



Berdaya Internet: Nyaman dan Aman Ketika Bermain di Ruang Digital

Rita Gani, Citra Rosalyn Anwar*

Mafindo Bandung, Fakultas Ilmu Komunikasi, Universitas Islam Bandung, Indonesia

Mafindo Makasar, Fakultas Ilmu Komunikasi, Teknologi Pendidikan Univeritas Negeri Makasar, Indonesia

ARTICLE INFO

Article history :

Received : 13/08/2022

Revised : 22/11/2022

Published : 26/12/2022



Creative Commons Attribution-
NonCommercial-ShareAlike 4.0
International License.

Volume : 2

No. : 2

Halaman : 115-120

Terbitan : **Desember 2022**

ABSTRAK

Ruang digital menjanjikan banyak “mainan” untuk kehidupan manusia saat ini, terutama semenjak tahun 2020 lalu saat pandemi Covid-19 melanda negeri, karena banyak aktivitas yang berpindah ke dunia virtual, yang mengandalkan jaringan internet. Perkembangan angka penetrasi internet di tanah air pun menunjukkan angka yang signifikan untuk membuktikan tingginya pengguna internet saat ini setidaknya data hotsuit we are social yang dirilis Januari 2021 lalu mengungkap bahwa saat ini ada sekitar 274,9 juta pengguna internet di Indonesia dan 170 juta jiwa merupakan pengguna media sosial. Namun tidak semua pengguna internet berperilaku baik di dunia digital, bahkan tidak mempunyai daya kritis untuk memilih apa saja yang harus dibagikan di ruang publik. Kurangnya kesadaran ini memicu banyaknya tindak kejahatan di dunia digital, beberapa kasus karena unggahan data pribadi di ruang publik seperti media sosial. Karena itu, melindungi data pribadi dan data digital lainnya menjadi perlu dilakukan, karena bagian dari konsep Berdaya Internet yang menjadi salah satu tema dari Program Tular Nalar. Dengan metode deskriptif yang menekankan pada proses paparan data dan pengamatan, maka tulisan ini bisa menjadi bagian pengetahuan dari pengguna internet, khususnya terkait perlindungan data pribadi.

Kata Kunci : Berdaya internet; Perlindungan data pribadi; Berpikir kritis.

ABSTRACT

The digital space promises a lot of "toys" for human life today, especially since 2020 when the Covid 19 pandemic hit the country because many activities have shifted to the virtual world, which relies on the internet network. The development of internet penetration in the country figures shows a significant number to prove the current high internet users. The We Are Social Hootsuite data released last January 2021 revealed that currently there are around 274.9 million internet users in Indonesia, and 170 million people are media users, social. However, not all internet users behave well in the digital world and do not even have the critical power to choose what to share in the public sphere. This lack of awareness has led to many crimes in the digital world, in some cases due to uploading personal data in public spaces such as social media. Therefore, it is necessary to protect personal data and other digital, because it is part of the concept of Empowering the Internet that is one of the themes of the Contagious Reason Program. With a descriptive method that emphasizes the process of data exposure and observation, this paper can be part of the knowledge of internet users, especially regarding the protection of personal data.

Keywords : Internet power; Personal data protection; Critical thinking.

A. Pendahuluan

Pandemic Covid-19 tak pelak memberikan banyak perubahan dalam tatanan kehidupan masyarakat di tanah air, salah satunya adalah penggunaan teknologi informasi berbasis internet yang menjadi bagian yang tidak dapat dipisahkan dari kehidupan masyarakat. Ruang digital menjadi realitas baru dari aktivitas masyarakat, seperti pemerintahan digital, masyarakat digital dan ekonomi digital. Pembatasan ruang-ruang tatap muka untuk mengantisipasi penyebaran virus corona, digantikan oleh aktivitas online yang hingga saat ini masih mendominasi tatanan kehidupan kita. Dukungan pemerintah baik dalam bentuk penyediaan infrastruktur maupun regulasi yang jelas juga dilakukan untuk mewujudkan penyediaan ruang digital yang lebih baik di berbagai bidang, sehingga setiap pengguna internet bisa berselancar di ruang digital dengan aman dan nyaman. Maka terhitung sejak bulan Maret 2020, saat pertama kali virus Covid-19 terdeteksi di tanah air, kita seperti “dipaksa” untuk meleak teknologi, dan harus bisa menggunakan internet dengan baik. Namun perubahan yang seketika ini menimbulkan berbagai permasalahan di berbagai titik, ketidaksiapan pengguna internet seringkali memicu kesalahan dalam penggunaannya, bahkan menimbulkan efek negatif yang merugikan. Kondisi ini disebabkan karena meningkatnya penetrasi pengguna internet di tanah air, tidak diikuti oleh peningkatan kemampuan media literasi masyarakat terutama literasi digital. Padahal kemampuan untuk memahami seluk beluk dunia digital menjadi salah satu solusi untuk mengurai berbagai tindak kejahatan yang terjadi di dunia digital. Beberapa kasus kejahatan siber yang terjadi disebabkan karena pengguna internet yang tidak memahami aturan dari fitur atau aplikasi yang digunakannya, bahkan membuka “data pribadi” dengan bebas kepada publik. Beberapa bentuk kasus kejahatan siber yang dialami masyarakat, antara lain penipuan, pinjaman online, pencurian informasi (data), phishing, spam, doxing dan sebagainya (Akbar 2021). Direktorat Tindak Pidana Siber Bareskrim Polri merilis data dari Januari hingga November 2020 terjadi sebanyak 4.250 laporan kejahatan siber. Sekitar 1.158 kasus diantaranya merupakan kasus penipuan dan 267 kasus akses ilegal (APJII 2020).

Data tersebut seolah menjelaskan bahwa keasyikan berselancar di dunia digital seringkali membuat penggunanya lengah sehingga membuka ruang-ruang pribadi yang harusnya tersimpan rapi. Karena itu poin perlindungan data dan informasi perlu diperhatikan tidak saja bagi organisasi maupun perusahaan tetapi juga bagi setiap individu pengguna internet, supaya pengguna internet bisa nyaman dan aman selama berinteraksi di ruang digital. Keamanan digital ini, juga menjadi salah satu pilar dari empat pilar literasi digital yang dirilis oleh Kominfo dan selanjutnya menjadi bagian paparan dalam kegiatan Gerakan Nasional Literasi Digital (GNLD) yang secara serentak dilaksanakan di 34 provinsi di Indonesia pada bulan Mei 2021 lalu. Tujuan kegiatan ini tentu untuk meningkatkan pengetahuan dan pemahaman masyarakat Indonesia tentang literasi digital sehingga penggunaannya semakin cakap (melek digital) (Donny 2020).

Mendukung program tersebut, berbagai bentuk kegiatan kolaborasi dari pemerintah, masyarakat, komunitas dan organisasi yang peduli pada peningkatan literasi digital pun banyak diadakan, dengan sasaran yang beragam. Tentu tujuannya adalah untuk mendorong masyarakat berdaya internet. Salah satunya adalah kolaborasi Mafindo, Love Frankie, Maarif Institute dalam program Tular Nalar, yang berfokus pada kegiatan pengembangan kurikulum literasi digital untuk para dosen dan guru di seluruh Indonesia. Program yang sudah berlangsung sebelum GNLD ini, melibatkan expert dan para dosen di bidang komunikasi khususnya sebagai fasilitator. Seperti namanya, Tular Nalar diharapkan dapat menjangkiti atau menginfeksi setiap individu pengguna internet dengan berbagai nilai-nilai baik seputar dunia digital yang tertuang dalam tiga aspek utama yang diturunkan menjadi delapan kompetensi, dan disebarkan menjadi delapan tema dalam berbagai kelas. Gelinding pengetahuan yang memuat aspek utama, tema dan kompetensi tersebut, merupakan nalar kebaikan tentang literasi digital yang siap ditularkan ke berbagai tempat. Sehingga Tular Nalar tidak hanya sebagai jargon semata, tetapi juga menjadi praktik dalam keseharian guna menghindarkan orang dari bencana darurat literasi (Astuti, Mulyati, and Lumakto 2020).

B. Metode Penelitian

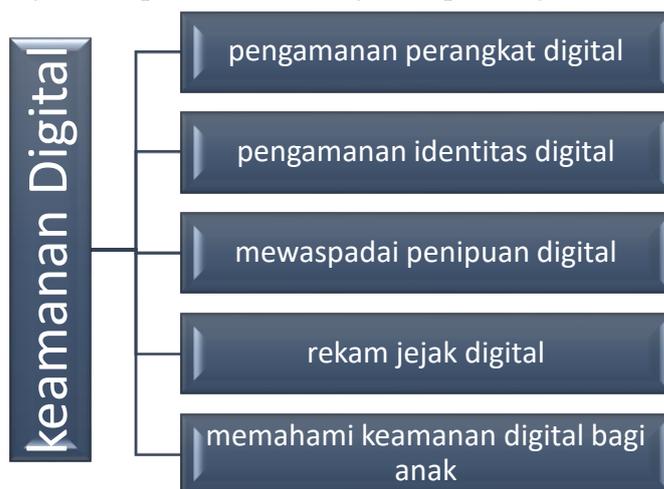
Data pribadi telah berubah menjadi komoditas paling berharga di dunia saat ini, karena aktivitas yang dilakukan di dunia digital membutuhkan data pribadi dari penggunanya (Setiawan and Yulianto 2020). Kamus Besar Bahasa Indonesia (KBBI) menjelaskan bahwa data pribadi adalah data yang berkenaan dengan

ciri seseorang, misalnya nama, umur, jenis kelamin, pendidikan, pekerjaan, alamat dan kedudukan dalam keluarga. Sedangkan dalam RUU Perlindungan Data Pribadi dalam (Monggilo and Banyumurti 2020) menjelaskan data pribadi sebagai setiap data tentang seseorang yang teridentifikasi dan atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non-elektronik. Data ini digunakan sebagai “pintu masuk” seseorang ketika menggunakan internet. Namun pada praktiknya banyak pengguna internet yang tidak begitu peduli akan pentingnya melindungi data pribadi sehingga membiarkan siapa saja bisa memasuki pintu tersebut. Hal itu membuka jalan bagi para penjahat digital untuk melakukan aksi kriminal. Data pribadi juga akan meninggalkan jejak digital bagi kita, karena itu juga diperlukan pemahaman pengguna untuk menyaring berbagai hal sebelum mempostingnya di dunia digital, terutama di media sosial (Masyhuri and Zainuddin 2008).

Kemampuan berpikir kritis merupakan salah satu hal yang perlu dipahami oleh pengguna media digital, terutama untuk “menahan” informasi negatif yang sedianya terjadi dan disebarkan melalui berbagai platform di dunia digital. Cohen (2015) menjelaskan bahwa yang dimaksud dengan berpikir kritis adalah “seperangkat keterampilan dan pemahaman, termasuk kemampuan untuk bermain dengan kata-kata, sensitivitas untuk menangkap konteks, emosi, dan perasaan, dan keterbukaan pikiran untuk menjadi kreatif dan mendapatkan pandangan baru”. Sejalan dengan konsep ini, kecerdasan individu selama berselancar di dunia digital juga dibutuhkan, terutama untuk menjaga keamanan data pribadinya, dalam hal ini, Allen (2004) menjelaskan bahwa kecerdasan dalam berpikir akan membantu kita dalam working out where and how to look for the information you need, understanding that information in relation to your own work, deciding which information is relevant to your topic and which is not, dan identifying when you need to find out more information to make sense of a problem.

Beberapa poin tersebut perlu menjadi pertimbangan bagi setiap pengguna internet sebelum membagikan informasi di dunia digital. Pemahaman setiap individu untuk bisa menggunakan ruang digital dengan cerdas dan baik merupakan salah satu kesiapan untuk memasuki fase baru yang di sebut sebagai revolusi digital, yang merupakan istilah untuk menggambarkan suatu fase dalam sejarah perkembangan teknologi ketika terjadi peralihan dari penerapan teknologi mekanik analog menuju penerapan teknologi elektronik digital di hampir semua bidang (Isbah 2021)

Melengkapi langkah cerdas di atas, pengguna internet juga perlu memahami lima indikator atau kompetensi yang perlu ditingkatkan untuk menjaga keamanan digital dan melindungi data pribadinya. Lima kompetensi ini menjadi bagian dari pilar keamanan digital, seperti bagan di bawah ini:



Gambar 1. Peta kompetensi keamanan digital
Sumber : Kominfo-Siberkreasi & Delloite (2021)

Secara umum, keamanan digital dapat dimaknai sebagai sebuah proses untuk memastikan penggunaan layanan digital, baik secara daring maupun luring dapat dilakukan secara aman dan nyaman (Sammons &

Cross, 2017 dalam Kominfo, 2021:3). Tidak hanya untuk mengamankan data yang kita miliki melainkan juga melindungi data pribadi yang bersifat rahasia. Dengan memahami peta kompetensi keamanan digital tersebut, maka setiap pengguna internet akan bisa menikmati kehidupan di ruang digital dengan nyaman dan aman.

Dalam tulisan ini, Penulis menggunakan metode deskriptif, yang dikatakan Masyhuri (2008 h. 34) sebagai penelitian yang memberi gambaran secermat mungkin mengenai suatu individu, keadaan, gejala atau kelompok tertentu. Sedangkan tujuan dari penelitian deskriptif ini adalah untuk membuat deskripsi, gambaran atau lukisan secara sistematis, faktual dan akurat mengenai fakta-fakta, sifat-sifat serta hubungan antar fenomena yang diselidiki Nazir (2005 h. 54). Diharapkan dengan menggunakan metode ini akan didapatkan gambaran perilaku dan konsep dasar tentang bagaimana proses perlindungan data pribadi yang harusnya dilakukan oleh pengguna internet.

C. Hasil dan Pembahasan

Seperti Dewa Janus bermuka dua, maka perkembangan internet pun memiliki sisi positif dan negatif. Ia bisa menjadi penyedia informasi apa pun yang dibutuhkan dan bahkan juga untuk yang tidak dibutuhkan. Tetapi di lain sisi internet juga menjadi media bagi tidak kejahatan, seperti cyber crime.

Ada banyak indikasi yang menggambarkan bocornya data pribadi seseorang, misalnya pesan sms penipuan, sms iklan spam, email spam bahkan whatsapp spam atau penipuan melalui panggilan telepon yang mengaku-aku dari perbankan. Pengguna internet di Negara ini sangat banyak, uraian data-data penelitian dari berbagai sumber tentang ini memberikan gambaran bahwa internet dan dunia digital merupakan bagian yang tidak terpisahkan dari kehidupan masyarakat Indonesia saat ini. Namun di antara kerumunan tersebut berapa banyak yang peduli dan mampu memberdayakan internet dengan baik, terutama untuk mengamankan data-data pribadinya?. Jawabnya tidaklah banyak, mengingat cukup tingginya kasus kebocoran data pribadi belakangan ini. Sepanjang tahun 2021 ini ada beberapa kasus kebocoran data digital yang terjadi di tanah air, seperti temuan kebocoran 1.3 juta data pengguna eHAC yang pertama kali ditemukan oleh peneliti vpnMentor, kebocoran pada 279 juta data peserta BPJS Kesehatan yang diperjualbelikan di situs Raid Forum, hingga akses aplikasi Peduli Lindungi seorang warga dengan menggunakan NIK Presiden Joko Widodo. Kasus-kasus ini membuktikan bahwa data penduduk berpotensi menjadi jalan bagi penjahat digital untuk melakukan aksi kejahatan.

Untuk mengatasi kelengahan tersebut, maka tema berdaya internet merupakan kapasitas dasar yang harus dimiliki oleh setiap pengguna internet dan karenanya menjadi bagian dari materi program Tular Nalar. Salah satu bagian penting dalam tema ini adalah kompetensi perlindungan data pribadi yang memuat beberapa poin seperti; (1) Apa makna privasi?, (2) Bahaya kebocoran privasi, (3) Apa data yang tidak boleh dibagikan?, (4) Bagaimana melindungi data pribadi dan keluarga di media sosial ataupun platform digital pada umumnya?, (5) Apa yang harus dilakukan ketika data pribadi kita sudah telanjur beredar?, (6) Praktik terlarang: doxing, cyber-vigilante, (7) Perlindungan privasi dalam Undang-Undang.

Ancaman digital adalah ancaman dari tindak kejahatan yang berupaya merusak data, mencuri data, atau mengganggu kehidupan di dunia maya secara umum. Ini bisa menjadi pintu masuk keberbagai jenis kejahatan lainnya. Keamanan sempurna dan permanen di ruang digital memang tidak mungkin sepenuhnya bisa dilakukan, karena tidak ada solusi tunggal untuk kita menjaga keamanan data digital kita. Dalam konteks ini, keamanan digital bukan lagi semata soal “alat” yang akan digunakan, tetapi juga tentang bagaimana seseorang memahami ancaman yang dihadapi dan cara menghadapinya. Kerugian-kerugian akan muncul bila pengguna internet tidak bisa melindungi data pribadinya, seperti dilansir dari katadata.co.id, ada beberapa kerugian yang muncul akibat data dicuri antara lain adalah; (1) Butuh dana dan waktu untuk memulihkan data yang bocor, (2) Berpotensi dikucilkan dan perundungan, (3) Secara psikologis menyebabkan stres dan merasa tidak aman, (4) Terjebak dalam pinjaman yang tidak dilakukan (Pramadi 2020).

Selain melindungi data, pengguna internet juga perlu melindungi perangkat karena menjadi tempat menyimpan data pribadi dan files penting. Maka keamanan digital juga dibutuhkan untuk menjaga perangkat yang dimiliki sehingga terhindar dari pencurian, akses ilegal, instruksi berbahaya seperti spyware, virus, atau segala jenis kode berbahaya atau malware yang menyusup ke komputer, handphone dan jenis perangkat digital lainnya.

Berdasarkan pengamatan atas berbagai kasus yang terjadi dan kajian literatur terkait perlindungan data pribadi, maka penulis menguraikan beberapa bentuk langkah bijak yang bisa dilakukan untuk melindungi data pribadi, antara lain adalah; (1) Menggunakan password yang nyaman dan dengan tingkat keamanan yang dipahami oleh penggunanya. Jangan membuat password yang sulit untuk diingat meskipun lebih aman, jadi kombinasikanlah huruf dan angka yang memudahkan pengguna untuk mengingat. Misalnya : Tehbotol2000, 36derajatcelcius, Nasi Padang 15500, dan sebagainya; (2) Lindungi perangkat digital yang dimiliki sehingga data-data yang berada di perangkat digital tidak mudah diakses oleh orang lain. Pengoptimalan perlindungan perangkat digital merupakan salah satu upaya untuk tetap dapat menggunakan perangkat digital secara lebih nyaman untuk menunjang aktivitas ataupun pekerjaan sehari-hari pun bisa dilakukan; (3) Lakukan pengaturan privasi di setiap akun media sosial yang digunakan. Setiap jenis media sosial memiliki fitur pengaturan yang berbeda-beda. Jadi sebelum menggunakannya, cek ricek dahulu bagaimana setingan yang berlaku. Misalnya aturan untuk menset postingan untuk publik, hanya bisa diakses oleh teman (friend only), atau hanya untuk akses pribadi di media sosial facebook, atau pengaturan kolom komentar dan akses pribadi di instagram; (4) Jangan memberikan informasi mengenai data pribadi yang terlalu banyak di media sosial. Pengguna harus membatasi dan bisa membedakan mana hal-hal yang sifatnya pribadi yang tidak menjadi konsumsi publik dan mana yang bersifat umum. Postingan seperti foto ktp, kartu keluarga, data paspor, alamat rumah, situasi kamar tidur, alamat sekolah anak dan sebagainya merupakan bagian dari data pribadi yang tak layak di posting di media sosial, karena bisa mengundang pelaku kejahatan siber; (5) Pahami bahwa ruang digital akan memuat rekam jejak digital penggunanya. Rekam jejak pribadi ini akan bisa dilacak kapanpun dan sulit dihilangkan dari ruang digital, mengingat saat ini setiap orang bisa “merekamnya” baik dalam bentuk screen shoot maupun rekaman. Tugas pengguna internet yang baik adalah meninggalkan rekam jejak positif di ruang digital terutama di berbagai platform media sosial yang dimiliki; (6) Link yang didapat pastikan memang langsung mengarah pada situs yang dituju: abaikan atau langsung ditutup bila ada link-link lain yang muncul, yang mungkin berisi iklan dan spam lainnya; (7) Perhatikan alamat url dari situs yang dikunjungi: hal ini perlu dilakukan supaya kita bisa mengakses di situs yang resmi; (8) Perhatikan akses yang diminta oleh aplikasi yang baru diinstal: apalagi bila aplikasi tersebut meminta beberapa data yang tidak ada hubungannya dengan akses, sebaiknya diabaikan saja; (9) Gunakan akses pribadi (kuota pribadi) bila melakukan transaksi keuangan (ebanking) dan jangan menggunakan wifi umum (publik). Hal ini bertujuan untuk menghindari kebocoran data yang dimungkinkan terjadi karena wifi publik yang digunakan oleh banyak orang; (10) Hargai privasi orang lain: setiap orang memiliki karakteristiknya ketika terhubung di dunia digital terutama di media sosial. Ada yang senang mengekspos foto-foto kegiatannya dan ada menganggap hal tersebut sebagai wilayah pribadi dan tidak mengeksposnya ke ruang publik. Maka bila akan memposting foto bersama teman, kolega dan sebagainya, sebaiknya meminta proses izin pada mereka sebelum menggunggahanya di media sosial; (11) Gunakan password yang berbeda untuk setiap akun sosmed: ini perlu dilakukan untuk menghindari masuknya hacker dan sejenisnya pada media sosial yang kita gunakan; (12) Kenyamanan dan rasa aman selama “bermain” di ruang digital juga perlu diberikan pada anak-anak. Orang tua dan orang dewasa yang menemani anak-anak dalam berkegiatan di ruang digital bisa menggunakan berbagai fitur pengendalian untuk orang tua termasuk memastikan keamanan pada mesin pencarian, sehingga anak-anak aman dan hanya bisa mengakses berbagai hal yang positif. Orang tua juga harus menjaga data pribadi anak dan memeriksa pengaturan fitur privasi.

D. Kesimpulan

Kita tidak bisa untuk menghindar dari kehidupan digital, karena dunia digital adalah dunia kita saat ini. Berbagai interaksi yang terjadi di ruang internet membutuhkan pemahaman dari penggunanya agar terhindar dari berbagai kejahatan siber yang belakangan marak terjadi.

Maka adalah perlu bagi kita untuk bisa memberikan perlindungan dan keamanan pada data pribadi di ruang digital. Peningkatan kesadaran pengguna internet akan pentingnya poin ini, sejatinya akan memberikan kenyamanan dan keamanan selama terhubung di dunia digital. Ini adalah tanggung jawab setiap individu, yang harus dilakukan selama dunia digital menjadi bagian dari aktivitas kesehariannya.

Daftar Pustaka

- Akbar, Caesar. 2021. "6 Kasus Kebocoran Data Pribadi Di Indonesia." *Tempo.Co*. Retrieved (<https://nasional.tempo.co/read/1501790/6-kasus-kebocoran-data-pribadi-di-indonesia>).
- Allen, M. 2004. *Smart Thinking: Skills for Critical Understanding & Writing*. Australia: Oxford University Press.
- APJII. 2020. *Laporan Survei Internet APJII 2019-2020 (Q2)*.
- Astuti, S. ..., H. Mulyati, and G. Lumakto. 2020. "In Search of Indonesian-Based Digital Literacy Curriculum through TULAR NALAR [Paper Presentation]. 'Islam, Media and Education in the Digital Era.'"
- Donny, B. U. 2020. "Kerangka Literasi Digital Indonesia." Retrieved (www.literasidigital.id).
- Isbah, F. M. 2021. *Perspektif Ilmu-Ilmu Sosial Di Era Digital: Disrupsi, Emansipasi Dan Rekognisi*. Yogyakarta: UGM Press.
- Masyhuri, and M. Zainuddin. 2008. *Metodologi Penelitian Sosial Dan Ekonomi, Teori Dan Aplikasi*. Bandung: Penerbit Alfabeta.
- Monggilo, Kurnia, and Banyumurti. 2020. *Cakap Bermedia Digital*. Direktorat Jenderal Aplikasi Informatika.
- Pramadi, Y. 2020. "Indonesia Di Tengah Belantara Digital: Merdeka Atau Tidak Berdaya?" *Jurnal Masyarakat Dan Budaya* 22(2):243–55.
- Setiawan, A., and E. Yulianto. 2020. *Pengantar Keamanan Media Digital, Informatika*. Bandung.