Etika Profesi

Adi Wahyu Pribadi

Diskusi

- Tini adalah mahasiswa Informatika yang bekerja magang di sebuah startup teknologi. Startup ini memiliki **sistem pemesanan online untuk pelanggan**.
- Suatu hari, Tini menemukan celah keamanan (*vulnerability*) yang cukup serius di sistem pemesanan tersebut. Dengan celah ini, Tini dapat mengakses informasi pesanan pelanggan secara detail (nama, alamat, nomor telepon, dan rincian pesanan).
- Tini mencoba mengeksploitasi celah itu untuk “membuktikan diri” bahwa ia mahir. Tini mengunduh sebagian data untuk melakukan analisis sendiri.
- Setelah mempelajari data, Tini pun tergoda untuk memamerkan temuannya kepada teman-teman sekelas dengan cara menampilkan beberapa data sensitif pelanggan dalam presentasi tugas kuliah. Tujuannya agar terlihat “keren” dan kompeten di mata dosen dan teman-teman.

1. Apa yang salah dalam tindakan Tini?
2. Apa dampak etis dan hukum dari tindakan tersebut terhadap perusahaan dan pelanggan?
3. Jika Tini beralasan “hanya ingin menunjukkan keterampilan IT” atau “membantu perusahaan memecahkan masalah”, apakah alasan tersebut bisa dibenarkan?
4. Bagaimana seharusnya seorang profesional TI menangani penemuan celah keamanan seperti ini?
5. Apakah ini termasuk pelanggaran etika umum, etika profesi, atau keduanya? Mengapa?

Etika (Ethics)

Etika adalah cabang filsafat yang mempelajari prinsip-prinsip umum tentang baik dan buruk, benar dan salah, serta tanggung jawab manusia. Etika bersifat teoritis dan universal, sering kali merujuk pada sistem nilai yang dikembangkan melalui penalaran filosofis.

Berasal dari kata “ethos” (Yunani) yang berarti kebiasaan atau adat.

Etika berkaitan dengan nilai-nilai dan prinsip-prinsip yang menentukan perilaku seseorang terhadap baik-buruk atau benar-salah.

Etika lebih bersifat konseptual dan reflektif; menuntut kita memikirkan apa yang seharusnya dilakukan.

Ciri Khas:

- Bersifat objektif dan sistematis.
- Contoh: Etika utilitarianisme (menilai tindakan berdasarkan konsekuensi terbaik untuk mayoritas).

Moral (Morals)

Moral adalah **keyakinan atau nilai pribadi** tentang benar dan salah yang dipegang individu atau kelompok, sering kali dibentuk oleh budaya, agama, atau pengalaman hidup. Moral lebih bersifat subjektif dan praktis.

Berasal dari kata “mos” (Latin) yang berarti kebiasaan atau adat istiadat.

Moral merujuk pada norma atau aturan yang menjadi pedoman perilaku di masyarakat tertentu.

Sifatnya lebih praktis dan sering muncul dalam bentuk aturan konkret (misalnya norma adat, norma sosial).

Ciri Khas:

- Bersifat personal atau kelompok tertentu.
- Contoh: Keyakinan bahwa berbohong selalu salah, meski untuk alasan baik.

Perbedaan Etika dan Moral

- Etika adalah kerangka teoritis (misalnya, "Apa yang mendefinisikan keadilan?"), sementara moral adalah penerapan praktis ("Apakah saya boleh berbohong untuk menyelamatkan nyawa?").
- Etika cenderung universal, sedangkan moral bisa berbeda antar kelompok atau individu.

Etiket (Etiquette)

Etiket adalah norma **sopan santun** atau **tata cara perilaku dalam masyarakat atau situasi tertentu**. Fokusnya pada kesopanan, bukan pada prinsip moral.

Kumpulan aturan kesopanan yang berlaku dalam interaksi sosial.

Lebih menekankan aspek tata krama, sopan santun, dan cara berinteraksi yang sopan.

Meskipun penting, etiket bersifat kontekstual dan dapat berbeda antar budaya atau masyarakat.

Ciri Khas:

- Bersifat konvensional dan situasional.
- Contoh: Mengucapkan "terima kasih", menggunakan sendok dan garpu saat makan.

Hubungan Etika, Moral, dan Etiket

- Etika → landasan berpikir filosofis tentang apa yang baik dan buruk.
- Moral → implementasi nilai-nilai dan norma di masyarakat.
- Etiket → aturan perilaku sopan-santun yang lebih teknis atau praktis dalam interaksi.

Misal

- Etika: “Apakah menghormati guru itu baik atau buruk?”
- Moral: “Dalam budaya kita, menghormati guru adalah kewajiban.”
- Etiket: “Dalam pertemuan, siswa berdiri ketika guru masuk sebagai tanda hormat.”

Etika Profesi

Etika yang diterapkan secara khusus pada suatu profesi tertentu, seperti dokter, pengacara, atau profesional TI.

Dilandasi oleh kode etik yang disusun oleh organisasi profesi (misalnya ACM, IEEE di bidang IT).

Tujuan: menjaga kualitas layanan, kepercayaan publik, dan integritas profesi.

Etika Umum

Prinsip dasar etika yang berlaku untuk setiap orang tanpa memandang profesi.

Berhubungan dengan nilai-nilai universal (kejujuran, keadilan, rasa hormat).

Menjadi landasan perilaku individu dalam kehidupan sehari-hari.

Istilah	Sumber Otoritas	Fokus	Contoh Pelanggaran
Etika	Filsafat, teori	Prinsip universal	Mencuri melanggar prinsip keadilan.
Moral	Budaya/agama/individu	Keyakinan pribadi	Menolak membantu orang karena egois.
Etiket	Norma sosial	Kesopanan	Tidak memberi salam saat bertamu.
Etika Profesi	Kode profesi	Tanggung jawab pekerjaan	Dokter membocorkan data pasien.

Berbagai Teori Etika lainnya

- Etika Utilitarianisme
- Etika Deontologi (Kantianisme)
- Etika Virtue (Kebajikan)
- Etika Hak (Rights-Based Ethics)
- Etika Kepedulian (Ethics of Care)
- Etika Egoisme

Etika Utilitarianisme

- Definisi:

  Menilai tindakan berdasarkan konsekuensi yang menghasilkan kebahagiaan atau kebaikan terbesar bagi mayoritas.

- Prinsip Kunci:

  "Tindakan benar adalah yang memaksimalkan manfaat dan meminimalkan penderitaan."

- Kritik:

  Utilitarianisme dapat mengabaikan hak individu atau kelompok minoritas, karena fokusnya pada total “manfaat bersih” terbesar.

Contoh

Penjadwalan Sumber Daya: Seorang manajer proyek TI memutuskan untuk menambah jam kerja dua orang timnya selama beberapa hari agar tenggat waktu terpenuhi. Keputusan ini dibuat karena jika proyek selesai tepat waktu, manfaatnya dirasakan oleh klien dan seluruh perusahaan (karyawan lain tetap berstatus kerja dan menerima bonus). Meskipun beberapa anggota tim mengalami ketidaknyamanan, hal ini dianggap sah dari sudut pandang utilitarian karena keuntungan keseluruhan lebih besar.

Penataan Lalu Lintas Data: Dalam sebuah sistem jaringan, kebijakan bandwidth diatur sedemikian rupa agar mayoritas pengguna memperoleh koneksi cepat, walaupun sebagian kecil pengguna (dengan kebutuhan khusus) mungkin merasakan keterbatasan.

Etika Deontologi (Kantianisme)

- Definisi:

  Menekankan kewajiban moral dan aturan universal, terlepas dari konsekuensi.

- Prinsip Kunci:

  "Tindakan benar adalah yang sesuai dengan prinsip moral yang bisa diterapkan secara universal." (Immanuel Kant)

- Kritik

  Terlalu kaku, mengharuskan seseorang tetap mengikuti “aturan universal” meskipun kondisi tertentu mungkin menuntut fleksibilitas.

  Kurang mempertimbangkan konsekuensi bagi pihak lain.

Contoh

Larangan Berbohong dalam Audit Keamanan: Seorang konsultan TI menemukan bahwa perusahaan tempatnya bekerja melakukan pelanggaran kebijakan data. Menurut Kantianisme, ia tetap harus jujur melaporkan temuan tersebut sesuai kewajiban moral, meskipun konsekuensinya mungkin memberatkan.

Kontrak Kerja: Seorang programmer menolak mengambil jalan pintas (memalsukan hasil tes) untuk memenuhi target klien, karena itu melanggar prinsip kejujuran dan integritas.

Etika Virtue (Kebajikan)

- Definisi:

  Berfokus pada karakter individu dan pengembangan sifat-sifat baik (seperti kejujuran, keberanian, kebijaksanaan).

- Prinsip Kunci:

  "Apa yang dilakukan oleh orang yang bijaksana (virtuous) dalam situasi ini?" (Aristoteles)

- Kritik

  Sulit memberikan panduan aksi yang spesifik, karena bergantung pada penilaian “kebajikan” setiap individu.

  Keberagaman budaya membuat definisi “kebajikan” bervariasi.

Contoh

Konsistensi dalam Kejujuran: Seorang pengembang perangkat lunak secara konsisten menjaga kejujuran dalam proses coding dan bug reporting, bukan karena aturan atau konsekuensi, melainkan karena ia memiliki karakter jujur dan bertanggung jawab.

Kepemimpinan yang Bijaksana: Seorang CTO (Chief Technology Officer) selalu mengutamakan kebijaksanaan dan kehati-hatian dalam mengambil keputusan teknologi untuk kepentingan jangka panjang, bukan hanya mengincar keuntungan sesaat.

Etika Hak (Rights-Based Ethics)

- Definisi:

  Menekankan hak individu yang tidak boleh dilanggar, seperti hak hidup, kebebasan, dan privasi.

- Prinsip Kunci:

  "Tindakan etis adalah yang menghormati hak dasar manusia."

- Kritik

  Dalam situasi konflik hak (misalnya, kebebasan ekspresi vs hak privasi), menentukan mana hak yang lebih diutamakan bisa menjadi kompleks.

  Memerlukan landasan hukum atau norma sosial yang diakui bersama.

Contoh

Hak Privasi Data: Sebuah perusahaan teknologi menerapkan kebijakan privasi yang ketat untuk melindungi hak pengguna. Perusahaan meminimalkan pengumpulan data, hanya memproses data dengan persetujuan pengguna, dan memusnahkan data yang tidak diperlukan.

Hak Kebebasan Bersuara: Platform media sosial menyediakan ruang diskusi bebas, tetapi tetap menghormati hak orang lain dengan menghapus konten yang mengandung ujaran kebencian.

Etika Kepedulian (Ethics of Care)

- Definisi:

  Berfokus pada relasi interpersonal, empati, dan tanggung jawab terhadap orang-orang terdekat.

- Prinsip Kunci:

  "Tindakan etis adalah yang memperhatikan kebutuhan dan konteks hubungan spesifik." (Carol Gilligan)

- Kritik

  Terkesan bias pada hubungan yang dekat, sehingga kesulitan memberikan panduan universal pada setiap situasi.

  Rentan menempatkan beban berat pada pelaku yang terlalu “peduli” hingga kurang menyeimbangkan aspek lain.

Contoh

Perancangan Produk Inklusif: Tim desain aplikasi memperhatikan kebutuhan pengguna lansia atau penyandang disabilitas agar mereka dapat mengakses layanan dengan mudah. Pendekatan ini didasari kepedulian terhadap kelompok rentan, bukan sekadar kewajiban hukum.

Pendekatan Personalisasi: Seorang leader tim TI yang selalu mempertimbangkan kondisi personal anggotanya. Misal, jika seorang anggota memiliki masalah keluarga, leader memberikan dukungan dan waktu fleksibel.

Etika Egoisme

- Definisi:

  Menganggap tindakan benar adalah yang menguntungkan diri sendiri secara rasional.

- Prinsip Kunci:

  "Tindakan etis adalah yang memaksimalkan kebaikan untuk diri sendiri." (Ayn Rand)

- Kritik

  Rentan berbenturan dengan nilai moral umum, karena bisa menghalalkan tindakan yang merugikan pihak lain asalkan memenuhi kepentingan pribadi pelaku.

  Sulit menjaga kerja sama atau kepercayaan di lingkungan sosial/profesional jangka panjang.

Contoh

Pengambilan Keputusan Bisnis Pribadi: Seorang programmer freelance lebih memilih proyek yang memberi keuntungan terbesar bagi dirinya meskipun proyek tersebut kurang berdampak positif bagi masyarakat, karena dia mengedepankan kepentingan pribadi.

Penggunaan Celah Teknologi: Seorang developer aplikasi menambahkan fitur tersembunyi untuk “menambang data” demi keuntungan sendiri, selama dia merasa hal itu tidak segera merugikan pengguna secara nyata.

Tugas

Analisis studi kasus berdasarkan

1. Etika Utilitarianisme
2. Etika Deontologi (Kantianisme)
3. Etika Kebajikan
4. Etika Hak
5. Etika Kepedulian
6. Etika Egoisme

Kasus Etika: “Penggunaan Data Pengguna di Perusahaan E-Commerce”

Tio adalah seorang lead developer pada perusahaan e-commerce **X** yang sangat populer. Platform ini mengumpulkan beragam data pengguna—mulai dari riwayat pencarian, lokasi, hingga sebagian informasi kartu kredit—untuk menampilkan rekomendasi produk yang lebih “personal.” Namun, mekanisme **opt-in** atau **persetujuan tertulis** tidak sepenuhnya jelas bagi pengguna. Selain itu, Tio mengetahui bahwa ada kemungkinan data tersebut dijual ke pihak ketiga untuk analisis pasar.

Tio mulai merasa tidak nyaman dengan praktik ini. Ia khawatir bahwa privasi pelanggan terabaikan dan mereka tidak sepenuhnya tahu data apa saja yang dikumpulkan serta bagaimana data tersebut diolah. Namun, pihak manajemen berpendapat bahwa cara ini **efektif meningkatkan pendapatan** dan **mempercepat inovasi** produk, serta lazim di industri. Tio menghadapi dilema: apakah ia harus menegur manajemen, melapor ke regulator, atau diam saja agar tidak merusak kariernya?

Diskusi Tini

Kesalahan Tini:

- **Eksploitasi Celah Tanpa Izin**: Tini memanfaatkan kerentanan sistem untuk mengakses data pelanggan di luar kewenangannya.
- **Pelanggaran Kerahasiaan**: Data pelanggan bersifat sensitif dan seharusnya tidak diunduh atau disimpan secara pribadi tanpa prosedur resmi.
- **Penyebaran Data Sensitif**: Tini menampilkan data pelanggan dalam presentasi umum, melanggar hak privasi dan kepercayaan yang diberikan perusahaan/pelanggan.
- **Perilaku Tidak Profesional**: Alih-alih melaporkan temuan ke atasan atau tim keamanan, Tini justru memamerkannya demi pengakuan.

Diskusi Tini

Dampak Etis:

- **Ketidakpercayaan**: Pelanggan dan karyawan lain kehilangan kepercayaan pada perusahaan karena data pelanggan bisa diekspos.
- **Pelanggaran Integritas Profesi**: Tini sebagai calon profesional TI menunjukkan ketidakbertanggungjawaban dalam melindungi data sensitif.

Dampak Hukum:

- **Pelanggaran Privasi**: Undang-undang perlindungan data (misalnya GDPR General Data Protection Regulation/Regulasi Umum Perlindungan Data di Eropa atau regulasi lain di negara setempat) dapat menghukum pemrosesan atau penyebaran data tanpa izin.
- **Tuntutan Hukum**: Perusahaan bisa digugat pelanggan atau diawasi otoritas terkait karena dianggap lalai dalam melindungi data.
- **Tanggung Jawab Individu**: Tini berisiko terjerat persoalan hukum internal perusahaan (perjanjian kerahasiaan/Non-Disclosure Agreement) dan peraturan eksternal (cyberlaw).

Diskusi Tini

Jika Tini beralasan “hanya ingin menunjukkan keterampilan IT” atau “membantu perusahaan memecahkan masalah”, apakah alasan tersebut bisa dibenarkan?

- **Tidak Dibolehkan**: Meskipun niatnya terlihat positif, caranya salah.
- **Cara yang Benar**: “Membantu perusahaan” seharusnya dilakukan dengan melaporkan celah secara internal (responsible disclosure), bukan memamerkan data tanpa otorisasi.
- **Prinsip Profesionalisme**: Profesional TI wajib mematuhi kode etik, termasuk menjaga kerahasiaan data dan menaati prosedur pelaporan bug. Keinginan unjuk keterampilan tidak boleh melanggar privasi dan keamanan.

Diskusi Tini

Bagaimana seharusnya seorang profesional TI menangani penemuan celah keamanan seperti ini?

1. **Responsible Disclosure**

Laporkan penemuan kerentanan kepada tim keamanan atau atasan di perusahaan secara internal terlebih dahulu.

Ikuti alur pelaporan yang berlaku, misalnya bug bounty program atau SOP perusahaan.

2. **Dokumentasi yang Aman**

Lakukan dokumentasi celah secara singkat dan aman, hindari menyimpan data sensitif secara pribadi.

Jika perlu bukti teknis, anonimisasi data pelanggan sebelum digunakan untuk bukti laporan.

3. **Koordinasi dan Perbaikan**

Bekerjasama dengan tim terkait untuk menguji dan memperbaiki celah.

Hindari mempublikasikan detail kerentanan sebelum pihak perusahaan siap, demi melindungi pengguna.

Diskusi Tini

Apakah ini termasuk pelanggaran etika umum, etika profesi, atau keduanya? Mengapa?

1. **Pelanggaran Etika Umum:**

Tini melanggar norma moral dengan menyalahgunakan kepercayaan dan hak privasi orang lain.

Menunjukkan ketidakhormatan terhadap kepentingan dan keamanan data pelanggan.

2. **Pelanggaran Etika Profesi:**

Dalam kode etik profesi TI (seperti ACM/IEEE), perlindungan data dan tanggung jawab menjaga kerahasiaan termasuk pilar utama.

Tini mengingkari integritas profesional dengan memamerkan data sensitif secara tidak sah dan tidak bertanggung jawab.

Jadi tindakan Tini melanggar keduanya, karena melanggar nilai-nilai umum (jujur, adil, menghormati privasi) dan kaidah profesional (kerahasiaan, integritas, tanggung jawab terhadap pengguna dan organisasi).

Diskusi Tini

- Tini melakukan pelanggaran serius pada aspek privasi, kerahasiaan data, dan kepercayaan.
- “Niat membantu” atau “unjuk kemampuan” bukan alasan yang membenarkan pelanggaran etika dan hukum.
- Langkah yang benar adalah melakukan responsible disclosure dan menjaga kerahasiaan data hingga celah tersebut ditangani.
- Kasus ini mencerminkan perlunya sikap profesionalisme dan tanggung jawab sosial dalam pengembangan serta pemeliharaan teknologi informasi.

Next Course

Pelajari!

ACM Code of Ethics and Professional Conduct (2018).

IEEE Code of Ethics.

Etika Profesi

Pertemuan Kedua

Review

- Etika → teoritis
- Moral
- Etiket

Diskusi

Apa pentingnya sebuah profesi memiliki kode etik tersendiri?

Definisi Profesi: Memiliki keahlian khusus, diakui secara formal, dan memiliki tanggung jawab sosial.

Karakteristik Profesi Informatika/TI:

- Berbasis pengetahuan ilmiah dan keterampilan teknis (software engineering, data science, dsb).
- Organisasi profesi atau himpunan ahli (misalnya, ACM, IEEE-CS).
- Standar kompetensi dan continuous professional development.

Apa bedanya Profesi dan Pekerjaan?

Programmer Freelancer → Profesi atau Pekerjaan?

Kode Etik

- **Pengantar Kode Etik**: Fungsi dan pentingnya panduan moral bagi profesional TI, menjaga kepercayaan publik dan menjamin keselamatan/dampak sosial.

- **Kode Etik ACM**: Struktur kode etik, prinsip-prinsip seperti keadilan, privasi, integritas, dan tanggung jawab profesional.

- **Kode Etik IEEE**: Poin-poin kunci seperti keselamatan publik, tanggung jawab kepada klien, kolega, serta pentingnya kompetensi dan integritas.

Kode Etik ACM

https://www.acm.org/code-of-ethics

1. GENERAL ETHICAL PRINCIPLES
2. PROFESSIONAL RESPONSIBILITIES
3. PROFESSIONAL LEADERSHIP PRINCIPLES
4. COMPLIANCE WITH THE CODE

Next Pertemuan

Hukum dan Regulasi IT di Indonesia

- UU ITE
- UU Perlindungan Data
- Regulasi Internasional dan Nasional

Kerangka Hukum dan Regulasi Bidang IT

Etika Profesi

Tujuan

- Memahami Kerangka Hukum Terkait Teknologi Informasi
  - UU ITE
  - UU Perlindungan Data Pribadi
  - Regulasi Internasional (GDPR di Eropa)
- Mengetahui Konsekuensi Hukum bagi Pelanggaran Etika
  - Resiko hukum yang dihadapi jika terjadi pelanggaran privasi, pelanggaran hak cipta, atau cybercrime
- Mengerti Peran Profesional TI dalam Penegakan Regulasi
  - Tanggung jawab dan kewajiban profesional TI untuk mematuhi hukum serta melaporkan potensi pelanggaran

Outcome

- Mengidentifikasi undang-undang yang relevan dengan aktivitas TI serta menjelaskan cakupan dan sanksi yang diatur.
- Menganalisis kasus sederhana yang berkaitan dengan pelanggaran hukum TI dan memberikan solusi sesuai hukum yang berlaku.
- Menunjukkan sikap tanggung jawab profesional dalam konteks kepatuhan hukum dan pelaporan pelanggaran.

Apa risiko hukum jika seorang developer membobol data pelanggan, selain risiko etika?

Apa konsekuensi bagi perusahaan?

UU ITE

Sejarah Terbentuknya UU ITE

Latar Belakang

- Memasuki era digital pada awal 2000-an, transaksi elektronik di Indonesia mulai berkembang pesat (e-commerce, internet banking, dsb).
- Pemerintah memandang perlu adanya payung hukum yang jelas untuk mengatur kegiatan transaksi elektronik, keamanan data, dan pemanfaatan internet secara lebih luas.

Sejarah Terbentuknya UU ITE

Proses Pembentukan

- Rancangan Undang-Undang Informasi dan Transaksi Elektronik (RUU ITE) digagas sejak awal 2000-an oleh Kementerian Komunikasi dan Informatika (Kominfo) bersama pemangku kepentingan lain.
- UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik akhirnya disahkan pada 21 April 2008.
- Selanjutnya, UU ITE sempat mengalami revisi melalui UU No. 19 Tahun 2016 yang bertujuan untuk menyesuaikan sejumlah pasal, terutama terkait penghinaan/ pencemaran nama baik di ranah online.

Sejarah Terbentuknya UU ITE

Tujuan Awal

- Memberikan kepastian hukum bagi transaksi elektronik (validitas tanda tangan digital, bukti elektronik, dan sebagainya).
- Mengatur pemanfaatan internet secara aman dan bertanggung jawab, termasuk upaya pencegahan cybercrime.
- Menangkal potensi kerugian ekonomi dan sosial akibat penyalahgunaan teknologi informasi.

Isi Utama UU ITE

Pengakuan Informasi dan Dokumen Elektronik

- UU ITE menegaskan bahwa dokumen elektronik dapat menjadi alat bukti hukum yang sah (pasal-pasal tentang keabsahan bukti elektronik).
- Mengatur tata cara penggunaan tanda tangan elektronik sebagai pengganti tanda tangan basah dalam transaksi digital.

Isi Utama UU ITE

Pengaturan Transaksi Elektronik

- Menjamin kepastian hukum bagi e-commerce, internet banking, dan sejenisnya.
- Mencakup perlindungan konsumen digital dan persyaratan penyelenggaraan sistem elektronik.

Isi Utama UU ITE

Larangan dan Sanksi Terkait Konten Ilegal

- Pasal-pasal yang mengatur penyebaran konten pornografi, perjudian online, akses ilegal (hacking), pemerasan online, dsb.
- Dalam revisi UU 19/2016, beberapa ketentuan diperjelas, misalnya ketentuan pemidanaan atas ujaran kebencian, penghinaan, dan pencemaran nama baik di media elektronik.

Isi Utama UU ITE

Pemblokiran dan Penghapusan Konten

- Pemerintah (melalui Kominfo) diberikan kewenangan untuk memblokir akses atau memerintahkan penghapusan konten yang dianggap melanggar ketentuan.
- Mekanisme ini diatur lebih lanjut dalam peraturan pelaksana (PP/Perkominfo).

Isi Utama UU ITE

Tanggung Jawab Penyelenggara Sistem Elektronik

- Mengharuskan para penyelenggara platform internet (penyedia layanan email, e-commerce, dsb.) memenuhi standar keamanan informasi, perlindungan data pribadi, dan kewajiban pelaporan insiden.

Poin-Poin Kontroversial UU ITE

Pasal Pencemaran Nama Baik/Penghinaan

- Diatur pada Pasal 27 ayat (3) UU ITE, yang sering disebut sebagai “pasal karet” karena frasa “penghinaan dan/atau pencemaran nama baik” dirasa terlalu luas.
- Banyak kasus pengguna media sosial dipidana karena dianggap menghina seseorang atau institusi; kerap dikhawatirkan membatasi kebebasan berpendapat.

Poin-Poin Kontroversial UU ITE

Kebebasan Ekspresi dan Sensor

- Wewenang pemblokiran situs atau konten yang diberikan kepada pemerintah memunculkan kekhawatiran atas transparansi dan akuntabilitas proses pemblokiran.
- Dikhawatirkan bisa menimbulkan *overblocking* (pemblokiran berlebihan) atau disalahgunakan untuk membungkam kritik.

Poin-Poin Kontroversial UU ITE

Ancaman Pidana Diperluas

- Denda dan ancaman penjara bagi pelanggaran tertentu dirasa cukup berat, sehingga memunculkan efek “membungkam” (chilling effect) bagi masyarakat.
- Meski revisi 2016 menurunkan ancaman pidana pada beberapa pasal, problem interpretasi masih menjadi tantangan.

Poin-Poin Kontroversial UU ITE

Definisi yang Kurang Spesifik

- Beberapa istilah seperti “merugikan orang lain,” “muatan kesusilaan,” atau “menyebarkan informasi bohong” berpotensi ditafsirkan berbeda-beda.
- Minimnya penjelasan mendetail membuat pasal-pasal ini bisa menjerat pengguna internet tanpa batasan jelas.

Implementasi UU ITE di Indonesia

Penegakan Hukum

- Sejak diundangkan, banyak kasus pencemaran nama baik, hoaks, dan ujaran kebencian diproses melalui UU ITE.
- Polisi kerap menggunakan UU ITE dalam menangani laporan pencemaran nama baik di media sosial, misalnya Twitter, Facebook, Instagram, YouTube, dsb.

Implementasi UU ITE di Indonesia

Contoh Kasus

- Kasus pencemaran nama baik yang diajukan oleh pejabat, figur publik, atau perseorangan yang merasa dirugikan oleh unggahan di media sosial.
- Pemblokiran situs-situs tertentu oleh Kominfo karena dianggap mengandung unsur pornografi, SARA, atau berita palsu.

Implementasi UU ITE di Indonesia

Kritik dari LSM dan Masyarakat

- Banyak Lembaga Swadaya Masyarakat (LSM) seperti SAFEnet menyoroti penerapan UU ITE, menilai perlu adanya revisi lebih lanjut untuk melindungi kebebasan berekspresi.
- Terdapat aspirasi agar pasal pencemaran nama baik dipindahkan ke ranah perdata, bukan pidana, karena dapat diselesaikan dengan ganti rugi daripada penjara.

Implementasi UU ITE di Indonesia

Upaya Revisi dan Petunjuk Teknik

- Pemerintah dan DPR sempat mendiskusikan revisi lanjutan untuk memperjelas definisi dan meniadakan atau mempersempit “pasal-pasal karet”.
- Surat Keputusan Bersama (SKB) Tiga Menteri tahun 2021 memberikan pedoman penanganan kasus pencemaran nama baik, mengupayakan penyelesaian di luar pidana (restorative justice).

Implementasi UU ITE di Indonesia

Transformasi Digital dan Perlindungan Data Pribadi

- Kemajuan teknologi menuntut Indonesia terus menyesuaikan regulasi.
- Keterkaitan UU ITE dengan UU Perlindungan Data Pribadi (UU PDP, disahkan 2022) serta aturan turunannya menjadi langkah menuju ekosistem digital yang lebih aman.

UU Perlindungan Data Pribadi (PDP)

Sejarah Terbentuknya UU PDP

Latar Belakang

- Seiring dengan meningkatnya digitalisasi (e-commerce, media sosial, fintech, dsb.), kasus kebocoran data dan penyalahgunaan informasi pribadi menjadi sorotan besar di Indonesia.
- Sebelumnya, perlindungan data diatur secara parsial dalam beberapa regulasi (misalnya UU ITE, PP PSTE) tanpa ada payung hukum khusus yang komprehensif.

Sejarah Terbentuknya UU PDP

Proses Pembahasan

- Pembahasan RUU Perlindungan Data Pribadi (RUU PDP) dimulai sejak sekitar 2016-2017 oleh Kementerian Komunikasi dan Informatika (Kominfo) bersama DPR.
- RUU ini beberapa kali tertunda penyelesaiannya, antara lain karena perbedaan pandangan soal lembaga otoritas pengawas data pribadi.

Sejarah Terbentuknya UU PDP

Pengesahan

- Setelah melalui proses diskusi dan konsultasi publik yang panjang, RUU PDP disahkan menjadi UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi pada 17 Oktober 2022.
- Pengesahan ini menjadi tonggak penting, mengingat Indonesia telah lama dianggap perlu memiliki kerangka hukum serupa General Data Protection Regulation (GDPR) di Uni Eropa.

Sejarah Terbentuknya UU PDP

Tujuan Utama

- Memberikan perlindungan hukum bagi pemilik data (subjek data) agar data pribadi mereka tidak dieksploitasi atau disalahgunakan.
- Mendorong tata kelola data yang lebih bertanggung jawab di sektor publik maupun swasta.
- Meningkatkan kepercayaan masyarakat dan pelaku bisnis terhadap ekosistem digital di Indonesia.

Isi Pokok UU PDP

Definisi Data Pribadi

- Mengatur definisi “data pribadi” secara eksplisit, mencakup data yang mengidentifikasi langsung (nama, NIK, alamat) maupun data yang mengarah pada identitas tertentu (data biometrik, informasi kesehatan, dsb.).

Isi Pokok UU PDP

Hak Subjek Data

- Subjek data memiliki hak untuk mengakses, memperbaiki, menghapus, bahkan menarik persetujuan atas penggunaan data pribadi mereka.
- Ada pula ketentuan tentang right to be forgotten (hak untuk dilupakan) dalam kasus tertentu.

Isi Pokok UU PDP

Kewajiban Pengendali dan Pemroses Data

- Pihak yang mengumpulkan atau mengolah data (data controller dan data processor) wajib menerapkan prinsip transparansi, keamanan, dan keabsahan pemrosesan data.
- Wajib ada persetujuan (consent) yang jelas dari subjek data jika data akan digunakan atau dibagikan ke pihak ketiga.

Isi Pokok UU PDP

Sanksi Administratif dan Pidana

- UU PDP memuat ketentuan denda administratif dan sanksi pidana bagi pelanggaran berat (seperti kebocoran data yang disengaja, penyalahgunaan data untuk penipuan, dsb.).
- Denda bisa mencapai persentase dari pendapatan tahunan (mirip konsep GDPR), meski implementasinya masih menunggu peraturan teknis.

Isi Pokok UU PDP

Lembaga Pengawas

- UU PDP mengamanatkan pembentukan lembaga pengawas independen yang bertanggung jawab memastikan kepatuhan pelaku usaha/pemerintah terhadap standar perlindungan data pribadi.
- Pada tahap awal, peran pengawasan sementara dipegang Kementerian Kominfo, menunggu pembentukan lembaga tersendiri.

Isi Pokok UU PDP

Transisi dan Peraturan Pelaksana

- Ada masa transisi (dua tahun sejak UU disahkan) bagi perusahaan dan instansi pemerintah untuk menyesuaikan sistem pengelolaan data mereka.
- Rincian teknis terkait tata cara pemberian sanksi, standar keamanan, dan mekanisme pelaporan pelanggaran diatur dalam peraturan pemerintah atau aturan turunan lain.

Next Week!

Hak Cipta

Paten

Merek

Rahasia Dagang

Pembajakan Software

Plagiarisme karya digital

Pelanggaran lisensi open source

Hak Kekayaan Intelektual & Etika Penggunaan Karya Digital

Materi Kuliah | Etika Profesi dan Hukum Teknologi Informasi

1. Hak Cipta (Copyright)

- Hak eksklusif atas karya seni, sastra, ilmu pengetahuan
- Berlaku otomatis sejak karya diciptakan
- Contoh: buku, musik, film, software
- Durasi: seumur hidup + 70 tahun
- Pelanggaran: duplikasi tanpa izin

2. Paten

- Hak eksklusif atas penemuan/invensi teknologi
- Syarat: Baru, Inventif, Dapat diterapkan
- Durasi: 20 tahun (paten biasa), 10 tahun (paten sederhana)
- Contoh: alat kesehatan, mesin, proses kimia

3. Merek (Trademark)

- Tanda pembeda barang/jasa: nama, logo, simbol
- Fungsi: identitas, reputasi, perlindungan konsumen
- Durasi: 10 tahun dan dapat diperpanjang
- Contoh: logo Nike, nama Tokopedia

4. Rahasia Dagang

- Informasi bernilai ekonomi yang dirahasiakan
- Contoh: resep Coca-Cola, strategi bisnis, algoritma
- Tidak dibatasi waktu selama dirahasiakan

5. Pembajakan Software

- Penggunaan software tanpa lisensi resmi
- Contoh: crack, serial number ilegal, share lisensi
- Dampak: ilegal, rawan malware, rugikan developer

6. Plagiarisme Karya Digital

- Mengaku karya digital orang lain sebagai milik sendiri
- Contoh: copy-paste artikel, unggah ulang video
- Pencegahan: kutipan, atribusi, lisensi CC

7. Pelanggaran Lisensi Open Source

- Tidak mematuhi ketentuan lisensi open source
- Contoh lisensi: GPL, MIT, Apache
- Pelanggaran: hapus atribusi, tidak buka kode saat diwajibkan

Macam-macam Lisensi

Lisensi Proprietary (Tertutup / Komersial)

Karakteristik

- Kode sumber (source code) tidak dibuka untuk umum. Pengguna hanya mendapatkan hak pakai (user license) tanpa hak untuk melihat atau memodifikasi kode sumbernya.
- Biasanya mengharuskan pengguna membeli lisensi resmi atau membayar biaya tertentu (subscription atau sekali bayar).
- Pemilik hak cipta menahan hampir semua hak. Pengguna terikat pada End User License Agreement (EULA) yang membatasi penggunaan, distribusi, dan modifikasi.
- Pembaruan, dukungan, dan fitur tambahan dapat diberikan selama masa berlangganan atau sesuai ketentuan.

Lisensi Proprietary (Tertutup / Komersial)

Contoh: Microsoft Windows (OS), Microsoft Office, Adobe Photoshop.

Ciri utama:

- Pengguna dilarang mengakses, mempelajari, apalagi mengubah dan mendistribusikan ulang kode sumber. Hak cipta sepenuhnya berada di pihak pengembang/penyedia.

Lisensi Open Source

Secara garis besar, lisensi *open source* membuka akses kode sumber dan mengizinkan orang lain untuk melihat, memodifikasi, serta mendistribusikannya dengan syarat tertentu.

Namun, di dalam open source, ada beberapa varian penting:

A. Lisensi Copyleft (Contoh: GPL, AGPL, LGPL)
   a. GNU General Public License (GPL)
   b. GNU Lesser General Public License (LGPL)
   c. GNU Affero General Public License (AGPL)

B. Lisensi Open Source “Permissive”
   a. MIT License
   b. BSD License (varian: 2-Clause, 3-Clause)
   c. Apache License 2.0

GNU General Public License (GPL)

- Mewajibkan setiap turunan/pengembangan (derivative work) juga dirilis di bawah lisensi yang sama (GPL).
- Pengguna boleh mengubah, memperbaiki, dan mendistribusikan ulang dengan syarat hasil modifikasi juga tetap terbuka kode sumbernya dan tetap GPL.
- Tujuannya adalah memastikan karya turunan tidak di-close source sehingga ekosistem kolaborasi terus terbuka.
- Ciri khas: Efek copyleft—karya turunan wajib dipublikasikan dengan lisensi yang sama.

GNU Lesser General Public License (LGPL)

- Mirip GPL, namun lebih longgar. Biasanya dipakai untuk pustaka (library).
- Program proprietary dapat menggunakan pustaka berlisensi LGPL tanpa mewajibkan seluruh program menjadi open source.
- Ciri khas: Fleksibel untuk integrasi dengan perangkat lunak lain, tetapi file pustakanya sendiri tetap wajib terbuka.

GNU Affero General Public License (AGPL)

- Serupa GPL, tetapi menambahkan ketentuan bahwa jika perangkat lunak dijalankan sebagai layanan jaringan (misalnya web service), kode sumbernya juga harus dibagikan kepada pengguna layanan.
- Ciri khas: Mencegah “mengunci” modifikasi pada server. Pengguna (klien) tetap berhak memperoleh versi modifikasinya.

MIT License

- Sangat sederhana dan permisif: hanya mewajibkan mencantumkan copyright serta isi lisensi MIT dalam distribusi ulang.
- Tidak memaksa proyek turunan untuk ikut open source. Boleh dicampur dengan komponen proprietari.
- Ciri khas: Fleksibilitas tinggi—dikenal sebagai lisensi “pribadi favorit” banyak developer karena aturannya sangat ringan.

BSD License
(varian: 2-Clause, 3-Clause)

- Hampir sama permisifnya dengan MIT.
- Memiliki beberapa klausa seperti advertising clause (pada BSD 4-Clause lama) yang sekarang jarang digunakan.
- Ciri khas: Mengizinkan hampir segala penggunaan, hanya mewajibkan mencantumkan pernyataan hak cipta serta disclaimer

Apache License 2.0

- Mirip MIT/BSD dari sisi permisif, tetapi memiliki ketentuan paten yang lebih eksplisit.
- Menjamin pengguna tidak akan dituntut pelanggaran paten oleh kontributor utama.
- Ciri khas: Terdapat perlindungan paten bagi pengguna dan ketentuan mengenai penggunaan merek dagang.

Ringkasan *Open Source*

Copyleft (GPL/AGPL/LGPL) → mewajibkan karya turunan tetap open source.

Permissive (MIT/BSD/Apache) → sangat longgar, membolehkan karya turunan menjadi proprietary.

Lisensi Creative Common

Lisensi Creative Commons (CC)

Lisensi Creative Commons sering ditemui pada karya non-perangkat lunak seperti teks, foto, video, musik, infografis, dan sejenisnya.

1. CC-BY (Atribusi):
   - Bebas digunakan, disalin, diadaptasi, bahkan dikomersialisasi asalkan memberikan kredit (atribusi) kepada pencipta aslinya.
   - Ciri khas: Syarat utama hanya mencantumkan nama kreator/sumber aslinya.
2. CC-BY-SA (Atribusi - ShareAlike):
   - Bebas digunakan dan diadaptasi dengan wajib memberikan atribusi, serta karya turunan wajib didistribusikan dengan
   - lisensi yang sama (ShareAlike).
   - Ciri khas: Mirip copyleft. Jika memodifikasi karya CC-BY-SA, kita harus menyebarkannya di bawah CC-BY-SA juga.

Lisensi Creative Commons (CC)

3. CC-BY-NC (Atribusi - NonCommercial):
   - Pengguna boleh memakai dan mengadaptasi karya asalkan tidak untuk tujuan komersial (non-komersial).
   - Tetap wajib atribusi. Jika ingin memanfaatkan secara komersial, harus izin khusus.
   - Ciri khas: Pembatasan pada penggunaan komersial.
4. CC-BY-ND (Atribusi - NoDerivatives):
   - Boleh didistribusikan dan digunakan untuk apa saja, termasuk komersial, tetapi tidak boleh diubah atau dimodifikasi.
   - Ciri khas: Dilarang membuat karya turunan (NoDerivatives).

Lisensi Creative Commons (CC)

5. CC-BY-NC-SA, CC-BY-NC-ND:
   - Kombinasi dari ketentuan Non-Commercial dan ShareAlike atau Non-Commercial dan No-Derivatives.
   - Contoh: CC-BY-NC-SA = boleh pakai, wajib atribusi, tidak boleh komersial, dan harus ShareAlike.
6. CC0 (Public Domain Dedication):
   - Penulis melepas hak ciptanya sejauh diizinkan hukum, menjadikan karyanya “public domain”.
   - Ciri khas: Tidak ada batasan, siapapun dapat memodifikasi atau mengkomersialkan tanpa wajib atribusi (murni bebas).

Public Domain

Cakupan: Karya yang masa perlindungan hak ciptanya sudah habis (misalnya karya sangat lama, umumnya 70 tahun setelah kematian pencipta, tergantung undang-undang negara).

Ciri khas:

- Karya tersebut dapat digunakan oleh siapa saja, untuk tujuan apa saja, tanpa meminta izin.
- Tidak ada kewajiban mencantumkan atribusi, meski secara moral/etika banyak yang tetap mencantumkan sumbernya.

Pelanggaran

Pelanggaran Kekayaan Intelektual

- plagiarisme (jiplak karya tulis, karya digital, atau bukan karya sendiri tapi diakui sebagai hasil sendiri)
- Software bajakan
- Penggunaan materi tanpa izin (foto copy buku tanpa izin)
- Pelanggaran Merek Paten (nama mirip)

Pelanggaran Lisensi *Open source*

Open source ≠ bebas pakai seutuhnya tanpa aturan

- lisensi *open source* biasanya mewajibkan hal-hal seperti pencantuman kredit pada pembuat asli, atau pembukaan kembali kode jika kita memodifikasi dan mendistribusikan program (terutama untuk lisensi copyleft seperti GPL)

Kenapa Melanggar?

- Kurangnya Pengetahuan dan Edukasi
- Budaya Menyepelekan Pelanggaran
- Motivasi Ekonomi dan Keterjangkauan
- Tekanan Akademik dan Kemalasan
- Lemahnya Penegakan Hukum dan Aturan

Catatan Kasus terkait Kekayaan Intelektual

- **Plagiarisme Skripsi**: Kasus mahasiswi UMP Palembang yang menjiplak skripsi alumni Unsri mencuat tahun 2024. Korban (alumni Unsri) mengetahui skripsinya dijiplak setelah melihat dokumen pelaku, kemudian mengadukannya lewat media sosial. Hasil investigasi kampus menyimpulkan terjadi plagiarisme 100%, karena skripsi pelaku identik dengan milik korban (hanya ganti nama).

- **Plagiarisme Tugas Kuliah**: Kasus Safrina di Unair (2024) merupakan contoh plagiarisme tugas antar mahasiswa. Safrina menyalin tugas temannya (Putri) kata demi kata hanya mengganti nama. Korban mengungkap hal ini di Twitter hingga viral. Safrina telah meminta maaf dan berdamai dengan korban, namun nama baiknya tercemar.

Catatan Kasus terkait Kekayaan Intelektual

- **Plagiarisme Karya Digital:** Kasus Rico di Unnes (2022) menyoroti plagiasi di luar tugas akademik formal. Rico, yang juga kreator konten, mengambil karya ilustrator lain lalu memposting seolah karyanya sendiri (bahkan menambahkan video proses seakan-akan ia yang membuat)

- **Pembajakan Buku:** Sesekali aparat melakukan razia fotokopi ilegal di sekitar kampus. Sebagai contoh hipotetis, di tahun-tahun awal implementasi UU Hak Cipta 2014, beberapa copy center di kota pelajar pernah diperingatkan karena menggandakan buku teks secara massal tanpa izin penerbit. Penerbit dan penulis buku akademik sering mengeluhkan penjualan rendah karena mahasiswa lebih memilih kopi bajakan.

Statistik

- **Tingkat Pembajakan Software**: Menurut survei BSA (*Business Software Alliance*), 83% software di Indonesia pada 2017 tidak berlisensi resmi (bajakan)

- **Statistik Plagiarisme Akademik**: Sebuah survei internal dengan Turnitin di Universitas Tarumanagara tahun 2020 menemukan banyak tugas mahasiswa memiliki *similarity index* tinggi antara 30-83%.

Budaya “***Copy-Paste***”: Survei informal menunjukkan banyak mahasiswa mengaku minimal sekali dua kali melakukan copy-paste dari internet tanpa menyebut sumber.

Ketika dosen menilai tugas bisa menemukan pola jawaban tugas yang identik antar mahasiswa (>50% isi sama), menandakan kolaborasi ilegal atau saling menyalin.

Penutup

- Hargai Hak Kekayaan Intelektual
- Gunakan software & konten digital secara legal
- Jadilah profesional yang beretika dan bertanggung jawab

Keamanan Etika Siber

Etika Profesi

Tujuan

- Memahami fondasi keamanan informasi
- Menilai isu etika di dunia siber
- Menunjukkan sikap profesionalisme

Fondasi Keamanan

Pilar CIA

- Confidentiality (Kerahasiaan)
  - Hanya pihak berwenang yang boleh melihat data
  - Enkripsi disk/database - Access-control list & MFA (Multi Factor Authentication)
- Integrity (Integritas)
  - Data harus tetap benar, lengkap, dan tidak diubah tanpa izin.
  - Hash + digital signature - Versioning, checksum, audit-log
- Availability (Ketersediaan)
  - Data/layanan dapat diakses saat dibutuhkan.
  - Redundansi, load-balancer - Backup & disaster-recovery plan

Parkerian Hexad

Don Parker (1998) menilai CIA terlalu sempit, lalu menambah tiga dimensi sehingga total menjadi enam:

- Possession/Control
  - Siapa yang memegang atau mengendalikan aset?
  - Flashdisk karyawan hilang → data tidak bocor (masih terenkripsi) tetapi organisasi kehilangan kendali fisik.
- Authenticity
  - Jaminan bahwa entitas/data memang asli dan dapat dipercaya.
  - Deep-fake video → merusak keaslian bukti; sertifikat TLS palsu.
- Utility
  - Apakah data masih berguna bagi pemilik sahnya?
  - Ransomware mengenkripsi file: data tetap ada & rahasia, tapi tidak bisa dipakai ⇒ hilang utilitas.

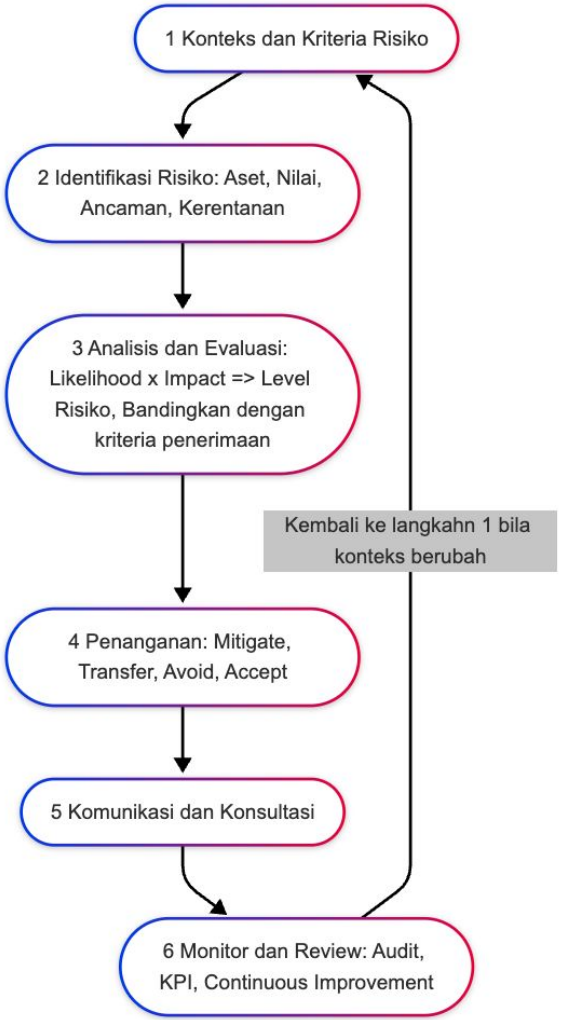
Menganalisa Serangan Ransomware

Aspek	**Terdampak**	**Alasan**
Confidentiality	Ya (sering)	Pelaku memfilter data sebelum enkripsi
Integrity	Ya	File diubah
Availability	Ya	Sistem tidak bisa diakses
Possession	Ya	Penyerang memegang salinan data
Authenticity	Kadang	File ransom menimpa file asli, meta data diubah
Utility	Ya	Data tidak dapat digunakan sampai tembusan dibayar

Siklus Manajemen Risiko (ISO/IEC 27005)

ISO 27005 : 2022 menyediakan kerangka sistematis untuk =

mengidentifikasi → menganalisis → menangani → memantau risiko keamanan informasi.



Threat Modeling

Langkah Umum	Penjelasan Ringkas	Tools/Metodologi Populer
1. Scope & Asset Mapping	data-flow-diagram, arsitektur cloud.	MS Threat Modeling Tool, draw.io
2. Identifikasi Ancaman	Gunakan taksonomi seperti STRIDE (Spoofing, Tampering, Repudiation, Information-disclosure, Denial-of-service, Elevation-of-privilege) atau LINDDUN (untuk privasi)	STRIDE, PASTA, LINDDUN
3. Pemetaan Kerentanan	Library CVE, OWASP Top 10, mis-config cloud, logic flaw.	OWASP ZAP, ScoutSuite
4. Penilaian Risiko Tiap Ancaman	Likelihood x Impact → High / Med / Low.	Risk matrix 5x5
5. Mitigasi & Validasi	Tambah kontrol desain (enkripsi, rate-limit, input-validation) dan rencanakan test (pentest/scan).	IaC security rules, unit-test, pentest
6. Dokumentasi / Re-model	Simpan temuan ke backlog DevSecOps; perbarui tiap iterasi.	Jira, GitLab issues

Layered Defence (defence-in-depth)

1. People / Policy Layer → SOP, pelatihan phishing, NDA.
2. Physical Layer → IDC tier-III, CCTV, kartu RFID.
3. Perimeter / Network → Firewall NGFW, IDS/IPS, segmentation VLAN, WAF.
4. Endpoint / Host → Hardening OS, EDR, patch-management.
5. Application → Secure-coding, input-validation, token-based auth.
6. Data → Column-level encryption, tokenisation, backup immutabel.
7. Monitoring & Response → SIEM, SOAR, playbook IR, backup off-site.

Kategori Kontrol (ISO 27001 – Annex A & NIST)

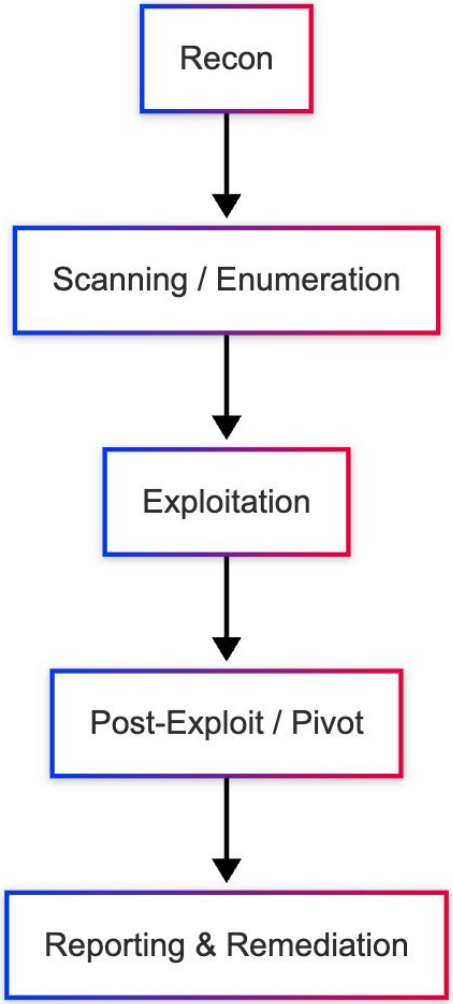
Kategori	Tujuan	Contoh Kontrol
Preventive	Mencegah kejadian	MFA, least-privilege (RBAC), patch, disable USB, secure coding, network segmentation
Detective	Menemukan kejadian dengan cepat	IDS/IPS, SIEM alert, file-integrity-monitoring, audit-log review, honeypot
Corrective	Memulihkan & memperbaiki	Restore backup, re-image server, revoke token, apply patch darurat
Deterrent	Mengurangi niat penyerang	Banner hukum (“access logged”), denda kebijakan, CCTV terlihat
Compensating	Alternatif ketika kontrol utama tak bisa dipasang	Enkripsi file saat disk-encryption belum tersedia; VPN site-to-site mengganti MPLS terenkripsi
Recovery	Menyambung operasional	DR site failover, cold-standby server, kontrak cyber-insurance
Directive	Mengarahkan perilaku	Kebijakan, prosedur, SLA keamanan vendor, framework DevSecOps

Hacking & Etika

Definisi & Klasifikasi

Jenis Hacker	Deskripsi	Contoh Aksi
White Hat	Pen-testing tersertifikasi; kontrak; laporan kerentanan	Red-Team audit bank, Bug-Bounty Program
Gray Hat	Tanpa izin penuh - namun berniat melapor/tanpa eksploitasi finansial	Menemukan mis-config S3 publik lalu email admin
Black Hat	Eksploitasi untuk keuntungan/sabotasé	Ransomware gang, carding

Siklus Penetration Test



Responsible Disclosure Workflow

1. Discover kerentanan.
2. Privately report ke vendor/owner (sertakan PoC terbatas).
3. Koordinasi perbaikan (grace-period 30-90 hari).
4. Public disclose setelah patch or deadline → edukasi ekosistem.

Standar: ISO/IEC 29147, RFC 9116

Etis: Menjaga kerahasiaan data, minimal exposure

Etika & Kerangka Hukum

Sudut Etik	Penerapan
ACM/IEEE	Integritas & perlindungan publik → wajib izin eksploitasi
Deontologi	Hacking tanpa consent = memperalat orang sebagai “sekadar sarana”
Utilitarian	Bug-bounty terkoordinasi memberi manfaat kolektif > risiko terbatas

Studi Kasus Singkat

Kasus	Dilema	Pelajaran Etis
Heartbleed 2014	Tim penemu menunda publikasi 2 minggu ✚ vendor patch	Disclosure terkoordinasi >> “full-disclosure” instan
Tokopedia Breach 2020	Data 91 juta akun dijual - vendor lambat notifikasi	Pentingnya IR Plan & UU PDP notifikasi 72 jam

Cyber Crime & Regulasi

Tipologi Cybercrime (ITU Classification)

1. Offences against confidentiality, integrity, availability – akses ilegal, malware, DDoS.
2. Computer-related offences – pemalsuan, penipuan e-commerce, carding.
3. Content offences – pornografi anak, hate-speech.
4. Offences against copyright/IP – pelanggaran lisensi software, DHT P2P.

Regulasi Utama Indonesia

Instrumen	Titik Kunci	Sanksi
UU ITE 11/2008 & *Amend.* 19/2016	Pasal 30 (akses ilegal), 32 (intersepsi/manip data), 27(3) pencemaran nama	Penjara ≤ 12 thn &/atau denda ≤ Rp 12 m
UU PDP 27/2022	Hak subjek data, kewajiban notifikasi ≤ 72 jam, denda admin ≤ 2 % pendapatan, pidana kebocoran disengaja	Denda Rp 6 m — Rp 60 m + pidana
PP 71/2019 (PSTE)	Klasifikasi data strategis/kritis; kewajiban penempatan DC	Teguran → denda → blokir
SKB 3 Menteri 2021	Pedoman delik pencemaran nama (restorative justice)	—

Lembaga Penegak: BSSN (proteksi & early-warning), **Siber POLRI** (Dittipidsiber), **Kominfo** (sanksi adm./blokir), **OJK & BI** (sektor keuangan).

Kerja Sama & Norma Global

- Budapest Convention (Council of Europe) – Indonesia observer; panduan harmonisasi pasal & bantuan hukum lintas-negara.
- ASEAN CERT-to-CERT & Interpol ASEAN Desk – koordinasi insiden.
- ISO 27001/27701, PCI-DSS, NIST CSF – kerangka best-practice compliance.

Kontroversi & Tantangan

Isu	Penjelasan
Pasal 27(3) UU ITE	“Pencemaran nama baik” → frasa luas (*pasal karet*), rawan kriminalisasi kritik.
Pengecualian Instansi Publik (UU PDP)	Pemerintah bisa memproses data demi “keamanan nasional” → perlu kontrol kuat agar tak disalahgunakan.
Penegakan Lemah	Banyak kebocoran data besar (SIM card, e-health) tak kunjung ada sanksi tegas - menimbulkan “impunitas”.

Implementasi & Best Practice

1. Governance – tetapkan Data Protection Officer, kebijakan IR & privacy-by-design.
2. Compliance – mapping aset → DPIA (Data-Protection-Impact-Assessment).
3. Technical Controls – hardening, micro-segmentation, EDR, Zero-Trust.
4. Awareness – program pelatihan phishing simulation + kebijakan BYOD.
5. Incident Handling – ikuti NIST IR Lifecycle (Prepare→Identify→Contain→Eradicate→Recover→Lessons Learnt).

Tugas: 9 kelompok (@ 5 - 6 orang)

#	Kategori / Kasus	Contoh Insiden & Tahun	Keterangan Ringkas (mengapa relevan)
1	**Data Breach Besar**	Tokopedia 2020, BPJS 2021	Memetakan rantai kebocoran, notifikasi UU PDP, dampak reputasi & finansial.
2	**Ransomware Layanan Kritis**	WannaCry 2017, RSUD Indonesia 2023	Analisis CIA & Parkerian Hexad; etika membayar tebusan vs keselamatan publik.
3	**Industrial / OT Attack**	Stuxnet 2010, Colonial Pipeline 2021	Menunjukkan risiko siber pada infrastruktur fisik & implikasi keamanan nasional.
4	**Bug-Bounty & Ethical Hacking**	Heartbleed 2014, Gojek Bug 2019	Menyorot *responsible disclosure*, peran white-hat, dan dilema publikasi.
5	**Privasi & Media Sosial**	Cambridge Analytica 2018, FaceApp issue 2019	Mengkaji eksploitasi data profil, micro-targeting politik, hak privasi pengguna.
6	**Disinformasi / Deepfake**	Video deepfake Zelensky 2022, Hoaks Pemilu 2019	Hubungan antara kebebasan berekspresi, etika media, dan ancaman demokrasi.
7	**Cryptocurrency & DeFi Hack**	Ronin Bridge (Axie) 2022, FTX leak 2023	Keamanan smart-contract, pencucian uang kripto, regulasi aset digital.
8	**Critical DDoS & CDN Failure**	AWS “275 Gbps” attack 2020, Fastly outage 2021	Dampak availability global, strategi mitigasi multi-CDN & ethical hosting.
9	**Insider Threat / Malicious Insider**	Edward Snowden 2013, Tesla engineer leak 2020	Menilai kebijakan least-privilege, zero-trust, dan dilema whistleblowing.

Deliverable & Format Tugas

Berkas	Isi ringkas	Format
A. Report (6-8 hal)	• Deskripsi singkat insiden • **Timeline terperinci** (T-0 sampai mitigation) • Analisis CIA + Parkerian • Threat-model STRIDE & root-cause • Pemetaan regulasi (UU ITE, UU PDP, GDPR, dll.) • Analisis etika ≥ 2 teori • Rekomendasi kontrol prevent-detect-correct	PDF
B. Infografis Timeline	Visual alur peristiwa & aktor	PNG/Canva ≤ 2 MB
C. Video/PPT Peer-Teaching	10 menit / total slide	MP4 / PPTX
D. Refleksi Individu	“pelajaran personal & relevansi bagi karier”	PDF

Rubrik Penilaian

Komponen	Bobot
Akurasi fakta & keutuhan timeline	20
Analisis risiko (ISO 27005) & threat-model	20
Analisis etika multidimensi	20
Kedalaman referensi & sitasi	15
Kreativitas / kejelasan infografis & presentasi	15
Refleksi individu	5
Kedisiplinan (ketepatan waktu, format)	5

Tanggung Jawab Sosial & Keberlanjutan Teknologi

Etika Profesi

Tujuan

- Menjelaskan dampak sosial (positif–negatif) penerapan TI: kesenjangan digital, inklusi, disrupsi kerja.
- Menganalisis isu keberlanjutan: jejak karbon pusat data, e-waste, green-software.
- Merumuskan strategi etis—people, planet, profit—dalam siklus hidup proyek TI.

Outcome Pembelajaran

- Memetakan dampak sosial & lingkungan suatu sistem TI
- Menggunakan kerangka triple bottom line untuk menilai studi kasus TI.
- Menyusun rencana mini “Green-IT Initiative” di lingkungan kampus/komunitas.

Why Care?

- Jejak emisi sektor ICT
  - Sektor ICT kini menyumbang ~2 % dari seluruh emisi GRK—setara industri penerbangan—dan bisa naik jika pertumbuhan data-center & AI tak diimbangi energi terbarukan.
  - https://documents1.worldbank.org/curated/en/099121223165540890/pdf/P17859702a98880540a4b70d57876048abb.pdf
- E-waste global
  - Dunia menghasilkan 62 Mt e-waste (2022); hanya 22 % yang didaur-ulang secara resmi. Tanpa intervensi, timbulan akan mencapai 82 Mt (2030), memperparah limbah toksik & hilangnya sumber daya kritis.
  - https://ewastemonitor.info/the-global-e-waste-monitor-2024/

Definisi Tanggung Jawab Sosial TI

- CSR (Corporate Social Responsibility)
  - Komitmen sukarela organisasi untuk beroperasi secara etis, berkelanjutan, dan memberi nilai bagi masyarakat.
- CDR (Corporate Digital Responsibility)
  - Turunan CSR yang berfokus pada pemanfaatan data dan teknologi digital secara bertanggung jawab—privasi, keberlanjutan, keadilan algoritmik, literasi digital publik.
- Triple Bottom Line (TBL)
  - Kerangka evaluasi kinerja organisasi berdasarkan People, Planet, Profit.

Prinsip Kunci CSR-IT

1. **Etika & Transparansi** – kode etik developer, disclosure algoritma, open-source governance.
2. **Inklusi & Akses** – menutup “digital divide”, desain aksesibilitas, bahasa lokal.
3. **Perlindungan Data** – privacy-by-design, keamanan siber, kepatuhan UU ITE & UU PDP.
4. **Keberlanjutan** – green-IT (virtualisasi, pendingin efisien, energi terbarukan), program daur-ulang e-waste.
5. **Keadilan Algoritmik** – audit bias, fairness metrics, human-in-the-loop.
6. **Pemberdayaan Komunitas** – literasi digital, pelatihan coding, dukungan start-up sosial.

Contoh CSR-IT

Perusahaan	Inisiatif	Dampak
Microsoft	*AI for Accessibility* Grant	300+ solusi inklusif (speech-to-text, navigasi tunanetra).
Google	Operasi 24/7 data-center **carbon-free** (target 2030)	Emisi listrik Scope-2 turun 66 % di 2022.
Gojek	Program **#GoGreener** – “carbon footprint calculator” & offset ride	>20 jt kg CO_2 offset; edukasi publik karbon.
Telkom Indonesia	*Indonesia NEXT* – bootcamp digital skill mahasiswa	50 000+ peserta, sertifikasi cloud & data-science.

Triple Bottom Line (TBL)

Dimensi	Fokus di dunia TI	Contoh indikator
People	Inklusi digital, kesejahteraan karyawan & pengguna, privasi	% desa tersambung internet, tingkat aksesibilitas aplikasi, pelatihan reskilling
Planet	Emisi karbon, konsumsi listrik DC & AI, e-waste	PUE data-center, ton e-waste didaur-ulang, rasio energi terbarukan
Profit	Nilai ekonomi & inovasi berkelanjutan	ROI proyek green-IT, efisiensi biaya listrik, reputasi pasar

Dampak Positif TI

Sisi Positif	Penjelasan	Ilustrasi
Akses informasi & pembelajaran	MOOCs, e-learning, tele-health	UN SDG4 – peningkatan literasi
Efisiensi & inovasi ekonomi	Otomasi logistik, fintech UMKM	Studi WB: produktivitas SMB naik >15 %
Pengurangan jejak fisik	E-signature, rapat daring → kurangi perjalanan	1 jam meeting online ≈ hemat 12 kg CO_2 (Nature, 2023)

Dampak Negatif TI

Sisi Negatif	Penjelasan	Ilustrasi
Kesenjangan keterjangkauan	Akses internet, perangkat mahal	2,6 miliar orang masih offline (ITU, 2023)
Dampak pekerjaan	Otomasi → reskilling paksa	Contoh: kasir ↦ self-checkout
Emisi & limbah	62 Mt e-waste (2022) ; 1,5–4 % emisi global dari ICT	

Kesenjangan Digital

1. **Access gap** – sinyal/broadband.
2. **Affordability gap** – harga perangkat/data.
3. **Skill gap** – literasi digital.
4. **Usage gap** – konten relevan bahasa lokal.

Green Computing Concepts

Bidang	Praktik
Perangkat & Arsitektur	ARM-based server hemat 30 % energi; sleep-mode agresif pada edge-device
Perangkat Lunak	“Carbon-aware scheduling” (Azure, 2023) memindah kerja batch ke jam surplus energi surya
Virtualisasi & Container	Konsolidasi VM → turunkan footprint fisik DC
Energi Terbarukan	Power-Purchase Agreement (PPA) untuk 24 × 7 CFE (Google target 2030)

Jejak Karbon Cloud & AI

- ICT menyumbang ± 1,5 – 4 % emisi GRK global (World Bank 2023).
- Latihan GPT-3 ≈ 550 t CO_2e (Wired 2023).
- Data-center & jaringan = 62 % konsumsi listrik sektor ICT.

Tantangan e-Waste

Fakta (Global E-waste Monitor 2024)	Dampak
62 juta ton e-waste dihasilkan 2022 (naik 2,6 Mt/tahun)	22 % saja yang didaur ulang resmi; kerugian SDA ≈ US$ 62 milyar
Proyeksi **82 Mt pada 2030**	Risiko toksik (Pb, Hg) & hilang logam tanah-langka

Solusi: desain modular, skema take-back, right-to-repair, ekonomi sirkular komponen.

Kerangka & Standar Terkait

Standar / Kerangka	Pokok Pengaturan
ISO 26000	Pedoman CSR – inklusi, konsumen, lingkungan
GRI 418 / 419	Laporan dampak privasi & kepatuhan sosial
SASB – Software & IT Services	Metrik emisi, kebocoran data, energi DC
ISO 14001	Sistem manajemen lingkungan (EMS)
ITU-T L.1470	Jalur penurunan emisi GHG sektor ICT 1.5 °C
Science Based Targets initiative (SBTi-ICT)	Target emisi terverifikasi untuk operator & vendor
SDG 4, 9, 12, 13	Pendidikan, inovasi, konsumsi-produksi bertanggung jawab, aksi iklim

Studi Kasus

Google 24/7 Carbon-Free Energy (CFE) Goal – Road to 2030

https://sustainability.google/reports/247-carbon-free-energy/

Target & Definisi

- Net-zero scope 1-3 2030
- Operasi 24 jam × 365 hari hanya dari energi karbon-free di setiap grid
- CFE Score = porsi listrik bebas-karbon per jam
- CFE Score adalah Persentase jam dalam setahun di mana beban listrik suatu situs dipenuhi oleh sumber listrik bebas karbon. Skor 100 % = 24 × 365 jam terpakai = carbon-free.

Pilar Strategi Google

1. Procurement PPA RE baru (≈ 4 GW dibubuhi kontrak 2024)
2. Grid-level innovation - geothermal, green-hydrogen peaker
3. Advanced Nuclear - SMR (Small Modular Reactor) deal w/ Kairos Power (500 MW)
4. Hourly Matching AI - memindahkan beban ke jam surplus RE

PPA (Power Purchase Agreement) = Kontrak jangka panjang untuk membeli listrik (dan/atau sertifikat energi terbarukan) langsung dari pengembang pembangkit—contoh: PPA angin 200 MW di Texas.

Tambahan “RE” (Renewable Energi) menegaskan listrik yang dibeli bersumber 100 % bebas emisi.

Kemajuan Global

- 64 % CFE rata-rata kantor + DC (2022-2023)
- 7 tahun berturut-turut 100 % “annual RE matching”
- 20 data-center sudah ≥ 90 % CFE per jam

Dampak & Co-benefit

- Menurunkan PUE DC global ke 1.10 (2023)
- Transfer best-practice: open-source Hourly CFE Score API
- Memacu pasar PPA +4 GW (2024)

PUE (Power Usage Effectiveness) adalah Rasio total energi fasilitas ÷ energi IT. Semakin dekat 1.0 → semakin efisien; pusat data Google rata-rata ≈ 1,10 (2023).

Dampak CSR Google

- emisi Scope 2 listrik turun 66 % (vs 2019)
- 1,5 miliar perangkat mendapat peringatan phishing via Safe Browsing
- dan 100 % perangkat **Nest** baru diproduksi dengan plastik daur ulang.

Nest = produk smart home buatan google.

Privasi, Big Data & Bias Algoritmik

Etika Profesi

Tujuan

1. Memahami prinsip dasar privasi data dan konsep privacy-by-design dalam siklus Big Data & AI.
2. Mengidentifikasi sumber bias algoritmik serta metrik fairness yang lazim digunakan.
3. Merancang mitigasi teknis-organisasional agar sistem Big Data/ML tetap etis dan patuh regulasi.

Outcome

1. Menjelaskan 7 prinsip inti privacy-by-design dan menerapkannya pada skenario pengumpulan data kampus.
2. Menggambarkan alur Big-Data Pipeline (Ingest→Store→Process→Serve→Retire) serta titik-titik risiko privasi.
3. Mengklasifikasi 4 jenis bias (sampling, measurement, historical, aggregation) pada contoh dataset nyata.
4. Menghitung dan menafsirkan satu metrik fairness (mis. Demographic Parity atau Equalized Odds).
5. Merumuskan checklist mitigasi: DPIA, differential privacy, explainability report, dan kebijakan UU PDP.

Mengapa Peduli Privasi?

- GDPR (General Data Protection Regulation) adalah regulasi privasi Uni Eropa yang memberikan kewenangan pada regulator untuk menjatuhkan denda sangat besar (hingga 4% dari omset global tahunan) kepada perusahaan yang melanggar. Denda terbesar seringkali diberikan kepada perusahaan teknologi besar atas pelanggaran seperti transfer data ilegal, kurangnya dasar hukum pemrosesan, atau kegagalan melindungi data pengguna.
- **Kepercayaan adalah Aset Paling Berharga**. Kehilangan kepercayaan pengguna dapat menghancurkan reputasi bisnis.

Mengapa Peduli Privasi?

Risiko Kebocoran Data:

- Lebih dari 5 miliar data pribadi dilaporkan bocor secara global pada tahun 2023 saja.
- Di Indonesia, insiden kebocoran data telah menimpa berbagai sektor: e-commerce, pemerintahan, telekomunikasi, dan finansial.

Konsekuensi Finansial yang Sangat Besar:

- Regulasi seperti GDPR memberikan denda yang sangat signifikan
- Meta (Irlandia): €1.2 Miliar (Mei 2023) atas transfer data ilegal ke AS.
- TikTok (Irlandia): €345 Juta (September 2023) atas pelanggaran terkait data anak.

Data Pribadi (UU PDP)

Menurut UU No. 27 Tahun 2022 (UU PDP), Data Pribadi adalah "**setiap data tentang orang perseorangan yang teridentifikasi dan/atau dapat diidentifikasi**."

- Data Pribadi Bersifat Umum (Identifiable)

  Nama lengkap, jenis kelamin, kewarganegaraan,agama, status perkawinan, data yang dikombinasikan untuk mengidentifikasi seseorang (misal: alamat + tanggal lahir).

- Data Pribadi Bersifat Spesifik (Sensitive)

  Data Kesehatan, data Biometrik & Genetika (sidik jari, wajah, DNA), data keuangan pribadi, pandangan politik, catatan kejahatan, data anak, dll., memerlukan perlindungan lebih ketat dan dasar hukum yang lebih kuat untuk diproses.

Privacy by Design (PbD 7)

Privacy by Design (PbD) adalah pendekatan proaktif, bukan reaktif.
Privasi harus menjadi setelan bawaan (default setting).

1. **Proaktif, bukan Reaktif**: Antisipasi risiko privasi sebelum terjadi.
2. **Privasi sebagai Pengaturan Default**: Pengguna tidak perlu melakukan apa pun untuk terlindungi; perlindungan maksimal adalah standar.
3. **Privasi Tertanam dalam Desain**: Privasi adalah komponen inti dari sistem, bukan tambahan.
4. **Fungsionalitas Penuh (Positive-Sum)**: Ciptakan solusi "win-win" yang memenuhi tujuan bisnis dan privasi, bukan mengorbankan satu sama lain.
5. **Keamanan End-to-End**: Perlindungan data sepanjang siklus hidupnya (pengumpulan, penggunaan, pemusnahan).
6. **Visibilitas dan Transparansi**: Jaga agar proses dan kebijakan tetap terbuka, jelas, dan dapat diverifikasi.
7. **Hormati Privasi Pengguna**: Utamakan kepentingan dan hak-hak individu.

Pipeline Big Data

Perjalanan Data: Dari Sumber Mentah ke Keputusan Cerdas

Bagaimana data diolah dalam ekosistem Big Data untuk menghasilkan wawasan atau melatih model AI?

Pipeline Big Data

ETL (Extract, Transform, Load)

- Extract: Mengambil data mentah dari berbagai sumber (aplikasi, sensor, database).
- Transform: Membersihkan, menstandarkan, dan mengubah data ke format yang dapat digunakan.
- Load: Memuat data yang telah diubah ke dalam sistem penyimpanan.

Machine Learning (ML)

- Data yang bersih dari Warehouse digunakan untuk melatih algoritma guna membuat prediksi, klasifikasi, atau rekomendasi.

Pipeline Big Data

Data Lake

- Penyimpanan data mentah dalam skala masif.
- Fleksibel, hemat biaya, tetapi berisiko menjadi "rawa data" (data swamp).

Data Warehouse

- Penyimpanan data terstruktur, terfilter, dan terorganisir.
- Dioptimalkan untuk analisis dan pelaporan bisnis yang cepat.

Risiko Re-identifikasi

Re-identifikasi adalah proses mengambil data yang telah dibuat "anonim" dan melacaknya kembali untuk mengidentifikasi individu spesifik yang menjadi sumber data tersebut. Sehingga kemungkinan data anonim dapat dikaitkan kembali dengan individu tertentu.

- **Netflix Prize**: Kompetisi 2006-2009 di mana Netflix merilis data anonim pengguna, tetapi peneliti berhasil mengidentifikasi individu dengan menggabungkan data tersebut dengan sumber eksternal.
- **Strava Heatmap**: Aplikasi Strava merilis peta aktivitas pengguna (heatmap) pada 2017, yang secara tidak sengaja mengungkap lokasi pangkalan militer rahasia karena pola aktivitas personel.

Regulasi Global - GDPR, UU PDP, CPRA

Aturan Main Global dalam Perlindungan Data

- **GDPR (*General Data Protection Regulation*)**: Regulasi privasi Uni Eropa yang berlaku sejak 2018, fokus pada perlindungan data warga UE dengan denda ketat.
- **UU PDP**: Undang-Undang Perlindungan Data Pribadi Indonesia (berlaku efektif Oktober 2024), mengatur pengelolaan data pribadi dengan sanksi denda hingga Rp60 miliar.
- **CPRA (*California Privacy Rights Act*)**: Perluasan dari CCPA di California, memberikan hak lebih besar kepada konsumen untuk mengontrol data mereka, seperti menolak penjualan data.

Regulasi Global - GDPR, UU PDP, CPRA

Aspek	GDPR (Uni Eropa)	UU PDP (Indonesia)	CPRA (California, AS)
Fokus Utama	Hak Individu (Subjek Data) & Kewajiban Pengendali Data	Hak Subjek Data & Kewajiban Pengendali/Prosesor Data	Hak Konsumen & Transparansi
Hak Kunci	Hak untuk dihapus, diakses, portabilitas data, menolak pemrosesan.	Sangat mirip dengan GDPR (hak untuk dihapus, diperbarui, akses, dll).	Hak untuk mengetahui, menghapus, dan menolak penjualan/pembagian data (opt-out).
Sanksi	Denda hingga €20 juta atau 4% dari omset global tahunan.	Sanksi administratif (termasuk denda hingga 2% dari pendapatan tahunan), dan sanksi pidana.	Denda per pelanggaran, lebih tinggi untuk pelanggaran yang melibatkan anak di bawah umur.
Ciri Khas	Standar global, kewajiban DPIA, peran Data Protection Officer (DPO).	Terinspirasi GDPR, pembentukan lembaga pengawas, berlaku untuk semua sektor.	Fokus pada "penjualan" dan "pembagian" data, memberikan hak opt-out.

Regulasi Global - GDPR, UU PDP, CPRA

- **GDPR** adalah regulasi paling komprehensif dan ketat, menjadi acuan global.
- **UU PDP** mengadopsi banyak elemen GDPR, namun disesuaikan dengan konteks Indonesia, termasuk sanksi pidana.
- **CPRA** lebih spesifik pada hak konsumen di California, dengan penekanan pada penjualan data dan perlindungan anak.

	GDPR	UU PDP	CPRA
Wilayah	Eropa	Indonesia	California, AS
Denda maksimal	4% pendapatan tahunan	Rp60 miliar	$7.500 per pelanggan
Hak Konsumen	Penghapusan, portabilitas	Penghapusan, koreksi	tolak penjualan data

Jenis Bias Algoritmik

Bias Algoritmik adalah kesalahan sistematis yang berulang dalam sistem AI, yang menghasilkan output yang tidak adil atau diskriminatif terhadap kelompok tertentu. Akar Masalah Utama: Data yang Bias.

- Sampling Bias:
  - Terjadi ketika data pelatihan tidak mewakili populasi dunia nyata.
  - Model pengenalan wajah yang dilatih 95% pada wajah Kaukasia akan gagal mengenali wajah dari etnis lain secara akurat.
- Jenis Bias Lainnya:
  - Historical Bias: Mencerminkan bias dan ketidaksetaraan yang sudah ada di masyarakat (misal: data historis menunjukkan lebih sedikit perempuan di posisi C-level).
  - Measurement Bias: Kesalahan dalam pengukuran atau pengumpulan data (misal: kamera dengan sensor buruk untuk warna kulit gelap).

Metrik Fairness

Digunakan untuk memastikan keadilan antar kelompok

- **Demographic Parity (DP)**:
  - Konsep: Peluang untuk mendapatkan hasil positif harus sama untuk semua kelompok.
  - Contoh: Persentase pelamar kerja pria yang lolos seleksi awal harus sama dengan persentase pelamar kerja wanita.
  - P(outcome | group A) = P(outcome | group B).
- **Equal Opportunity (EO)**:
  - Konsep: Di antara semua orang yang sebenarnya memenuhi syarat, peluang untuk mendapatkan hasil positif harus sama untuk semua kelompok.
  - Contoh: Di antara semua pelamar yang berkualifikasi, persentase pria dan wanita yang diterima harus sama.
  - P(true positive | group A) = P(true positive | group B).

Mitigasi Teknis

- Alat Bantu untuk Privasi dan Keadilan yang Lebih Baik
- Ada berbagai pendekatan teknis untuk mengurangi risiko privasi dan mendeteksi bias.
    - **Differential Privacy**
    - **SHAP (SHapley Additive exPlanations)**
    - **Federated Learning**

Mitigasi Teknis

Differential Privacy:

- Tujuan: Melindungi privasi individu dalam dataset.
- Cara Kerja: Menambahkan "gangguan" (noise) matematis yang terkontrol pada data. Cukup untuk menganonimkan individu, tetapi cukup kecil untuk menjaga akurasi analisis data agregat.
- Analogi: Seperti menjawab survei dengan sedikit keacakan untuk melindungi jawaban personal kita.

Mitigasi Teknis

SHAP (SHapley Additive exPlanations):

- Tujuan: Menjelaskan keputusan model AI (Explainable AI).
- Cara Kerja: Menunjukkan seberapa besar kontribusi setiap fitur (misal: usia, pendapatan, lokasi) terhadap sebuah prediksi spesifik.
- Manfaat: Sangat berguna untuk mendeteksi bias dengan mengungkap fitur-fitur yang tidak seharusnya berpengaruh besar.

Mitigasi Teknis

Federated Learning:

- Tujuan: Melatih model AI tanpa mengumpulkan data mentah.
- Cara Kerja: Model dikirim ke perangkat pengguna (misal: ponsel), dilatih secara lokal, dan hanya ringkasan pembaruan model (bukan data pribadi) yang dikirim kembali ke server.
- Contoh: Digunakan oleh Google untuk Gboard (prediksi kata).

DPIA (Data Protection Impact Assessment)

adalah proses wajib di bawah GDPR/UU PDP untuk mengidentifikasi dan meminimalkan risiko perlindungan data dari sebuah proyek.

1. Langkah 1: **Deskripsi Proyek**: Apa tujuan pemrosesan data? Data apa yang dikumpulkan?
2. Langkah 2: **Penilaian Kebutuhan**: Mengapa pemrosesan ini diperlukan dan proporsional?
3. Langkah 3: **Konsultasi**: Siapa saja pemangku kepentingan yang perlu dilibatkan (misal: Subjek Data, DPO)?
4. Langkah 4: **Identifikasi Risiko**: Apa saja risiko terhadap hak dan kebebasan individu (misal: diskriminasi, re-identifikasi, kebocoran)?
5. Langkah 5: **Mitigasi Risiko**: Langkah-langkah apa yang akan diambil untuk mengurangi risiko tersebut (misal: enkripsi, anonimitas, kontrol akses)?
6. Langkah 6: **Persetujuan & Tinjauan**: Tanda tangan dari penanggung jawab dan jadwal untuk peninjauan ulang.

Studi Kasus: (Correctional Offender Management Profiling for Alternative Sanctions)

Memprediksi kemungkinan seorang terdakwa akan melakukan kejahatan lagi. Skor ini digunakan hakim untuk menentukan hukuman atau pembebasan bersyarat.

Masalah (Investigasi ProPublica 2016):

- Algoritma ditemukan memiliki bias rasial yang signifikan.
- **Terdakwa Kulit Hitam**: Hampir dua kali lebih mungkin diberi label risiko tinggi secara keliru dibandingkan terdakwa kulit putih (tingkat False Positive yang tinggi).
- **Terdakwa Kulit Putih**: Lebih mungkin diberi label risiko rendah secara keliru (tingkat False Negative yang tinggi).

Dampak: Keputusan yang mengubah hidup manusia (penjara vs. kebebasan) dipengaruhi oleh algoritma yang bias, memperkuat ketidaksetaraan rasial yang sudah ada.

Komitmen Industri & Regulasi

- EU AI Act: Regulasi AI untuk transparansi dan mitigasi bias.
- Model Card: Dokumentasi performa dan batasan model AI.
- Google’s AI Principles: Hindari bias, pastikan AI bermanfaat.

Kesimpulan

- **Privasi Bukan Pilihan, Tapi Kewajiban**. Dengan adanya UU PDP dan risiko reputasi, mengabaikan privasi adalah strategi yang buruk.
- **Data "Anonim" Jarang Benar-benar Aman**. Risiko re-identifikasi adalah nyata. Jangan pernah meremehkan nilai dari pola data.
- **Bias Algoritmik Sering Berakar dari Data yang Bias**. Kualitas dan representasi data pelatihan Anda sangatlah penting (Garbage In, Garbage Out).
- **Keadilan Itu Kompleks**. Gunakan metrik fairness (seperti DP & EO) untuk mengukur, tetapi pahami konteks dan keterbatasannya.
- **Pendekatan Proaktif adalah Kunci**. Gunakan alat seperti Privacy by Design, DPIA, dan mitigasi teknis untuk membangun sistem yang lebih baik dari awal, bukan memperbaikinya setelah terjadi kerusakan.

Kecerdasan Buatan & Etika Pengambilan Keputusan

Etika Profesi

Outcome

- Menjelaskan siklus hidup model AI & titik kritis etika.
- Mengidentifikasi 4 risiko utama (bias, lack-explainability, safety, misuse) pada studi kasus AI nyata.
- Menggunakan AI Risk Matrix (severity × likelihood) untuk menilai contoh aplikasi otonom.
- Membuat rekomendasi Responsible-AI Checklist (10 poin) yang selaras EU AI Act & UU PDP.

Pendahuluan

- **AI (Artificial Intelligence)**: Teknologi yang memungkinkan mesin meniru kemampuan manusia, seperti belajar, berpikir, dan membuat keputusan.
- **Ethical Decision Making**: Proses pengambilan keputusan oleh AI atau manusia yang mempertimbangkan nilai moral, keadilan, dan dampak sosial, agar tidak merugikan individu atau kelompok.

Evolusi AI (1956 → GPT-4)

- **1956**: Dartmouth Conference, kelahiran AI oleh John McCarthy.
- **1980-an**: Sistem berbasis aturan (expert systems).
- **1990-an - 2000-an**: Kebangkitan Machine Learning
- **2010-an**: Deep learning dan big data.
- **2023**: GPT-4 (OpenAI), AI multimodal canggih.

Rantai Nilai Data-Model-Produk

1. **DATA (Fondasi)**
    a. Aktivitas: Pengumpulan, pembersihan, pelabelan, dan augmentasi data.
    b. Prinsip Kunci: "Garbage In, Garbage Out". Kualitas dan representasi data menentukan kualitas dan keadilan model.
2. **MODEL (Otak)**
    a. Aktivitas: Pemilihan algoritma, pelatihan model pada data, evaluasi performa, dan validasi.
    b. Prinsip Kunci: Menyeimbangkan akurasi dengan interpretasi (explainability).

Rantai Nilai Data-Model-Produk

3. PRODUK (Aplikasi)

a. Aktivitas: Integrasi model ke dalam antarmuka pengguna (misal: aplikasi, website, sistem diagnosis).

b. Prinsip Kunci: Desain yang berpusat pada manusia dan menyertakan pengawasan yang bermakna.

4. UMPAN BALIK (Siklus)

a. Aktivitas: Memantau performa model di dunia nyata, mengumpulkan umpan balik pengguna, dan menggunakannya untuk menyempurnakan data dan model.

b. Prinsip Kunci: Perbaikan berkelanjutan dan adaptasi.

Prinsip AI OECD (5) vs Google (7)

Peta Jalan Etika: Panduan Global vs. Komitmen Industri

- **OECD (5)**: Inclusive growth, human-centered, transparency, safety, accountability.
- **Google (7)**: Social benefit, avoid bias, safety, accountability, privacy, scientific rigor (standar yang ketat), appropriate use.

Contoh Keberhasilan AI: Radiologi 2023

- AI di radiologi (contoh: DeepMind, 2023).
- Deteksi kanker paru-paru dari CT scan dengan akurasi >90%.
- Membantu dokter, meningkatkan diagnosis dini.

Kegagalan AI: COMPAS, TayBot, Tesla Crash

- COMPAS (2016): Bias rasial dalam prediksi residivisme.
- TayBot (2016): Chatbot Microsoft jadi rasis dalam 24 jam.
- Tesla Crash (2016-2020): Autopilot gagal deteksi rintangan.

Risiko 1: Bias (Skema)

- Sumber bias:
  - Sampling bias (data tidak representatif).
  - Algorithmic bias (desain model diskriminatif).
- Dampak: Ketidakadilan, diskriminasi.

Risiko 2: Explainability (Black-Box vs XAI)

- Black-Box: Model AI tidak transparan (contoh: deep neural networks).
- XAI: Teknik seperti SHAP untuk menjelaskan keputusan AI.
- Penting untuk kepercayaan dan akuntabilitas.

Risiko 3: Safety & Robustness (Adversarial Attack)

- Adversarial Attack: Manipulasi input (noise kecil) untuk menipu AI.
- Contoh: Gambar kucing jadi anjing karena noise.
- Solusi: Tingkatkan robustness model.

Risiko 4: Misuse (Deepfake Election)

- Deepfake Election: Video palsu kandidat pemilu (contoh: India, 2024).
- Dampak: Penyebaran misinformasi, manipulasi pemilih.
- Solusi: Deteksi deepfake, regulasi ketat.

Kerangka Responsible AI

- Lapisan 1: Prinsip etika (fairness, transparency).
- Lapisan 2: Tata kelola (kebijakan, pengawasan).
- Lapisan 3: Teknologi (XAI, differential privacy).
- Lapisan 4: Budaya organisasi (pendidikan etika).

EU AI Act – Tabel Tier Risiko

Tier	Contoh	Aturan
Minimal Risk	Filter Spam	Tanpa regulasi khusus
Limited Risk	Chatbot	Transparansi wajib
High Risk	AI Rekrutmen	Pengawasan ketat
Unacceptable Risk	Manipulasi massal	Dilarang

NIST AI RMF – Prepare-Measure-Manage-Govern

- **Prepare**: Identifikasi risiko awal.
- **Measure**: Ukur performa dan dampak AI.
- **Manage**: Mitigasi risiko yang terdeteksi.
- **Govern**: Tetapkan kebijakan tata kelola.

Checklist 10-Poin Responsible AI

1. Pastikan data bebas bias.
2. Terapkan XAI (Explainable AI) untuk transparansi.
3. Lindungi privasi pengguna.
4. Uji keamanan model.
5. Libatkan pemangku kepentingan.
6. Tetapkan tata kelola AI.
7. Monitor dampak sosial.
8. Hindari misuse AI.
9. Patuhi regulasi (EU AI Act, dll.).
10. Edukasi tim tentang etika AI.

Media Sosial, Disinformasi, dan Etika Konten Digital

Tujuan Kuliah

1. Memahami ekosistem disinformasi (*hoaks*, *deep-fake*, *echo-chamber*) di platform media sosial.
2. Membedakan batas kebebasan berekspresi vs kewajiban moderasi konten.
3. Merancang strategi etis—teknis dan kebijakan—untuk mitigasi penyebaran mis/dis-informasi.

Krisis Informasi

Tahun 2016

Aksi 212 terkait kasus penistaan agama yang menjerat Gubernur DKI Jakarta saat itu, Basuki Tjahaja Purnama (Ahok). Peristiwa ini menunjukkan mobilisasi massa yang sangat besar dan menjadi titik awal meningkatnya polarisasi berbasis agama dan politik.

Disinformasi:

- **Jumlah Peserta Aksi yang Dilebih-lebihkan**: Angka peserta aksi digelembungkan secara masif di media sosial dan grup percakapan, seringkali mencapai 7 juta orang, untuk membangun narasi kekuatan umat.
- **Tenaga Kerja Asing dari Tiongkok**: Isu serbuan 10 juta tenaga kerja ilegal dari Tiongkok yang akan mengambil alih pekerjaan lokal dan memiliki hak pilih. Isu ini terus diulang hingga beberapa tahun berikutnya.
- **Hoaks "The Next Habibie"**: Kisah mahasiswa Indonesia bernama **Dwi Hartanto** di Belanda yang diklaim jenius luar biasa di bidang kedirgantaraan, namun ternyata sebagian besar klaimnya adalah kebohongan.

Krisis Informasi

Tahun 2020

Pandemi COVID-19 melanda Indonesia. Seluruh fokus bergeser ke isu kesehatan, ketidakpastian, dan kebijakan pemerintah dalam menangani pandemi.

Disinformasi:

- **Konspirasi COVID-19:** Teori bahwa virus corona adalah senjata biologis, buatan elite global, atau bahkan tidak ada sama sekali (hanya flu biasa yang dibesar-besarkan).
- **Obat Ajaib dan Metode Pencegahan Aneh:** Hoaks tentang berbagai cara menyembuhkan COVID-19, seperti minum rebusan bawang putih, berkumur air garam, hingga mengonsumsi obat-obatan keras tanpa resep dokter.
- **Data Pasien yang Ditutupi/Dilebihkan:** Ada dua narasi yang saling bertentangan: pemerintah menutupi jumlah kasus sebenarnya, atau sebaliknya, rumah sakit "meng-COVID-kan" semua pasien meninggal untuk mendapatkan dana.

Krisis Informasi

disinformasi meledak seiring penggunaan media sosial secara besar-besaran dan meningkatnya polarisasi global.

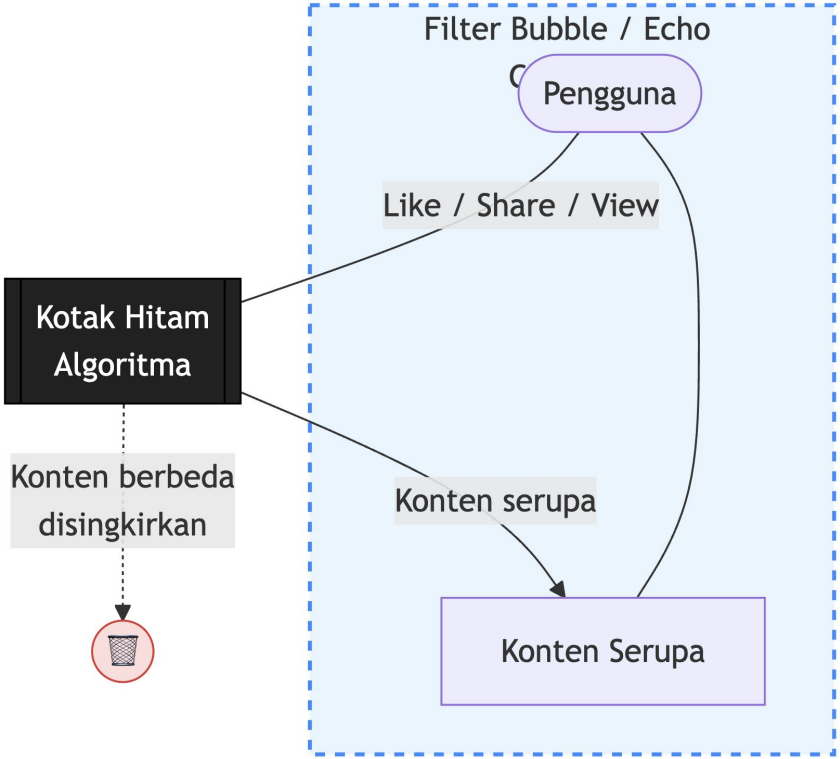
Membedah Kebohongan Digital

Kategori	Definisi	Niat (Intent)	Contoh
Misinformasi	Informasi salah, tapi disebar tanpa niat jahat.	Tidak ada niat buruk.	Nenek menyebar info kesehatan keliru di grup WA karena percaya itu benar.
Disinformasi	Informasi salah yang sengaja dibuat & disebar untuk menipu atau merugikan.	Ada niat menipu, memprovokasi, atau merusak.	Akun anonim membuat video hoaks untuk menjatuhkan lawan politik.
Malinformasi	Informasi asli yang disebar untuk merugikan seseorang atau kelompok.	Ada niat merusak dengan fakta.	Menyebarkan riwayat percakapan pribadi seseorang untuk mempermalukannya (*doxing*).

Anatomi Penyebaran Hoaks

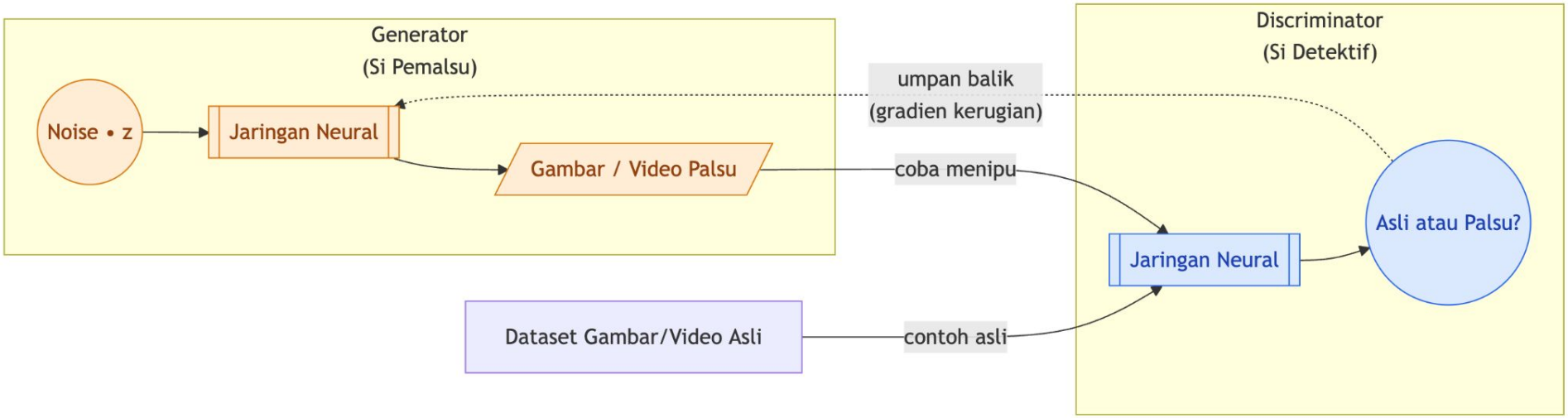
1. Penciptaan (Origin)
    - Konten palsu dibuat oleh individu/kelompok.
    - Tujuan: politik, finansial, ideologi.
2. Amplifikasi Awal (Amplify)
    - Disebar oleh bots atau akun bayaran untuk menciptakan momentum awal.
    - Disebar di grup tertutup (WhatsApp, Telegram).
3. Penyebaran Viral (Viral)
    - Diambil alih oleh influencer & pengguna asli yang percaya.
    - Algoritma platform mendorong konten populer.
4. Dampak Dunia Nyata (Impact)
    - Keputusan keliru, kepanikan publik, konflik sosial, kerugian finansial.

Algoritma Rekomendasi & Filter Bubble



- **Tujuan Algoritma**: Membuat pengguna tetap di platform selama mungkin (*engagement*).
- **Efek Samping**: Hanya melihat konten yang mengkonfirmasi keyakinan Anda.
- ***Echo Chamber***: Ruang di mana opini yang sama terus diulang dan diperkuat.
- ***Filter Bubble***: Isolasi intelektual akibat personalisasi konten oleh algoritma.

Deep-fake (*Generative Adversarial Network*/GAN)



Deep-fake (*Generative Adversarial Network*/GAN)

1. ***Generator*** (Pemalsu)
    - AI yang bertugas menciptakan gambar/video palsu (misal: wajah politisi).
    - Tujuannya: Menipu si detektif.
2. ***Discriminator*** (Detektif)
    - AI yang bertugas mendeteksi apakah gambar/video itu asli atau palsu.
    - Tujuannya: Menangkap si pemalsu.

Dampak Sosial

1. **Konflik Sosial**:
    - Memicu kekerasan dan persekusi terhadap kelompok minoritas (contoh: kasus Rohingya di Myanmar).
2. **Kepercayaan Publik**:
    - Mengikis kepercayaan masyarakat pada institusi media, pemerintah, dan sains.

Upaya Membersihkan Platform

1. ***Hard Moderation* (Tindakan Keras)**
    - Takedown: Konten dihapus sepenuhnya.
    - Akun diblokir/dihapus.
2. ***Soft Moderation* (Tindakan Lunak)**
    - Labeling: Konten diberi label "Informasi Salah".
    - *Shadow-ban*: Jangkauan konten dikurangi tanpa notifikasi.
    - Konten tidak direkomendasikan algoritma.
3. ***No Action* (Aman)**
    - Konten dianggap tidak melanggar kebijakan.

Hukum vs. Kebebasan Berekspresi

- **Kewajiban Negara Melindungi Warga**:
  - UU ITE (Indonesia): Pasal 27(3) tentang pencemaran nama baik, Pasal 28(1) tentang berita bohong yang merugikan konsumen, Pasal 28(2) tentang ujaran kebencian (SARA).
  - SKB 3 Menteri 2021: Pedoman interpretasi UU ITE.
- **Hak Individu untuk Berekspresi**:
  - UUD 1945 Pasal 28E (3): "Setiap orang berhak atas kebebasan berserikat, berkumpul, dan mengeluarkan pendapat."
  - ICCPR Pasal 19: Standar PBB untuk kebebasan berekspresi.

Dilema Etis Utama: Di mana batas antara melindungi publik dari disinformasi berbahaya dan membungkam kritik yang sah terhadap kekuasaan?

Toolkit: Teknik OSINT & Fact-Checking

- **Reverse Image Search (Google Images, TinEye):**
    - Melacak sumber asli sebuah gambar dan melihat apakah sudah pernah digunakan dalam konteks berbeda.
- **Analisis Metadata (EXIF Data):**
    - Melihat data tersembunyi sebuah foto: kapan, di mana, dan dengan perangkat apa foto diambil.
- **Forensik Digital (InVid, Forensically):**
    - Alat untuk menganalisis manipulasi pada video dan gambar (misal: kloning, error level).
- **Verifikasi di Platform Fact-Check:**
    - Cek kebenaran klaim di situs terpercaya (CekFakta.com, TurnBackHoax.id, Mafindo, Snopes).
- **Analisis Akun (Botometer):**
    - Mengecek kemungkinan sebuah akun Twitter adalah bot atau bukan.

Siklus Ekonomi Disinformasi & Clickbait

Bagaimana konten sensasional menghasilkan keuntungan dan terus berulang.

1. Konten Sensasional

Judul provokatif & gambar heboh dibuat untuk memancing reaksi.

2. Menarik Perhatian & Emosi

Pengguna merespon dengan klik, suka, komentar, dan membagikan (engagement).

3. Jangkauan & Views Naik

Algoritma mendorong konten populer, membuatnya semakin viral.

4. Pendapatan Iklan Naik

Semakin banyak views, semakin besar pendapatan dari iklan (Ad Revenue).

5. INSENTIF

Membuat LEBIH BANYAK konten sensasional untuk keuntungan lebih besar.

Merancang Aturan Main Komunitas

Contoh 6 Pasal Etika Komunitas Forum Diskusi Mahasiswa "Integritas Akademika"

- Pasal 1: Tujuan & Nilai: Ruang ini untuk diskusi yang sehat, terbuka, kritis, dan saling menghormati, berdasarkan nilai-nilai akademik.
- Pasal 2: Larangan Ujaran Kebencian: Dilarang keras konten yang menyerang individu/kelompok berdasarkan SARA (Suku, Agama, Ras, Antargolongan), gender, atau orientasi seksual.
- Pasal 3: Larangan Disinformasi: Klaim faktual yang signifikan (terutama terkait kebijakan kampus, kesehatan, atau politik) wajib menyertakan sumber yang kredibel. Penyebaran hoaks akan ditindak.
- Pasal 4: Aturan Spam: Dilarang melakukan spamming, promosi komersial tidak relevan, dan aktivitas scamming.
- Pasal 5: Proses Moderasi: Laporan akan ditinjau oleh tim moderator gabungan (dosen & mahasiswa). Pengguna berhak mengajukan banding.
- Pasal 6: Sanksi: Pelanggaran akan dikenai sanksi bertahap: (1) Peringatan, (2) Skorsing sementara, (3) Pemblokiran permanen.

Rangkuman

1. **Disinformasi adalah Ekosistem**: Ini bukan sekadar "berita bohong", tapi rantai kompleks yang melibatkan pembuat, penyebar (bot & manusia), platform, dan kita sebagai konsumen.
2. **Algoritma adalah Pedang Bermata Dua**: Didesain untuk engagement, namun menciptakan filter bubble yang mempercepat penyebaran hoaks dan polarisasi.
3. **Moderasi itu Sulit**: Menyeimbangkan keamanan publik dari hoaks berbahaya dengan perlindungan kebebasan berekspresi adalah tantangan etis dan teknis terbesar platform.
4. **Anda Punya Kekuatan**: Dengan alat dasar (*OSINT, fact-checking*), kita semua bisa menjadi konsumen informasi yang lebih kritis dan tidak mudah tertipu.
5. **Ikuti Aliran Uang**: Model bisnis berbasis iklan (*attention economy*) memberi insentif ekonomi pada konten yang paling sensasional, bukan yang paling benar.

Etika dalam Penelitian & Publikasi Ilmiah

Etika Profesi

Tujuan

- Memahami praktek etis riset ilmiah (plagiarisme, fabrikasi, falsifikasi, gift authorship).
- Menjelaskan proses *peer-review*, *open-science*, dan lisensi publikasi (*open-access*, *pre-print*).
- Menerapkan pedoman sitasi (APA/IEEE) & manajemen data riset (FAIR principles).

Outcome

1. Membedakan 4 bentuk pelanggaran etika riset dan konsekuensinya.
2. Menulis ringkasan paper (abstract 150 kata) tanpa plagiarisme (< 10 % Turnitin).
3. Menyusun daftar referensi dengan manager (Zotero/Mendeley) format IEEE.
4. Merancang rencana manajemen data riset singkat (FAIR + UU PDP).

Krisis Kredibilitas & Pelanggaran Etika Riset

Kasus **Retraction Graphene-Oxide** (2023)

https://retractionwatch.com/2024/09/03/faked-data-prompts-retraction-of-nature-journal-study-claiming-creation-of-a-new-form-of-carbon/

- **Latar Belakang**: Pada tahun 2023, sebuah artikel yang dipublikasikan di jurnal ternama mengenai potensi aplikasi graphene-oxide dalam bidang biomedis ditarik kembali (retracted).
- **Klaim Utama Artikel**: Peneliti mengklaim telah menemukan metode sintesis graphene-oxide yang sangat efisien dan menunjukkan hasil spektakuler dalam menghambat sel kanker secara in-vitro.
- **Alasan Retraksi**: Setelah publikasi, komunitas ilmiah mulai menyuarakan keraguan. Analisis independen menunjukkan adanya kejanggalan pada gambar mikroskop (TEM/SEM) yang disajikan. Diduga kuat gambar tersebut telah dimanipulasi secara digital untuk melebih-lebihkan hasil. Selain itu, beberapa plot data spektroskopi tampak "terlalu sempurna" dan tidak konsisten.

Krisis Kredibilitas & Pelanggaran Etika Riset

Kasus **Retraction Graphene-Oxide** (2023)

- Investigasi:
  - Investigasi Institusional: Universitas tempat peneliti bernaung melakukan investigasi internal.
  - Temuan: Ditemukan adanya fabrikasi (menciptakan data yang tidak pernah ada) dan falsifikasi (mengubah data yang ada agar sesuai dengan hipotesis).
- Konsekuensi:
  - Bagi Peneliti: Kehilangan kredibilitas, pencabutan gelar (jika terkait disertasi), pemecatan, dan kemungkinan masuk daftar hitam pendanaan riset.
  - Bagi Institusi: Kerusakan reputasi yang serius.
  - Bagi Sains: Waktu dan sumber daya peneliti lain terbuang untuk mencoba mereplikasi hasil palsu tersebut, menghambat kemajuan ilmu pengetahuan yang sebenarnya.

Definisi Plagiarisme

Plagiarisme adalah tindakan mengambil ide, proses, hasil, atau kata-kata orang lain tanpa memberikan kredit (atribusi) yang semestinya.

Ini adalah "pencurian kekayaan intelektual".

Tingkatan Plagiarisme

1. **Plagiarisme Langsung (Direct Plagiarism)**: Menyalin kata demi kata (copy-paste) tanpa tanda kutip dan tanpa sitasi.
2. **Plagiarisme Mosaik (Patchwork Plagiarism)**: Meminjam frasa dari berbagai sumber dan menyusunnya menjadi kalimat baru tanpa sitasi yang memadai.
3. **Parafrase yang Tidak Benar**: Mengubah beberapa kata tetapi tetap mempertahankan struktur kalimat asli tanpa memberikan sitasi.
4. **Plagiarisme Ide**: Menyajikan gagasan atau konsep orisinal orang lain seolah-olah itu milik sendiri, bahkan jika diungkapkan dengan kata-kata yang berbeda.
5. **Self-Plagiarism**: Mempublikasikan ulang karya sendiri yang sudah pernah dipublikasikan tanpa memberitahu editor atau pembaca.

Interpretasi Skor Similarity (Contoh: Turnitin)

Skor Similarity	Interpretasi	Tindakan yang Disarankan
<10% (Biru/Hijau)	Kemungkinan besar aman. Kesamaan biasanya berupa istilah umum, nama institusi, atau kutipan yang disitasi dengan benar.	Periksa secara singkat untuk memastikan tidak ada paragraf yang disalin sepenuhnya.
10% - 25% (Kuning)	Perlu perhatian. Mungkin berisi parafrase yang kurang baik, kutipan yang lupa disitasi, atau terlalu banyak mengandalkan satu sumber.	Periksa setiap bagian yang ditandai. Perbaiki parafrase, tambahkan sitasi yang hilang, dan variasikan sumber.
> 25% (Merah)	Indikasi kuat adanya plagiarisme. Terdapat porsi teks yang signifikan yang identik atau sangat mirip dengan sumber lain.	Wajib direvisi total. Tulis ulang dengan pemahaman sendiri dan pastikan semua sumber disitasi dengan benar.

Fabrikasi vs Falsifikasi

Kriteria	Fabrikasi (Mengarang Data)	Falsifikasi (Memalsukan Data)
Definisi	Menciptakan data atau hasil dari nol, lalu mencatat atau melaporkannya seolah-olah itu nyata.	Memanipulasi materi, peralatan, atau proses riset; atau mengubah/menghilangkan data agar tidak akurat.
Tindakan	"Making things up" (Mengada-ada).	"Changing things" (Mengubah yang ada).
Contoh	Seorang peneliti tidak pernah melakukan survei, namun ia mengisi sendiri 100 lembar kuesioner.	Seorang peneliti menghapus 3 data outlier dari hasil eksperimennya agar hasil uji statistiknya signifikan.
Tujuan	Menciptakan bukti untuk mendukung hipotesis yang tidak pernah diuji.	Mengubah bukti yang ada agar lebih sesuai dengan hipotesis yang diinginkan.

Integritas dan Praktik Terbaik dalam Publikasi

Masalah Kepenulisan: Gift/Honorary Authorship

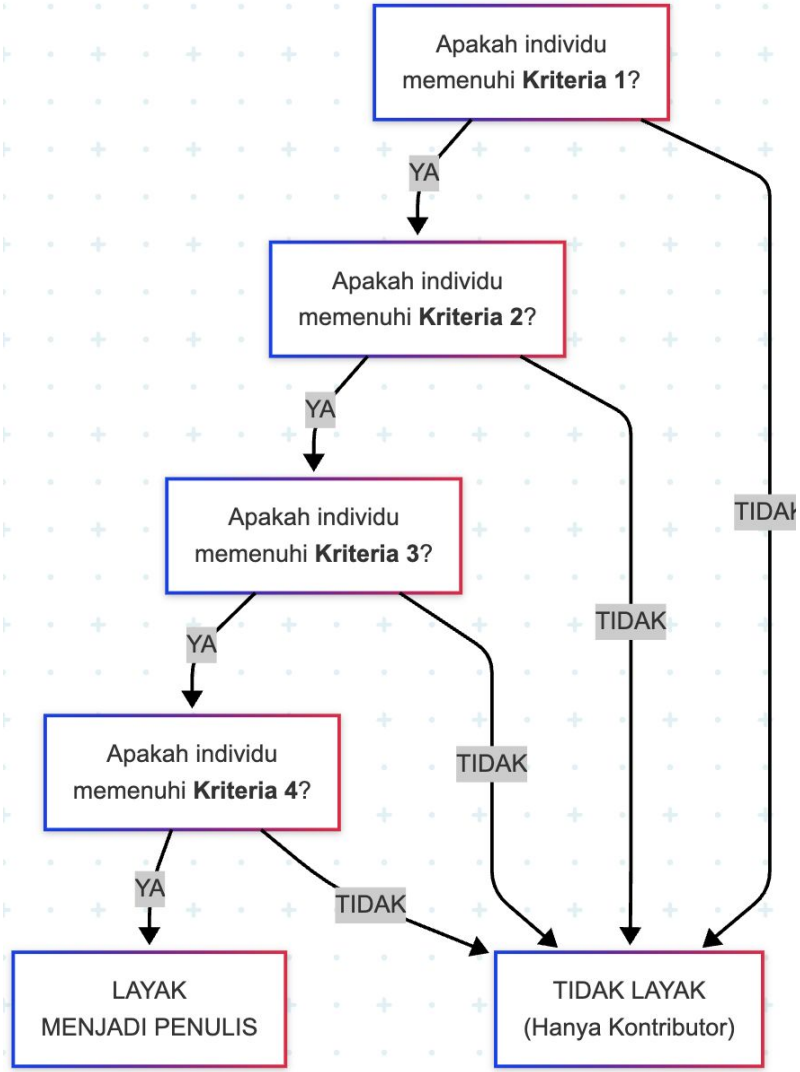
Kriteria Kepenulisan ICMJE: International Committee of Medical Journal Editors (ICMJE) menetapkan 4 kriteria yang SEMUANYA HARUS TERPENUHI untuk bisa menjadi penulis:

1. Kontribusi substansial terhadap konsepsi atau desain karya; ATAU akuisisi, analisis, atau interpretasi data untuk karya tersebut; DAN
2. Menyusun draf karya atau merevisinya secara kritis untuk konten intelektual yang penting; DAN
3. Persetujuan akhir terhadap versi yang akan dipublikasikan; DAN
4. Setuju untuk bertanggung jawab atas semua aspek pekerjaan untuk memastikan bahwa pertanyaan terkait akurasi atau integritas bagian mana pun dari pekerjaan diselidiki dan diselesaikan dengan tepat.

Diagram alur kelayakan menjadi penulis

Jika seseorang memberikan kontribusi pada penelitian tetapi **tidak memenuhi SEMUA empat kriteria**, maka ia tidak layak menjadi penulis. Namun, kontribusinya tetap harus diakui.

Orang-orang seperti ini harus dimasukkan ke dalam bagian **Ucapan Terima Kasih (*Acknowledgements*)**, bukan sebagai penulis.



Integritas dan Praktik Terbaik dalam Publikasi

- **Gift Authorship**: Memberikan status penulis kepada seseorang yang tidak memenuhi keempat kriteria, biasanya sebagai bentuk penghormatan (misalnya, kepala departemen, senior) atau untuk meningkatkan peluang publikasi. Ini adalah pelanggaran etika.
- **Kontributor**: Individu yang berkontribusi tetapi tidak memenuhi keempat kriteria (misal: hanya menyediakan dana, melakukan pengumpulan data rutin, atau memberikan komentar umum) harus dicantumkan dalam bagian ***acknowledgements*** (ucapan terima kasih).

Prinsip Dasar Integritas Riset: *Singapore Statement*

1. **Kejujuran (Honesty)**: Jujur dalam semua aspek penelitian, termasuk dalam penyajian data, pelaporan hasil, dan pengakuan kontribusi.
2. **Akuntabilitas (Accountability)**: Bertanggung jawab atas kegiatan penelitian dari pendanaan hingga publikasi.
3. **Kesopanan Profesional (Professional Courtesy)**: Perlakukan kolega, staf, dan mahasiswa dengan adil dan hormat.
4. **Penatalayanan yang Baik (Good Stewardship)**: Kelola sumber daya penelitian (misalnya dana, peralatan) dengan bijak dan efisien, serta peduli terhadap dampak penelitian pada manusia, hewan, dan lingkungan.

Prinsip Dasar Integritas Riset: *Singapore Statement*

Istilah "*Singapore Statement*" digunakan karena pernyataan mengenai prinsip-prinsip dasar integritas riset ini dirumuskan dan disepakati dalam acara ***2nd World Conference on Research Integrity*** (Konferensi Dunia ke-2 tentang Integritas Riset) yang diselenggarakan di Singapura.

Istilah "***Singapore Statement***", tidak hanya merujuk pada empat prinsip dasarnya (Kejujuran, Akuntabilitas, Kesopanan Profesional, dan Penatalayanan yang Baik), tetapi juga secara tidak langsung merujuk pada sebuah momen bersejarah di Singapura pada tahun 2010, di mana komunitas riset dunia berkumpul untuk menyepakati fondasi etika yang berlaku secara global.

Proses Peninjauan Sejawat (*Peer-Review*)

Proses peninjauan sejawat (peer review) adalah sistem kontrol kualitas untuk publikasi akademik. Sebelum sebuah naskah ilmiah (artikel, paper) diterbitkan oleh sebuah jurnal, editor akan mengirimkannya kepada beberapa ahli independen di bidang yang sama (disebut "peninjau" atau "rekan sejawat") untuk dievaluasi secara kritis.

Tujuannya adalah untuk memastikan bahwa penelitian tersebut valid, orisinal, signifikan, dan disajikan dengan jelas. Peninjau memberikan masukan untuk perbaikan dan rekomendasi kepada editor apakah naskah tersebut layak untuk diterima, perlu direvisi, atau harus ditolak.

Jurnal Predator (*Predatory Journal*)

Jurnal predator (*Predatory Journal*) adalah entitas penerbitan yang mengeksploitasi model publikasi akses terbuka (***Open Access***) untuk mencari keuntungan finansial tanpa memberikan layanan editorial dan publikasi yang semestinya. Secara esensial, mereka adalah penipu berkedok jurnal ilmiah.

Model bisnis yang sederhana: membebankan biaya publikasi (***Article Processing Charges/APC***) kepada penulis tanpa melalui proses peninjauan sejawat (*peer-review*) yang ketat, proses penyuntingan (*editing*), ataupun pengarsipan yang kredibel. Mereka memprioritaskan keuntungan di atas integritas dan kualitas akademik.

Ciri-ciri Jurnal Predator (*Predatory Journal*)

1. Proses Peer Review Palsu atau Tidak Ada: Janji publikasi yang sangat cepat (hitungan hari atau minggu) adalah tanda bahaya utama, karena proses peer review yang benar membutuhkan waktu berbulan-bulan.
2. Email Agresif dan Tidak Personal: Mengirimkan email spam yang memuji-muji Anda dan mengundang untuk submit artikel dengan bahasa yang terlalu bombastis.
3. Transparansi Biaya yang Buruk: Biaya publikasi sering kali disembunyikan dan baru diinformasikan setelah naskah diterima.
4. Dewan Redaksi (Editorial Board) Fiktif: Nama-nama editor yang dicantumkan sering kali palsu atau dicatut tanpa izin. Jika Anda tidak mengenali satu pun nama di dewan redaksi, ini patut dicurigai.
5. Nama Jurnal Meniru Jurnal Bereputasi: Menggunakan nama yang sangat mirip dengan jurnal ternama untuk mengecoh penulis (misalnya, "Journal of Economics and Finance" vs. "International Journal of Economics and Finance Studies").
6. Situs Web Tidak Profesional: Tampilan situs web yang buruk, penuh kesalahan ketik (typo), gambar berkualitas rendah, dan metrik palsu (misalnya, "Global Impact Factor" yang tidak diakui).
7. Skop Jurnal Terlalu Luas: Satu jurnal menerima artikel dari berbagai bidang ilmu yang tidak saling berhubungan (misalnya, kedokteran, teknik, dan sastra dalam satu jurnal).
8. Tidak Terindeks di Basis Data Kredibel: Jurnal predator tidak akan ditemukan di basis data terkemuka seperti Scopus, Web of Science, atau Directory of Open Access Journals (DOAJ).

Negara yang Paling Banyak Menerbitkan Jurnal Predator?

Berdasarkan data dan analisis dari berbagai studi scientometric, India secara konsisten menempati urutan teratas sebagai negara dengan jumlah penerbit jurnal predator terbanyak. Sejumlah besar jurnal yang teridentifikasi sebagai predator berlokasi dan dioperasikan dari India.

Negara yang Penulisnya Terkena Perangkap Jurnal Predator

1. Kazakhstan: ~17%
2. Indonesia: ~16.7%
3. Irak: ~12.9%
4. Albania: ~12.1%
5. Malaysia: ~11.6%

Lisensi Publikasi: *Creative Commons* (CC)

Lisensi	Ikon	Deskripsi	Contoh Penggunaan dalam Riset
CC-BY (Atribusi)	CC BY	Paling Bebas. Orang lain boleh menyalin, mendistribusikan, dan membuat karya turunan (bahkan untuk tujuan komersial), selama mereka memberikan atribusi (kredit) kepada Anda.	Ingin hasil riset disebarkan seluas-luasnya tanpa batasan untuk mendorong inovasi.
CC-BY-NC-SA (Atribusi-NonKomersial-BerbagiSerupa)	CC BY NC SA	Orang lain boleh menyalin, mendistribusikan, dan membuat karya turunan, TAPI: 1. NC: Tidak untuk tujuan komersial. 2. SA: Karya turunan harus dibagikan dengan lisensi yang sama. 3. Tetap wajib Atribusi (BY).	Ingin riset digunakan untuk pendidikan dan riset lanjutan, tapi tidak ingin ada pihak yang menjual kembali data atau hasil riset Anda untuk keuntungan.

FAIR Principles

Prinsip yang bertujuan agar data riset lebih bernilai dan dapat digunakan kembali

1. **Findable**: Data dan metadata harus mudah ditemukan oleh manusia dan mesin. Praktinya memberikan Identifier unik (seperti DOI), mendaftarkan data di repository.
2. **Accessible**: Data dapat diakses menggunakan protokol standar (misal, via internet). Jika perlu autentikasi, prosesnya harus jelas. Praktiknya menyimpan data di repository publik/institusional, menyediakan informasi cara mengakses.
3. **Interoperable**: Data dapat diintegrasikan dengan data lain dan dapat diproses oleh aplikasi atau alur kerja. Praktiknya menggunakan format file yang umum (.CSV, .TXT), menggunakan kosakata/ontologi standar.
4. **Reusable**: Data dideskripsikan dengan baik dan memiliki lisensi yang jelas agar dapat digunakan kembali untuk riset di masa depan. Praktiknya menyertakan file README yang detail, memberikan lisensi (misal: *Creative Commons*), mencatat *provenance* (asal-usul data).

Kesimpulan

Integritas riset adalah fondasi dari kepercayaan publik dan kemajuan ilmu pengetahuan. Etika bukan sekadar aturan untuk menghindari hukuman, melainkan sebuah komitmen profesional untuk menjunjung tinggi kejujuran, akuntabilitas, dan transparansi. Memahami dan menghindari pelanggaran seperti plagiarisme, fabrikasi, dan falsifikasi adalah kewajiban dasar. Di era sains modern, praktik seperti peer-review yang ketat, kepenulisan yang adil (kriteria ICMJE), dan manajemen data yang baik (prinsip FAIR) menjadi standar. Dengan mematuhi kerangka hukum seperti UU PDP dan menggunakan alat bantu seperti manajer referensi dan Data Management Plan, kita tidak hanya melindungi diri dan institusi, tetapi juga berkontribusi pada ekosistem riset yang sehat, kredibel, dan bermanfaat bagi masyarakat luas.

Etika Profesi Berbasis Risiko dalam Proyek TI

Manajemen Risiko Etika dalam Siklus Hidup Proyek TI

Tujuan

- Memahami konsep *risk-based thinking* pada isu etika sepanjang siklus proyek TI (ide → deploy → retire).
- Mampu mengidentifikasi, menilai, dan memilih perlakuan terhadap risiko etika (legal, reputasi, sosial) menggunakan matriks standar seperti ISO 27005/NIST.
- Menetapkan mekanisme eskalasi & *whistleblowing* bila konflik kepentingan atau pelanggaran terdeteksi.

Agenda

- Mengapa Etika = Risiko?
- Kerangka Kerja & Contoh
- Studi Kasus & Analisis
- Mekanisme Eskalasi

Mengapa Perlu *Risk-Based Ethics*?

Dalam ekonomi digital, kegagalan etika berdampak langsung dan terukur. Pendekatan berbasis risiko menggeser paradigma "etika sebagai beban" menjadi "etika sebagai strategi mitigasi kerugian".

Mengapa Perlu *Risk-Based Ethics*?

Statistik & Konsekuensi Nyata:

- **Denda Regulasi**: Pelanggaran privasi di bawah GDPR (Eropa) atau UU PDP (Indonesia) dapat mengakibatkan denda hingga persentase signifikan dari omzet tahunan global. Contoh: Denda jutaan Euro yang dikenakan pada perusahaan teknologi karena pengumpulan data tanpa persetujuan yang jelas.
- **Kerugian Reputasi**: Sebuah studi oleh IBM (2023) menemukan bahwa biaya rata-rata pelanggaran data adalah $4.45 juta, di mana kehilangan kepercayaan pelanggan dan rusaknya reputasi menjadi faktor biaya terbesar.
- **Retraction & Kepercayaan Publik**: Model AI yang terbukti bias atau tidak adil sering kali harus ditarik dari peredaran (*retraction*). Hal ini tidak hanya membuang biaya riset dan pengembangan, tetapi juga merusak kepercayaan publik terhadap produk dan perusahaan.

Definisi: Risiko Etika vs Risiko Keamanan

Aspek	**Risiko Keamanan (Security Risk)**	**Risiko Etika (Ethical Risk)**
Fokus Utama	Perlindungan aset informasi dari akses tidak sah. Mengacu pada CIA Triad (Confidentiality, Integrity, Availability).	Perlindungan manusia (pengguna, masyarakat, kelompok rentan) dari dampak negatif teknologi, baik yang disengaja maupun tidak.
Sumber Ancaman	Eksternal (hacker, malware) atau internal (kesalahan manusia, pegawai jahat).	Desain sistem itu sendiri, model bisnis, tujuan pengumpulan data, atau bias yang tidak disadari dalam algoritma.
Contoh Kegagalan	Sistem diretas, data pelanggan dicuri dan dijual di web gelap.	Sebuah sistem rekrutmen AI bekerja sempurna sesuai desain, tetapi secara sistematis menolak kandidat perempuan karena dilatih dengan data historis yang bias gender.
Pertanyaan Kunci	"Apakah sistem kita aman dari serangan?"	"Apakah sistem kita, meskipun aman, dapat menyebabkan kerugian, diskriminasi, atau ketidakadilan bagi orang lain?"

Definisi: Risiko Etika vs Risiko Keamanan

RISIKO KEAMANAN	RISIKO ETIKA
Fokus: Melindungi SISTEM	Fokus: Melindungi MANUSIA
Ancaman: Serangan, bug, breach	Ancaman: Desain, model bisnis, bias
Contoh: Data dicuri oleh hacker.	Contoh: AI menolak kandidat kerja karena bias gender.
Pertanyaan: "Apakah sistemnya aman?"	Pertanyaan: "Apakah sistemnya adil & tidak merugikan?"

Kerangka Kerja: Adaptasi Siklus ISO 27005

Menyuntikkan "Titik Etika" dalam Proses Manajemen Risiko

1. **Tetapkan Konteks**
    - Prinsip Etis & Dampak Sosial
2. **Penilaian Risiko (*Assessment*)**
    - Identifikasi Risiko Bias, Privasi, Manipulasi
    - Ukur Dampak pada Manusia
3. **Perlakuan Risiko (*Treatment*)**
    - Pilih Opsi yang Selaras dengan Nilai Etis
4. **Komunikasi & Monitoring**
    - Dokumentasikan dalam Risk Register & Pantau Terus

Kategori Umum Risiko Etika

1. **Bias & Diskriminasi Algoritmik**
    - AI yang tidak adil terhadap kelompok tertentu.
2. **Pelanggaran Privasi & Pengawasan**
    - Pengumpulan data berlebihan dan tidak transparan.
3. **Manipulasi & Desain Adiktif**
    - Dark patterns yang menipu pengguna.
4. **Kurangnya Transparansi (Black Box)**
    - Tidak bisa menjelaskan keputusan AI.
5. **Dampak Sosial & Ekonomi Negatif**
    - Menghilangkan pekerjaan, memperlebar kesenjangan.
6. **Lisensi & Vendor Lock-in**
    - Terjebak secara legal/teknis oleh lisensi software.

Menilai Risiko: Matriks Dampak x Kemungkinan

Seberapa serius risikonya?

- **Dampak (Impact)**: Seberapa parah kerugian jika terjadi? (Finansial, Reputasi, Sosial)
- **Kemungkinan (Likelihood)**: Seberapa sering bisa terjadi?
- **Zona Merah/Oranye (Tinggi/Ekstrem)**: Butuh tindakan segera!

Empat Opsi Perlakuan Risiko (4T)

Opsi	**Deskripsi**	**Kata Kunci**
Mitigate (Mitigasi)	Mengurangi dampak atau kemungkinan risiko.	KURANGI
Transfer (Transfer)	Mengalihkan dampak (biasanya finansial) ke pihak lain.	ALIHKAN
Avoid (Hindari)	Menghentikan aktivitas penyebab risiko.	HENTIKAN
Accept (Terima)	Menerima risiko (hanya untuk dampak sangat rendah).	TERIMA

Jalur Eskalasi & Whistleblowing

Jika Anda Melihat Pelanggaran, Apa yang Harus Dilakukan?

1. **Lapor ke Atasan Langsung**
   - Jalur pertama dan tercepat.
2. **Gagal? Lapor ke Saluran Formal Internal**
   - Komite Etik, HR, atau Legal.
3. **Diabaikan? Gunakan Saluran Whistleblowing**
   - Mekanisme pelaporan anonim dan aman.
4. **Langkah Terakhir (Ancaman Publik): Eskalasi Eksternal**
   - Regulator (Kominfo), Asosiasi Profesi (ACM/IEEE), Media.

Studi Kasus 1: Telemedicine "SehatQ"

- **Produk**: Aplikasi Telemedicine dengan diagnosis AI.
- **Fitur**: Minta akses data kesehatan, lokasi, dan kontak.
- **Model Bisnis**: Gratis dengan iklan dari perusahaan farmasi.

Diskusi:

- Risiko privasi apa yang paling menonjol?
- Bagaimana model bisnisnya dapat menciptakan konflik kepentingan?

Studi Kasus 2: E-Commerce "NusaMarket"

- **AI Rekomendasi:** Personalisasi produk.
- **Dynamic Pricing:** Harga berubah secara real-time.
- **Gig-Economy:** Kurir berstatus "mitra".
- **Kemitraan Data:** Menjual data tren belanja.

Diskusi:

- Identifikasi 4 risiko etika.
- Beri skor pada Matriks Risiko.
- Pilih perlakuan (4T) untuk risiko tertinggi.

Likelihood	Dampak: 1. Tidak Signifikan	2. Minor	3. Moderat	4. Mayor	5. Katastropik
5. Hampir Pasti	Sedang (5)	Tinggi (10)	Tinggi (15)	Ekstrem (20)	Ekstrem (25)
4. Sangat Mungkin	Rendah (4)	Sedang (8)	Tinggi (12)	Tinggi (16)	Ekstrem (20)
3. Mungkin	Rendah (3)	Sedang (6)	Sedang (9)	Tinggi (12)	Tinggi (15)
2. Jarang	Rendah (2)	Rendah (4)	Sedang (6)	Sedang (8)	Tinggi (10)
1. Sangat Jarang	Rendah (1)	Rendah (2)	Rendah (3)	Rendah (4)	Sedang (5)

ID	Deskripsi Risiko	Kategori Risiko	Dampak (1-5)	Likelihood (1-5)	Skor Risiko	Pemilik Risiko	Rencana Perlakuan (4T)	Detail Aksi / Justifikasi
E-004	*Dynamic pricing* menciptakan diskriminasi harga berdasarkan data pengguna (misal: lokasi, riwayat belanja, model perangkat) yang dianggap tidak adil.	Bias & Diskriminasi Algoritmik	4	4	**16 (Tinggi)**	Head of Pricing & Revenue	**Mitigasi**	*Avoid* tidak memungkinkan karena ini adalah fitur inti bisnis. **Aksi:** 1. Tetapkan batas atas dan bawah (floor & ceiling price) yang wajar untuk setiap produk. 2. Keluarkan variabel demografis sensitif dari algoritma. 3. Sediakan transparansi terbatas pada halaman produk ("Harga dapat bervariasi berdasarkan permintaan").
E-005	Model "kemitraan" dengan kurir **mengabaikan hak-hak pekerja** (upah di bawah UMR, tidak ada jaminan sosial/kesehatan), mengarah pada potensi eksploitasi.	Dampak Sosial & Ekonomi	5	3	**15 (Tinggi)**	Head of Logistics (NusaKirim)	**Mitigasi**	*Avoid* akan menghancurkan model bisnis logistik. **Aksi:** 1. Buat skema asuransi kecelakaan & kesehatan yang disubsidi perusahaan. 2. Lakukan audit rutin terhadap algoritma penentu upah untuk memastikan keadilan. 3. Bangun forum komunikasi dua arah (wadah aspirasi) dengan perwakilan mitra kurir.

E-006	Mesin rekomendasi AI menciptakan ***filter bubble***, memanipulasi pengguna untuk perilaku konsumtif dan secara tidak sadar membatasi pilihan mereka.	Manipulasi & Perilaku Adiktif	3	5	**15 (Tinggi)**	Head of Product & AI	**Mitigasi**	Fitur personalisasi sangat penting untuk *engagement*. **Aksi:** 1. Tambahkan tombol/fitur "Lihat Produk Populer Lainnya" yang tidak dipersonalisasi. 2. Berikan pengguna kontrol untuk mengatur ulang atau menonaktifkan sementara histori personalisasi mereka di pengaturan akun.
E-007	**Penjualan data "anonim"** ke pihak ketiga memiliki risiko dapat diidentifikasi ulang (*re-identified*), yang dapat menyebabkan pelanggaran privasi masif.	Pelanggaran Privasi	4	2	**8 (Sedang)**	Chief Data Officer (CDO)	**Terima & Mitigasi**	Risiko diterima karena merupakan sumber pendapatan, namun perlu dimitigasi. **Aksi:** 1. Terapkan teknik anonimisasi yang lebih kuat seperti *Differential Privacy*. 2. Lakukan audit dan *penetration testing* oleh pihak ketiga secara berkala untuk menguji kemungkinan re-identifikasi.

Etika IT di Masa Depan

Dilema Etis di Era Quantum, Web3, dan Metaverse

Tujuan Pembelajaran

1. Mengenal Teknologi Baru dan Bahayanya
2. Menimbang Dampak dari Semua Sisi
3. Membuat Daftar Periksa Etika

The Next Wave: Teknologi Pengubah Dunia

- **Komputasi Kuantum:** Bisa menciptakan komputer super cepat, tapi juga mengancam keamanan data saat ini.
- **Web3 / Blockchain:** Mulai benar-benar digunakan (bukan sekadar tren), namun masih punya masalah soal konsumsi energi dan peraturan yang belum jelas.
- **Metaverse / Spatial Computing:** Inovasi yang masih sangat baru, tujuannya untuk menciptakan cara kita berinteraksi yang benar-benar baru.
- **Neuro-Teknologi:** Teknologi untuk menghubungkan otak manusia langsung dengan komputer, tapi punya risiko sangat besar terhadap privasi.

Quantum & Ancaman 'Q-Day'

- **Q-Day**: Hari di mana komputer kuantum mampu memecahkan enkripsi yang kita gunakan saat ini (RSA, ECC).
- **Algoritma Shor**: "Kunci utama" kuantum yang dapat memecahkan enkripsi modern.
- **Ancaman HNDL (Harvest Now, Decrypt Later)**: Musuh mencuri data terenkripsi sekarang, menyimpannya, lalu mendekripsinya saat Q-Day tiba.

Solusi: Post-Quantum Cryptography (PQC)

Algoritma	**Tipe**	**Basis Matematika**	**Keterangan**
CRYSTALS-Kyber	Enkripsi Kunci (KEM)	Lattice-based	Standar utama untuk enkripsi.
CRYSTALS-Dilithium	Tanda Tangan Digital	Lattice-based	Standar utama untuk otentikasi.
Falcon	Tanda Tangan Digital	Lattice-based	Alternatif tanda tangan digital.
SPHINCS+	Tanda Tangan Digital	Hash-based	Cadangan dengan basis berbeda.

Etika Komputasi Kuantum

Kategori	Manfaat (Potensi Positif)	Bahaya (Potensi Negatif)
Dampak pada Kemajuan & Kesejahteraan (Profit & People)	✅ Penemuan Terobosan: • Akselerasi penemuan obat dan material baru. • Optimalisasi sistem kompleks (logistik, keuangan, riset iklim).	❌ Dekripsi & Peretasan: • Kemampuan membobol hampir semua sistem enkripsi saat ini. • Ancaman terhadap keamanan data finansial, rahasia negara, dan infrastruktur pertahanan.
Dampak pada Prinsip & Masyarakat (People & Principle)	✅ Pemecahan Masalah Global: • Membantu mengatasi perubahan iklim melalui simulasi yang akurat.	❌ Pengawasan Massal: • Potensi untuk menciptakan sistem pengawasan total yang mampu memecahkan semua jenis komunikasi pribadi.

Jejak Karbon Blockchain: PoW vs. PoS

Prinsip Etis: Inovasi harus mempertimbangkan dampak lingkungan.

Fitur	**Proof-of-Work (PoW)**	**Proof-of-Stake (PoS)**
Keamanan	Sangat Tinggi Teruji dan sulit untuk diserang.	Tinggi Keamanan didasarkan pada modal yang dipertaruhkan (staked).
Konsumsi Energi	Sangat Boros Membutuhkan daya komputasi masif (penambangan).	Sangat Efisien Sekitar 99.95% lebih hemat energi dibandingkan PoW.
Cara Kerja	Verifikasi transaksi melalui pemecahan teka-teki matematika yang kompleks.	Verifikasi transaksi oleh validator yang dipilih berdasarkan jumlah aset yang mereka "kunci" atau pertaruhkan.
Contoh Populer	Bitcoin (BTC)	Ethereum (ETH) pasca "The Merge"

Studi Kasus: 'The DAO Hack' (2016)

- **"Code is Law" ... Sampai Kode Itu Cacat**
- **Masalah**: $50 juta dana investasi dicuri karena bug pada kode smart contract yang bersifat immutable (permanen).
- **Dilema Etis**:
    - Apakah melanggar prinsip "kode adalah hukum" dibenarkan untuk menyelamatkan dana pengguna?
    - Siapa yang berhak memutuskan? Ini memicu perpecahan (*hard-fork*) pada jaringan Ethereum.

NFT & Kepemilikan Intelektual (IP)

Saat Beli NFT, Apa yang Sebenarnya kita Beli?

- **Fakta**: NFT adalah sertifikat kepemilikan atas token di blockchain.
- **Miskonsepsi**: kita tidak secara otomatis membeli hak cipta atau hak komersial atas gambar/karya aslinya.
- **Kuncinya**: Selalu periksa lisensi yang melekat pada NFT tersebut.

Arsitektur Metaverse: 3 Lapisan Risiko

1. **Lapisan Hardware (Headset, Haptic Suit)**
    - Risiko: Keamanan biometrik, kesehatan fisik & mental.
2. **Lapisan Platform (Horizon Worlds, Decentraland)**
    - Risiko: Pelecehan, privasi data interaksi, moderasi konten.
3. **Lapisan Ekonomi (Properti Virtual, Avatar, NFT)**
    - Risiko: Penipuan, gelembung spekulatif, perlindungan konsumen.

Isu Kemanusiaan: Pelecehan Avatar

'It's Not Real, But It Feels Real'

- Dampak Imersif: Pelecehan di ruang virtual (serangan verbal, invasi ruang pribadi, sentuhan virtual) memiliki dampak psikologis yang nyata.
- Tantangan:
  - Identitas anonim mempersulit penegakan hukum.
  - Siapa yang bertanggung jawab? Platform? Pengguna?
  - Kelompok rentan (wanita, anak-anak) menjadi target utama.

Neuro-Data: Batas Privasi Terakhir

Pikiran Anda Adalah Data

- **Neuro-data**: Data yang berasal dari aktivitas sistem saraf Anda (sinyal otak, detak jantung).
- **Risiko Etis**:
  - Dekode Pikiran: Menerjemahkan pikiran tanpa persetujuan.
  - Manipulasi Keputusan: Mempengaruhi pilihan Anda secara subliminal.
  - Bias Neurologis: Diskriminasi berdasarkan "pola pikir" saat rekrutmen.
- **Acuan Global**: UNESCO menyerukan perlindungan kebebasan kognitif.

Radar Etis: 10 Pertanyaan Sebelum Memulai Proyek

1. ***Purpose & Necessity***: Adakah tujuan sosial yang jelas?
2. ***Stakeholder Vulnerability***: Siapa yang paling rentan dirugikan?
3. ***Data Longevity & PQ-Threat***: Amankah data ini untuk 30 tahun ke depan?
4. ***Energy & Carbon Footprint***: Berapa jejak karbonnya? PoW?
5. ***Governance / Upgradability***: Bagaimana cara memperbaiki bug atau kesalahan?
6. ***Identity & Consent***: Bagaimana izin (consent) dikelola?
7. ***Financial Fairness***: Apakah ada mekanisme anti-penipuan?
8. ***Bias & Inclusion***: Apakah teknologi ini inklusif untuk semua?
9. ***Redress & Exit***: Bagaimana cara pengguna menyelesaikan sengketa atau keluar?
10. ***Regulatory Alignment***: Apakah sejalan dengan regulasi (EU AI Act, MiCA)?