

BAB VI ETIKA DAN PRIVASI DIGITAL

Tujuan Pembelajaran (*Chapter IV Learning Objectives*)

Menjelaskan pengertian Etika Digital

Mengidentifikasi ruang lingkup Etika dalam penggunaan TIK

Menyebutkan contoh pelanggaran Etika dalam penggunaan TIK

Memahami ruang lingkup Privasi Digital

Memahami ruang lingkup Netiket

Memahami konsep keamanan data

Menerapkan Etika dan Privasi Digital

A. Pengertian Etika Digital

Etika (*ethic*) bermakna sekumpulan azaz atau nilai yang berkenaan dengan akhlak, tata cara (adat, sopan santun) mengenai benar dan salah tentang hak dan kewajiban yang dianut oleh suatu golongan atau masyarakat. Sedangkan era digital merupakan istilah yang digunakan dalam kemunculan digital, jaringan internet khususnya teknologi informasi komputer (TIK). Oleh karena itu apabila ingin membahas mengenai etika digital maka kita juga perlu mengetahui pengertian dari TIK. TIK dalam konteks yang lebih luas, merangkum semua aspek yang berhubungan dengan mesin (komputer dan telekomunikasi) dan teknik yang digunakan untuk menangkap (mengumpulkan), menyimpan, memanipulasi, menghantarkan, dan menampilkan suatu bentuk informasi. Komputer yang mengendalikan semua bentuk ide dan informasi memainkan peranan penting dalam pengumpulan, pemrosesan, penyimpanan dan penyebaran informasi suara, gambar, teks, dan angka yang berdasarkan mikroelektronik. Berdasarkan pengertian tersebut maka dalam penggunaan TIK dapat disimpulkan sebagai sekumpulan azaz atau nilai yang berkenaan dengan akhlak, tata cara, (adat, sopan santun) nilai mengenai benar dan salah, hak dan kewajiban tentang pemanfaatan TIK melalui media online dan digital. Untuk menerapkan etika digital, diperlukan terlebih dahulu mengenal dan memaknai prinsip yang terkandung di dalam TIK di antaranya adalah :

1. Tujuan teknologi informasi memberikan bantuan kepada manusia untuk menyelesaikan masalah, menghasilkan kreativitas, membuat manusia lebih berkarya jika tanpa menggunakan teknologi informasi dalam aktivitasnya.

2. Prinsip *High-tech-high-touch* : jangan memiliki ketergantungan kepada teknologi tercanggih tetapi lebih penting adalah meningkatkan kemampuan aspek "*high touch*" yaitu "manusia".
3. Sesuaikan teknologi informasi kepada manusia : seharusnya teknologi informasi dapat mendukung segala aktivitas manusia bukan sebaliknya manusia yang harus menyesuaikan kepada teknologi informasi.

B. Ruang Lingkup Etika Digital

Etika digital tidak dapat dipisahkan dari permasalahan-permasalahan seputar penggunaan TIK. Beberapa ruang lingkup atau isu yang terkait dengan Etika meliputi: keamanan komputer, kejahatan dunia maya, privasi digital, netiket, pelanggaran HAKI (Hak Atas Kekayaan Intelektual) dan tanggung jawab profesi. Berikut penjelasan masing-masing ruang lingkup:

1. Keamanan Komputer

Keamanan komputer, juga dikenal sebagai *cybersecurity* atau keamanan Teknologi Informasi, adalah perlindungan sistem informasi dari pencurian atau kerusakan pada perangkat keras, perangkat lunak, dan informasi pada sistem komputer tersebut, serta dari gangguan atau kesalahan dari layanan yang diberikan.

2. Kejahatan dunia Maya (Cyber Crime)

Kejahatan dunia maya, juga disebut kejahatan komputer, adalah penggunaan komputer sebagai instrumen untuk tujuan ilegal. Kejahatan dunia maya terus berkembang seiring dengan kemajuan teknologi komputer saat ini. Beberapa jenis kejahatan dunia maya meliputi Denial of Services (melumpuhkan layanan sebuah sistem komputer), penyebaran virus, spam, *carding* (pencurian data kartu), dan lain lain.

3. Privasi Digital

Privasi digital adalah ketika seseorang menggunakan internet dan perangkat yang terhubung tanpa mengorbankan informasi yang dimiliki. Setiap pengguna memiliki tingkat kenyamanan yang berbeda dalam hal privasi digital. Privasi Digital mencakup tiga sub-kategori terkait yaitu privasi informasi, privasi komunikasi, dan privasi individu.

4. Netiket

Internet merupakan aspek penting dalam perkembangan teknologi komputer. Internet merupakan sebuah jaringan yang menghubungkan komputer di dunia sehingga komputer dapat mengakses satu sama lain. Internet menjadi peluang baru dalam perkembangan bisnis, pendidikan, kesehatan, layanan pemerintah dan bidang-bidang lainnya. Melalui internet, interaksi manusia dapat dilakukan tanpa harus bertatap muka. Tingginya tingkat pemakaian internet di dunia melahirkan sebuah aturan baru di bidang internet yaitu netiket. Netiket merupakan sebuah etika acuan dalam berkomunikasi menggunakan internet. Standar netiket ditetapkan oleh IETF (The Internet Engineering Task Force), sebuah komunitas internasional yang terdiri dari operator, perancang jaringan dan peneliti yang terkait dengan pengoperasian internet.

5. Pelanggaran HaKI

Hak kekayaan intelektual sama dengan hak atas sesuatu “benda” yang berasal dari otak. Pasal 499 KUH Perdata : “menurut paham undang-undang yang dimaksud dengan benda ialah tiap-tiap barang dan tiap-tiap hak yang dapat dikuasai oleh hak milik.” Konsekuensi dari batasan hak atas kekayaan intelektual (HAKI) ini adalah, terpisahnya antara hak atas kekayaan intelektual itu dengan hasil material yang menjadi bentuk jelmaannya. Yang dilindungi dalam kerangka hak atas kekayaan intelektual adalah haknya, bukan invensi dari hak tersebut. Namun demikian, dengan adanya berbagai kemudahan yang ditawarkan oleh internet menyebabkan terjadinya pelanggaran HaKI seperti pembajakan program komputer, penjualan program ilegal dan pengunduhan ilegal.

6. Tanggung Jawab Profesi

Seiring perkembangan teknologi, para profesional di bidang komputer sudah melakukan spesialisasi bidang pengetahuan dan sering kali mempunyai posisi yang tinggi dan terhormat di kalangan masyarakat. Maka dari itu mereka memiliki tanggung jawab yang tinggi, mencakup banyak hal dari konsekuensi profesi yang dijalannya. Para profesional menemukan diri mereka dalam hubungan profesionalnya dengan orang lain. Mencakup pekerja dengan pekerjaan, klien dengan profesional, profesional dengan profesional lain, serta masyarakat dengan profesional.

Banyak perkembangan teknologi yang sekarang ini ada di sekitar kita dan sudah menjadi bahan pokok yang tidak bisa dipisahkan dari kehidupan manusia. Tetapi dari perkembangan tersebut pasti juga membawa dampak negatif serta mendatangkan suatu kesempatan terutama bagi pihak-pihak yang bertujuan menyalahgunakannya untuk kepentingan/keuntungan pribadi, untuk itu diperlukan pemahaman mendalam mengenai etika komputer dan tanggung jawab profesi yang berlaku.

C. Contoh Pelanggaran Etika dalam Penggunaan TIK

1. Keamanan Komputer

Keamanan komputer pada dasarnya adalah perlindungan terhadap sistem komputer dan informasi dari bahaya, pencurian, dan penggunaan yang tidak sah. Mekanisme ini adalah proses mencegah dan mendeteksi penggunaan sistem komputer secara tidak sah oleh pihak lain. Seringkali terdapat istilah yang hampir sama dengan keamanan komputer seperti keamanan informasi dan keamanan siber. Salah satu cara untuk memastikan persamaan dan perbedaan di antara istilah-istilah ini adalah dengan membedakan aspek yang dijamin keamanannya.

- a. Keamanan informasi mengamankan informasi dari akses, modifikasi dan penghapusan oleh pihak yang tidak berwenang.
- b. Keamanan Komputer berarti mengamankan mesin komputer dengan cara selalu mengupdate dan memperbaiki sistem bila ada kerusakan sistem.
- c. Keamanan siber didefinisikan sebagai melindungi sistem komputer yang terhubung ke jaringan komputer.

Keamanan komputer terutama berkaitan dengan tiga hal utama, meliputi: (a) Kerahasiaan (Confidentiality) memastikan bahwa informasi hanya tersedia untuk audiens yang dituju; (b) Integritas (Integrity) melindungi informasi agar tidak dimodifikasi oleh pihak yang tidak berwenang; (c) Ketersediaan (Availability) melindungi informasi agar tidak dimodifikasi oleh pihak yang tidak berwenang.

Seperti yang telah dijelaskan di atas, keamanan komputer pada dasarnya adalah perlindungan terhadap ancaman keamanan. Ancaman keamanan komputer adalah bahaya yang mungkin dapat menghambat fungsi normal komputer Anda. Di zaman sekarang, ancaman terus meningkat ketika dunia menjadi digital.

Jenis ancaman keamanan komputer yang berbahaya adalah:

a. Virus

Virus komputer adalah program jahat yang dimuat ke komputer pengguna tanpa sepengetahuan pengguna. Virus ini mereplikasi dirinya sendiri dan menginfeksi file dan program pada PC pengguna. Tujuan utama virus adalah memastikan bahwa komputer korban tidak akan pernah dapat beroperasi dengan baik atau bahkan berhenti sama sekali.

b. Worm (Cacing Komputer)

Worm adalah suatu program yang dapat menyalin dirinya sendiri dari satu komputer ke komputer lain, tanpa memerlukan interaksi manusia. Risiko potensial di sini adalah akan menghabiskan ruang hard disk komputer karena worm dapat mereplikasi dalam volume yang banyak dan dengan kecepatan yang tinggi.

c. Phishing

Caranya adalah dengan mengaku sebagai orang atau pihak bisnis yang dapat dipercaya, phisher berusaha mencuri informasi keuangan atau informasi pribadi yang sensitif melalui email palsu atau pesan instan. Perilaku phishing ini sangat mudah dijalankan. Pengguna dapat diperdaya dan yakin bahwa itu adalah surat yang sah dan kemudian dapat memasukkan informasi pribadi yang diinginkan oleh phiser.

d. Botnet

Botnet adalah komputer yang tergabung dalam jaringan botnet untuk menjalankan perintah atau instruksi yang diberikan oleh penggerak botnet (bot herder atau bot master) yang dilakukan secara remote. Botnet sendiri adalah gabungan dari robot dan network atau lebih mudahnya aplikasi bot yang terkonfigurasi sehingga dapat berjalan otomatis dalam suatu jaringan. Apabila komputer terinfeksi botnet, maka saat komputer tersebut terhubung ke jaringan, komputer akan menjalankan instruksi yang diberikan oleh bot master.

e. Rootkit

Rootkit adalah program komputer yang dirancang untuk memberikan akses istimewa (unauthorized user) ke komputer sambil secara aktif menyembunyikan keberadaan proses tertentu, registry keys atau program tertentu dari proses deteksi malware. Setelah rootkit terinstal maka pengontrol rootkit akan dapat mengeksekusi file dari jarak jauh dan mengubah konfigurasi sistem pada mesin host.

f. Keylogger

Keylogger juga dikenal sebagai logger keystroke, keyloggers dapat melacak aktivitas real-time pengguna di komputer yang dijalankan. Mekanisme ini menyimpan catatan semua penekanan tombol yang dibuat di keyboard pengguna. Keylogger juga merupakan ancaman yang sangat kuat untuk mencuri kredensial masuk orang seperti nama pengguna dan kata sandi.

2. Kejahatan dunia maya

Kejahatan dunia maya, atau kejahatan yang berorientasi pada komputer, adalah kejahatan yang melibatkan komputer dan jaringan (Moore, 2005). Komputer mungkin digunakan untuk melakukan kejahatan, atau bisa juga menjadi sasaran (Warren, 2002). Kejahatan dunia maya dapat mengancam keamanan finansial seseorang atau suatu negara. Beberapa contoh kejahatan dunia maya:

a. *Cyberbullying*

Cyberbullying mengacu pada semua jenis pelecehan secara online, termasuk menguntit, pelecehan seksual, doxing (mengekspos informasi pribadi seseorang, seperti alamat rumah secara online tanpa persetujuan mereka), dan fraping (membobol media sosial seseorang dan membuat posting palsu atas nama mereka)

b. *Cryptojacking*

Cryptojacking adalah ketika peretas masuk ke perangkat user asli dan menggunakannya untuk menambang cryptocurrency tanpa sepengetahuan atau persetujuan user asli. Cryptominers melakukan ini dengan menggunakan JavaScript untuk menginfeksi perangkat user setelah user tersebut mengunjungi situs web yang terinfeksi.

c. *Cyberextortion*

Cyberextortion adalah versi digital dari pemerasan. Salah satu bentuk yang paling umum adalah ransomware, ketika peretas menginfeksi komputer Anda dengan malware yang mengenkripsi semua file Anda sampai Anda membayar uang tebusan untuk membukanya. Cyberextortion juga dapat merujuk pada pemerasan korban menggunakan informasi pribadi, foto, dan video mereka; atau mengancam bisnis yang menggunakan metode seperti serangan DDoS yang digerakkan oleh botnet.

d. *Cyberespionage*

Seperti yang disebutkan, banyak penjahat cyber hari ini sebenarnya adalah kelompok yang disponsori negara. Apakah itu orang Korea Utara, Iran, atau bahkan AS Equation Group yang berafiliasi dengan NSA, kekuatan dunia menggunakan kelompok peretas sebagai salah satu senjata dalam matriks rumit politik global. Mencuri rahasia intelijen dan menggunakan malware untuk menyerang pembangkit nuklir hanyalah dua cara di mana kelompok yang disponsori negara dapat melakukan beberapa hal menakutkan di panggung dunia.

Maraknya kejahatan dunia maya yang terjadi belakangan ini, selain menjadi perhatian juga perlu diupayakan penanggulangannya. Beberapa upaya penanggulangan yang bisa dilakukan adalah: (1) Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut. (2) Meningkatkan sistem pengamanan jaringan computer nasional sesuai standar internasional. (3) Meningkatkan pemahaman serta keahlian aparaturnya mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cybercrime*. (4) Meningkatkan kesadaran warga negara mengenai masalah *cybercrime* serta pentingnya mencegah kejahatan tersebut terjadi. (5) Meningkatkan kerjasama antar Negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cybercrime*, antara lain melalui perjanjian ekstradisi dan *mutual assistance treaties*.

D. Pengertian dan Ruang Lingkup Privasi Digital

Privasi Digital adalah definisi kolektif yang mencakup tiga sub-kategori terkait; privasi informasi, privasi komunikasi, dan privasi individu. Istilah ini sering digunakan dalam konteks hak privasi konsumen di ranah digital, dan biasanya digunakan dalam praktik bisnis dari banyak pemasar/bisnis/perusahaan untuk mengumpulkan dan menggunakan data dan informasi.

1. Privasi informasi, adalah gagasan bahwa individu harus memiliki kebebasan, atau hak, untuk menentukan bagaimana informasi digital mereka, terutama yang berkaitan dengan informasi yang dapat diidentifikasi secara pribadi, dikumpulkan dan digunakan. Uni Eropa memiliki berbagai undang - undang yang mengatur bagaimana informasi dapat dikumpulkan dan digunakan oleh perusahaan.

Beberapa dari undang-undang tersebut ditulis untuk memberikan agensi pada preferensi individu/konsumen dalam bagaimana data mereka digunakan. Di tempat lain, seperti di Amerika Serikat, undang-undang privasi dianggap oleh beberapa orang kurang berkembang. Sebagai contoh, beberapa undang-undang memungkinkan perusahaan untuk mengatur sendiri pengumpulan dan penyebaran informasi konsumen mereka sehingga konsumen tidak memiliki privasi sepenuhnya.

2. Privasi komunikasi adalah pengertian bahwa individu harus memiliki kebebasan, atau hak, untuk mengkomunikasikan informasi secara digital dengan harapan bahwa komunikasi mereka aman; yang berarti bahwa pesan dan komunikasi hanya akan dapat diakses oleh penerima asli pengirim. Namun, komunikasi dapat disadap atau dikirim ke penerima lain tanpa sepengetahuan pengirim, dengan berbagai cara. Komunikasi dapat disadap secara langsung melalui berbagai metode peretasan. Komunikasi juga dapat dikirim ke penerima tanpa sepengetahuan pengirim yang disebabkan platform atau media yang digunakan untuk mengirim informasi. Contoh dari ini adalah kegagalan untuk membaca kebijakan privasi perusahaan mengenai komunikasi di platform mereka dapat menyebabkan seseorang menganggap komunikasi mereka dilindungi padahal sebenarnya tidak. Selain itu, perusahaan sering kali diketahui kurang transparan dalam menggunakan informasi, ini bisa disengaja dan tidak disengaja.
3. Privasi individu adalah gagasan bahwa individu memiliki hak untuk hidup bebas di internet, dalam arti bahwa mereka dapat memilih jenis informasi apa yang mereka hadapi, dan yang lebih penting bahwa informasi yang tidak diinginkan tidak boleh mengganggu mereka. Contoh pelanggaran digital terhadap privasi individu adalah pengguna internet yang menerima iklan dan email/spam yang tidak diinginkan, atau virus komputer yang memaksa pengguna untuk melakukan tindakan yang sebaliknya tidak akan mereka lakukan. Dalam kasus seperti itu, individu, pada saat itu, tidak ada secara digital tanpa gangguan dari informasi yang tidak diinginkan, sehingga privasi individu mereka telah dilanggar.

TIK yang dapat menghantarkan dunia yang tidak bisa dibatasi oleh ruang dan waktu dapat menimbulkan masalah bagi privasi seseorang atau lembaga. Metode dapat dengan sengaja dibuat untuk mendapatkan informasi pribadi seseorang secara ilegal yang menyebabkan pelanggaran privasi dan informasi. Serangan terarah ini biasanya disebut sebagai peretasan, meskipun istilah itu merujuk pada praktik umum dan tidak membahas metode dan penerapan peretasan tertentu. Karena berkenaan dengan niat, dalam peretasan ada dua kategori invasi: (1) Serangan terarah terhadap seseorang secara individu, dan (2) Serangan terarah terhadap kelompok. Untuk kategori kedua, seorang hacker dapat secara efektif memperoleh informasi tertentu/individu tertentu dengan terlebih dahulu menargetkan kelompok yang lebih besar. Contoh kemungkinan ini adalah sebagai berikut: Jika seorang peretas, bernama individu-A, ingin mendapatkan informasi orang tertentu terhadap individu-B, maka dapat terlebih dahulu menargetkan platform atau grup yang memiliki informasi mengenai individu-B seperti agen kredit, atau mereka juga dapat menargetkan grup yang sebelumnya telah diserahkan/memberikan datanya oleh individu-B, seperti jaringan media sosial atau layanan data berbasis cloud. Melalui penargetan salah satu grup tersebut, individu-A dapat secara efektif memperoleh informasi individu-B dengan terlebih dahulu meretas semua data yang dimiliki grup tersebut, termasuk data individu lain. Setelah diperoleh, peretas dapat dengan mudah mengidentifikasi informasi individu-B dalam data dan mengabaikan yang lainnya.

E. Pengertian dan Ruang Lingkup Netiket

Netiket atau Netiquette merupakan Etika dalam menggunakan Internet. Internet sebagai sebuah kumpulan komunitas, diperlukan aturan yang akan menjadi acuan orang-orang sebagai pengguna Internet, dimana aturan ini menyangkut batasan dan cara yang terbaik dalam memanfaatkan fasilitas Internet. Berikut contoh netiket:

a. Netiket pada *one to one communications*

Yang dimaksud dengan *one to one communications* adalah kondisi dimana komunikasi terjadi antar individu “face to face” dalam sebuah dialog. Contoh dari Netiket pada *one to one communications* adalah berkomunikasi via *e-mail*.

Hal-hal yang perlu diperhatikan dalam mengirim email meliputi:

1) Jangan terlalu banyak mengutip

Jika harus mengutip pesan seseorang dalam jawaban e-mail, usahakan menghapus bagian-bagian yang tidak perlu, dan hanya menjawab bagian yang relevan saja. Pesan yang terlalu panjang memakan file yang besar yang membuat loading semakin lama.

2) Perlakukan e-mail secara pribadi

Jika seseorang mengirim informasi atau gagasan kepada anda secara pribadi (*private message*), Anda tidak sepatutnya mengirim/menjawabnya kembali ke dalam forum umum, karena pada dasarnya email adalah pesan pribadi.

3) Hati-hati dalam menggunakan huruf kapital

Karena penggunaan karakter huruf bisa dianalogikan dengan suasana hati si penulis. Huruf kapital mencerminkan penulis yang sedang emosi, marah atau berteriak. Walau begitu, ada kalanya huruf kapital dapat digunakan untuk memberi penegasan maksud. Tapi yang harus dicatat, gunakanlah penegasan maksud ini secukupnya saja, satu-dua kata dan jangan sampai seluruh kalimat/paragraf.

4) Jangan membicarakan orang lain

Jangan membicarakan orang atau pihak lain, apalagi kejelekannya. Berhati-hatilah terhadap apa yang ditulis. E-mail mempunyai fasilitas yang bernama "Forward", yang mengijinkan si penerima untuk meneruskan pesan tersebut kepada orang lain.

5) Jangan menggunakan CC (*carbon copy*)

Jika ingin mengirim email ke sejumlah orang (misalnya di *mailing-list*), jangan cantumkan nama-nama pada kolom CC, jika kita melakukan hal tersebut semua orang yang menerima email kita bisa melihat alamat-email orang lain. Umumnya seseorang tidak suka jika alamat emailnya dibeberkan didepan umum. Selalu gunakan BCC (Blind Carbon Copy), dengan cara ini setiap orang hanya bisa melihat alamat emailnya sendiri.

b. Netiket pada *one to many communications*

Konsep komunikasi *one to many communications* adalah bahwa satu orang bisa berkomunikasi kepada beberapa orang sekaligus. Hal itu seperti yang terjadi pada *mailing list* dan *net news*. Etika berinternet (netiket) bagi pengguna mailing list atau netnews antara lain adalah sebagai berikut :

- 1) Baca terlebih dahulu *mailing list* atau *netnews* satu atau dua bulan data diskusi, sebelum memutuskan untuk melakukan posting surat pertama kali kepada mailing list tersebut. Hal ini akan membantu kita untuk mengerti lingkungan mailing list yang akan kita masuki.
- 2) Tidak menyalahkan moderator atau pengurus system menyangkut perilaku yang dilakukan oleh anggota system tersebut.
- 3) Berhati-hatilah dengan kata-kata yang akan ditulis, karena kata-kata tersebut dapat diakses oleh orang banyak dan akan disimpan dalam waktu yang lama.
- 4) Jika dalam melakukan komunikasi terjadi selisih paham atau perdebatan secara pribadi dengan peserta lain, sebaiknya perdebatan dilanjutkan melalui jalur pribadi. Jika memang poin perdebatan perlu dikonsumsi publik, maka berikanlah ringkasan hasil diskusi.
- 5) Tidak etis dan tidak diperbolehkan mengirim teks yang berbau SARA, mengingat bahwa anggota yang berada pada komunitas memiliki budaya, lifestyle serta keyakinan yang berbeda-beda

c. *Information services*

Pada perkembangan internet, terdapat fasilitas dan berbagai layanan baru yang disebut layanan informasi (*information service*). Berbagai jenis layanan ini antara lain seperti *Gopher*, *Wais*, *Word Wide Web (WWW)*, *Multi-User Dimensions (MUDs)*, *Multi-User Dimensions which are object Oriented (MOOs)*, dll. Beberapa aturan yang ada pada Netiket adalah:

- 1) Amankan dulu diri anda, maksudnya adalah amankan semua properti anda, dapat dimulai dari mengamankan komputer anda, dengan memasang anti virus atau personal firewall
- 2) Jangan terlalu mudah percaya dengan Internet, sehingga anda dengan mudah mengunggah data pribadi anda. dan anda harus betul-betul yakin bahwa alamat URL yang anda tuju telah dijamin keamanannya.

- 3) dan yang paling utama adalah, hargai pengguna lain di internet, caranya sederhana yaitu,:
- a) Jangan biasakan menggunakan informasi secara sembarangan, misalnya plagiat.
 - b) Jangan berusaha untuk mengambil keuntungan secara ilegal dari Internet, misalkan melakukan kejahatan pencurian no kartu kredit
 - c) Jangan berusaha mengganggu privasi orang lain, dengan mencoba mencuri informasi yang sebenarnya terbatas.
 - d) Jangan menggunakan huruf kapital terlalu banyak, karena huruf kapital mencerminkan penulis emosi marah atau berteriak.
 - e) Jangan *flaming* (memanas-manasi), *trolling* (keluar dari topik pembicaraan) ataupun *junking* (memasang post yang tidak berguna) saat berforum.

F. Keamanan Data

Beberapa hal dan upaya yang perlu diperhatikan dalam aspek keamanan data antara lain:

1. Account Security

Setiap orang harus menggunakan pengelola kata sandi untuk membuat akun dan mengingat kata sandi yang kompleks dan berbeda untuk setiap akun, upaya ini merupakan hal penting yang dapat dilakukan orang untuk melindungi privasi dan keamanan akun pribadi.

2. Protect your Web browsing

Untuk mengamankan saat melakukan browsing data/berselancar di dunia maya, pengguna internet harus menginstal ekstensi HTTPS Everywhere. HTTPS Everywhere secara otomatis dapat mengarahkan ke versi situs yang aman ketika situs mendukungnya, sehingga menyulitkan penyerang - terutama jika Anda menggunakan Wi-Fi publik di kedai kopi, bandara, atau hotel - yang secara digital memungkinkan menyadap apa yang dilakukan. Cara lain juga dapat menggunakan jaringan pribadi virtual atau *Virtual Private Network* (VPN) apabila memungkinkan. Jika sering terhubung ke Wi-Fi publik, maka VPN dapat berguna karena menambah lapisan keamanan ke penjelajahan Anda ketika HTTPS tidak tersedia. VPN memungkinkan user membuat koneksi aman ke jaringan lain melalui Internet. VPN dapat digunakan

untuk mengakses situs web terbatas wilayah, melindungi aktivitas penelusuran user dari Wi-Fi publik, dan banyak lagi.

Dewasa ini VPN sangat populer, tetapi bukan karena alasan pada awalnya VPN tersebut dibuat. Awalnya VPN hanya cara untuk menghubungkan jaringan bisnis bersama dengan aman melalui internet atau memungkinkan user untuk mengakses jaringan bisnis dari rumah. Dalam istilah yang sangat sederhana, VPN menghubungkan PC, ponsel cerdas, atau tablet ke komputer lain (disebut server) di suatu tempat di internet, dan memungkinkan menjelajah internet menggunakan koneksi internet komputer tersebut. Jadi jika server itu berada di negara yang berbeda, itu akan tampak seolah-olah pengakses berasal dari negara itu, sehingga berpotensi mengakses hal-hal yang tidak bisa dilakukan secara normal di negara asal.

3. Update your software and devices

Sistem operasi telepon dan komputer, browser Web, aplikasi populer, dan bahkan perangkat rumah pintar sering menerima pembaruan dengan fitur baru dan peningkatan keamanan. Pembaruan keamanan ini biasanya jauh lebih baik untuk menghalangi peretas daripada perangkat lunak antivirus. Selain itu perlu juga diperhatikan untuk tidak sembarangan menginstal perangkat lunak yang tidak jelas. Setiap aplikasi aneh yang diinstall di ponsel dan setiap ekstensi peramban atau perangkat lunak yang diunduh dari situs web yang tidak jelas dapat menyebabkan potensi celah privasi dan keamanan.

4. Lock down your phone in case you lose it

Kita perlu memastikan tidak ada yang bisa masuk ke ponsel kita apabila kita kehilangannya atau seseorang mencurinya. Ponsel cerdas memiliki enkripsi secara default, tetapi kita masih perlu mengambil beberapa langkah untuk memastikan ponsel terkunci dengan benar apabila terjadi kehilangan. Upaya yang bisa dilakukan antara lain: (a) menggunakan kode sandi yang kuat di samping login biometrik (sidik jari atau wajah) dan (b) mengatur fitur pelacakan jarak jauh ponsel sehingga apabila terjadi kehilangan ponsel, maka kita dapat melihat area lokasi, serta memungkinkan menghapus semua data di ponsel dari jarak jauh.

5. *Enable encryption on your laptop*

Jika kita kehilangan laptop, pencuri yang mendapatkan perangkat kita memungkinkan mengakses ke data yang kita miliki. Bahkan tanpa kata sandi, pencuri biasanya masih dapat menyalin file dari laptop. Jika orang asing melihat-lihat laptop kita, mereka mungkin dapat melihat semua foto serta data dan informasi lainnya. Upaya yang dapat dilakukan untuk menanggulangi hal ini adalah dengan mengenkripsi drive penyimpanan di laptop, kata sandi dan kunci keamanan dapat melindungi data kita. Meskipun enkripsi mungkin terdengar seperti sesuatu dari film mata-mata berteknologi tinggi, namun sebenarnya itu sederhana dan memungkinkan untuk diaktifkan dengan perangkat lunak bawaan setiap sistem operasi.

G. Penerapan Etika dan Privasi Digital

Lima prinsip etika dalam era transformasi digital yang perlu diterapkan meliputi:

1. *Design for privacy, security and integrity*

Di era digital, transparansi dan integritas harus menjadi nilai inti yang dapat menjadi acuan perilaku profesional. Organisasi ataupun perorangan harus menggunakan data dengan cara yang bertanggung jawab dan etis karena, yang berarti tidak menggunakannya dengan cara yang dianggap mengganggu, manipulatif, atau tidak menghormati orang lain. Bersikap transparan berarti organisasi atau perorangan harus menyatakan niat mereka terkait penggunaan data dan memberikan persetujuan untuk menggunakan data tersebut. Beberapa pihak yang berorientasi bisnis sering kali dikritik karena jumlah data pelanggan yang mereka kumpulkan digunakan untuk tujuan monetisasi (keuntungan uang). Oleh sebab itulah, perlu adanya transparansi seputar pertukaran informasi terkait ketentuan antara pelanggan dan penyedia layanan. Manfaat apa pun yang diperoleh dari pengumpulan data yang bersifat pribadi (privasi) harus dibagikan oleh kedua belah pihak dan tidak dieksploitasi untuk keuntungan uang.

2. *Promote trust*

Pelanggan layanan digital (*user*) baik individu, kelompok maupun organisasi harus dapat mempercayai layanan digital dan data yang mereka gunakan. Pihak yang mengumpulkan dan mengelola data harus menjunjung tinggi prinsip bahwa integritasnya harus terjamin jika ingin dipercaya oleh konsumen. Memastikan

integritas data berarti bahwa organisasi memiliki kewajiban untuk memastikan bahwa data yang mereka miliki tunduk pada tata kelola dan prosedur audit yang kuat. Sederhananya, organisasi harus tahu bahwa data yang diberikan atau tersimpan tidak berubah dan disalah gunakan.

Infrastruktur digital saat ini dapat menyediakan kemampuan untuk tidak hanya menyimpan data, tetapi juga memungkinkan tersedianya layanan lain untuk berbagai kegunaan, termasuk validasi, replikasi, dan analisis. Jika konsumen digital mempercayai data yang menjadi dasar layanan yang mereka gunakan, maka data tersebut harus memiliki asal yang jelas, keterlacakan dari sumber ke antarmuka pengguna, dan memiliki kualitas yang memadai, serta sesuai dengan tujuan yang dimaksudkan. Jika asal dan kebenaran data tidak dapat diverifikasi, hal itu dapat menciptakan tingkat risiko yang signifikan bagi mereka yang menggunakan data tersebut, akibatnya setelah data diproses maka tindakan apa pun yang dilakukan sebagai konsekuensinya tidak dapat diurungkan.

3. *Beware of bias*

Pelanggaran etika yang tidak disengaja dapat disebabkan oleh banyak hal, tetapi salah satu alasan yang paling mungkin adalah karena bias bawah sadar yang dapat memengaruhi perilaku manusia. Bias konfirmasi mungkin adalah contoh yang paling terkenal, di mana individu mencari atau menafsirkan informasi dengan cara yang menegaskan keyakinan, hipotesis atau harapan mereka dan mengabaikan pendapat dan informasi yang bertentangan dengan ini. Ketika ada bias dalam data, ada risiko nyata bahwa sistem yang mengonsumsi data ini akan mewarisi bias itu. Yang menjadi perhatian khusus adalah algoritme *machine learning* yang digunakan untuk membuat jutaan keputusan setiap hari. Bias algoritmik telah menjadi perhatian belakangan ini, para ahli telah menyatakan bahwa bias seperti itu sekarang cepat menyebar di banyak industri dimana *machine learning* sering digunakan dengan sedikit tindakan yang diambil untuk mengidentifikasi atau memperbaikinya. Hal ini tentu mengkhawatirkan mengingat *machine learning* kini telah bergerak ke banyak sektor industri termasuk kedokteran, keuangan, dan hukum.

Cara mengatasi bias tentu saja dengan 'transparansi'. Ahli digital perlu secara aktif mengidentifikasi bias tersembunyi yang mungkin ada saat mereka mengembangkan, memastikan, dan menerapkan layanan digital. Sekali lagi,

kepercayaan konsumen juga harus dibangun dan dipertahankan, dengan memastikan pelanggan yang menggunakan sistem berbasis AI dan algoritma *machine learning* tahu bagaimana model inferensi telah dibangun dan data yang digunakan untuk mendukungnya cara kerja sistem tersebut.

4. *Ensure there is accountability*

Model dan algoritme adalah komponen fundamental dalam rentang layanan digital 'pintar' (*smart digital services*) yang terus berkembang dan menyediakan kecerdasan buatan dan kemampuan *machine learning*. Karena kemampuannya dalam menggabungkan data sosial dengan mesin pembuat keputusan, maka kemudian muncul kekhawatiran mengenai akuntabilitas terkait data dan layanan yang disediakan. Misalnya, jika algoritme digunakan oleh organisasi jasa keuangan untuk membuat keputusan yang biasanya dibuat oleh profesional yang berkualifikasi dan tersertifikasi, maka kemudian timbul pertanyaan bagaimana letak akuntabilitasnya. Oleh karena itu, organisasi yang ingin mengembangkan layanan digital harus memastikan bahwa layanan ini tidak digunakan untuk menghindari atau mengurangi akuntabilitas data dan informasi.

5. *Promote an ethical culture*

Budaya yang menjunjung tinggi etika dapat digambarkan sebagai sekumpulan nilai, keyakinan, dan norma bersama yang memengaruhi cara individu di dalamnya berpikir, merasa, dan berperilaku. Meskipun transformasi digital berpotensi menciptakan berbagai peluang dan kesuksesan di semua tingkatan dalam kehidupan, hal ini harus dicapai dengan tetap menjunjung etika melalui keadilan, kejujuran, dan integritas. Sebagai contoh, sebuah perusahaan digital memiliki tanggung jawab moral untuk melindungi karyawan dari mengambil risiko yang tidak perlu yang pada akhirnya terbukti dapat merusak individu dan organisasi. Jangan lupa bahwa reputasi profesional sama pentingnya bagi individu dan bagi organisasi secara keseluruhan, sehingga menjunjung tinggi etika sangatlah penting.

H. Rangkuman

Etika mencakup analisis dan penerapan nilai-nilai seperti benar, salah, baik, buruk dan tanggung jawab. Etika dan moral harus diterapkan dalam penggunaan teknologi informasi dan komunikasi. Meski berupa dunia digital, teknologi informasi dan komunikasi hanyalah media yang dikendalikan oleh manusia. Salah satu contoh penerapan etika dalam teknologi informasi dan komunikasi adalah netiket atau etika dan sopan santun berkomunikasi melalui Internet. Meski komunikasi melalui Internet banyak terjadi melalui tulisan dan simbol, namun pengguna Internet harus menjaga tutur katanya dan menerapkan etika yang baik. Jika seseorang memiliki etika yang baik, maka orang tersebut juga memiliki moral yang baik. Begitu juga sebaliknya.

Dengan maraknya penggunaan teknologi di era digital saat ini berpotensi menimbulkan banyaknya pelanggaran etika yang mengancam keamanan komputer dan data, oleh karena itu sebagai pengguna kita harus dapat melakukan beberapa upaya yang dapat digunakan untuk mencegah penyalahgunaan data yang kita miliki. Beberapa upaya yang bisa dilakukan diantaranya: (1) *account security*, (2) *protect your web browsing*, (3) *update your software and devices*, (4) *lock down your phone in case you lose it*, (5) *enable encryption on your laptop*.

Selain memperhatikan etika dan moral, penggunaan komputer dan alat-alat teknologi informasi dan komunikasi lainnya harus juga memperhatikan lima prinsip. Lima prinsip etika dalam era transformasi digital, meliputi: (1) *design for privacy, security and integrity*, (2) *promote trust*, (3) *beware of bias*, (4) *ensure there is accountability*, (5) *promote an ethical culture*. Penggunaan teknologi dan layanan digital yang mengabaikan lima prinsip tersebut tentunya dapat mendatangkan dampak negatif bagi pengguna

I. Latihan

1. Yang tidak termasuk dalam etika komputer yang oleh Richard Mason (1986), adalah

_____.

- a) Privasi
- b) Akurasi
- c) Properti
- d) Akses
- e) Konektivitas

2. Apa yang dimaksud dengan *information privacy* ?
 - a) Hak individu dan perusahaan untuk membiarkan pemerintah mengakses semua informasi pribadi Anda.
 - b) Hak individu dan perusahaan untuk menolak atau membatasi pengumpulan dan penggunaan informasi tentang pribadi dan perusahaan.
 - c) Hak individu dan perusahaan untuk membiarkan publik mengakses semua informasi.
 - d) Hak individu dan perusahaan untuk menyensor orang lain untuk mengekspresikan pendapat mereka sendiri tentang mereka.
 - e) Hak individu dan perusahaan untuk menolak atau membatasi hak akses informasi.
3. Istilah yang telah kita pelajari, yang didefinisikan sebagai "praktik mengambil karya atau ide orang lain dan menganggapnya sebagai milik Anda" dikenal sebagai _____.
 - a) *Piracy*
 - b) *Privacy*
 - c) *Theft*
 - d) *Plagiarism*
 - e) *Infringement*
4. Manakah dari berikut ini yang merupakan contoh *intellectual property*?
 - a) Penemuan
 - b) Ide ide
 - c) Karya seni
 - d) Hak Cipta
 - e) Semua benar
5. Hak yang diberikan untuk penemuan (*invention*) dikenal sebagai:
 - a) *Patent*
 - b) *Trademark*
 - c) *Copyright*
 - d) *Artwork*
 - e) *Intellectual property*

6. Orang-orang profesional TI memiliki tanggung jawab penting untuk memahami dan menegakkan aturan mengenai *Digital Ethics and Privacy*, karena ____.
- a) Profesional TI lebih berpengetahuan tentang undang-undang hak cipta dan privasi.
 - b) Profesional TI cenderung melanggar kebijakan ini
 - c) Banyak organisasi profesional TI yang menggunakan komputer untuk operasi sehari-hari mereka.
 - d) Banyak aset organisasi profesional TI disimpan dalam format digital.
 - e) Banyak organisasi profesional TI bersifat publik.
7. Apa yang dimaksud dengan *Netiquette*?
- a) Etika dalam berkomunikasi di sekitar jejaring Anda.
 - b) Tanggung jawab atas tindakan orang lain di internet.
 - c) Cara berkomunikasi yang benar dan dapat diterima di dan menggunakan internet.
 - d) Tanggung jawab atas tindakan pribadi di internet.
 - e) Aturan untuk melakukan percakapan tatap muka.
8. Pengetahuan dan pemahaman tentang *Netiquette* berguna, karena ____.
- a) Ini menjelaskan beberapa batasan teknis interaksi tatap muka.
 - b) Ini akan membantu Anda menciptakan kesan positif pada orang-orang yang Anda temui di dunia maya.
 - c) Ini menjelaskan komunikasi yang sudah digunakan oleh jutaan programmer.
 - d) Ini akan membantu melakukan percakapan dengan orang lain.
 - e) semua benar
9. Masalah etika dimana file dari komputer dapat diakses oleh pengguna lain tanpa sepengetahuan pemiliknya, dikenal sebagai ...
- a) *digital plagiarism*
 - b) *improper use of computer resources*
 - c) *phishing*
 - d) *file sharing*
 - e) *cybercrime*

10. Berikut saran untuk melindungi diri sendiri dari ancaman dunia maya, kecuali ...

- a) Memberikan sandi Anda hanya kepada teman-teman Anda
- b) Melindungi identitas Anda (data privacy)
- c) Melakukan update software dan sistem di perangkat Anda
- d) Jangan berikan user id dan password akun Anda
- e) Jangan melakukan apa pun yang dapat merusak reputasi Anda

J. Referensi

Moore, R. L. (2005). Cyber crime: Investigating High-Technology Computer Crime.
Mississippi: Anderson Publishing.

Munir. (2017). Pembelajaran Digital. Bandung: Alfabeta.