

Nama : Reifandra Kinadi
Kelas : If 1B-Pagi
NIM : 3312501048

Kode Etik

Kode etik informatika adalah seperangkat prinsip moral yang membimbing perilaku profesional di bidang TI, seperti menjaga kerahasiaan data, tidak menyalahgunakan komputer, tidak mencuri perangkat lunak, dan menghindari kerugian bagi orang lain.

Kode etik dalam profesi informatika mencakup kejujuran, menjaga kerahasiaan data, menghargai hak kekayaan intelektual, dan tidak menggunakan teknologi untuk merugikan orang lain

Prinsip Utama Kode Etik Bidang Informatika

1. Transparansi dan Akuntabilitas

Bertanggung jawab atas Tindakan dan hasil kerja, memastikan transparansi dalam pengembangan dan pengoperasian system.

2. Tidak merugikan orang lain

Menghindari Tindakan yang dapat menyebabkan kerugian fisik, psikis, sabotase sistem, kebocoran data penting atau merusak data orang lain.

3. Tidak mengganggu pekerjaan orang lain

Tidak mengganggu kinerja sistem komputer orang lain tanpa izin.

4. Kejujuran

Tidak membuat sistem yang sengaja menjatuhkan sistem lain untuk keuntungan pribadi dan tidak menyajikan informasi yang tidak akurat.

Beberapa Pelanggaran Kode Etik Bidang Informatika

1. Pembajakan perangkat lunak, film, lagu dan lainnya.
2. Penyebaran berita palsu (hoax).
3. Penyalahgunaan komputer untuk melakukan penipuan atau tindakan lainnya.
4. Pencurian identitas dan penggunaan informasi kartu kredit orang lain tanpa izin.
5. Penyebaran data sensitif atau informasi pribadi tanpa persetujuan pemiliknya.

Tugas-1

Dari pelanggaran tersebut, identifikasi melanggar peraturan ITE No. 1 Tahun 2024 pasal berapa?

Jenis Pelanggaran	Pasal UU ITE (No. 1 Tahun 2024 Yang Terkait)
Pembajakan perangkat lunak, film, lagu dan lainnya.	Tidak secara langsung diatur sebagai "pembajakan hak cipta". Pembajakan software lebih diatur dalam UU Hak Cipta, bukan UU ITE
Penyebaran berita palsu (hoax).	Pasal 28 ayat (1) UU ITE menyebutkan bahwa yang dipidana adalah penyebaran informasi palsu yang menimbulkan kerugian atau keresahan publik.
Penyalahgunaan komputer untuk melakukan penipuan atau tindakan lainnya.	Pasal 30 ayat 1 UU ITE adalah: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun".
Pencurian identitas dan penggunaan informasi kartu kredit orang lain tanpa izin.	Pasal 32 Undang-Undang ITE mengatur tentang larangan mengubah, mengurangi, menambah, menghapus, memindahkan, atau mengakses Informasi dan/atau Dokumen Elektronik milik orang lain atau milik publik secara sengaja dan tanpa hak. Pelanggaran terhadap pasal ini dapat berupa tindakan yang mengakibatkan data rahasia menjadi terbuka dan dapat diakses publik secara tidak semestinya. Sanksi pidananya diatur dalam Pasal 48 UU ITE.
Penyebaran data sensitif atau informasi pribadi tanpa persetujuan pemiliknya.	Sama dengan poin 4: Pasal 32 UU ITE untuk pengungkapan data pribadi.

Tugas-2

Dengan menerapkan konsep pengambilan informasi, carilah kode etik masing-masing profesi di atas dan cantumkan referensi

Pengembangan dan Rekayasa		
Profesi	Kode Etik	Referensi
Software Engineer / Developer	<ol style="list-style-type: none"> 1. Menjaga kepentingan publik 2. Menghasilkan software berkualitas 3. Jujur dalam pekerjaan teknis 4. Menghormati privasi & kerahasiaan data pengguna 	<u>ACM/IEEE – Software Engineering Code of Ethics</u>
Web Developer	<ol style="list-style-type: none"> 1. Membuat situs yang aman dan dapat diakses 2. Tidak menyisipkan malware/backdoor 3. Menghormati hak cipta (assets, fonts, gambar) 	<u>ACM/IEEE Software Engineering Code of Ethics</u>
Game Developer	<ol style="list-style-type: none"> 1. Tidak menciptakan game yang merugikan publik 2. Transparansi dalam monetisasi (lootbox, IAP) 3. Menjaga privasi pemain 	<u>Game Developer Code of Ethics</u>
AI & Machine Learning Engineer	<ol style="list-style-type: none"> 1. Menghindari bias dan diskriminasi AI 2. Transparansi model AI 3. Melindungi data pribadi yang digunakan untuk training 	<u>Principles for Algorithmic Transparency & Accountability</u>

Data dan Analisis		
Profesi	Kode Etik	Referensi
Data Analyst	<ol style="list-style-type: none"> 1. Tidak memanipulasi data 2. Menjaga akurasi dalam interpretasi 3. Menjaga privasi data pengguna 	<u>ACM Code of Ethics</u>

Data Scientist	<ol style="list-style-type: none"> 1. Menggunakan data secara etis 2. Tidak membuat model yang merugikan pengguna 3. Menghindari bias analisis 	<u>Data Science Code of Ethics</u>
Data Engineer	<ol style="list-style-type: none"> 1. Menjaga keamanan pipeline data 2. Memastikan integritas data 3. Tidak menyalahgunakan akses database 	<u>ACM Code of Ethics</u>

Infrastruktur dan Operasional		
Profesi	Kode Etik	Referensi
Cloud Engineer	<ol style="list-style-type: none"> 1. Menjaga keamanan layanan cloud 2. Menjaga kerahasiaan data pelanggan 3. Tidak menyalahgunakan akses root/privileged 	<u>ISACA Code of Professional Ethics</u>
DevOps Engineer	<ol style="list-style-type: none"> 1. Mengembangkan pipeline aman 2. Tidak men-deploy sistem berbahaya 3. Transparansi perubahan sistem 	<u>DevOps Ethics & Principles</u>
System Administrator	<ol style="list-style-type: none"> 1. Tidak menyalahgunakan akses admin 2. Menjaga uptime dan keamanan sistem 3. Menjaga kerahasiaan data user 	<u>SAGE / USENIX System Administrators Code of Ethics</u>
IT Support / Help Desk / IT Maintenance	<ol style="list-style-type: none"> 1. Tidak membuka file pribadi user tanpa izin 2. Profesional & sopan 3. Melaporkan pelanggaran keamanan 	<u>Help Desk Institute Code of Ethics</u>

Lainnya		
Profesi	Kode Etik	Referensi
Cybersecurity Analyst	<ol style="list-style-type: none"> 1. Tidak menyalahgunakan kerentanan 2. Melakukan ethical hacking sesuai izin 3. Melindungi sistem & data 	<u>Cybersecurity Code of Ethics</u>
UX/UI Designer	<ol style="list-style-type: none"> 1. Mendesain antarmuka yang inklusif & ramah pengguna 	<u>UI/UX Professional Code of Ethics</u>

	2. Tidak menipu (dark patterns) 3. Menjaga privasi data pengguna	
Business Intelligence	1. Mengolah data secara akurat 2. Tidak memanipulasi insight demi keuntungan pribadi 3. Menjaga kerahasiaan data perusahaan	ACM Code of Ethics

Tugas-3

Dari contoh-contoh tersebut, tuliskan pengalaman Anda dalam menegakkan prinsip moral untuk menjaga etika bidang IT.

- 1. Tidak menggunakan akun yang terhubung dengan computer lab kampus.
- 2. Tidak menyebarkan foto sensitif teman.
- 3. Tidak meretas akun teman yang sedang terhubung dengan laptop saya.
- 4. Tidak membuka HP teman tanpa izin.
- 5. Tidak membuka aplikasi yang bersifat privasi, misalnya whatsapp, Instagram, facebook dll.

Tugas-4

Menggunakan konsep pencarian informasi di internet, carilah etika profesi menurut IPKIN, cantumkan link terkait data yang Anda peroleh!

Jawab :

IPKIN adalah organisasi profesi bidang komputer dan informatika yang berdiri sejak tahun 1974. Sebagai organisasi profesi, IPKIN menetapkan prinsip-prinsip etika yang harus dipatuhi oleh seluruh profesional IT di Indonesia. Etika ini dibuat untuk memastikan setiap pekerja IT bekerja secara profesional, bertanggung jawab, dan menjaga integritas dalam penggunaan teknologi.

Berdasarkan hasil pencarian dari modul resmi dan referensi pendidikan terkait IPKIN, etika profesi IPKIN mencakup prinsip-prinsip berikut:

1. Tanggung Jawab Terhadap Masyarakat
 - a) Tidak menyebarkan malware, hoax, atau konten merusak.
 - b) Menggunakan kompetensi untuk hal positif dan konstruktif.

2. Kejujuran dan Integritas

- a) Tidak memalsukan data atau sertifikasi.
- b) Tidak melakukan plagiarisme program / software.
- c) Tidak menyalahgunakan akses sistem.

3. Menjaga Kerahasiaan Informasi

- a) Data pribadi pengguna
- b) Rahasia Perusahaan
- c) Informasi sensitif yang diakses selama bekerja

4. Kompetensi Profesional

Profesional harus bekerja sesuai kemampuan, terus mengembangkan ilmu, dan tidak menerima pekerjaan di luar keahlian yang dapat membahayakan sistem atau pengguna.

5. Tanggung Jawab Terhadap Profesi

- a) Tidak melakukan tindakan yang mencoreng profesi
- b) Mematuhi standar professional
- c) Menghargai hasil karya dan hak cipta orang lain

6. Menghormati Pengguna dan Klien

- a) Transparan
- b) Tidak menipu
- c) Tidak memberikan layanan palsu
- d) Memberikan solusi yang tepat sesuai kebutuhan

Referensi (Sumber Pencarian Internet)

1. Modul Etika Profesi TIK Universitas Nusa Mandiri

<https://repository.nusamandiri.ac.id/repo/files/236268/download/Modul-Etika-Profesi-TIK.pdf>

2. Modul Etika Profesi Komputer Flipbook

https://fliphmtl5.com/lpkm/qosw/MODUL_ETIKA_PROFESI_KOMPUTER/

3. Etika Komputer UGM (referensi terkait peran IPKIN dalam etika profesi)

<https://ayukhusnulkhotimah.web.ugm.ac.id/2018/04/12/etika-komputer/>

Tugas-5

Masing-masing Isu tersebut di atas: Carilah masing-masing 1 contoh kasus yang Anda temui di media sosial (mungkin sudah viral) dan bagaimana penyelesaian masalah yang sudah dilakukan oleh pemerintah

Kejahatan Komputer

Kasus: Pencurian Data & Peretasan PDNS 2024 (Viral di X, TikTok, Instagram)

Pada tahun 2024, server PDNS (Pusat Data Nasional Sementara) diretas oleh kelompok hacker BrainCipher menggunakan ransomware "Brain Chiper". Data pelayanan pemerintah ikut terdampak (KTP, layanan imigrasi, BPJS, dan lain-lain).

Penyelesaian oleh Pemerintah:

1. Pemerintah membentuk Satgas Penanganan Ransomware PDNS (Kominfo, BSSN, BIN, Polri).
2. Server dipulihkan dengan backup dan sistem pemulihan darurat.
3. Penyidikan dilakukan untuk melacak pelaku dan menemukan titik kebocoran.
4. Pemerintah memperketat sistem keamanan nasional dan mempercepat pembangunan Pusat Data Nasional Baru.
5. Edukasi keamanan siber untuk instansi diperketat.

Cyber Ethics

Kasus: BRI Life (2021) Kebocoran Data Nasabah

1. Diduga ada kebocoran data sekitar 2 juta nasabah BRI Life.
2. Data yang bocor sangat sensitif: foto KTP, NPWP, akta kelahiran, rekam medis, foto buku tabungan, dan sebagainya.
3. Pelaku menawarkan data tersebut di forum online, dengan harga sekitar US\$ 7.000 (sekitar Rp 101 juta).
4. Ada klaim bahwa hacker memperoleh akses dengan menembus komputer karyawan BRI Life dan bahkan karyawan Bank BRI.
5. BRI Life menyatakan bahwa sistem yang dibobol adalah sistem syariah mereka ("stand-alone system").

Penanganan oleh Pemerintah / Lembaga Terkait

1. Kominfo

- a) Kominfo memanggil Direksi BRI Life untuk klarifikasi soal dugaan kebocoran data.
 - b) Kominfo menyelidiki sistem elektronik BRI Life dan menemukan indikasi “celah keamanan” di sistem mereka.
 - c) Kominfo juga menyatakan akan bekerja sama dengan BSSN (Badan Siber dan Sandi Negara) untuk mengevaluasi dan memperkuat keamanan sistem BRI Life.
2. Polri (Bareskrim)
 - a) Bareskrim Polri menyelidiki dugaan kebocoran data tersebut melalui Direktorat Tindak Pidana Ekonomi Khusus (Dittipideksus).
 - b) Ini menunjukkan bahwa kasus dianggap potensi kejahatan siber (data breach), bukan sekadar insiden teknis.
 3. Ajakan Pengesahan RUU Perlindungan Data Pribadi
 - a) Kasus ini digunakan sebagai argumen publik dan oleh DPR / anggota legislatif agar RUU Perlindungan Data Pribadi (PDP) segera disahkan.
 - b) Karena insiden seperti ini menggarisbawahi lemahnya regulasi perlindungan data pribadi di Indonesia.
 4. Investigasi Internal oleh BRI Life
 - a) BRI Life menyatakan bahwa mereka sedang melakukan investigasi mendalam: mengajak tim forensik siber independen untuk menelusuri “jejak digital”.
 - b) Mereka menyatakan komitmen untuk memperbaiki tata kelola TI dan data (information governance) agar lebih aman dan sesuai peraturan.

E-Commerce

Kasus: Kebocoran Data Tokopedia (91 Juta Akun)

1. Sekitar 91 juta data akun Tokopedia dilaporkan bocor dan dijual di dark web/RaidForums.
2. Data yang bocor termasuk: nama lengkap, email, nomor HP, tanggal lahir, username, tanggal daftar, dan beberapa lainnya.
3. Data semula dilaporkan “hanya” 15 juta, tetapi pelaku klaim punya data 91 juta.
4. Data tersebut ditawarkan dengan harga ~US\$ 5.000 (sekitar Rp 73–74 juta).
5. Link unduhan data 91 juta akun sempat dibagikan di grup Facebook dan bisa diakses beberapa waktu.

Penanganan oleh Pemerintah / Lembaga Terkait

1. Pemeriksaan oleh Polri

- a) Polri, lewat Direktorat Siber, memeriksa 3 ahli IT internal Tokopedia terkait kebocoran data tersebut.
 - b) Analisis forensik digital dilakukan: memeriksa anomali IP, jejak akses, dan potensi pelanggaran keamanan.
2. Tanggapan Tokopedia
 - a) Tokopedia mengakui ada “upaya pencurian data” tetapi menyatakan bahwa password pengguna masih aman karena terenkripsi.
 - b) Tokopedia menyarankan pengguna untuk mengganti password secara berkala demi menjaga keamanan.
 3. Peran Kominfo
 - a) Kominfo memanggil direksi Tokopedia untuk menjelaskan dugaan kebocoran data.
 - b) Ada dorongan publik dan dari pakar keamanan siber agar RUU Perlindungan Data Pribadi (PDP) segera disahkan agar ada dasar hukum kuat untuk menindak kebocoran data seperti ini.

Pelanggaran Hak atas Kekayaan Intelektual

Kasus: Penutupan IndoXXI (Pembajakan Film)

Salah satu kasus pelanggaran HKI yang paling viral di Indonesia adalah IndoXXI, situs yang membagikan film bajakan secara gratis.

1. Bentuk Pelanggaran
 - a) Menyediakan film, drama, dan serial tanpa izin dari pemegang hak cipta.
 - b) Mendistribusikan ulang konten berhak cipta secara ilegal.
 - c) Menyebabkan kerugian besar pada industri film dan platform streaming legal.
2. Mengapa Kasus Ini Viral?
 - a) IndoXXI sangat populer di media sosial.
 - b) Banyak netizen mengeluhkan pemblokirannya ketika pemerintah bertindak.
 - c) Kasusnya menjadi trending karena jutaan orang pernah memakai situs tersebut.

Penanganan Pemerintah

Pemerintah Indonesia melalui Kominfo, Kepolisian, dan pemilik hak cipta melakukan beberapa langkah:

1. Pemblokiran Situs Secara Nasional
 - a) Sejak 2020, pemerintah **memblokir puluhan domain IndoXXI**.

- b) Semua ISP di Indonesia (Telkomsel, Indihome, XL, dll) diwajibkan memutus akses.
2. Tindakan Hukum terhadap Pengelola
 - a) Aparat melakukan penyelidikan terhadap pembuat server dan pengelola situs.
 - b) Beberapa operator situs mirror ditangkap berdasarkan:
 - 1) UU 28 Tahun 2014 tentang Hak Cipta
 - 2) UU ITE Pasal 32 dan 48 (distribusi konten ilegal)
 3. Takedown Konten & Domain Mirror
 - a) Pemerintah bekerja sama dengan interpol dan penyedia hosting luar negeri untuk:
 - 1) Menghapus domain tiruan
 - 2) Memutus server streaming illegal
 4. Edukasi Publik dan Kampanye Anti Pembajakan
 - a) Kampanye besar-besaran: "**Stop Nonton Film Bajakan**"
 - b) Kerja sama dengan:
 - 1) Asosiasi Produser Film Indonesia
 - 2) Platform legal (Netflix, Vidio, Disney+)
 - 3) Komunitas creator
 5. Penegakan Sistem "Trusted Copyright Enforcement"
 - a) Sistem digital pemerintah untuk mempercepat:
 - 1) Laporan
 - 2) Takedown
 - 3) Pemantauan konten berhak cipta di internet