LITERASI MEDIA SOSIAL: KESADARAN KEAMANAN DAN PRIVASI DALAM PERSPEKTIF GENERASI MILENIAL

SOCIAL MEDIA LITERACY: MILLENIAL'S PERSPECTIVE OF SECURITY AND PRIVACY AWARENESS

Donna Revilia[1], Irwansyah[2]
[1,2] Departemen Ilmu Komunikasi, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Indonesia
Salemba, Jakarta Pusat
email : donnarevilia11@gmail.com[1], dr.irwansyah.ma@gmail.com[2]
(Diterima: 09-04-2019; Direvisi: 08-05-2020; Disetujui terbit: 25-5-2020)

Abstrak

Situs media sosial memberi masyarakat analog kemampuan menjangkau audiens global, dan berjasa dalam sarana konektivitas untuk mencari informasi, bersosialisasi, dan mempengaruhi, sayangnya juga memberikan celah terjadinya pelanggaran privasi dan keamanan terhadap data pribadi pengguna. Generasi milenial sebagai generasi yang "selalu terhubung" menjadi target dari kurangnya kesadaran akan pentingnya prosedur keamanan dan privasi ini. Salah satu karakteristik mereka yaitu berbagi data dengan berbagai perangkat *online* dan konvergensi media menambah resiko ancaman digital, bagaimana kondisi kerentanan keamanan *cyber* serta sejauh mana pemahaman tentang ancaman tersebut menjadi masalah menarik untuk diteliti. Penelitian bertujuan untuk mengetahui kondisi literasi digital penggunaan media sosial di kalangan generasi millenial. Metode yang digunakan dalam penelitian ini adalah *survey*, wawancara dan observasi, analisis data kondisi literasi digital pada generasi milenial dilakukan menggunakan *Technology Acceptance Model (*TAM*)*. Hasil penelitian ditemukan bahwa pengguna yang lebih lama menggunakan media sosial tidak mempengaruhi tingkat literasi media sosial. Pengguna yang pernah mengalami ancaman lebih menunjukkan kesadaran dengan meningkatkan level keamanan akun media sosial, dan lebih waspada sebelum mengijinkan akses ke perangkat pribadi. Individu yang lebih sadar akan pengaturan kata sandi umumnya memiliki tingkat kesadaran lebih tinggi tercermin dari niat mereka untuk berperilaku aman saat menggunakan media sosial.
Kata kunci: media sosial, literasi digital, generasi milenial, privasi, keamanan, teknologi, *acceptance model*

Abstract

Social media sites has given the analog community ability to reach global audience, providing connectivity to reach information, socialize and influence, unfortunately, it also provides room for violations of user's personal data. Millennials as the "always connected" generation are targets of the lack awareness of the importance security and privacy procedures. Millenials characteristic, sharing personal data with various online devices increases the risk of digital threats, how they capture the situation of cybersecurity vulnerabilities and how their understanding the threat becomes interesting problem to study. This research was aimed at finding the conditions of millennials digital literacy as active users of social media. The method used is mixed method by survey, interview and observation, data analysis of digital literacy conditions of millennials using the theory of Technology Acceptance Model (TAM). The results found that users use social media in years do not influence their social media literacy level. Users who have social media threats experienced show more awareness by increasing security level of their account and more vigilant before allowing access from social media accounts. Individuals more aware of their password settings generally have a higher level of awareness reflected in their intention to behave safely when using social media.
Keywords*: social media; digital literacy; millenial generation; privacy, security, technology acceptance model*

PENDAHULUAN

Awal tahun 2019 riset yang dilakukan oleh perusahaan media We Are Social yang bekerja sama dengan Hootsuite, merilis data perkembangan jumlah pengguna internet Indonesia yang semakin pesat

dengan kenaikan sebanyak 20 persen dibandingkan jumlah pada tahun 2018, dalam rilisnya ada 150 juta pengguna media sosial di Indonesia dilansir dari tekno.kompas.com. Padahal setahun 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 (Kompas.com, 15/04/2018). Terangkatnya kasus kebocoran data pengguna ini bukanlah hal baru, kasus Facebook sebagai media sosial yang dimahkotai peringkat pertama dengan jumah pengguna aktif mencapai 2.271 miliar (dilansir dari CNBC Indonesia, 24 Februari 2019) ini seolah – olah membangunkan masyarakat digital akan isu privasi dan keamanan yang sama pentingnya dengan keamanan dunia analog.

Kekhawatiran tentang keamanan di media sosial juga dikemukakan oleh Nuha et.al (2018) dalam penelitian mereka, jejaring sosial *online* menjadi sumber ancaman tingkat lanjut untuk intelijen dan penjahat *cyber* yang mengalihkan fokus serangan mereka ke jejaring sosial. Ini menunjukkan bahwa sifat penggunaan jejaring sosial menjadi sarana ancaman yang berpindah dengan mudah dari satu pengguna ke pengguna lain (Bozart, 2010). Saluran jejaring sosial memainkan peran penting dalam memfasilitasi penetrasi ancaman keamanan, geografis, politik, dan sosial menurut Mansour dalam Zolait (2016). Internet, telepon seluler, dan jejaring sosial *online* semuanya diperkenalkan selama tahun-tahun pertumbuhan generasi milenial. Generasi milenial adalah "penduduk asli" teknologi dibanding generasi lain, tidak peduli kecakapan teknologi individu mereka, dipandang sebagai "imigran" (Hershatter and Epstein, 2010) yang menjadikan mereka target yang rentan terhadap ancaman privasi dan keamanan *cyber*.

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 milennial (Centre for Strategic and International Studies, 2017).

Generasi milenial adalah generasi yang lahir antara tahun 1981-2000, atau yang saat ini berusia 19 tahun hingga 38 tahun, begitu mudahnya terpapar ancaman keamanan di dunia digital, karakteristik mereka berbagi data pribadi dengan berbagai perangkat *online* yang disebabkan oleh konvergensi media menambah resiko ancaman digital, bagaimana mereka menangkap situasi kerentanan keamanan *cyber* ini serta sejauh mana pemahaman mereka tentang ancaman tersebut menjadi masalah yang menarik untuk diteliti. Perilaku tersebut tergantung pada realisasi aktual dan pengalaman mereka di media sosial. Sebagai contoh, pengguna yang menjadi korban pencurian identitas atau *cyber bullying* akan memiliki perspektif keamanan dan kepercayaan yang sangat berbeda dari mereka yang tidak. (Zhang and Gupta, 2016). Penelitian ini dilakukan bertujuan untuk mengetahui bagaimana kondisi literasi digital terhadap penggunaan media sosial di kalangan generasi milenial yang merupakan pengguna aktif dari media sosial.

LANDASAN TEORI

Media Sosial

Pada tahun 1979, Tom Truscott dan Jim Ellis dari Duke University telah menciptakan Usenet, sistem diskusi di seluruh dunia yang memungkinkan pengguna Internet untuk mengirim pesan publik. Ketersediaan akses Internet berkecepatan tinggi semakin menambah popularitas konsep tersebut, yang mengarah pada penciptaan situs jejaring sosial seperti MySpace (tahun 2003) dan Facebook (tahun 2004). Lalu terciptakan istilah 'media sosial' dan berkontribusi pada keunggulan yang dimilikinya hingga saat ini (Kaplan and Haenlein, 2010).

Web 2.0 adalah istilah yang pertama kali digunakan pada tahun 2004 untuk menggambarkan cara baru di mana pengembang perangkat lunak dan pengguna akhir (*end user*) mulai memanfaatkan *World Wide Web*; sebagai platform di mana konten dan aplikasi tidak lagi dibuat dan diterbitkan oleh individu, melainkan terus dimodifikasi dengan partisipatif dan kolaboratif oleh semua pengguna (Kaplan and Haenlein, 2009).

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 (Kaplan and Haenlein, 2010). Setidaknya ada enam jenis sosial media yang dikelompok berdasarkan kehadiran sosial/kekayaan media dan presentasi diri/pengungkapan diri yang dijelaskan dalam Tabel 1 (Kaplan and Haenlein 2010).

Tabel 1. Klasifikasi Media Sosial berdasarkan kehadiran sosial / kekayaan media dan presentasi diri / pengungkapan diri

presentasi diri/ pengungkapan diri	**kehadiran sosial / kekayaan media**		
	Rendah	**Medium**	**Tinggi**
Tinggi	*Blogs and microblogs* (e.g Twitter)	*Social Networking Sites* (e.g Facebook)	*Virtual Social Worlds* (e.g Second Life)
Rendah	*Collaborative Projects* (e.g Wikipedia)	*Content Communities* (e,g Youtube)	*Virtual Game Worlds* (e.g World of Warcraft

Sumber: (Kaplan and Haenlein, 2010)

Information Security di era IoT

Internet of Things didefinisikan sebagai infrastruktur jaringan global yang dinamis dengan konfigurasi sendiri dan komunikasi yang dapat dioperasikan. Sederhananya, 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. (Ali, Ali, and Badawy 2015) 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. IoT memungkinkan orang dan hal-hal untuk terhubung kapan saja, di mana saja, dengan apa pun dan siapa pun, idealnya menggunakan setiap jalur/jaringan dan layanan apa pun. Kevin Ashton pertama kali menggunakan istilah *Internet of Things*, (Nuamah and Seong, 2017) Kevin adalah salah satu perintis yang

berbicara tentang IoT. Menurut Atzori A.lera et al dalam Ali, Ali, and Badawy (2015) diklasifikasikan IoT ke tiga paradigma yaitu, berorientasi internet (*Middleware*), berorientasi hal (Sensor), dan berorientasi semantik (Pengetahuan). Di era IoT dimana semua dapat terhubung dengan internet, memperbesar celah ancaman keamanan dan privasi. *Cyber security* menjadi isu yang penting dalam IoT yang berkaitan erat dengan privasi dan keamanan data pengguna, pada kasus Facebook, resiko data yang dicuri dan dikumpulkan untuk dijual kembali menjadi kasus yang dapat mengganggu keamanan. Mengenai keamanan, IoT akan dihadapkan pada tantangan yang lebih berat karena beberapa alasan seperti: IoT memperluas 'internet' tradisional, jaringan seluler dan jaringan sensor dan sebagainya, setiap 'hal' akan terhubung ke 'internet', dan 'hal-hal ini' akan berkomunikasi satu sama lain. Karena itu masalah keamanan dan privasi akan muncul. Pengguna harus lebih memperhatikan masalah kerahasiaan, keaslian, dan integritas data dalam IoT (Suo et al. 2012).

Generasi Milenial

Pew Research Center membagi demografis (cohort) menjadi 4 generasi yaitu (Taylor and Keeter, 2010) :

1. Generasi *baby boomer* yaitu generasi yang lahir setelah Perang Dunia II. Pada era tersebut kelahiran bayi sangat tinggi karena itu disebut generasi *baby boomer.*
2. Generasi X (Gen-Xer), generasi yang lahir pada tahun 1965 hingga 1980.
3. Generasi milenial adalah generasi yang lahir antara tahun 1981-2000. Generasi milenial (dikenal sebagai Generasi Y)
4. Generasi Z merupakan generasi yang lahir setelah tahun 2000 hingga saat ini.

Keberadaan generasi milennial bertepatan dengan tumbuh pesatnya teknologi web.2.0 dimana muncul jejaring media sosial (*social media*) yang tumbuh subur diiringi dengan munculnya smartphone, dan berkembangnya teknologi internet. Itu sebabnya generasi milenial disebut sebagai generasi yang "melek teknologi". Penggunaan teknologi tersebut sudah menjadi bagian dari hidup mereka yang tertanam sebagai bagian dari jati diri (Taylor and Keeter, 2010).

Didukung juga oleh riset Alvara Research Center pada *survey* penggunaan internet di Indonesia tahun 2015 yang memperlihatkan komposisi *addicted user* pada generasi milenial lebih besar dibanding dengan gen-Xer, begitu pula dalam hal konsumsi internet, terutama terjadi pada *younger millennial generation* yang berusia 19-29 tahun. Berdasarkan data tersebut semakin muda pengguna maka semakin tinggi pula konsumsi internetnya hal ini memperkuat persepsi bahwa generasi milenial berkomunikasi dan aktualisasi diri dengan internet sebagai kebutuhan pokok mereka (Purwandi, 2020).

Berdasarkan penelitian-penelitian yang telah dilakukan sebelumnya didapatkan karakteristik generasi milenial sebagai berikut:

1. Menggunakan *User Generated Content* (UGC) dibandingkan platform lainnya.
2. Ponsel lebih penting dari televisi.
3. Akun media sosial adalah kewajiban.
4. Metode baca digital dan mulai meninggalkan media konvensional.
5. Fasih berteknologi dibandingkan orang tua mereka
6. Efektif bekerja walaupun tidak loyal.
7. Lebih memilih transaksi non tunai.

Generasi milenial yang disebut generasi "melek teknologi" tersebut tidak

serta merta menjadikan mereka generasi dengan literasi digital yang memadai terhadap pemahaman mereka tentang keamanan dan privasi. Oleh sebab itu, penelitian ini sangat relevan untuk mengetahui kondisi literasi digital pada generasi milenial, terutama pemahaman media sosial, dimana generasi milenial dan masyarakat digital dihadapkan pada dua konsep yang tidak bisa dilepaskan yaitu kebebasan dan privasi.

Privasi

Privasi telah ada sejak lama, didefinisikan sebagai ruang privat (*private sphere*). Samuel D. Warren dan Louis D. Brandeis (1890) menyebut privasi juga sebagai "*the right to be let alone*" atau jika diartikan dalam bahasa Indonesia menjadi hak untuk dibiarkan sendiri (Collste, 1992). Definisi ini masih berlaku, namun harus ditempatkan dalam lingkungan modern di mana harus hidup berdampingan dengan minat masyarakat dalam kehidupan berjaringan (*networked life*). Dengan kata lain, fenomena media sosial yang agak baru dan konsekuensinya terhadap kesediaan untuk berbagi informasi pribadi harus diperhitungkan (Hiselius, 2015). Privasi mungkin adalah masalah yang paling banyak dibahas dalam etika-TIK. Privasi memungkinkan orang untuk mengekspresikan diri secara individu atau kolektif tanpa terlalu khawatir tentang konsekuensi ekspresif mereka (Schachter, 2003 dalam Youm & Park, 2016). Ini menjelaskan mengapa anonimitas diizinkan sebagai hak kebebasan berbicara (Youm and Park, 2016). Dalam istilah praktis, seringkali terjadi setiap hari melalui informasi sederhana yang kita pilih untuk dibagikan, atau tidak untuk dibagikan. Jadi, privasi dan perlindungan privasi harus digambarkan sebagai fenomena yang sangat dinamis. (Hiselius, 2010). Di Indonesia, media sosial kerap menjadi celah pelanggaran privasi. Adanya *right to be forgotten*/hak untuk dilupakan memicu perdebatan ilmiah yang timbul oleh keputusan antara hak seseorang atas privasi dan kebebasan berekspresi melalui internet (Tirosh, 2016).

Kebebasan

Dalam dunia digital, kebebasan dapat dikaitkan dengan kebebasan untuk berekspresi dan kebebasan mengakses internet. Internet menjadi ruang baru bagi individu untuk berekspresi dan mencari informasi. Meskipun internet adalah protokol yang sebagian besar terbuka, negara telah melakukan upaya untuk membatasi dan bahkan kadang-kadang mengkooptasi kebebasan dalam internet menurut Howard, 2011 dalam Gainous, Wagner, Gray, Gainous, & Wagner (2016). Media sosial memberikan kebebasan dalam berekspresi, beberapa generasi milenial memanfaatkan layanan ini untuk mencari nafkah, berjualan *online*, sampai menjadi terkenal dan viral. Banyaknya keuntungan dari kebebasan ini tentu tidak tanpa resiko, ijin data pribadi yang selalu diminta platform aplikasi media sosial yang digunakan sebagai syarat untuk masuk sering diabaikan. Padahal ketika pengguna mengijinkan akses, maka data yang terdapat pada perangkat pribadi pengguna akan langsung tersimpan dalam database aplikasi tersebut, mungkin nantinya data digunakan untuk dianalisis dan dikomersialkan kembali dengan bentuk data agregat.

Penelitian Sejenis

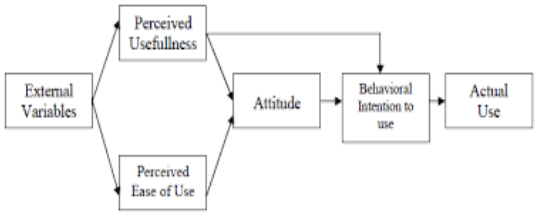
Penelitian sejenis pernah dilakukan oleh Zolait dkk dengan judul "*User Awareness of Social Media Security: The Public Sector Framework*" tahun 2014.

Tujuan penelitian ini adalah untuk menguji faktor yang mempengaruhi keamanan pengguna di antara pengguna media sosial di sektor pendidikan. Menggunakan *convenience sampling* dari 338 pengguna media sosial yang dipilih secara acak termasuk mahasiswa dan anggota staf Universitas Bahrain, serta individu dari luar Universitas Bahrain. Temuan mengungkapkan, baik kesadaran pengguna dan pengetahuan pengguna memiliki pengaruh kuat pada sikap pengguna untuk berperilaku aman saat menggunakan media sosial tersebut. Peneliti menemukan bahwa responden bidang studi yang terkait dengan keamanan informasi memiliki kesadaran yang lebih tinggi, yang tercermin dalam niat mereka. Niat tidak cukup untuk menginstruksikan tingkat kesadaran pengguna tentang masalah keamanan media sosial (Zolait, 2016).

Penelitian lainnya yang dilakukan oleh Tuunainen dkk dengan judul "*Users' Awareness of Privacy on Online Social Networking sites – Case Facebook*" tahun 2009 melihat perilaku privasi dari perspektif perlindungan privasi dan pengungkapan informasi. Dalam studi empiris ini, disajikan hasil survei terhadap 210 pengguna Facebook. Hasil penelitian ini menunjukkan, bahwa sebagian besar responden, yang adalah pengguna aktif Facebook, mengungkapkan sejumlah besar informasi pribadi. Selain itu, sebagian besar responden tidak mengetahui atau memahami kebijakan privasi Facebook dan ketentuan penggunaannya (Tuunainen, 2009). Penelitian-penelitan di atas belum menggambarkan secara detil kondisi literasi suatu generasi. Maka dalam penelitian ini penulis menggunakan celah tersebut untuk melakukan penelitian pada generasi milenial dengan menggunakan *Technology Acceptance Model* (TAM).

***Technology Acceptance Model* (TAM)**

Sejalan dengan tujuan dari penelitian ini yaitu untuk mengetahui bagaimana kondisi literasi digital terhadap penggunaan media sosial di kalangan generasi milenial terdapat beberapa variabel yang dapat membantu mengidentifikasi kondisi literasi digital pada generasi milenial dalam kaitannya tentang pemahaman mereka tentang keamanan dan privasi serta kebebasan dalam bermedia sosial, variabel tersebut ditelaah dengan menggunakan teori TAM. *Technology Acceptance Model* (TAM) adalah teori sistem informasi yang dikembangkan untuk membuat prediksi tentang penerimaan teknologi. TAM didasarkan pada hubungan kausal antara keyakinan - sikap - niat - perilaku dalam *Theory of Reasoned Action* (TRA) (Fădor, 2014). *Technology Acceptance Model* (TAM) dikembangkan oleh Davis (1989) dalam Zolait (2016) untuk mempelajari perilaku dan tingkat penerimaan pengguna terhadap penggunaan komputer atau teknologi baru. Teori ini terdiri dari faktor-faktor yang memiliki sebagai berikut: Kegunaan yang dirasakan (sejauh mana pengguna percaya penggunaan sistem tertentu akan meningkatkan kinerja mereka). Persepsi kemudahan penggunaan (sejauh mana pengguna percaya bahwa menggunakan sistem tertentu itu mudah dan tidak memerlukan upaya apapun).



Gambar 1. Kerangka pemikiran Teori *Technology Acceptance Model* (TAM)
Sumber: (Zolait, 2016)

Berdasarkan penelitian sebelumnya didapatkan kerangka pemikiran yang

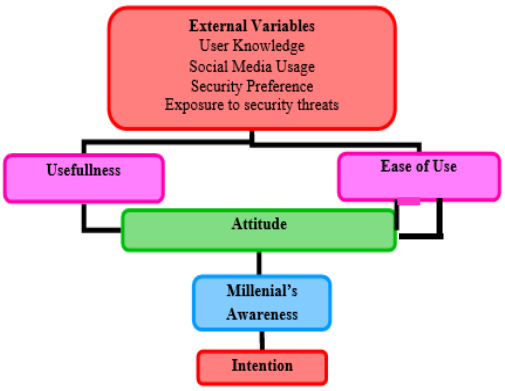
memiliki faktor-faktor: variabel eksternal (pengetahuan pengguna, penggunaan media sosial, preferensi keamanan, dan paparan terhadap ancaman keamanan) dan variabel teoretis (persepsi manfaat, persepsi kemudahan penggunaan, sikap terhadap keamanan media sosial, niat perilaku, dan penggunaan aktual). Kedua variabel digunakan untuk mempelajari perilaku pengguna media sosial dan tingkat kesadaran mereka tentang keamanan media sosial (Zolait, 2016) yang dalam penelitian ini akan diterapkan kepada kesadaran keamanan dan privasi pada generasi milenial.

METODE PENELITIAN

Metode penelitian dilakukan dengan menggunakan metode campuran. 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. (Leech and Onwuegbuzie, 2009). 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 penelitian dibandingkan menggunakan satu pendekatan saja (Creswell and Clark, 2017). Data kuantitatif penelitian ini didapatkan dari hasil *survey* sederhana menggunakan kuesioner *online* dan data kualitatif dilakukan melalui wawancara dari informan untuk mendapatkan hasil yang lebih komprehensif yang hasilnya akan ditampilkan dalam bentuk gambar.

Model Penelitian

Model penelitian mengadaptasi dari teori TAM yang berfokus pada dua variabel eksternal yaitu *perceived usefulnes* dan *perceived ease of use* yang didalamnya juga terdapat variabel *user knowledge, social media usage, security preference* dan *exposure to security threats*, yang menentukan sikap terhadap kesadaran generasi milenial dan mempengaruhi keputusan akhir mereka dalam berperilaku dengan teknologi. Berikutnya didapatkan kerangka teori seperti dibawah ini.



Gambar 2. Kerangka Penelitian berdasarkan *Technology Acceptance Model* terhadap Milenial
Sumber: (Zolait 2016)

Teknik Pengumpulan dan Sumber Data

Penelitian ini menggunakan teknik pengumpulan data *purposive sampling* kepada generasi milenial dari berbagai latar belakang pekerjaan dan usia, lalu dilakukan *survey* sederhana dengan kuesioner *online*, dan wawancara dilakukan untuk mengeksplor jawaban yang lebih mendalam dari partisipan.

Metode Analisis Data

Analisis dilakukan dengan *Technology Acceptance Model* (TAM). Statistik deskriptif digunakan untuk menjabarkan hasil analisis data yang sudah terkumpul.

HASIL PENELITIAN DAN PEMBAHASAN

Profil Informan

Profil informan merupakan variabel berdasarkan usia, bidang studi / pekerjaan saat ini, sudah berapa lama menggunakan media sosial dan waktu rata-rata harian yang dihabiskan di media sosial. Informan dalam penelitian ini adalah generasi milenial dengan rentang usia 26 - 33 tahun, semuanya pekerja baik dalam pemerintahan maupun swasta, dan mayoritas sudah menggunakan media sosial lebih dari 10 tahun, dan yang paling lama sudah menggunakan media sosial selama 19 tahun. Setiap harinya informan menggunakan media sosial, dengan lama 1 jam perhari sampai 15 jam perhari. Mayoritas pengguna menggunakan media sosial lebih dari 3 jam per hari.

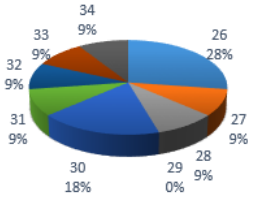


Diagram 1. Usia Responden

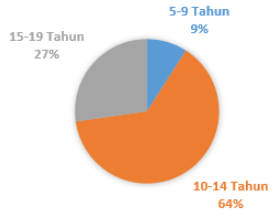
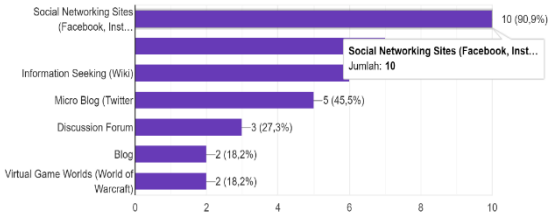


Diagram 2. Lama gunakan media sosial

Penggunaan Media Sosial

Hampir semua informan adalah pengguna aktif SNS seperti Facebook dan Instagram, sementara yang lainnya aktif pengguna layanan *content communities* (Youtube) dan *collaborative project* seperti Wikipedia, diikuti pengguna aktif Twitter, dan sisanya menggunakan forum diskusi dan *game virtual game worlds*.

Temuan penelitian dengan tujuan dalam penggunaan media sosial, mayoritas informan mengatakan menggunakan media sosial untuk tujuan *entertainment*, berikutnya untuk tujuan bersosialisasi, sisanya untuk akses berita dan pendidikan.



Grafik 1. Penggunaan media social

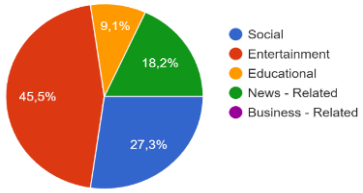
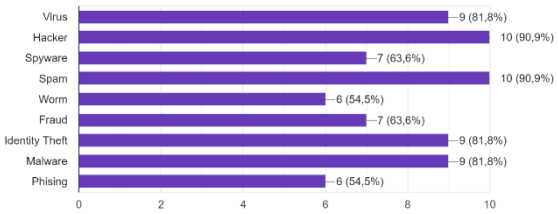


Diagram 3. Tujuan penggunaan Media Sosial

Keakraban Pengguna dengan Keamanan Informasi

Mayoritas informan akrab dengan istilah *hacker* dan *spam* (90.9%), lalu dengan virus, *identity theft* dan *malware* sebanyak 81.8%, 63.6% akrab dengan istilah *spyware* dan *fraud*, hanya 54,5% akrab dengan istilah *worm* dan *phishing*

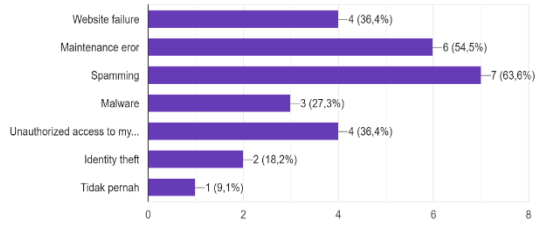


Grafik 2. Keakraban dengan istilah keamanan informasi

Ancaman keamanan yang dialami oleh pengguna aktif

Sebagian besar sebanyak 63.6% dari mereka pernah terkena ancaman terhadap *spamming*, 54.5% mengalami *maintenance error*, 36.4% mengalami keamanan dari kegagalan situs web dan akses tidak sah ke

akun dan data mereka, dengan 27.3. % dari pengguna telah menghadapi *malware*, dan 18.2% pengalami pencurian identitas lalu hanya 9.1% pengguna yang tidak pernah mengalami ancaman apapun.



Grafik 3. Ancaman yang pernah dialami pengguna

Tindakan pencegahan keamanan

Temuan tindakan pencegahan keamanan menunjukkan 54.5% informan menggunakan 7 - 8 karakter panjang preferensi, dan 45.5% menggunakan lebih dari 8 karakter kata sandi, tentang preferensi privasi 63.6% pengguna menggunakan mode *private*, sisanya mengatakan tergantung pada akun media sosialnya.

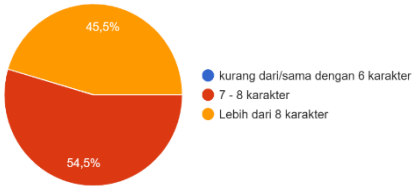


Diagram 4. Panjang preferensi kata sandi yang digunakan

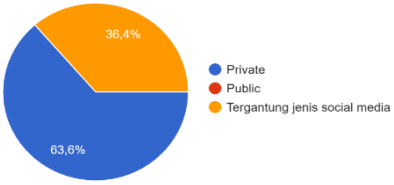


Diagram 5. Preferensi privasi akun

Akuntabilitas keamanan

Dalam hal akuntabilitas pengguna, temuan menunjukkan bahwa lebih dari setengah informan (63.6%) percaya bahwa pengguna itu sendiri harus bertanggung jawab untuk melindungi informasi mereka sendiri, lalu sisanya percaya bahwa keamanan adalah tanggung jawab dari situs web media sosial.

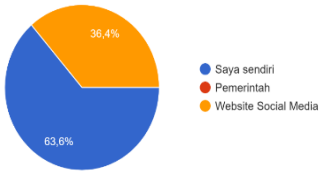


Diagram 6. Pihak yang bertanggung jawab terhadap keamanan media sosial

Definisi keamanan informasi

Di antara jumlah total responden, 81.8% sepenuhnya setuju dengan definisi keamanan informasi sebagai ‘privasi dan kerahasiaan’, dan minoritas yang bahkan lebih kecil (18.2%) memahami bahwa keamanan adalah aman dari ancaman serangan kemanan di media sosial. Temuan ini menunjukkan bahwa mayoritas tidak akrab dengan konsep keamanan informasi dan definisinya.

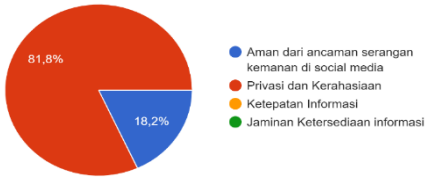


Diagram 7. Pemahaman tentang definisi keamanan informasi

Pengetahuan keamanan informasi

Dalam hal pengetahuan, pengguna memiliki keyakinan pengetahuan teoritis dan keterampilan teknis yang seimbang. Dalam hal pengaturan preferensi kata sandi, temuan menunjukkan bahwa lebih dari setengah responden (63.6%) menggunakan campuran huruf besar dan kecil dan sisanya (36.4%) menggunakan berbagai karakter yang berbeda (?, !, _, #) dalam kata sandi mereka.

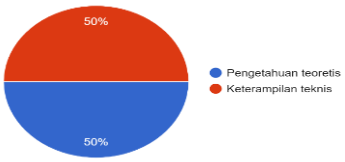


Diagram 8. Pengetahuan tentang keamanan informasi

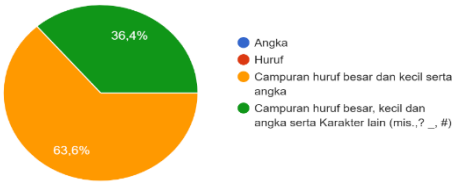


Diagram 9. Preferensi Kata sandi

Masalah keamanan dalam hal psikologis

Data selanjutnya menyajikan temuan yang berkaitan dengan masalah keamanan media sosial mengingat lima faktor psikologis. Dalam hal perilaku kesengajaan responden, penelitian ini menunjukkan bahwa 36.4% responden menggunakan kata sandi yang sama untuk akun media sosial yang berbeda, 27.3% menggunakan nama pengguna yang sama untuk akun media sosial yang berbeda, 18.2% selalu menggunakan kata 'ingat saya' fitur kata sandi, dan tidak satupun pengguna selalu memperbarui kata sandi mereka secara teratur.

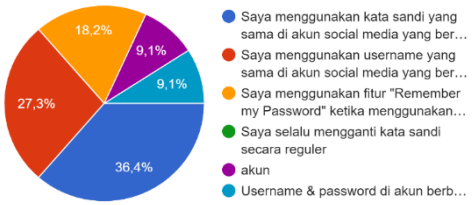


Diagram 10. Faktor Psikologis: Perilaku yang disengaja

Penjelasan kekhawatiran keamanan oleh faktor psikologis

Dalam hal perilaku yang tidak disengaja, temuan mengungkapkan bahwa 36,4% responden selalu lupa untuk keluar dari akun media sosial mereka, 18.2% selalu lupa untuk menghapus kata sandi setelah keluar dari akun media sosial mereka, 9.1% selalu mengungkapkan informasi pribadi atau sensitif mereka pada media sosial, dan 27.3% mengatakan selalu transfer data dari satu perangkat ke perangkat yang lain.

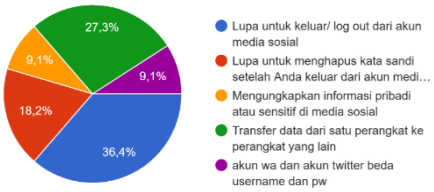


Diagram 11. Faktor Psikologis: Perilaku yang tidak disengaja

Dalam hal persepsi kemudahan penggunaan, hasilnya menunjukkan bahwa 45.5% akan melewatkan prosedur keamanan di media sosial jika mereka terlalu rumit, 45.5% akan menggunakan situs web tidak aman bahkan jika itu membantu, dan 9.1% akan menggunakan situs web tidak aman jika semua teman mereka menggunakannya.

Diagram 12. Faktor Psikologis: Persepsi kemudahan penggunaan

Dalam hal sikap, temuan menunjukkan 45.5% pengguna media sosial sangat peduli keamanan informasi dan menggunakan semua fitur keamanan seperti password dan enkripsi, 27.3% responden jarang khawatir tentang keamanan informasi ketika menggunakan media sosial pada komputer mereka, dan 18.2% kurang peduli tentang keamanan informasi ketika menggunakan media sosial pada perangkat mobile mereka sendiri dan 9.1% khawatir media sosial akan diretas dan digunakan untuk hal – hal yang merugikan.

Diagram 13. Faktor Psikologis: Sikap

Dalam hal kegunaan, 36.4% responden selalu membaca semua prosedur keamanan di media sosial sebelum memulai, 36.4% menganggap prosedur keamanan hanya melindungi situs web media sosial, 18.2% membaca kebijakan keamanan situs media sosial sebagai hal yang jarang berguna atau sebagai pemborosan waktu, sementara 9.1% percaya prosedur keamanan sama sekali tidak berguna untuk melindungi informasi pribadi mereka.

Diagram 14. Faktor Psikologis: Memberikan Manfaat

Semua pengguna mengetahui bahwa saat akan masuk ke akun media sosial, penyedia aplikasi akan meminta akses kepada perangkat pribadi yang sedang digunakan pengguna (mis. galeri, kontak, email, dll) Dalam hal kepedulian dan kesempatan untuk membaca prosedur keamanan dan privasi, 45.5% pengguna pernah membaca prosedur ketentuan keamanan dan privasi, 45.5% tidak yakin selalu membaca prosedur atau tidak, dan 9.1% mengatakan tidak pernah membaca prosedur keamanan dan privasi.

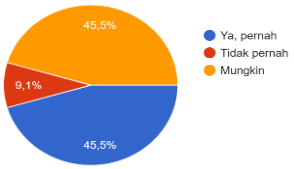


Diagram 15. Kesadaran membaca prosedur keamanan dan privasi

Setelah mengetahui ketentuan keamanan dan privasi, 45.5% mengijinkan (*allow*) data dan informasi yang diminta penyedia *website social media* untuk mengakses data pada perangkat pengguna, 18.2% selalu mengijinkan (*allow*) walaupun tahu resikonya, selama pengguna bisa masuk ke akun media sosial, 18.2% tidak mengijinkan (*deny*) akses terhadap perangkat pribadi karena ancaman privasi dan keamanan dan hanya 9.1% selalu mengijinkan walaupun tidak membaca dengan lengkap prosedur keamanan dan privasi.

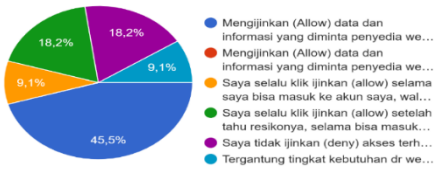


Diagram 16. Kesadaran akan akses keamanan dan privasi ke dalam perangkat pribadi

Pembahasan

Subjek dalam penelitian ini adalah generasi milenial dengan rentang usia 26 – 33 tahun, semuanya sudah bekerja baik dalam pemerintahan maupun swasta, dan mayoritas informan sudah menggunakan media sosial lebih dari 10 tahun, dan yang paling lama sudah menggunakan media sosial selama 19 tahun. Setiap harinya informan menggunakan media sosial, dengan lama 1 jam perhari sampai 15 jam perhari. Mayoritas pengguna menggunakan media sosial lebih dari 3 jam per hari. Sehubungan dengan waktu yang dihabiskan di media sosial, mayoritas responden adalah pengguna sedang.

Kerentanan terhadap ancaman yang dialami oleh pengguna aktif media sosial menunjukkan bahwa mayoritas pernah mengalami ancaman keamanan, hal ini menunjukkan tingkat kerentanan generasi milenial terhadap ancaman di media sosial sangat tinggi. Secara umum, konvergensi media memudahkan semua orang untuk mengakses media sosial karena dapat diakses dari hampir semua komputer, laptop, atau perangkat seluler. Ini menunjukkan bahwa mayoritas pengguna media sosial sangat akrab dengan media sosial.

Mayoritas total responden, mengenal definisi keamanan informasi sebagai 'privasi dan kerahasiaan', dan minoritas memahami bahwa keamanan adalah aman dari ancaman serangan kemanan di media sosial. Temuan ini menunjukkan bahwa mayoritas tidak akrab dengan konsep keamanan informasi dan definisinya. Pada hal kekuatan kata sandi pun, kewaspadaan generasi milenial dalam menggunakan kata sandi sangat rendah karena tidak satupun pengguna selalu memperbarui kata sandi mereka secara teratur. Kekhawatiran tentang kepedulian generasi milenial terhadap pentingnya prosedur keamanan dalam persepsi kemudahan penggunaan pun tampak sangat mengkhawatirkan ditunjukkan dari kenyataan bahwa 45.5% akan melewatkan prosedur keamanan di media sosial jika mereka terlalu rumit dan 45.5% akan menggunakan situs web tidak aman bahkan jika itu membantu.

Dalam faktor sikap temuan penelitian menunjukkan semua pengguna mengetahui bahwa saat akan masuk ke akun media sosial, penyedia aplikasi akan meminta akses kepada perangkat pribadi yang sedang digunakan pengguna (mis. galeri, kontak, email, dll) dan mengijinkan (*allow*) data dan informasi yang diminta penyedia *website* media sosial untuk mengakses data pada perangkat pribadi. Hal ini menunjukkan sikap yang cenderung mengesampingkan prioritas keamanan selama dapat bermedia sosial.

Terdapat empat variabel eksternal dalam teori ini yang dapat memengaruhi keputusan keamanan dan privasi pengguna, yang pertama yaitu pengetahuan pengguna, data menunjukkan bahwa pengetahuan pengguna tentang masalah keamanan dan faktor kesadaran pengguna memiliki pengaruh kuat pada sikap pengguna, serta niat pengguna untuk berperilaku aman saat menggunakan situs web media sosial. Kedua dari faktor penggunaan media sosial menunjukkan lamanya pengguna dalam menggunakan media sosial selama bertahun-tahun tidak berpengaruh secara signifikan dalam perilaku literasi mereka terhadap ancaman keamanan dan privasi dalam bermedia sosial. Ketiga mengenai preferensi kata sandi generasi milenial berada dalam tingkat sangat rendah karena tidak satupun pengguna selalu memperbarui kata sandi mereka secara teratur. Keempat dari faktor terpapar masalah keamanan pengguna yang pernah mengalami ancaman pada akun media sosial lebih menunjukkan kesadaran mereka dengan meningkatkan *level* keamanan *password* akun media sosial, dan lebih waspada sebelum mengijinkan akses ke perangkat pribadi pengguna dari akun media sosial. Ini berarti bahwa pengguna yang merasakan masalah keamanan informasi dan kemudahan penggunaannya telah dianggap sebagai pengguna aktif media sosial berdasarkan masalah keamanan. Dengan kata lain, pengalaman menentukan bagaimana pengguna aktif media sosial mendasarkan keputusan mereka dalam mengikuti pedoman keamanan informasi tertentu untuk berperilaku aman akan mempengaruhi sikap mereka mengenai keamanan media sosial, yang juga akan mempengaruhi niat mereka untuk berperilaku aman ketika mereka menggunakan situs media sosial. Pengguna yang berpikir bahwa pedoman keamanan informasi merepotkan atau tidak bermanfaat untuk menjaga keamanan informasi mereka akan memilih untuk mengabaikannya, dan mereka yang merasa nyaman dan berguna akan mengikuti pedoman keamanan mereka.

PENUTUP

Kesimpulan

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 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 di kalangan 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 berpengaruh secara signifikan dalam perilaku kesadaran literasi mereka terhadap ancaman keamanan dan privasi dalam bermedia sosial.

Dalam penelitian ini peneliti menemukan variabel baru yang dapat memberikan konstribusi terhadap kesadaran generasi milenial terhadap keamanan dan privasi di media sosial yaitu faktor pengalaman. Pengguna yang pernah mengalami ancaman pada akun media sosial lebih menunjukkan kesadaran mereka dengan meningkatkan *level* keamanan *password* akun media sosial, dan lebih waspada sebelum mengijinkan akses ke perangkat pribadi pengguna dari akun media sosial. Temuan pemahaman terhadap definisi keamanan menunjukkan bahwa mayoritas tidak akrab dengan konsep keamanan informasi dan definisinya. Kewaspadaan generasi milenial dalam menggunakan kata sandi sangat rendah karena tidak satupun pengguna selalu memperbarui kata sandi mereka secara teratur.

Bahkan hasil yang lebih m engkhawatirkan 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 tercermin dari niat mereka memberikan perhatian lebih jauh dalam menciptakan kata sandi yang lebih rumit untuk berperilaku aman saat menggunakan media sosial.

Dampak dari penelitian ini adalah memberikan kesadaran pada kenyataan bahwa generasi milenial yang dikatakan adalah generasi yang fasih akan teknologi ternyata tidak dibarengi dengan kewaspadaan yang cukup dalam hal keamanan dan privasi di dunia *cyber*, dan diharapkan dapat memberi dorongan untuk meningkatkan kewaspadaan terhadap ancaman keamanan dan privasi pada generasi milenial yang masih rentan. Studi ini diharapkan dapat memberikan kontribusi pada pembuat kebijakan untuk meningkatkan kesadaran tentang kebijakan dan peraturan yang diperlukan untuk mengatur perlindungan informasi warga dan negara saat menggunakan media sosial. Manfaat dari penelitian ini yaitu dapat menggambarkan kondisi untuk melihat bahwa masih rendahnya kewaspadaan generasi milenial terhadap ancaman

keamanan dan privasi, walaupun tingkat literasi mereka sudah dalam level yang cukup, hal ini dapat memberikan rekomendasi dari penelitian ini yaitu diharapkan penyedia aplikasi media sosial dapat membuat suatu prosedur dan pedoman keamanan dan privasi yang lebih sederhana dan ringkas dimana bisa dibaca oleh pengguna media sosial dengan waktu yang singkat.

Keterbatasan waktu dan dana, peneliti tidak dapat menganalisis lebih banyak variabel kepada lebih banyak responden karena itu diharapkan perkembangan penelitian yang dilakukan oleh peneliti masa depan untuk melakukan *survey* dan wawancara lebih dalam untuk mendapatkan hasil yang lebih mewakilkan kondisi literasi pada suatu generasi untuk mendapatkan hasil yang memuaskan.

Saran

Secara teoritis penelitian pada milenial memberikan satu variabel baru dari hasil penelitian ini, yaitu variabel pengalaman, dan hendaknya penelitian selanjutnya dapat menemukan variabel baru yang dapat ditelaah dengan lebih dalam, dan dilakukan untuk mengetahui lebih jauh tentang perilaku generasi milenial ini tidak hanya di media sosial tetapi juga dalam platform digital lainnya.

Media sosial memberi kebebasan berbagi informasi, juga memberi organisasi platform tersebut kontrol dan akses ke informasi pribadi pengguna. Terkadang juga digunakan untuk menyebarkan berita palsu yang menyebabkan keresahan di masyarakat. Masalah-masalah di atas perlu diatasi karena kepercayaan pengguna hanya dapat diperoleh dengan meningkatkan kontrol dan menurunkan risiko tersebut. Seberapapun manfaat dan kemudahan pemakaian media sosial hendaknya dibarengi dengan kemampuan literasi media sosial yang baik agar selalu berperilaku aman dan cerdas menggunakan media sosial.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada Kementerian Riset dan Teknologi Republik Indonesia yang mendanai penelitian melalui beasiswa Saintek, lalu penulis juga ingin berterima kasih kepada LIPI dimana tempat penulis bekerja yang sudah mau terlibat dalam penelitian ini.

DAFTAR PUSTAKA

Ali, Zainab, Hesham Ali, and Mahmoud Badawy. "Internet of Things (IoT): Definitions, Challenges and Recent Research Directions." *International Journal of Computer Applications* 128 no.1 (2015): 37–47. http://doi.org/10.5120/ijca2015906430

Bozart, Jane. *Social Media for Trainers_ Techniques for Enhancing and Extending Learning*, 2010.

Centre for Strategic and International Studies. "Ada Apa Dengan Milenial? Orientasi Sosial, Ekonomi Dan Politik." *Survei Nasional CSIS 2017*, no. November(2017): 1–45.

Collste, Goran. *Global ICT-Ethics : The Case of Privacy*, 1992. https://doi.org/10.1108/14779960810866819.

Creswell, John W, and Vicki L Plano Clark. *Designing and Conducting Mixed Methods Research*. Sage publications, 2017.

Fădor, Gianina Lala. *The Emergence and Development of the Technology Acceptance Model* (TAM), (2014). 149–61.

Gainous, Jason, Kevin Wagner, Tricia

Gray, Jason Gainous, and Kevin Wagner. *Internet Freedom and Social Media Effects : Democracy and Citizen Attitudes in Latin America*, 2016. "https://doi.org/10.1108/OIR-11-2015-0351.

Hershatter, Andrea, and Molly Epstein. "Millennials and the World of Work: An Organization and Management Perspective." *Journal of Business and Psychology* 25 no.2 (2010): 211–23. https://doi.org/10.1007/s10869-010-9160-y.

Hiselius, Patrik. *ICT / Internet and the Right to Privacy*, 2010.

Kaplan, Andreas M, and Michael Haenlein. "The Fairyland of Second Life: Virtual Social Worlds and How to Use Them." *Business Horizons* 52 no.6 (2009): 563–72.

———.*Users of the World , Unite ! The Challenges and Opportunities of Social Media*, 2010. https://doi.org/10.1016/j.bushor.2009.09.003.

Leech, Nancy L, and Anthony J Onwuegbuzie. "A Typology of Mixed Methods Research Designs." *Quality & Quantity* 43 no.2 (2009): 265–75.

Nuamah, Joseph, and Younho Seong. *Human Machine Interface in the Internet of Things (IoT)*, 2017. https://doi.org/10.1109/SYSOSE.2017.7994979.

Nuha, Nurul, Abdul Molok, Atif Ahmad, and Shanton Chang. "Online Social Networking Threats." *Encyclopedia of Social Network Analysis and Mining*, (2018.):1681–1681. https://doi.org/10.1007/978-1-4939-7131-2_100808.

Purwandi, Lilik. "Indonesia 2020 : The Urban Middle Class Millenials INDONESIA 2020 : The Urban Middle-Class Millennials." *Alvara Research Center*, no. April (2020.)

Suo, Hui, Jiafu Wan, Caifeng Zou, and Jianqi Liu. "Security in the Internet of Things: A Review." *Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012* 3 (March) 2012: 648–51. https://doi.org/10.1109/ICCSEE.2012.373.

Taylor, Paul, and Scott Keeter. "Millennials: A Portrait of Generation Next." *Pew Research Center*, no. February (2010.): 141. www.pewresearch.org/millennials.

Tuunainen, Virpi Kristiina. "Users ' Awareness of Privacy on Online Social Networking S Ites – Case Facebook," no. January (2009).

Youm, Kyu Ho, and Ahran Park. "The ' Right to Be Forgotten ' in European Union Law : Data Protection Balanced With Free Speech ?",2016. https://doi.org/10.1177/1077699016628824.

Zhang, Zhiyong, and Brij B Gupta. "Social Media Security and Trustworthiness : Overview and New Direction." *Future Generation Computer Systems*, 2016. https://doi.org/10.1016/j.future.2016.10.007.

Zolait, Ali. "User Awareness of Social Media Security : The Public Sector Framework User Awareness of Social Media Security : The Public Sector Framework Ali Hussein Saleh Zolait *, Reem R . Al-Anizi , Suhair Ababneh , Fatima BuAsalli and Noora Butaiba,"no.January (2016). https://doi.org/10.1504/IJBIS.2014.064973.