
Pencegahan kerugian	Sistem AI seharusnya tidak memiliki atau hanya memiliki sedikit dampak negatif terhadap manusia atau lingkungan (materiil maupun non-materiil) dan menunjukkan pertimbangan khusus terhadap individu (kelompok) yang layak dilindungi.
Keadilan	Sistem AI harus memastikan bahwa keuntungan dan kerugian didistribusikan secara merata dan adil, secara proporsional dan dengan mempertimbangkan kebebasan memilih dari pihak yang terkena dampak, yang juga mencakup kemungkinan keberatan.
Kemampuan menjelaskan	Proses, kemampuan, dan tujuan sistem AI harus transparan dan dikomunikasikan sehingga pihak yang secara langsung maupun tidak langsung terpengaruh dapat mempertanyakan keputusan jika terdapat keraguan.

Berdasarkan keempat prinsip tersebut, pedoman ini mengusulkan tujuh persyaratan inti untuk memfasilitasi implementasi prinsip-prinsip etika dalam praktik.

Persyaratan Inti

Dengan persyaratan inti ini, kelompok ahli tersebut membahas para pengembang sistem AI, serta pengguna dan pemangku kepentingan. Dalam hal apa pun, persyaratan tersebut harus dipantau, dievaluasi, dan dipertimbangkan sepanjang siklus hidup sistem AI. Ketujuh persyaratan inti tersebut sama pentingnya, meskipun beberapa persyaratan lebih penting daripada yang lain dalam kasus penggunaan tertentu. Misalnya, jika sistem AI digunakan dalam konteks industri, keragaman atau perlindungan data akan memainkan peran yang lebih kecil daripada dalam aplikasi di mana orang secara langsung terpengaruh.



Gambar 9.1 Persyaratan Inti Untuk Sistem AI Yang Dapat Dipercaya Menurut Pedoman Etika

Tujuh persyaratan untuk AI yang dapat dipercaya dijelaskan secara rinci dalam Tabel 9.2.

Tabel 9.2 Persyaratan Untuk AI Yang Dapat Dipercaya

Persyaratan Inti Referensi Prinsip	Keterangan
Keutamaan tindakan dan pengawasan manusia	▪ Evaluasi hak-hak fundamental terlebih dahulu (Pedoman 63)

<i>Penghormatan terhadap otonomi manusia</i>	▪ Memungkinkan pengambilan keputusan dan penilaian yang berdasarkan informasi oleh pengguna dan pemangku kepentingan (Pedoman 64) ▪ Memungkinkan pengawasan manusia secara operasional melalui keterlibatan manusia, manusia sebagai komandan, atau manusia sebagai pengendali serta secara eksternal oleh otoritas pengawas (Pedoman 65)
Ketangguhan teknis dan keamanan <i>Pencegahan kerusakan</i>	▪ Memastikan ketahanan dan perlindungan terhadap serangan dan pelanggaran keamanan baik pada tingkat perangkat lunak (misalnya, peracunan data, kebocoran model) maupun perangkat keras (Pedoman 67) ▪ Mengembangkan tindakan pencegahan keselamatan dan rencana penahanan, memastikan fungsi yang tepat, serta mengidentifikasi, menilai, dan menanggulangi risiko melalui langkah-langkah (Pedoman 68) ▪ Memastikan ketepatan hasil melalui proses pengembangan dan evaluasi yang tepat serta informasi tentang tingkat ketepatan yang diberikan kepada pengguna (Pedoman 69) ▪ Memastikan keandalan (fungsi sempurna meskipun terdapat berbagai macam masukan dan situasi aplikasi) dan reproduksibilitas (perilaku yang sama dalam kondisi yang sama) (Pedoman 70)
Perlindungan privasi dan kualitas data <i>Pencegahan kerusakan</i>	▪ Melindungi data pribadi dan informasi pribadi di semua tahapan siklus hidup dan tidak menggunakannya secara tidak sah atau dengan cara yang diskriminatif (Pedoman 72) ▪ Kumpulan data harus berkualitas tinggi bahkan sebelum sistem AI dilatih untuk menghindari kekurangan, bias, kesalahan, dan ketidakakuratan, dan masukan data berbahaya yang akan membahayakan integritas sistem harus dipastikan; kumpulan data dan proses untuk memastikan kualitas dan integritas data harus diuji dan didokumentasikan di semua tahapan siklus hidup (Pedoman 73) ▪ Menetapkan protokol yang tepat untuk memastikan bahwa hanya personel yang berkualifikasi yang dapat mengakses data pribadi dalam keadaan yang diperlukan (Pedoman 74)

Transparansi <i>Kemampuan menjelaskan</i>	▪ Membuat catatan data, proses, dan hasil sistem AI dapat dilacak melalui dokumentasi (Pedoman 76) ▪ Mengkomunikasikan hasil yang memengaruhi kehidupan masyarakat kepada pihak yang terdampak secara tepat waktu dan berdasarkan kebutuhan (Pedoman 77) ▪ Memberi tahu masyarakat tentang interaksi dengan sistem AI serta kemampuan dan keterbatasannya sesuai dengan kebutuhan mereka dan menawarkan mereka kesempatan untuk berinteraksi dengan manusia jika terjadi potensi dampak terhadap hak-hak mendasar (Pedoman 78)
Keberagaman, non-diskriminasi, dan keadilan <i>Keadilan</i>	▪ Hindari distorsi baik dalam fungsi sistem AI maupun dengan memanfaatkan distorsi pengguna dan pemangku kepentingan (misalnya persaingan tidak sehat) dan atasi distorsi yang ada selama pengembangan dan melalui proses pengawasan yang tepat dan keberagaman staf. ▪ Jadikan sistem AI dapat digunakan dan diakses oleh semua orang, terlepas dari karakteristik atau kemampuan pribadi mereka, dengan bantuan desain universal atau desain untuk semua (Pedoman 81). ▪ Libatkan pemangku kepentingan dan karyawan dalam pengembangan dan selama fase penggunaan (Pedoman 82).
Kesejahteraan sosial dan lingkungan <i>Keadilan dan pencegahan kerusakan</i>	▪ Mengevaluasi dan meminimalkan dampak lingkungan selama semua fase siklus hidup dan di seluruh rantai pasokan (Pedoman 84) ▪ Mempertimbangkan dampak pada hubungan dan ikatan sosial serta mempertahankan peran sosial (Pedoman 85) ▪ Menilai dampak pada demokrasi, masyarakat, dan lembaga ▪ dan menghindari dampak negatif (Pedoman 86)
Akuntabilitas <i>Keadilan</i>	▪ Memastikan verifikasi melalui penilaian auditor internal dan eksternal, terutama untuk aplikasi yang berdampak pada hak-hak fundamental dan aplikasi yang kritis terhadap keselamatan (Pedoman 88) ▪ Mengidentifikasi, menilai, meminimalkan, dan melaporkan dampak negatif, memungkinkan pelaporan insiden, dan melakukan penilaian dampak siklus hidup (Pedoman 89) ▪ Mengidentifikasi kepentingan dan nilai-nilai serta membuat kompromi dengan mempertimbangkan

	prinsip-prinsip etika dan hak-hak fundamental atau – jika kompromi tidak memungkinkan – mengembangkan, memperkenalkan, atau menggunakan sistem AI secara berbeda; membenarkan semua kompromi, mendokumentasikannya, terus meninjau kesesuaiannya, dan mendapatkan perubahan jika perlu (Pedoman 90) ▪ Menyediakan perlindungan hukum yang memadai, dengan memberikan perhatian khusus kepada orang dan kelompok yang rentan (Pedoman 91)

Metode untuk Mengimplementasikan Persyaratan Inti

Persyaratan etika dapat diimplementasikan menggunakan metode teknis atau non-teknis yang digunakan di seluruh siklus hidup. Proses teknis mencakup metode yang sudah dikenal dari bidang pengembangan perangkat lunak lainnya serta metode yang menjadi subjek penelitian intensif.

Tabel 9.3 Metode Teknis Untuk Implementasi Persyaratan Etika Untuk AI

Prosedur Teknis	Contoh
Membangun arsitektur untuk AI yang dapat dipercaya	▪ Definisi perilaku atau kondisi yang diinginkan (Daftar Putih) dan yang tidak diinginkan (Daftar Hitam) serta pembatasan yang sesuai (Pedoman 95) ▪ Siklus Sense-Plan-Act yang memastikan bahwa sistem AI mengenali semua elemen lingkungan yang diperlukan untuk memenuhi persyaratan (sense), hanya menjalankan rencana yang memenuhi persyaratan (plan), dan hanya menjalankan tindakan yang mewujudkan persyaratan tersebut (act) (Pedoman 96)
Mengintegrasikan etika dan supremasi hukum ke dalam desain (Etika melalui Desain)	Mengintegrasikan pendekatan seperti privasi sejak tahap perancangan, keamanan sejak tahap perancangan, dan prinsip serupa selama pengembangan (Pedoman 98)
Mewujudkan metode penjelasan	Pendekatan seperti AI yang dapat dijelaskan (xai) (Pedoman 99)
Uji dan periksa	▪ Sifat-sifat non-deterministik dan spesifik konteks dari sistem AI selama pengujian untuk stabilitas, ketahanan, dan fungsionalitas dalam kondisi yang ditentukan untuk memvalidasi hasil sistem dan proses yang mendasarinya (Pedoman 100) ▪ Sepanjang seluruh siklus hidup dan sedini mungkin, sistem AI harus diuji secara holistik, termasuk semua komponen dan di semua lingkungan, dengan keragaman tim pengujian dan opsi pengujian eksternal seperti Red Team

	atau program bug bounty untuk menciptakan keandalan yang lebih luas (Pedoman 101)
Parameter kualitas layanan berkembang	Mengembangkan indikator kualitas layanan yang dapat digunakan untuk mengevaluasi hasil dan pelatihan sistem AI, termasuk metrik perangkat lunak tradisional seperti fungsionalitas, kinerja, kegunaan, keandalan, keamanan, dan pemeliharaan (Pedoman 102)

Metode non-teknis yang dapat digunakan untuk memenuhi persyaratan mencakup berbagai langkah yang dapat digunakan oleh organisasi secara mandiri atau memerlukan kerja sama dari lembaga sosial yang lebih luas.

Organisasi dapat memastikan bahwa kode etik eksternal dan internal dikembangkan dan diimplementasikan, serta mendorong implementasi akuntabilitas sebagai dasar kerangka kerja internal dan eksternal untuk tata kelola dan pengendalian sistem AI (termasuk proses pengawasan yang tepat, pemeriksaan kepatuhan, dan berbagi praktik terbaik). Ini juga mencakup memastikan keragaman dan inklusi dalam tim yang mengembangkan, mengimplementasikan, menyebarkan, menguji, memelihara, menyebarkan, dan memantau sistem AI serta keterlibatan berbagai pemangku kepentingan yang luas dan beragam dalam proses ini.

Meskipun langkah-langkah lain dapat mendukung organisasi individual, langkah-langkah tersebut memerlukan keterlibatan kelembagaan yang lebih luas. Ini termasuk regulasi (termasuk legislasi), standarisasi (termasuk standar resmi, norma khusus sektor, atau label kualitas), pendidikan dan pengembangan keterampilan AI serta keterlibatan pemangku kepentingan dan promosi dialog sosial.

Alat untuk Implementasi

Untuk melengkapi pedoman etika, Kelompok Pakar Tingkat Tinggi telah mengembangkan daftar penilaian untuk AI yang dapat dipercaya (Daftar Penilaian untuk AI yang Dapat Dipercaya atau ALTAI). Setelah fase uji coba pada tahun 2019, versi final pertama dari daftar penilaian diterbitkan sebagai PDF dan sebagai alat berbasis web pada Juni 2020. Daftar penilaian ini berisi pertanyaan tentang persyaratan inti individu, yang dimaksudkan untuk berfungsi sebagai inspirasi bagi para pemangku kepentingan yang terlibat dalam berbagai fase siklus hidup sistem AI.

Sebagaimana ditekankan oleh anggota Kelompok Pakar Tingkat Tinggi tentang AI, etika harus dirancang sepraktis mungkin. Karena alasan ini, tidak mengherankan bahwa banyak pedoman etika telah dikembangkan untuk konteks spesifik. Ini termasuk, misalnya, Administrasi Digital dan Etika: Pedoman Praktis untuk AI dalam Administrasi (Versi 1.0), yang dikembangkan oleh para ahli dari Institut Teknologi Austria (AIT) untuk Kementerian Federal Seni, Budaya, Layanan Sipil dan Olahraga (BMKÖS). Untuk pengembangan dan penggunaan sistem AI yang etis dalam penelitian dan sains, sebuah pedoman dikembangkan sebagai bagian dari pendanaan Horizon 2020 untuk mendukung pelamar dalam menangani kriteria etika dan menunjukkan kepatuhan (Pendekatan Etika Berdasarkan Desain dan Etika Penggunaan untuk Kecerdasan Buatan). Perangkat konsorsium ETAPAS (Adopsi Teknologi Etis dalam Layanan

Administrasi Publik), yang dapat digunakan untuk mendukung penggunaan teknologi disruptif (termasuk AI), juga ditujukan untuk administrasi publik.

Untuk mendukung implementasi prinsip-prinsip etika, Kelompok Dampak Etika AI, yang dipimpin oleh Asosiasi Teknologi Listrik, Elektronik & Informasi (VDE) dan Bertelsmann Stiftung, telah mengembangkan kerangka kerja untuk penilaiannya (Dari prinsip ke praktik: Bagaimana kita dapat membuat etika AI terukur?). Ini menyajikan metode untuk menilai aspek etika dan juga matriks risiko untuk mengklasifikasikan aplikasi. Pada tahun 2021, Fraunhofer IAIS mengembangkan pedoman untuk desain kecerdasan buatan yang dapat dipercaya (katalog pengujian AI), yang berisi dimensi keadilan, otonomi dan kontrol, transparansi, keandalan, keamanan dan perlindungan data serta penilaian lintas dimensi.

Di luar Eropa, ada juga upaya untuk mengembangkan pedoman etika. Rekomendasi UNESCO tentang Etika Kecerdasan Buatan, yang diadopsi pada tahun 2021, mengidentifikasi nilai-nilai inti berikut: penghormatan terhadap, perlindungan dan promosi hak asasi manusia, kebebasan mendasar dan martabat manusia; kesejahteraan lingkungan dan ekosistem; keragaman dan inklusivitas; dan hidup dalam masyarakat yang damai, adil, dan saling terhubung. Berdasarkan hal ini, dirumuskan prinsip-prinsip yang harus dipatuhi oleh sistem AI: Proporsionalitas dan tidak membahayakan; Perlindungan dan keamanan; Keadilan dan non-diskriminasi; Keberlanjutan; Hak atas privasi dan perlindungan data; Pengawasan dan kontrol manusia; Transparansi dan penjelasan; Tanggung jawab dan akuntabilitas; Kesadaran dan pelatihan; dan Tata kelola dan kolaborasi multi-pemangku kepentingan dan adaptif. Meskipun tidak identik dengan Pedoman Etika Eropa, topik serupa dibahas. Hal ini menunjukkan pentingnya global dalam menangani masalah etika, yang, bagaimanapun, hanya dapat menemukan jawaban berdasarkan situasi dan lokal. Banyak pedoman etika lainnya dapat ditemukan, misalnya, dalam Inventaris Global Pedoman Etika AI dari AlgorithmWatch.

9.2 PEDOMAN & KEBIJAKAN AI YANG RELEVAN

Terdapat banyak pedoman etika untuk kecerdasan buatan di seluruh dunia. Ini termasuk tidak hanya kerangka kerja nasional untuk masing-masing negara, tetapi juga pedoman yang dikembangkan secara khusus dari kelompok kepentingan, organisasi non-pemerintah (LSM), dan perusahaan swasta, yang semuanya bertujuan untuk memastikan penggunaan dan pengembangan teknologi AI yang aman.

Tantangannya bukanlah kurangnya deskripsi teoritis atau pedoman tentang etika AI, tetapi lebih pada implementasi praktis dalam pekerjaan sehari-hari dan dalam proyek. Bagian ini didedikasikan untuk menyajikan beberapa pedoman etika AI yang paling penting dan diakui secara luas. Perhatian khusus telah diberikan pada pedoman yang memiliki relevansi global dan telah dikeluarkan oleh organisasi yang merupakan pemimpin dalam penelitian dan aplikasi AI. Beberapa juga menyediakan informasi, sumber daya, dan alat untuk mengimplementasikan AI dengan percaya diri.

Rekomendasi Dewan OECD tentang Kecerdasan Buatan

Penunjukan

OECD/LEGAL/0449 Rekomendasi Dewan tentang Kecerdasan Buatan (Referensi dalam subbagian ini merujuk pada rekomendasi ini).

Penerbit

Organisasi: Komite Ekonomi Digital OECD (Organisasi untuk Kerja Sama dan Pembangunan Ekonomi) Otoritas dan pengaruh: OECD tidak memiliki kekuasaan legislatif langsung atas anggotanya (38 negara). Sebaliknya, otoritas dan pengaruhnya didasarkan pada kemampuannya untuk mengumpulkan dan menganalisis data, membuat rekomendasi kebijakan independen, dan menyediakan kerangka kerja untuk dialog dan kerja sama antar negara. OECD menerbitkan berbagai laporan yang memberikan wawasan tentang praktik terbaik dan rekomendasi. Namun, implementasi selalu bersifat sukarela.

Kelompok sasaran

Penerima: Anggota (38 negara) dan non-anggota serta pemangku kepentingan AI yang berperan aktif dalam siklus hidup sistem AI, termasuk organisasi dan individu yang menggunakan atau mengoperasikan AI (Bab I dan II dari Rekomendasi). Lingkup penerapan: Rekomendasi ini bersifat lintas sektor.

Mengapa Pedoman Ini Penting untuk AI Kita?

Di platform daringnya, OECD menyediakan informasi yang relevan tentang penggunaan AI di negara-negara anggotanya dan untuk negara-negara non-anggota serta berbagi praktik terbaik.

Daftar Isi

Prinsip Etika Bagian pertama menguraikan lima prinsip yang relevan bagi semua pemangku kepentingan dalam penggunaan AI. Sejalan dengan hal tersebut, bagian kedua berisi lima rekomendasi bagi anggota dan non-anggota yang telah menandatangani draf rekomendasi untuk mengimplementasikannya dalam kebijakan nasional dan internasional mereka.

1. Prinsip-prinsip untuk penggunaan AI tepercaya yang bertanggung jawab:

I. Pertumbuhan inklusif, pembangunan berkelanjutan, dan kesejahteraan

AI harus bermanfaat bagi manusia dan planet dengan mempromosikan pertumbuhan inklusif, pembangunan berkelanjutan, konservasi alam, dan kualitas hidup (Bagian 1.1).

II. Nilai-nilai yang berpusat pada manusia dan keadilan

Sepanjang siklus hidup sistem AI, prinsip-prinsip dasar supremasi hukum, hak asasi manusia, dan nilai-nilai demokrasi harus dihormati dan perlindungan yang tepat, sebanding dengan kemajuan teknologi, harus diterapkan untuk memastikan kebebasan, keadilan, dan otonomi manusia. Ini mungkin termasuk kemungkinan intervensi manusia jika diperlukan. Tujuannya adalah masyarakat yang adil dan merata (Bagian 1.2).

III. Transparansi dan Keterjelasan

Sistem AI harus memastikan transparansi dan pengungkapan sehingga masyarakat dapat memahami dan menantang hasil berbasis AI, serta memberi kesempatan kepada

orang-orang yang dinilai negatif oleh sistem AI untuk menantang keputusan tersebut (Bagian 1.3).

IV. Ketahanan, keamanan, dan perlindungan

Sistem AI harus berfungsi dengan kuat dan aman selama seluruh siklus hidupnya. Potensi risiko harus terus dinilai dan dipantau oleh pemangku kepentingan AI (Bagian 1.4).

V. Akuntabilitas

Operator AI harus bertanggung jawab atas berfungsinya sistem AI dengan benar dan atas kepatuhan terhadap prinsip-prinsip yang disebutkan di atas, berdasarkan peran mereka, konteks, dan sesuai dengan perkembangan terkini (Bagian 1.5).

2. Rekomendasi untuk pedoman nasional dan kerja sama internasional untuk AI yang dapat dipercaya:

I. Investasi dalam penelitian dan pengembangan AI

Memfasilitasi investasi publik dan swasta dalam penelitian dan pengembangan sistem AI dan kumpulan data terbuka untuk mendorong inovasi dalam AI yang dapat dipercaya (Bagian 2.1)

II. Promosi Ekosistem Digital untuk AI

Ekosistem tersebut mencakup, khususnya, teknologi dan infrastruktur digital dan, jika sesuai, mekanisme untuk berbagi pengetahuan dan data AI (Bagian 2.2).

III. Membentuk Lingkungan Politik yang Kondusif untuk AI

Pemerintah harus mendorong lingkungan kebijakan yang mendukung transisi yang gesit dari fase penelitian dan pengembangan ke fase penerapan dan operasional untuk sistem AI yang dapat dipercaya (Bagian 2.3).

IV. Membangun Kapasitas Manusia dan Mempersiapkan Transformasi Pasar Tenaga Kerja

Pemerintah harus bekerja sama erat dengan para pemangku kepentingan untuk mempersiapkan transformasi dunia kerja dan masyarakat. Mereka harus memungkinkan orang untuk menggunakan sistem AI secara efektif di semua bidang aplikasi dan mendistribusikan manfaat AI secara luas dan adil (Bagian 2.4).

V. Kerja Sama Internasional untuk AI yang Dapat Dipercaya

Pemerintah harus bekerja sama untuk mempromosikan pertukaran pengetahuan AI dan inisiatif multi-pemangku kepentingan internasional, lintas sektoral, dan terbuka (Bagian 2.5).

Definisi AI: Sistem AI adalah sistem berbasis mesin yang menentukan cara menghasilkan keluaran seperti prediksi, konten, rekomendasi, atau keputusan untuk tujuan eksplisit atau implisit dari masukan yang diterimanya, yang dapat memengaruhi lingkungan fisik atau virtual. Sistem AI yang berbeda memiliki tingkat otonomi dan kemampuan adaptasi yang berbeda setelah diterapkan (Bab I). Bidang aplikasi: Tidak ada batasan pada aplikasi atau teknologi AI tertentu.

Instruksi tindakan: Rekomendasi ditujukan kepada negara dan pemangku kepentingan (organisasi dan individu) yang secara langsung atau tidak langsung terlibat dalam atau terpengaruh oleh sistem AI (Bab I).

Validitas dan aktualitas

Tanggal publikasi: versi terkini tertanggal 11 Agustus 2023 (adaptasi dari versi asli tertanggal 22 Mei 2019). Diterbitkan di bawah: Instrumen hukum OECD

Implementasi dan pemantauan

Mekanisme implementasi: Negara-negara anggota menyetujui dokumen rekomendasi secara sukarela dan dengan maksud untuk mempertimbangkan atau menerapkan prinsip atau langkah-langkah yang terkandung di dalamnya di tingkat nasional, dengan kecepatan mereka sendiri dan sesuai dengan prosedur mereka sendiri.

Pemantauan dan evaluasi: OECD akan mendukung implementasi Prinsip-prinsip tersebut dengan menyediakan data dan panduan tentang metrik, kebijakan, dan praktik di bidang AI dan akan menjadi pusat dialog dan pertukaran praktik terbaik untuk kebijakan AI. Hasilnya dapat ditemukan di masing-masing.

Integrasi Hukum dan Regulasi

Status Hukum: Negara-negara anggota menyetujui dokumen rekomendasi secara sukarela. Kekuatan OECD terletak pada kemampuannya untuk memengaruhi pembuatan kebijakan negara-negara anggotanya melalui penelitian, analisis, dan pertukaran praktik terbaik.

Integrasi ke dalam hukum yang ada: Rekomendasi tersebut mencerminkan tujuan bersama dan standar yang disepakati di antara anggota dan dapat dipertimbangkan atau diimplementasikan dalam hukum atau tindakan nasional.

Penerapan Global: Rekomendasi tersebut memiliki dampak internasional.

Peraturan Eksekutif tentang Pengembangan dan Penggunaan Kecerdasan Buatan yang Aman, Terjamin, dan Terpercaya

Penunjukan

Peraturan Eksekutif 14110 tentang Pengembangan dan Penggunaan Kecerdasan Buatan yang Aman, Terjamin, dan Terpercaya (Referensi dalam subbagian ini merujuk pada Peraturan Eksekutif.)

Penerbit

Organisasi: Kantor Eksekutif Presiden Amerika Serikat. Otoritas dan Pengaruh: Peraturan Eksekutif secara langsung mencerminkan otoritas Presiden atas cabang eksekutif dan mengikat semua pejabat administrasi dalam interpretasi hukum.

Kelompok sasaran

Penerima: Perintah Eksekutif ini terutama berlaku untuk otoritas federal dengan dampak tidak langsung pada perusahaan swasta di berbagai sektor. Lingkup penerapan: Perintah eksekutif tidak menggantikan undang-undang, tetapi didasarkan pada kewenangan diskresioner yang diberikan oleh hukum federal AS. Namun, perintah ini berisi mandat khusus untuk berbagai lembaga, misalnya, "untuk melatih tenaga kerja federal tentang isu-isu AI,

kepala setiap lembaga harus menetapkan atau meningkatkan ketersediaan dan penggunaan program pelatihan dan pengenalan AI untuk karyawan, manajer, dan eksekutif (Pasal 10.2 (g))”.

Daftar Isi

Prinsip Etika Menurut Pasal 2, pengembangan dan penggunaan AI harus didorong dan dikelola sesuai dengan delapan prinsip dan prioritas panduan:

1. AI harus aman dan terjamin. Mencapai tujuan ini membutuhkan penilaian sistem AI yang kuat, andal, dapat diulang, dan terstandarisasi, serta kebijakan, lembaga, dan mekanisme lain yang sesuai (Pasal 2 (a)).
2. Mendorong inovasi, persaingan, dan kolaborasi yang bertanggung jawab, termasuk investasi dalam pendidikan, pelatihan, pengembangan, penelitian, dan kapasitas terkait AI. Pada saat yang sama, memperjelas masalah kekayaan intelektual (IP) untuk melindungi penemu dan pencipta. Selain itu, mendorong ekosistem dan pasar yang adil, terbuka, dan kompetitif untuk AI dan teknologi terkait (Pasal 2 (b)).
3. Mendukung pekerja Amerika. Hal ini membutuhkan adaptasi pelatihan kerja dan pendidikan untuk memfasilitasi akses ke peluang yang diciptakan oleh AI bagi tenaga kerja yang beragam. Di tempat kerja itu sendiri, AI tidak boleh digunakan dengan cara yang merusak hak, menurunkan kualitas pekerjaan, menciptakan pengawasan yang tidak tepat terhadap karyawan, mengurangi daya saing di pasar, memperkenalkan risiko kesehatan dan keselamatan baru, atau menyebabkan gangguan yang merugikan di tempat kerja (Pasal 2 (c)).
4. Mempromosikan keadilan dan hak-hak sipil untuk membatasi penggunaan sistem AI yang tidak bertanggung jawab yang mereproduksi ketidaksetaraan yang ada dan jenis diskriminasi berbahaya baru serta memperburuk bahaya daring dan fisik (Pasal 2 (d)).
5. Melindungi konsumen, pasien, penumpang, dan siswa dengan meningkatkan undang-undang perlindungan konsumen yang ada dan menerapkan perlindungan yang tepat terhadap penipuan, bias yang tidak disengaja, diskriminasi, pelanggaran privasi, dan bahaya lain yang disebabkan oleh AI (Pasal 2 (e)).
6. Meningkatkan perlindungan privasi untuk membuat pengumpulan, penggunaan, dan penyimpanan data menjadi sah dan aman serta meminimalkan risiko terhadap perlindungan dan kerahasiaan data (Pasal 2 (f)).
7. Mempromosikan penggunaan AI oleh pemerintah federal. Semua pegawai federal harus menerima pelatihan yang sesuai untuk memahami manfaat, risiko, dan keterbatasan AI untuk fungsi pekerjaan mereka dan untuk memodernisasi infrastruktur TI pemerintah federal, menghilangkan hambatan birokrasi, dan memastikan bahwa AI yang aman dan menghormati hak asasi manusia diterapkan dan digunakan (Pasal 2 (g)).
8. Memperkuat kepemimpinan AS di luar negeri, termasuk merintis sistem dan langkah-langkah keamanan yang diperlukan untuk penggunaan teknologi ini secara bertanggung jawab (Pasal 2 (h)).

Definisi AI Istilah “kecerdasan buatan” mengacu pada sistem berbasis mesin yang mampu membuat prediksi, rekomendasi, atau keputusan yang memengaruhi lingkungan dunia nyata atau virtual untuk serangkaian tujuan yang ditentukan manusia. Sistem

kecerdasan buatan menggunakan masukan mesin dan manusia untuk (A) memahami lingkungan dunia nyata dan virtual, (B) mengabstraksikan persepsi ini ke dalam model melalui analisis secara otomatis, dan (C) merumuskan informasi atau opsi tindakan melalui inferensi model (Pasal 3 (b) dan 15 USC 9401(3)). Bidang aplikasi: Tidak ada batasan untuk aplikasi atau teknologi AI tertentu. Instruksi untuk tindakan: Perintah eksekutif berisi instruksi khusus untuk tindakan, termasuk jadwal waktu dan otoritas yang bertanggung jawab atas implementasi.

Validitas dan aktualitas

Tanggal publikasi: Perintah Eksekutif ditandatangani pada 30 Oktober 2023, diterbitkan pada 1 November 2023. Diterbitkan

Implementasi dan pemantauan

Mekanisme implementasi: Perintah eksekutif berlaku langsung untuk semua pegawai negeri sipil. Pemantauan dan Evaluasi: Dewan AI Gedung Putih dibentuk di dalam Kantor Eksekutif Presiden. Dewan ini mengoordinasikan kegiatan lembaga pemerintah federal untuk memastikan pengembangan, komunikasi, dan keterlibatan industri yang efektif dalam kegiatan AI (Pasal 12).

Integrasi hukum dan peraturan

Status hukum: melengkapi hukum AS yang ada (kewenangan diskresioner) dan mewajibkan berbagai lembaga untuk merekrut dan mengembangkan talenta TI serta mengintegrasikan sistem AI (generatif) ke dalam proses kerja sehari-hari. Integrasi ke dalam hukum yang ada: Spesifikasi untuk ruang lingkup diskresioner hukum, tetapi sesuai dengan hukum yang berlaku dan bergantung pada ketersediaan dana (Pasal 13). Penerapan Global: Perintah Eksekutif terutama berlaku secara nasional di AS, namun Pasal 11 mengamanatkan "memperkuat kepemimpinan AS di luar negeri" dengan beberapa kegiatan yang harus diimplementasikan seperti:

- Memperluas kerja sama dengan sekutu dan mitra internasional di forum bilateral, multilateral, dan multi-pemangku kepentingan yang relevan
- menciptakan kerangka kerja internasional yang kuat untuk mengelola risiko dan menuAI manfaat dari AI
- mendorong standar teknis global yang bertanggung jawab untuk pengembangan dan penggunaan AI di luar sektor militer dan intelijen, seperti:
 - Nomenklatur dan terminologi AI
 - Praktik terbaik dalam hal pengumpulan, pemrosesan, perlindungan, privasi, kerahasiaan, penanganan, dan analisis data
 - Kepercayaan, verifikasi, dan keamanan sistem AI
 - Manajemen risiko AI (berdasarkan prinsip-prinsip Kerangka Kerja Manajemen Risiko AI 100-1 NIST)

Alat Kepatuhan untuk Berbagai Kesempatan

Ada banyak alasan bagus mengapa pengawasan dan manajemen risiko harus dipraktikkan terkait dengan sistem AI. Alasan-alasan bagus ini termasuk Undang-Undang AI, yang sebenarnya hanya akan memengaruhi sangat sedikit aplikasi, tetapi terutama pengawasan dan manajemen risiko hanya memfasilitasi manajemen proyek yang baik.

Memikirkan transparansi dan akuntabilitas sejak awal proyek AI jauh lebih mudah daripada harus membangunnya setelah fakta.

Bab-bab sebelumnya telah menjelaskan bagaimana bidang hukum lain berbatasan dengan Undang-Undang AI. Bagian ini didedikasikan untuk alat-alat umum yang digunakan untuk mendukung proses tata kelola baik yang terkait dengan Undang-Undang AI maupun dengan bidang-bidang yang berdekatan. Tujuannya bukan untuk memberikan daftar lengkap, karena daftar ini akan berkembang pesat dalam beberapa bulan mendatang, tetapi untuk memberikan titik kontak awal dan gambaran umum tentang berbagai cara.

Sebelum kita membahas alat-alat ini, beberapa peringatan perlu disampaikan. Saat ini tidak ada manajemen kualitas untuk pembuatan atau penggunaan alat-alat ini, dan, antara lain, terdapat variasi yang luas dalam cakupan dan kualitas dokumentasi dan kontekstualisasi atau pengujian alat-alat ini. Siklus Plan-Do-Check-Act dapat membantu dalam mengevaluasi alat tata kelola, yang berasal dari ISO 9001:2015. Langkah pertama adalah merumuskan tujuan penggunaan alat tersebut dan sasaran yang ingin dicapai oleh alat tata kelola tersebut. Pencapaian sasaran ini kemudian diuji secara sistematis dan, berdasarkan hasil pengujian ini, tujuan dan sasaran serta proses pengujian dievaluasi. Proses ini kemudian harus dimasukkan ke dalam dokumentasi sistem AI dan tersedia bagi para pelaksana.

Bagaimanapun, penting untuk menggunakan alat yang tepat untuk fase yang tepat dan, misalnya, untuk memeriksa keadilan sehubungan dengan pengembangan sistem AI, tetapi juga selama operasi yang sedang berlangsung. Hal ini juga mencegah risiko yang terkait dengan pergeseran data. atau Pergeseran Model dapat terjadi. Alat-alat teknis juga harus diperlakukan dengan hati-hati, karena metode evaluasi, misalnya untuk penjelasan berdasarkan SHAP atau LIME ditemukan tidak memadai atau tidak dapat diandalkan oleh para ahli akademis. Semua proses dan alat tata kelola harus didokumentasikan dengan baik sehingga, jika terjadi perubahan, dimungkinkan untuk melacak hingga titik waktu mana metode mana yang digunakan.

Pemantauan rutin memudahkan mitigasi risiko. Di satu sisi, ini termasuk memantau kinerja sistem AI dalam hal jaminan kualitas berkelanjutan, tetapi juga penggunaan sistem AI dan pengeluarannya: Apakah ada penggunaan sistem AI yang tidak tepat? Langkah-langkah tata kelola mana yang berhasil dalam praktik dan mana yang tidak? Pilar inti tata kelola yang baik tetaplah upaya untuk memahami seberapa baik alat yang digunakan sebenarnya berfungsi.

Pendekatan Komprehensif

Pendekatan komprehensif pertama untuk memenuhi persyaratan Undang-Undang AI berasal dari konsorsium akademisi dan perusahaan Finlandia. Daftar pemeriksaan tata kelola dari proyek Tata Kelola dan Audit AI mencakup persyaratan penting untuk dokumen dan proses. Alat lain, misalnya, adalah Kerangka Kerja AI Bertanggung Jawab dari Laboratorium AI Bertanggung Jawab yang dapat digunakan untuk mengidentifikasi titik risiko awal berdasarkan penilaian mandiri.

Hak Dasar

Penilaian dampak hak asasi manusia dan hak fundamental semakin banyak diminta oleh organisasi, terutama karena Arahan Uji Tuntas Keberlanjutan Perusahaan yang baru yang akan berisi persyaratan untuk peninjauan rantai pasokan yang mungkin juga berlaku untuk perusahaan di sektor AI. Sistem AI yang dikembangkan atau diterapkan oleh organisasi tidak berbeda dalam konteks ini dengan produk, bahan, atau hubungan lain jika merupakan bagian dari rantai nilai perusahaan.

Sejumlah pedoman yang bermanfaat telah ada untuk memfasilitasi penilaian dampak terhadap hak-hak fundamental. Ini termasuk, misalnya, Panduan UNESCO untuk Implementasi Prinsip Etika dalam Konteks Sistem AI. Institut Hak Asasi Manusia Denmark telah mengembangkan salah satu panduan terlengkap untuk melakukan penilaian dampak AI, sekaligus menyediakan panduan langkah demi langkah melalui proses tersebut. Penilaian dampak terhadap hak-hak fundamental biasanya juga merupakan elemen inti dari pedoman etika, yang dibahas di bagian 9.1.

Perlindungan Data

Sudah ada sejumlah alat bantu yang bermanfaat terkait perlindungan data. Kami merekomendasikan, misalnya, lembar panduan (how-to sheets) dari otoritas perlindungan data Prancis, CNIL. Panduan ini membantu organisasi untuk mengidentifikasi dasar hukum dan tujuan pemrosesan data serta mengklarifikasi status hukum penyedia sistem AI. CNIL juga memberikan panduan tentang penilaian dampak perlindungan data, yang diperlukan untuk semua sistem AI yang memproses data pribadi.

Ada juga upaya untuk menggunakan penilaian dampak perlindungan data untuk melakukan penilaian dampak algoritmik. Tujuannya adalah untuk menciptakan penjelasan berlapis yang, di satu sisi, memberikan penjelasan tentang sistem secara keseluruhan dan, di sisi lain, memungkinkan untuk mendapatkan keputusan algoritmik dalam setiap kasus spesifik. Margot Kaminski dan Gianclaudio Malgieri mengusulkan elemen spesifik untuk ini. Perlu dicatat bahwa Undang-Undang AI juga mensyaratkan penjelasan berlapis, seperti Pasal 12. Pasal 86 UU AI menegaskan bahwa subjek data harus menerima penjelasan tentang peran sistem AI berisiko tinggi dalam pengambilan keputusan dan tentang elemen terpenting untuk hasil sistem AI berisiko tinggi dari Lampiran III UU AI (kecuali sistem AI dalam infrastruktur kritis).

Lingkungan dan keberlanjutan

Seperti dalam konteks hak-hak fundamental, Arahan Due Diligence Keberlanjutan Korporasi yang akan datang mensyaratkan peningkatan fokus pada keberlanjutan dan rantai pasokan, yang juga akan relevan untuk sistem AI. Sudah ada sejumlah alat yang dapat berguna untuk menentukan dan memantau aspek lingkungan, seperti Kalkulator Dampak CO2 Pembelajaran Mesin, Kalkulator Keberlanjutan CO2 atau perangkat lunak Spesifikasi Intensitas Karbon. Namun, alat-alat ini saat ini berfokus pada jejak karbon sistem AI dan paling baik menerjemahkan dampak lain (seperti konsumsi sumber daya) ke dalam ekuivalen karbon. Alat lebih lanjut akan dibutuhkan untuk lebih memahami konsumsi AI, konsumsi bahan baku, limbah, dan dampak lingkungan serupa. Selain itu, banyak dari alat-alat ini dirancang untuk

pengembang dan oleh karena itu tidak cocok untuk organisasi di tempat lain dalam rantai nilai, sehingga pelaporan menjadi lebih sulit bagi pihak yang menerapkan.

Kartu Model dan Lembar Data

Kartu model dan lembar data adalah salah satu alat yang paling dikenal untuk menciptakan transparansi mengenai kemampuan, struktur, dan input sistem AI. Peta model pertama kali diusulkan oleh Margaret Mitchell dan peneliti lain dalam sebuah artikel akademis yang diterbitkan pada tahun 2018. Saat membuat peta model, templat Wajah Berpelukan dapat memberikan inspirasi yang juga mencakup instruksi tentang cara membuatnya. Lembar data untuk dataset juga didasarkan pada sebuah artikel akademis yang diterbitkan oleh Timnit Gebru dan peneliti lain pada tahun 2018. Berbeda dengan peta model, lembar data hanya merujuk pada dataset dan oleh karena itu sangat cocok untuk memenuhi persyaratan dokumentasi dataset.

Manajemen Risiko

Pendekatan standar pertama untuk risiko terkait AI dapat ditemukan dalam ISO/IEC 23894:2023 di mana rekomendasi untuk menangani risiko spesifik AI dan kemungkinan proses manajemen risiko telah dikembangkan. Seri ISO 31000 tentang manajemen risiko dan ISO/IEC 31010:2019 khususnya juga dapat diadaptasi untuk penggunaan sistem AI. Kerangka Kerja Manajemen Risiko AI dari Institut Standar dan Teknologi Nasional AS juga banyak digunakan.

Melibatkan Pemangku Kepentingan

Seperti yang telah disebutkan beberapa kali, dalam beberapa kasus, melibatkan pemangku kepentingan eksternal dalam pengembangan dan pengawasan sistem AI dapat bermanfaat. Untuk memfasilitasi proses ini, Pusat Hukum Nirlaba Eropa, bersama dengan Society Inside, telah mengembangkan kerangka kerja untuk proses partisipatif. Kerangka kerja ini dibangun di atas tiga elemen – tujuan bersama, proses yang terpercaya, dan perubahan yang terlihat sebagai hasil dari keterlibatan – dan mencakup metodologi untuk keterlibatan yang sukses.

Kerangka Kerja Manajemen Risiko Kecerdasan Buatan

Penunjukan

Kerangka Kerja Manajemen Risiko Kecerdasan Buatan (AI RMF 1.0 atau NIST AI 100-1) (Referensi dalam subbagian ini mengacu pada kerangka kerja ini).

Penerbit

Organisasi: Institut Standar dan Teknologi Nasional (NIST). Otoritas dan Pengaruh: NIST adalah badan dari Departemen Perdagangan AS dan memainkan peran sentral secara nasional dan internasional dalam pengembangan standar, pengukuran, dan teknologi yang bertujuan untuk meningkatkan daya saing bisnis, meningkatkan inovasi, dan meningkatkan kualitas hidup.

Kelompok Sasaran

Penerima: Kerangka kerja ini ditujukan untuk organisasi dan individu yang merancang, mengembangkan, dan mengoperasikan sistem AI (Ringkasan Eksekutif NIST AI 100-1). Deskripsi ini ditujukan secara setara kepada manajer, pakar AI, pengguna AI, dan pihak-pihak

lain yang berkepentingan. Bidang aplikasi: Dukungan untuk implementasi dan pengoperasian manajemen risiko untuk aplikasi AI (lihat juga bagian 10.2).

Daftar Isi

Prinsip Etika: Menurut Bab 3, beberapa kriteria harus dipenuhi agar sistem AI dapat dipercaya. Karakteristik sistem AI yang dapat dipercaya meliputi:

1. Valid dan Andal

Validitas dan keandalan sistem AI seringkali dipastikan melalui pengujian dan pemantauan berkelanjutan untuk mengkonfirmasi fungsinya yang benar. Pengukuran validitas, akurasi, ketahanan, dan keandalan berkontribusi pada kepercayaan. Manajemen risiko AI harus memprioritaskan meminimalkan potensi dampak negatif dan dapat mencakup intervensi manusia dalam kasus di mana sistem AI tidak dapat mendeteksi atau memperbaiki kesalahan (Bagian 3.1).

2. Aman

Integrasi langkah-langkah keselamatan di seluruh siklus hidup sistem, dimulai dari tahap perencanaan dan desain paling awal, sangat penting untuk menghindari potensi kegagalan atau kondisi berbahaya. Strategi keselamatan AI yang efektif seringkali mencakup simulasi komprehensif, pengujian dalam aplikasi, pemantauan waktu nyata berkelanjutan, dan kemampuan untuk mematikan, beradaptasi, atau mengaktifkan intervensi manusia dengan aman jika terjadi penyimpangan dari fungsi yang dimaksudkan (Bagian 3.2).

3. Aman dan Tangguh

Sistem AI yang dapat menjaga kerahasiaan, integritas, dan ketersediaan melalui mekanisme perlindungan yang mencegah akses dan penggunaan yang tidak sah dapat digambarkan sebagai aman (Bagian 3.3).

4. Akuntabel dan Transparan

Transparansi mengacu pada seberapa mudah informasi tentang sistem AI dan hasilnya diakses oleh orang-orang yang berinteraksi dengan sistem tersebut, bahkan jika mereka tidak menyadari keberadaan sistem AI tersebut. Akuntabilitas berarti bahwa pengembang dan penyebar AI harus secara proaktif menyesuaikan langkah-langkah transparansi dan akuntabilitas mereka, terutama dalam konteks berisiko tinggi, untuk mengurangi risiko (Bagian 3.4).

5. Dapat Dijelaskan dan Diinterpretasikan

Transparansi, kemampuan menjelaskan, dan kemampuan menginterpretasikan saling mendukung. Transparansi dapat menjawab pertanyaan "apa yang terjadi dalam sistem". Kemampuan menjelaskan menjawab "bagaimana" suatu keputusan dibuat dalam sistem. Kemampuan menginterpretasikan menjawab "mengapa" suatu keputusan dibuat oleh sistem dan apa arti atau konteksnya bagi pengguna (Bagian 3.5).

6. Privasi yang Ditingkatkan

Nilai-nilai privasi seperti anonimitas, kerahasiaan, dan kontrol umumnya harus memandu keputusan untuk desain, pengembangan, dan penerapan sistem AI. Risiko terkait privasi

dapat memengaruhi keamanan, bias, dan transparansi serta disertai dengan pertukaran terhadap karakteristik lainnya (Bagian 3.6).

7. Adil – dengan Bias yang Merugikan Dikelola

Keadilan dalam AI mencakup kepedulian terhadap kesetaraan dan keadilan, mengatasi masalah seperti bias yang merugikan dan diskriminasi. Metode untuk keadilan bisa kompleks, karena persepsi keadilan bervariasi dari budaya ke budaya dan juga dapat berubah tergantung pada aplikasi AI. Pendekatan proaktif diperlukan (Bagian 3.7).

Definisi AI NIST AI 100-1 mengacu pada sistem AI sebagai sistem yang direayasa atau berbasis mesin yang dapat menghasilkan hasil seperti prediksi, rekomendasi, atau keputusan yang memengaruhi lingkungan dunia nyata atau virtual untuk serangkaian tujuan tertentu. Sistem AI dirancang untuk beroperasi dengan berbagai tingkat otonomi (diadaptasi dari: Rekomendasi OECD tentang AI:2019; ISO/IEC 22989:2022).

Bidang aplikasi: Tidak ada batasan untuk aplikasi atau teknologi AI tertentu. Petunjuk tindakan: NIST AI 100-1 menjelaskan prosedur untuk mengidentifikasi, menghindari, atau meminimalkan risiko yang berkaitan dengan sistem AI.

Validitas dan aktualitas

Tanggal publikasi: Januari 2023. Diterbitkan di bawah: National Institute of Standards and Technology.

Implementasi dan pemantauan

Mekanisme implementasi: Spesifikasi oleh NIST Pemantauan dan evaluasi: Deskripsi tersebut mengkarakterisasi kerangka kerja sebagai "dokumen hidup" yang terus dievaluasi oleh NIST dan disesuaikan dengan perubahan persyaratan dan temuan.

Integrasi hukum dan peraturan

Status hukum: Organisasi dapat menerapkan Kerangka Kerja Manajemen Risiko AI secara sukarela. Integrasi ke dalam hukum yang ada: NIST AI 100-1 dirujuk dalam beberapa persyaratan (misalnya, undang-undang, perintah eksekutif, undangan tender, atau pendanaan). Penerapan global: NIST AI 100-1 terutama berlaku secara nasional di AS, tetapi juga dirujuk secara internasional.

Pedoman Etika Formatif Lebih Lanjut

Tidak mudah untuk mengidentifikasi pedoman etika AI global "pertama", karena pengembangan pedoman etika AI telah menjadi proses berkelanjutan, yang berlangsung secara bersamaan di berbagai organisasi dan negara. Meskipun demikian, ada beberapa dokumen awal atau berpengaruh yang dianggap sebagai pelopor dalam debat etika AI dan menjadi dasar untuk pengembangan pedoman selanjutnya.

Deklarasi Montréal untuk Pengembangan Kecerdasan Buatan yang Bertanggung Jawab

Pada tanggal 3 November 2017, Université de Montréal memimpin proses untuk bersama-sama menciptakan Deklarasi Montréal yang didedikasikan untuk pengembangan kecerdasan buatan yang bertanggung jawab. Puluhan acara bertujuan untuk diskusi mendalam tentang tantangan sosial yang ditimbulkan oleh AI. Selain itu, sekitar 15 lokakarya deliberatif diadakan, di mana lebih dari 500 warga, pakar, dan pemangku kepentingan dari berbagai sektor masyarakat ikut serta. Tahun berikutnya, hasil konsultasi warga yang

komprehensif ini dipublikasikan dengan nama “Deklarasi Montreal untuk Pengembangan Kecerdasan Buatan yang Bertanggung Jawab”.

Deklarasi tersebut tidak hanya berisi penjelasan tentang sepuluh prinsip penggunaan AI yang etis, tetapi juga rekomendasi tentang bagaimana menangani transformasi digital. Prinsip-prinsip tersebut mencakup tuntutan untuk partisipasi demokratis, solidaritas, kesejahteraan, perlindungan privasi, kesetaraan, keragaman, dan inklusi.

Situs web ini juga menawarkan perangkat dan praktik terbaik untuk berbagai bidang penggunaan AI, menjelaskan kiat dan aktivitas untuk implementasi konkret di berbagai organisasi, termasuk industri perawatan kesehatan, pemerintah daerah, dan sektor keuangan. Diskusi masih berlangsung dan informasi baru akan dipublikasikan secara bertahap di situs web.

Desain yang Selaras Secara Etis

Salah satu dokumen komprehensif pertama yang membahas aspek etika pengembangan AI adalah pedoman “Desain yang Selaras Secara Etis” dari Inisiatif Global IEEE tentang Etika Sistem Otonom dan Cerdas, yang diterbitkan pada tahun 2016. Versi kedua yang telah diadaptasi tersedia.

Panduan ini mewakili visi Institut Insinyur Listrik dan Elektronik (IEEE) bahwa kesejahteraan manusia harus diprioritaskan dalam sistem otonom dan cerdas, dan menggabungkan analisis ilmiah dengan rekomendasi pragmatis yang berorientasi pada aplikasi. Panduan ini berfungsi sebagai referensi utama bagi para profesional di bidang teknologi, pendidikan, dan kebijakan, serta membahas desain standar, peraturan sertifikasi, dan legislasi di bidang ini.

Pedoman IEEE mencakup berbagai topik, termasuk transparansi, akuntabilitas, dan perlindungan data, serta penghormatan terhadap hak asasi manusia dan peningkatan kesejahteraan manusia.

Pedoman Desain yang Selaras Secara Etis juga telah menjadi titik awal pembuatan sejumlah standar (seri IEEE P7000™ dan seterusnya) dan program sertifikasi terkait, antara lain:

- IEEE P7001™ – Transparansi Sistem Otonom
- IEEE P7002™ – Proses Privasi Data
- IEEE P7003™ – Pertimbangan Bias Algoritma

Rekomendasi tentang Etika Kecerdasan Buatan

Ketika negara-negara anggota UNESCO mengadopsi “Rekomendasi tentang Etika Kecerdasan Buatan” pada November 2021, itu adalah tindakan persetujuan kolektif yang menunjukkan bahwa negara-negara di seluruh dunia mengakui pentingnya pertimbangan etis dalam menangani AI. UNESCO menekankan bahwa rekomendasi ini diadopsi secara bulat oleh semua 193 negara anggota. Negara-negara seperti AS, Tiongkok, dan Rusia, pemain utama di bidang teknologi AI, juga setuju.

Sebelum rekomendasi UNESCO diadopsi secara konsensus, hal ini didahului oleh proses panjang yang melibatkan berjam-jam negosiasi. Terutama tentang hak asasi manusia menjadi subjek negosiasi yang sangat kontroversial, menurut risalah Konferensi Umum UNESCO ke-41.

Rekomendasi UNESCO tentang penggunaan sistem AI secara etis mencakup sebelas bidang kebijakan utama, mulai dari dampak pada tenaga kerja, kesehatan, dan pendidikan hingga aspek-aspek yang sebelumnya diabaikan seperti kepentingan Global Selatan, bias gender, diskriminasi, dan isu keberlanjutan. Pendekatan holistik ini memberikan dasar bagi negara-negara di seluruh dunia untuk membentuk potensi beragam pengembangan AI dengan cara yang bertanggung jawab secara etis.

DAFTAR PUSTAKA

- Al-Shawabkeh, F. A. H., & Al-Jasmi, K. (2025). Artificial intelligence and transparency management in the public sector: A comparative legal study on accountability and oversight in European and American laws. *Journal of Posthumanism*, 5(5), 2326-2340.
- Annex, I. I. (2022). AI watch European landscape on the use of artificial intelligence by the public sector.
- Artzt, M., Belitz, O., Hembt, S., & Löfing, N. (Eds.). (2024). *International handbook of AI law: a guide to understanding and resolving the legal challenges of artificial intelligence*. Kluwer Law International BV.
- Braun, T., & Harasimiuk, D. E. (2025). *Legal, Regulatory and Ethical Non-binary Choices of the AI Act*. Routledge.
- Busuioc, M., Curtin, D., & Almada, M. (2023). Reclaiming transparency: contesting the logics of secrecy within the AI Act. *European Law Open*, 2(1), 79-105.
- Coglianesi, C. (2025). EU AI Act's Impact on Public Sector Use of AI. U of Penn Law School, Public Law Research Paper, (25-34).
- Collaborations, H. (2026). Public Policy for Responsible AI. *The Triple Helix of University-Government-Industry Partnerships and the Development of AI*, 91.
- De Almeida, P. G. R., Dos Santos, C. D., & Farias, J. S. (2021). Artificial intelligence regulation: a framework for governance. *Ethics and Information Technology*, 23(3), 505-525.
- DeStefano, M., Schneider, H., & Papathanasiou, K. (2024). *Compliance in Trade and Information Technology*.
- Djeffal, C. (2019). Artificial intelligence and public governance: normative guidelines for artificial intelligence in government and public administration. In *Regulating artificial intelligence* (pp. 277-293). Cham: Springer International Publishing.
- Farrell, E., Giubilei, M., Griecene, A., Hartog, E., HUPONT, T. I., Kotsev, A., ... & Ulrich, P. (2023). *Artificial intelligence for the Public Sector*.
- Fitsilis, F., von Lucke, J., De Vrieze, F., Mikros, G., Palmirani, M., Read, A., ... & Harris, M. (2024). *Guidelines for AI in Parliaments*. Westminster Foundation for Democracy, 1-49.
- Gavoor, A. A. (2026). *Governing AI Without Agencies: Self-regulatory Organizations and the Federal Backstop*.
- Gonzalez Torres, A. P., & Sawhney, N. (2023). Role of regulatory sandboxes and MLOps for AI-enabled public sector services. *The Review of Socionetwork Strategies*, 17(2), 297-318.

- Gonzalez Torres, A. P., & Sawhney, N. (2023). Role of regulatory sandboxes and MLOps for AI-enabled public sector services. *The Review of Socionetwork Strategies*, 17(2), 297-318.
- Hense, P., & Mustac, T. (2024). AI Act compact: Compliance, management & use cases in corporate practice. *Fachmedien Recht und Wirtschaft*.
- Hilliard, A., Gulley, A., Kazim, E., & Koshiyama, A. S. (2026). Artificial intelligence policy worldwide: a comparative analysis. *Royal Society Open Science*, 13(2).
- Jørgensen, B. N., & Ma, Z. G. (2025). Regulating AI in the energy sector: A scoping review of EU laws, challenges, and global perspectives. *Energies*, 18(9), 2359.
- Karlsfred, M. (2024). Legal Challenges in AI Deployment: Leveraging Security Standards for Compliance in the EU Context.
- KORSHENKO, V. (2024). Risk regulation approach to governing artificial intelligence on the example of the EU's Artificial Intelligence Act.
- Kouroutakis, A. (2024). Public Data, AI Applications. *European Yearbook of Constitutional Law 2023: Constitutional Law in the Digital Era*, 41.
- Krönke, C. (2025). Legal requirements for the use of AI in public administration. In *Buying AI* (pp. 39-62). Edward Elgar Publishing.
- Lawo, D., Neifer, T., Roßbach, Y. A., & Boden, A. (2025, July). Solutions & Challenges of AI Practitioners in AI Act Compliance. In *12th International Conference on Communities & Technologies* (pp. 1-11).
- Lawrence, C., Cui, I., & Ho, D. (2023, August). The bureaucratic challenge to AI governance: An empirical assessment of implementation at US federal agencies. In *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 606-652).
- Lund, B., Orhan, Z., Mannuru, N. R., Bevara, R. V. K., Porter, B., Vinaih, M. K., & Bhaskara, P. (2025). Standards, frameworks, and legislation for artificial intelligence (AI) transparency. *AI and Ethics*, 5(4), 3639-3655.
- Madiega, T. (2021, April). Artificial intelligence act.
- Manzoni, M., Medaglia, R., Tangi, L., van Noordt, C., Vaccari, L., & Gattwinkel, D. (2022). *AI Watch Road to the adoption of Artificial Intelligence by the Public Sector: A Handbook for Policymakers, Public Administrations and Relevant Stakeholders*.
- Marchetti, B. (2024). Artificial intelligence and public authorities: Does the european ai act protect public values?. *European Review of Public Law*, 36(1).
- Micklitz, H. W., & Sartor, G. (2024). Compliance and enforcement in the AIA through AI. *Yearbook of European Law*, 43, 297-341.

- Nevejans, N. (2025). European Union's Regulation on the placing on the market and use of AI systems: a critical overview of the AI Act. *Research Handbook on the Law of Artificial Intelligence*, 489-540.
- Novelli, C., Hacker, P., Morley, J., Trondal, J., & Floridi, L. (2025). A robust governance for the AI Act: AI office, AI board, scientific panel, and national authorities. *European Journal of Risk Regulation*, 16(2), 566-590.
- Olsen, H. P., Hildebrandt, T. T., Wiesener, C., Larsen, M. S., & Flügge, A. W. A. (2024). The right to transparency in public governance: Freedom of information and the use of artificial intelligence by public agencies. *Digital Government: Research and Practice*, 5(1), 1-15.
- Poullet, Y. (2021). Artificial Intelligence and Public Services: the Role of Public Authorities in the Service of the "Third Way" Drawn up by the European Commission. *European review of digital administration & law*, 2(2), 129-148.
- Schwartmann, R., Keber, T. O., & Zenner, K. (Eds.). (2025). *AI Act: a practical guide*. CF Müller.
- Smuha, N. A. (2025). Regulation 2024/1689 of the Eur. Parl. & Council of June 13, 2024 (eu artificial intelligence act). *International Legal Materials*, 64(5), 1234-1381.
- Utomi, E., Osifowokan, A. S., Donkor, A. A., & Yowetu, I. A. (2024). Evaluating the impact of data protection compliance on AI development and deployment in the US health sector. *World Journal of Advanced Research and Reviews*, 24(2), 1100-1110.
- Wachter, S. (2023). Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond. *Yale JL & Tech.*, 26, 671.
- Wachter, S. (2023). Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond. *Yale JL & Tech.*, 26, 671.
- Windholz, N. (2025). *The AI Act Handbook*. Carl Hanser Verlag GmbH Co KG.
- Wirtz, B. W., & Weyerer, J. C. (2023). Artificial Intelligence in the Public Sector. In *Global Encyclopedia of Public Administration, Public Policy, and Governance* (pp. 615-621). Cham: Springer International Publishing.

ATURAN PENGUNAAN Kecerdasan Buatan di Sektor Swasta dan Publik



Dr. Ir. Agus Wibowo, M.Kom, M.Si, MM.

BIO DATA PENULIS



Penulis memiliki berbagai disiplin ilmu yang diperoleh dari Universitas Diponegoro (UNDIP) Semarang. dan dari Universitas Kristen Satya Wacana (UKSW) Salatiga. Disiplin ilmu itu antara lain teknik elektro, komputer, manajemen, ilmu sosiologi dan ilmu hukum. Penulis memiliki pengalaman kerja pada industri elektronik dan sertifikasi keahlian dalam bidang Jaringan

Internet, Telekomunikasi, Artificial Intelligence, Internet Of Things (IoT), Augmented Reality (AR), Technopreneurship, Internet Marketing dan bidang pengolahan dan analisa data (komputer statistik), Ilmu Perpajakan.

Penulis adalah pendiri dari Universitas Sains dan Teknologi Komputer (Universitas STEKOM) dan juga seorang dosen yang memiliki Jabatan Fungsional Akademik Lektor Kepala (Associate Professor) yang telah menghasilkan puluhan Buku Ajar ber ISBN, HAKI dari beberapa karya cipta dan Hak Paten pada produk IPTEK. Sejak tahun 2023 penulis tercatat sebagai Dosen luar biasa di Fakultas Ekonomi & Bisnis (FEB) Universitas Diponegoro Semarang. Penulis juga terlibat dalam berbagai organisasi profesi dan industri yang terkait dengan dunia usaha dan industri, khususnya dalam pengembangan sumber daya manusia yang unggul untuk memenuhi kebutuhan dunia kerja secara nyata.



YAYASAN PRIMA AGUS TEKNIK

PENERBIT :

YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

ISBN 978-634-7227-93-5 (PDF)



9 786347 227935