P-ISSN : 2548-9739
E-ISSN : 2685-5240

KEAMANAN INFORMASI DATA PRIBADI PADA MEDIA SOSIAL

Mesra Betty Yel[1)], Mahyuddin K. M. Nasution[2)]

[1]Graduate Program Of Computer Science,
[2]Department Of Computer Science
Faculty of Computer Science and Information Technology,
Universitas Sumatera Utara, Medan, Indonesia
bettymesra86@gmail.com

ABSTRACT

The development of information technology and the internet today has changed the way humans communicate. One of them is the development of social media, social media has become a part of life to obtain, share and disseminate information. With the development of social media, the issue of information security and privacy has also become an important issue at this time. Social media as a source of leaking confidential information has become common nowadays. Without realizing it, a lot of data about someone's privacy has been leaked on the internet. Distributed privacy data can be caused by negligence or service providers. Information system security is an asset that must be protected. Security is generally defined as "quality or state of being secure to be free from danger". The research method is using the blended method. This research was conducted by searching and understanding the literature or related to information security on social media and library research. The six main points to consider when using an online application system regarding data privacy are security and data protection, user awareness, control arrangements, risk management, transparency, and ethics. Trust needs to be built into the design of Internet services, both through design and development activities for the management of a system that prioritizes user priority. It is possible that the user is given a choice of control mechanisms over whether or not to disclose personal information and its use.

Keywords: Social media data security

ABSTRAK

Perkembangan teknologi informasi dan internet saat ini telah mengubah cara manusia dalam melakukan komunikasi. Salah satunya adalah perkembangan media sosial, media sosial sudah menjadi bagian dari kehidupan untuk memperoleh, membagikan dan menyebarluaskan informasi. Semakin berkembangnya media sosial maka masalah keamanan informasi dan privasi juga menjadi hal yang penting saat ini. Media sosial sebagai salah satu sumber bocornya informasi rahasia sudah menjadi hal yang umum saat ini. Tanpa disadari, banyak data mengenai privasi seseorang yang telah bocor di internet. Data privasi yang tersebar bisa disebabkan oleh kelalaian maupun penyedia layanan. Keamanan sistem informasi merupakan aset yang harus dilindungi keamanannya. Keamanan secara umum diartikan sebagai “quality or state of being secure to be free from danger”. Metode penelitian dilakukan adalah menggunakan metode blended. Penelitian ini dilakukan dengan cara mencari dan serta memahami literatur atau yang berhubungan keamanan informasi pada media social dan penelitian pustaka. Enam poin utama yang harus dipertimbangkan saat menggunakan sistem

P-ISSN : 2548-9739
E-ISSN : 2685-5240

aplikasi online terkait privasi data yaitu keamanan dan data perlindungan, kesadaran pengguna, pengaturan kontrol, manajemen risiko, transparansi, dan etika. Perlu dibangun kepercayaan ke dalam rancangan layanan Internet, baik melalui kegiatan rancang bangun pengelolaan suatu sistem yang lebih mengedepankan user priority. Memungkinkan, user diberikan pilihan mekanisme kontrol terhadap perlu tidaknya dalam mengungkapkan informasi pribadi dan penggunaannya.

Kata Kunci: Keamanan data media social

1. PENDAHULUAN

Perkembangan teknologi informasi dan internet saat ini telah mengubah cara manusia dalam melakukan komunikasi. Salah satunya adalah perkembangan media sosial, media sosial sudah menjadi bagian dari kehidupan untuk memperoleh, membagikan dan menyebarluaskan informasi . Media sosial merupakan salah satu media yang sangat popular saat ini karena menyediakan kemudahan dan kecepatan yang memungkinkan seseorang membuat dan mendistribusikan sebuah informasi. Era teknologi informasi saat ini tidak hanya untuk berbalas pesan dan saling bertukar informasi namun juga memberikan kemudahan dalam melakukan segala hal. Banyak manfaat yang diperoleh dari kemajuan teknologi informasi. Tentunya penggunaan teknologi informasi pun ikut mengalami berkembang pesat, salah satunya terjadi pada bidang komunikasi. Semakin berkembangnya media sosial maka masalah keamanan informasi dan privasi juga menjadi hal yang penting saat ini. Media sosial sebagai salah satu sumber bocornya informasi rahasia sudah menjadi hal yang umum saat ini[1]. Privasi merupakan keleluasaan pribadi. Privasi melekat pada setiap manusia dan patut untuk dihargai. Pada era teknologi informasi ini, data mengenai privasi seseorang telah banyak tersebar pada internet. Tanpa disadari, banyak data mengenai privasi seseorang yang telah bocor di internet. Data privasi yang tersebar bisa disebabkan oleh kelalaian maupun penyedia layanan[2]. Keamanan sistem informasi menjadi hal penting dalam bermedia sosial, masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Perkembangan media sosial yang awalnya berfungsi untuk memudahkan pengguna melakukan melakukan interaksi sosial dengan menggunakan teknologi melalui internet sehingga mengubah cara penyebaran informasi sebelumnya yang bersifat penyebaran informasi yang dapat diterima oleh banyak pengguna yang menggunakan media social seperti media sosial facebook, Instagam,twitter, whatsapp maupun media sosial lainnya[3]

Sebuah riset pada tahun 2019 oleh perusahaan media We Are Social yang bekerja sama dengan Hootsuite,yang merilis data perkembangan jumlah pengguna internet di Indonesia yang menyatakan bahwa semakin pesat kenaikan pengguna internet yakni sebanyak 20 persen dibandingkan jumlah pada tahun 2018, dalam rilisnya dinyatakan bahwa ada 150 juta pengguna media sosial di Indonesia. Pada tahun sebelumnya yaitu tahun 2018, masyarakat online dikejutkan berita bocornya 87 juta data pribadi pengguna Facebook yang dicuri oleh Firma Cambridge Analytica, terlebih lagi sekitar satu juta data pribadi yang dicuri tersebut berasal dari Indonesia. Hasil survei CSIS pada Agustus 2017 menyebutkan 54,3 persen generasi milenial menggunakan media online setiap harinya, sebanyak 81,7 persen generasi milenial menggunakan Facebook, 70,3 persen menggunakan Whatsapp dan 54,7 persen menggunakan Instagram. Ini menjadikan peran media sosial sangat krusial untuk mempersuasi dan sekaligus juga memberikan kerentanan pada generasi millennial.[4]

P-ISSN : 2548-9739
E-ISSN : 2685-5240

Situs jejaring sosial adalah tempat online dimana pengguna dapat membuat sebuah profil dan jaringan personal yang dapat menghubungkan dengan pengguna lainnya. Bagi masyarakat modern, media sosial sudah menjadi bagian dari kehidupan untuk memperoleh atau membagikan informasi. Media sosial merupakan salah satu media yang trend saat ini, karena menyediakan kemudahan dan kecepatan yang memungkinkan seseorang membuat dan mendistribusikan sebuah konten. Media sosial didefinisikan sebagai sekelompok aplikasi berbasis Internet yang membangun fondasi ideologis dan teknologi Web 2.0, dan memungkinkan penciptaan dan pertukaran konten yang dibuat penggunanya [4]. Internet of Things didefinisikan sebagai infrastruktur jaringan global yang dinamis dengan konfigurasi sendiri dan komunikasi yang dapat dioperasikan. Secara sederhana dapat didefenisikan IoT berarti kemampuan untuk membuat segala sesuatu di sekitar kita mulai dari (mis. mesin, perangkat, ponsel, dan mobil) bahkan (kota dan jalan) dapat terhubung ke Internet dengan perilaku yang cerdas dan dengan mempertimbangkan keberadaan jenis otonomi dan privasi. Kemajuan teknologi informasi dan komunikasi, menghasilkan data dalam jumlah yang luar biasa. Data yang dihasilkan tidak akan bernilai jika mereka tidak dapat dianalisis, ditafsirkan dan dipahami. Sedangkan menurut Boyd, situs jejaring sosial adalah layanan berbasis web yang memungkinkan individu untuk (1) membuat profil publik atau semi-publik dalam sistem, (2) mengartikulasikan daftar pengguna lain dengan siapa mereka dapat berbagi koneksi, dan (3) melihat dan mencari daftar koneksi mereka dan yang dibuat oleh orang lain dalam sistem. Lebih jauh, Kaplan dan Haenlein mendefinisikan media sosial sebagai “sekelompok aplikasi berbasis Internet yang dibangun di atas fondasi ideologis dan teknologi Web 2.0, dan memungkinkan pembuatan dan pertukaran konten yang dibuat pengguna”. Media sosial sendiri dapat dibagi menjadi beberapa kelompok, antara lain proyek kolaborasi (misalnya Wikipedia), blog dan microblog (misalnya Twitter), situs jejaring sosial (mis. Facebook, LinkedIn, MySpace), komunitas konten (misalnya YouTube, Flickr), virtual social dunia (mis. Second Life) [5][6]. Seiring dengan keterbukaan terhadap data dan informasi, maka perlindungan terhadap informasi menjadi hal yang wajib. Dalam beberapa tahun terakhir, perkembangan pesat dan biaya yang lebih rendah dalam teknologi informasi dan komunikasi telah membuatnya lebih mudah diakses dan nyaman. Akibatnya, jumlah pengguna internet telah meledak. Penyalahgunaan data juga menjadi perhatian khusus. Banyak pelanggaran data yang terjadi karena implementasi yang buruk atau tidak adanya kontrol keamanan baik di perusahaan swasta maupun di organisasi pemerintahan. Banyak negara yang berusaha meningkatkan persyaratan keamanan dan menerapkanya di undang-undang mereka. Namun, sebagian besar kerangka keamanan bersifat reaktif dan tidak mengatasi ancaman yang relevan. Beberapa alasan mengapa data pribadi penting untuk dilindungi yaitu

1. Data pribadi menyangkut hak asasi dan privasi yang harus dilindungi, seperti tercantum dalam:
– Deklarasi Universal tentang Hak Asasi Manusia (Universal Declaration of Human Rights, 1948);
– UU Nomor 12 Tahun 2005 tentang Pengesahan International Covenant on Civil and Political Rights;
– UU No. 36 Tahun 2009 tentang Kesehatan mengatur tentang rahasia kondisi pribadi pasien;
– UU No. 10 Tahun 1998 tentang Perbankan mengatur data pribadi mengenai nasabah penyimpan dan simpanannya.
2. Data adalah aset atau komoditas bernilai tinggi di era big data dan ekonomi digital,
– Volume data di tahun 2015 diperkirakan mencapai 8 triliun GB

P-ISSN : 2548-9739
E-ISSN : 2685-5240

dan akan naik 40 kali lipat di tahun 2020. (OECD, 2018);
- Aplikasi AI berbasis data diproyeksikan dapat berkontribusi sebesar 13 triliun US Dollar bagi ekonomi global pada tahun 2030 (McKinsey,2018).

3. Pelanggaran privasi dan penyalahgunaan data pribadi makin banyak terjadi,
- Contoh aktivitas: digital dossier, direct selling, location-based messaging;
- Contoh kasus: Cambridge Analytica (2018).

4. Masyarakat belum sepenuhnya sadar akan pentingnya melindungi data pribadi,
- Jumlah pengguna internet di Indonesia terus meningkat, namun tidak seluruhnya menyadari pentingnya perlindungan data pribadi;
- Lebih dari 30% pengguna internet Indonesia belum sadar bahwa data dapat diambil (APJII, 2017).[7]

Kajian di bidang keamanan informasi terus berlangsung terus menerus dan ini menjadi tumpuan dari riset yang mungkin dikembangkan dengan melihat beberapa kajian yang bersifat lanjutan, yang melibatkan tidak saja bidang ilmu terkait seperti sistem komputer, sistem informasi, sains komputer, teknik informatika, dan teknologi informasi, tetapi secara bergandengan sesuai dengan kebutuhan melibatkan bidang ilmu lain, seperti manajemen, sains sosial, hukum dan etika[8].

2. METODOLOGI

2.1. Keamanan Sistem Informasi

Keamanan sistem informasi merupakan aset yang harus dilindungi keamanannya. Keamanan secara umum diartikan sebagai *"quality or state of being secure to be free from danger"*. Untuk menjadi aman adalah dengan cara dilindungi dari musuh dan bahaya dengan tinjauan sebagai berikut:

1. Physical Security yang memfokuskan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
2. Personal Security yang overlap dengan "phisycal security" dalam melindungi orang – orang dalam organisasi.
3. Operation untuk tujuan tertentu, khusus bagi pemilik data saat informasi ini dikumpulkan. Privacy menjamin keamanan data bagi pemilik informasidari orang lain.
4. Identification
   Sistem informasi memiliki karakteristik identifikasi jika bisa mengenali penggunaannya. Identifikasi adalah langkah pertama dalam memperoleh hak akses ke informasi yang diamankan. Security yang Identifikasi umumnya dilakukan dengan penggunaan user name dan user ID.
5. Authentication
   Autentikasi terjadi pada saat sistem dapat membuktikan bahwa pengguna memang benar-benar orang yang memiliki identitas yang diklaim.
6. Authorization
   Setelah identitas pengguna memfokuskan strategi untuk diautentikasi, sebuah proses yang disebut autorisasi memberikan jaminan bahwa pengguna (manusia dan komputer) telah mendapatkan autorisasi secara spesifik dan jelas untuk mengakses, mengubah, atau menghapus isi dari informasi.
7. Accountability
   Karakteristik ini dipenuhi jika sebuah sistem dapat menyajikan data semua aktivitas terhadap informasi yang telah dilakukan, dan siapa yang melakukan aktivitas itu. Keamanan mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.

P-ISSN : 2548-9739
E-ISSN : 2685-5240

8. Communications Security yang bertujuan mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan organisasi.
9. Network Security yang memfokuskan pada pengamanan peralatan jaringan data organisasi, jaringannya dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi. Perlindungan pada Informasi tersebut dilakukan untuk memenuhi aspek keamanan informasi.

Aspek-aspek keamanan informasi seharusnya dikontrol untuk perlindungan informasi yang terkait dengan keamanan informasi yaitu:

a. Privacy
   Informasi yang dikumpulkan, digunakan, dan disimpan oleh organisasi adalah dipergunakan hanya informasi terdiri dari perlindungan terhadap aspek Confidentiality, Integrity dan Avalability yaitu :
b. Confidentiality (kerahasiaan)
   Aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
c. Integrity (integritas)
   Aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin pihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.
d. Availability (ketersediaan)

Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan,memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait.[3]. Perlindungan adalah prasyarat untuk pengungkapan diri secara online, namun pengungkapan diri juga mengurangi privasi dengan memperluas ukuran data online yang dapat diakses oleh klien yang berbeda. Kepercayaan dicirikan sebagai keyakinan bahwa orang, pertemuan, atau perusahaan dapat dipercaya. Ini sering memiliki hubungan yang berlawanan dengan perlindungan, jika dilihat fakta bahwa individu perlu mengetahui data orang lain dengan tujuan akhir untuk mempercayainya[9]

2.2. Penelitian Terdahulu

Mayoritas informan sudah menggunakan media sosial lebih dari 10 tahun, dan yang paling lama sudah menggunakan media sosial selama 19 tahun, hal ini menggambarkan bahwa pengguna media sosial sudah menggunakan media sosial sejak platform tersebut muncul pertama kali, hal ini mengindikasikan teori Technology Acceptance Model (TAM) yang menyebutkan kemudahan pemakaian dan persepsi kegunaan teknologi yang menjadi penentu penggunaan teknologi tersebut, dapat disimpulkan bahwa mayoritas pengguna mengganggap media sosial bermanfaat dan mudah untuk dipakai dikalangan generasi milenial. Ini menunjukkan bahwa mayoritas pengguna media sosial sangat akrab dengan media sosial. Namun lamanya pengguna dalam menggunakan media sosial selama bertahun-tahun tidak menggunakan kata sandi sangat rendah karena tidak satupun pengguna selalu memperbarui kata sandi mereka secara teratur. Bahkan hasil yang lebih mengkhawatirkan adalah tentang kepedulian generasi milenial terhadap pentingnya prosedur keamanan dalam persepsi kemudahan penggunaan ditunjukkan dari pernyataan hampir setengah responden akan melewatkan prosedur keamanan di media sosial jika mereka terlalu rumit dan bahkan akan menggunakan situs web yang tidak aman asalkan itu dapat membantu. Dalam hal pengaturan keamanan, hasilnya menunjukkan bahwa individu yang lebih sadar akan pengaturan kata sandi mereka umumnya memiliki tingkat kesadaran yang lebih tinggi

P-ISSN : 2548-9739
E-ISSN : 2685-5240

tercermin dari niat mereka memberikan perhatian lebih jauh dalam menciptakan kata sandi yang lebih rumit untuk berperilaku aman saat menggunakan media sosial.[4]

Hasil analisis yang telah dilakukan oleh [1] bahwa beberapa mahasiswa yang telah mendapatkan mata kuliah keamanan informasi telah menerapkan tindakan-tindakan dalam menjaga keamanan informasi di media sosial. Akan tetapi untuk mahasiswa yang belum mendapatkan pemahaman mendalam tentang keamanan informasi masih melakukan tindakan yang tidak mencerminkan penjagaan informasi di media sosial. Hal lain yang dapat dilihat adalah mahasiswa Prodi Sistem Informasi telah memahami pentingnya keamanan informasi akan tetapi perilaku mereka tidak mencerminkan keamanan informasi, mereka juga belum memanfaatkan pengaturan privasi di media sosial.[1]

Privasi merupakan hal yang sangat krusial apalagi di era Teknologi Informasi saat ini. Data pribadi adalah data yang berupa identitas dan penanda personal seseorang yang bersifat pribadi. Di berbagai negara digunakan pula istilah informasi pribadi atau privacy. Adapun bahwa perlindungan privasi (dalam berbagai bentuk), sangat penting dalam era internet saat ini dan juga tentunya sebagai pertimbangan penting bagi orang yang memiliki tujuan untuk melakukan penelitian menggunakan Internet. Namun, perkembangan pesat dari masyarakat menyebabkan tantangan terkait dengan privasi karena meningkatnya kebutuhan pengungkapan diri pada tingkat interpersonal dan juga organisasi. Perlu adanya hukum-hukum khusus yang mengatur tentang privasi di Indonesia. Berbagai negara maju telah memiliki peraturan khusus tentang perlindungan data pribadi, namun hingga saat ini Indonesia belum mempunyai peraturan tersebut. Masalah ini hanya diatur dalam Pasal 26 UU ITE dan beberapa pasal lainnya [2]

Penelitian oleh [10] untuk mengukur kesadaran responden terhadap risiko yang dapat terjadi dari kebocoran informasi pribadi. Responden ditanya apakah mereka memposting pribadi yang nyata informasi di akun mereka, data menunjukkan bahwa dua pertiga (66%) responden khawatir tentang penyalahgunaan informasi pribadi di akun media sosial. Selain itu, 69% dari responden tidak ingin orang asing melihat informasi pribadi mereka. responden juga ditanya apakah penyedia akun mereka membagikan informasi profil mereka dengan situs web lain. Data menunjukkan sepertiga (35%) menjawab ya. Ini menyoroti kebutuhan untuk mengembangkan kerangka kerja yang memberi pengguna wewenang untuk mengizinkan atau melarang situs web menggunakan informasi data pribadi. Hasil menunjukkan bahwa pengguna berhati-hati dalam menerima permintaan pertemanan dari orang asing. Meskipun 71 persen responden menerima undangan untuk menambahkan orang yang tidak dikenal sebagai teman dan sebanyak 68 persen menolak permintaan ini.

2.3. Metode Penelitian

Metode penelitian dilakukan adalah menggunakan metode blended. Penelitian ini dilakukan dengan cara mencari, membaca, mempelajari, serta memahami literatur atau yang berhubungan keamanan informasi pada media social, serta dengan penelitian pustaka. Secara umum, penelitian metode campuran merupakan penelitian yang melibatkan pengumpulan, analisis, dan interpretasi data kuantitatif dan kualitatif dalam satu studi tunggal atau dalam serangkaian studi yang menyelidiki fenomena mendasar yang sama.[11] Penelitian metode campuran adalah desain penelitian dengan asumsi filosofis serta metode penyelidikan. Sebagai metodologi, ini melibatkan asumsi filosofis yang memandu arah pengumpulan dan analisis data dan campuran data kualitatif dan kuantitatif dalam satu studi atau serangkaian studi. Kombinasi ini dapat memberikan pemahaman yang lebih baik tentang masalah

P-ISSN : 2548-9739
E-ISSN : 2685-5240

penelitian dibandingkan menggunakan satu pendekatan saja[12]

3. HASIL DAN PEMBAHASAN

Privasi merujuk padanan dari Bahasa Inggris privacy adalah kemampuan satu atau sekelompok individu untuk mempertahankan kehidupan dan urusan personalnya dari publik, yang mana seseorang mengontrol arus informasi mengenai diri sendiri. Penggambaran lainnya mengenai privasi adalah hak individu untuk menentukan apakah dan sejauh mana seseorang bersedia membuka dirinya kepada orang lain.

1. Fungsi Privasi

Ada tiga fungsi privasi, yaitu:

a. Pengatur dan pengontrol interaksi interpersonal yang berarti sejauh mana hubungan dengan oang lain diinginkan
b. Merencanakan dan membuat strategi untuk berhubungan dengan orang lain, yang meliputi keintiman atau jarak dalam berhubungan dengan orang lain.
c. Memperjelas identitas diri sumber

2. Privasi Data

Data dapat dikatakan data pribadi jika pada data tersebut dapat digunakan untuk mengenali atau mengidentifikasi seseorang, contoh dari data pribadi adalah nomor identitas mahasiswa beserta nama mahasiswa tersebut pada absensi. Nomor identitas tersebut dapat digunakan sebagai salah satu cara untuk mengidentifikasi mahasiswa tersebut. Namun, apabila pada absensi tersebut hanya terdapat kumpulan nomor identitas mahasiswa tanpa dilengkapi dengan nama mahasiswa tersebut, maka hanya disebut data. Alasannya karena data tersebut belum bisa digunakan untuk mengidentifikasi seseorang

3. Privasi Komunikasi

Komunikasi adalah pengiriman dan penerimaan pesan atau berita antara dua orang atau lebih sehingga pesan yang dimaksud dapat dipahami. Privasi Komunikasi dalam teknologi informasi membahas tentang bagaimana cara seseorang dapat berkomunikasi satu sama lain melalui teknologi informasi tanpa dipantau oleh pihak ketiga. Karena setiap orang memiliki batasan privat, oleh karena itu kita juga harus menghargai batasan tersebut. Hanya melalui undang-undang dan metode tertentu, maka batasan pada privasi komuniasi dapat diabaikan [2]

4. Privasi Online

Berbagai data dan informasi yang dikumpulkan dengan peningkatan frekuensi dan dalam konteks yang berbeda, membuat individu menjadi lebih transparan. Bahkan, terkadang seseorang dengan mudahnya menyebarkan opininya melalui akun jejaring sosial yang akrab dan digandrungi remaja. biaya sosial dan finansial yang ditanggung untuk memperoleh dan menganalisis data ini meningkat tajam seiring dengan kemajuan teknologi. Fenomena ini menimbulkan masalah antara lain privasi. Ada kekhawatiran bahwa Internet dapat mengikis privasi [13]dan bahwa masalah privasi dalam interaksi sosial secara offline atau tatap muka semakin diperbesar masalah tersebut dalam interaksi secara online . Ada sejumlah ancaman khusus ketika melakukan transaksi secara online berkaitan dengan privasi. Sebagai contoh, pengaruh saat berselancar melalui media internet berarti bahwa saat beraktifitas secara online, secara tidak langsung kita meninggalkan data berupa jejak digital dibanyak bidang kehidupan kita yang sebelumnya dianggap "offline." Perkembangan yang sangat cepat dengan daya komputasi, seperti pengolahan kecepatan, meningkatkan kapasitas penyimpanan, konektivitas komunikasi yang lebih luas, dan ukuran kapasitas koneksi dengan biaya rendah semua pada akhirnya mempengaruhi privasi. Oleh karena itu, ada isu-isu privasi penting terkait dengan aktivitas online. Tentu saja, ada juga manfaat bagi kemajuan teknologi yang dijelaskan seperti (layanan pribadi, kenyamanan, efisiensi ditingkatkan). Pengguna dapat

P-ISSN : 2548-9739
E-ISSN : 2685-5240

memberikan informasi berharga tentang diri mereka sendiri untuk mengambil keuntungan dan manfaat. Seperti aktifitas yang dilakukan American Life Survey (2001) melaporkan bahwa lebih dari dua-pertiga dari pengguna bersedia untuk berbagi informasi pribadi mereka di bawah beberapa keadaan. Dalam beberapa situasi, privasi ekspresif dapat diperoleh melalui hilangnya privasi informasi kepada pihak ketiga. Misalnya, seseorang mungkin mengungkapkan informasi pribadi dan informasi kartu kredit untuk kenyamanan menyelesaikan sebuah transaksi online. Dengan cara ini, koleksi pribadi, informasi privasi ini dapat dianggap sebagai "pedang bermata dua"

5. Kebebasan Informasi

Kebebasan termasuk suatu yang bersifat asasi, yang umumnya para ahli memiliki konsepsi yang sama bahwa kebebasan ada pada setiap insan. Secara ekripsi, kebebasan senantiasa ada batasan baik kelemahan yang bersifat internal maupun eksternal. Pada dasarnya kebebasan bukan berarti berbuat kehendak hati melainkan ada batasnya untuk mengakui dan menghormati hak dan mewajibkan setiap manusia pada umumnya. Informasi telah mengenalkan suatu etika baru, bahwa setiap pihak yang mempunyai informasi memiliki naluri yang senantiasa mendesiminasikan kepada pihak lain, begitu pula sebaliknya. Teknologi informasi menjanjikan bahwa komunitas abad 21 akan memiliki jaringan komunikasi dan teknologi multi media sebagai tulang punggunanya. Penghargaan atas privasi dalam komunitas informatika yang mengglobal, amat sangat berbeda dalam suasana yang fiscal, demikian pula dalam kepentingan atas privasi data. Keperluan menjaga kerahasiaan data dan informasi pribadi tampak menjadi prioritas untuk meletakkan kepercayaan dalam jaringan interaksi komunikasi.

6. Anonimitas dalam Aktifitas Online

Anonimitas adalah tidak beridentitas. Contohnya bagi masyarakat peserta pemilu tentu saja ketika nyoblos tidak menuliskan nama pada kertas suara. Ini untuk menjamin kerahasiaan pada saat pemilu. Privasi dan anonimitas adalah 2 hal yang sangat erat kaitannya dan mirip. Tetapi prinsipnya Anonimitas adalah untuk privasi sedangkan privasi belum tentu membutuhkan anonimitas, walaupun biasanya memerlukan. Privasi bisa saja didapat dengan menerapkan sekuritas misalnya enkripsi. Contohnya, saat mengirimkan e-mail yang disertai alamat dan nama, namun isinya diacak untuk mencegah orang lain melihat isi e-mail. Di media digital seperti internet, apapun service yang digunakan sedikitnya seseorang telah membuka identitasnya sendiri. Bagaimana dan apa tentang diri seseorang tersebut yang dapat diketahui orang lain. Berikut ini langkah-langkah yang bisa dilakukan guna menjaga privasi ketika berselancar di dunia maya.

1. Mengubah pengaturan privasi atau keamanan. Pahami dan gunakan fitur setting pengamanan ini seoptimal mungkin.
2. Buat kata sandi sekuat mungkin. Ketika melakukan registrasi online, sebaiknya lakukan kombinasi antara huruf besar dan kecil, angka, dan simbol supaya tak mudah terlacak.
3. Rahasiakan password yang dimiliki.
4. Jangan gunakan pertanyaan mengenai tanggal lahir, alamat, nama ibu karena pertanyaan tersebut hampir selalu digunakan sebagai pertanyaan keamanan untuk database bank dan kartu kredit. Ini memberi peluang bagi peretas untuk mencuri identitas dan mencuri uang.
5. Selalu log out. Selalu ingat untuk keluar dari akun, khususnya jika menggunakan komputer fasilitas umum.
6. Wi-FI. Buat kata sandi untuk menggunakan wi-fi, jika tidak, mungkin saja ada penyusup yang masuk ke jaringan.
7. Jangan berbagi informasi sensitif yaitu menghindari pembagian informasi yang bersifat pribadi.

P-ISSN : 2548-9739
E-ISSN : 2685-5240

8. Persulit cara log in ke akun yaitu dengan memilih kata sandi yang kuat dan unik, serta menyalakan two-factor authentication.
9. Gunakan aplikasi dengan end-to-end encryption Ini merupakan fitur di aplikasi chatting untuk menjaga keamanan data pribadi di media sosial.
10. Selalu cek aplikasi yaitu memastikan sudah memahami berbagai akses yang dibutuhkan oleh aplikasi.[14]
11. Enam poin utama yang harus dipertimbangkan saat menggunakan sistem aplikasi online terkait privasi data yaitu keamanan dan data perlindungan, kesadaran pengguna, pengaturan kontrol, manajemen risiko, transparansi, dan etika.[15]

4. KESIMPULAN

Isu privasi dan kepercayaan adalah sangat krusial tidak hanya untuk desain sistem komputer tapi juga bagaimana penelitian dilakukan secara online. Beberapa point penting adalah keamanan dan data perlindungan, kesadaran pengguna, pengaturan kontrol, manajemen risiko, transparansi, dan etika. Pengembang sistem pada instansi yang mengelola informasi personal harus menerapkan pedoman atau SOP (Standar Operasional Prosedur) untuk membatasi jumlah informasi pribadi yang dikumpulkan dan peran kebijakan privasi (privacy policy) yang membutuhkan pengungkapan jati diri pada dasar Must Know (apa saja informasi yang perlu diketahui), karena berdasarkan asumsi umum bahwa semua administrator pengelola informasi memiliki akses penuh ke data pengguna, sehingga ada kemungkinan untuk perlunya regulasi yang cukup ketat. Perlu dibangun kepercayaan ke dalam rancangan layanan Internet, baik melalui kegiatan rancang bangun pengelolaan suatu sistem yang lebih mengedepankan user priority. Memungkinkan, user diberikan pilihan mekanisme kontrol terhadap perlu tidaknya dalam mengungkapkan informasi pribadi dan penggunaannya.

5. SARAN

Hingga saat ini masih banyak kasus penyalahgunaan data pribadi dalam sistem online. Beberapa kasus adalah mengungkapkan bahwa peningkatan kesadaran pengguna akan pentingnya melindungi data pribadi. Penelitian ini masih merupakan studi pendahuluan, sehingga masih banyak hal yang dapat digali berdasarkan penelitian ini, perlu dibangun sebuah algoritma dan sistem untuk menjaga keamanan dan kerahasiaan data privacy

DAFTAR PUSTAKA

[1] H. Gunawan, “Pengukuran Kesadaran Keamanan Informasi Dan Privasi Dalam Sosial Media,” *J. Muara Sains, Teknol. Kedokt. dan Ilmu Kesehat.*, vol. 5, no. 1, p. 1, 2021, doi: 10.24912/jmstkik.v5i1.3456.

[2] I. T. Islamy, S. T. Agatha, R. Ameron, B. H. Fuad, Evan, and N. A. Rakhmawati, “Pentingnya Memahami Penerapan Privasi di Era Teknologi Informasi,” *J. Teknol. Inf. dan Ilmu Komput.*, vol. 11, no. 2, pp. 21–28, 2018.

[3] T. Agustin, “Analisis Keamanan Sistem Informasi Terhadap Data Pribadi di Media sosial,” 2020.

[4] D. Revilia and N. Irwansyah, “Social Media Literacy: Millenial’s Perspective of Security and Privacy Awareness,” *J. Penelit. Komun. Dan Opini Publik*, vol. 24, no. 1, pp. 1–15, 2020, doi: 10.33299/jpkop.24.1.2375.

[5] M. M. AMANDA LENHART, “Social Networking Websites and Teens: An Overview,” 2008.

P-ISSN : 2548-9739
E-ISSN : 2685-5240

[6] D. M. Boyd and N. B. Ellison, "Social network sites: Definition, history, and scholarship," *J. Comput. Commun.*, vol. 13, no. 1, pp. 210–230, 2007, doi: 10.1111/j.1083-6101.2007.00393.x.

[7] L. Rizkinaswara, "Pahami Kebijakan Privasi di Media Sosial untuk Lindungi Data Pribadi," *https://aptika.kominfo.go.id/*, 2019. .

[8] M. K. M. Nasution, "Keamanan Informasi : Pendahuluan Keamanan Informasi : Pendahuluan," no. September, 2018, doi: 10.13140/RG.2.2.12303.64160.

[9] N. Senthil Kumar, K. Saravanakumar, and K. Deepa, "On Privacy and Security in Social Media - A Comprehensive Study," *Phys. Procedia*, vol. 78, no. December 2015, pp. 114–119, 2016, doi: 10.1016/j.procs.2016.02.019.

[10] N. Aldhafferi, C. Watson, and S. A.S.M, "Personal Information Privacy Settings of Online Social Networks and Their Suitability for Mobile Internet Devices," *Int. J. Secur. Priv. Trust Manag.*, vol. 2, no. 2, pp. 1–17, 2013, doi: 10.5121/ijsptm.2013.2201.

[11] N. L. Leech and A. J. Onwuegbuzie, "A typology of mixed methods research designs," *Qual. Quant.*, vol. 43, no. 2, 2009, doi: 10.1007/s11135-007-9105-3.

[12] John W. Creswell and Vicki L. Piano Clark, "Designing and Conducting Mixed Methods Research," *Aust. N. Z. J. Public Health*, vol. 31, no. 4, 2007, doi: 10.1111/j.1753-6405.2007.00096.x.

[13] R. T. Rust, P. K. Kannan, and N. Peng, "The customer economics of internet privacy," *Journal of the Academy of Marketing Science*, vol. 30, no. 4. 2002, doi: 10.1177/009207002236917.

[14] H. P. Yuwinanto, "Privasi online dan keamanan data," *Palimpsest (Iowa. City).*, no. 031, p. 11, 2015.

[15] D. Puspa, A. Soegiharto, A. Nizar Hidayanto, and Q. Munajat, "Data Privacy, What Still Need Consideration in Online Application System?," *J. Sist. Inf.*, vol. 16, no. 1, pp. 49–63, 2020, doi: 10.21609/jsi.v16i1.941.