Jurnal Komunikasi:
Malaysian Journal of Communication
Jilid 37(1) 2021: 379-395

Keselamatan Peribadi di *Facebook*: Ancaman dan Penyelesaian

INTAN SURIA HAMZAH
Universiti Pendidikan Sultan Idris

ABSTRAK

Di era globalisasi dan kecanggihan teknologi maklumat yang melanda dunia, masyarakat semakin terdedah dengan perubahan semasa dan ancaman jenayah seperti ancaman keselamatan peribadi melalui aplikasi dalam talian seperti *Facebook*. Justeru, kajian ini membincangkan bentuk-bentuk ancaman keselamatan peribadi melalui *Facebook dan* penyelesaiannya di Malaysia. *Facebook* merupakan salah satu medium komunikasi masa kini yang paling popular di Malaysia serta mempunyai jutaan pengguna setiap hari sama ada di dalam negara mahupun luar negara. Ianya bersifat mesra, mudah, cepat serta individu atau masyarakat boleh berkongsi segala aktiviti harian dalam bentuk status penulisan, gambar atau video kepada komuniti maya. Kajian ini bertujuan mengetengahkan bentuk-bentuk ancaman keselamatan peribadi yang bermula di *Facebook,* memberi kesedaran awam kepada masyarakat Malaysia sewaktu menggunakan *Facebook* dan memberi saranan terhadap langkah penyelesaian sebelum atau selepas berlaku penipuan di melalui media sosial. Kajian ini menggunakan kaedah kualitatif bagi mendapatkan data dan maklumat iaitu melalui Polis DiRaja Malaysia, Suruhanjaya Komunikasi dan Multimedia Malaysia serta kajian kepustakaan. Hasil kajian mendapati *Facebook* membantu manusia untuk berhubung, berniaga dan berkomunikasi. Namun begitu, ianya turut mempunyai kesan langsung terhadap keselamatan peribadi bagi individu, masyarakat mahupun organisasi menerusi ancaman jenayah siber, penipuan, kecurian data, eksploitasi dan kebocoran maklumat peribadi, penipuan cinta, fitnah, buli siber, pendorong masalah sosial remaja dan pasangan curang. Kajian ini dapat memberi sumbangan kepada kesedaran masyarakat awam untuk sentiasa berhati-hati semasa menggunakan *Facebook*, tidak sewenang-wenangnya memberikan butiran peribadi kepada orang yang tidak dikenali serta memberi pendedahan kepada tindakan yang perlu diambil apabila menjadi mangsa penipuan.

Kata kunci: *Media sosial, Facebook, komunikasi, ancaman, keselamatan peribadi.*

Personal Security on Facebook: Threats and Solutions

ABSTRACT

In the age of globalization and sophistication of information technology, society is increasingly exposed to current changes and criminal threats such as personal security threats through online applications like Facebook. Therefore, this study discusses the forms of personal security threats through Facebook and its solution in Malaysia. Facebook is one of the most popular communication mediums in Malaysia and has millions of users both domestically and abroad. It is friendly, easy, fast and can share all your daily activities whether in writing, picture or video status. This study aims to highlight the forms of personal security threats that start on Facebook, give public awareness to the Malaysian community while using Facebook and provide recommendations on remedial measures before or after fraud on social media. This study used qualitative methods to obtain data and information from the Royal Malaysian Police, the Malaysian Communications and Multimedia Commission as well as the library study. The study found that Facebook helps people to connect, trading and communicate with individuals and communities. However, it also has an impact on personal safety for individuals, communities and organizations through cybercrime threats, fraud,

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2021-3701-22

data theft, exploitation and leakage of personal information, love fraud, slander, cyberbullying, encourage teen problems and cheating couples. This study can help the public to be more cautious when using Facebook, not just provide personal information to strangers and give them exposure to the actions they need to take when they become victims of fraud.

Keywords: *Social media, Facebook, communication, threat, personal security.*

PENGENALAN

Rangkaian media sosial secara khususnya telah menjadi medium komunikasi bagi masyarakat masa kini. Dari aspek penggunaan di peringkat personal iaitu secara mikro ke jangkauan peringkat makro seperti komunikasi merentasi negara, rantau dan benua. Rangkaian media sosial telah menjadi berleluasa dalam kehidupan masyarakat dunia dan kini menjadi daya penggerak penting dalam perniagaan serta hubungan. Melalui kajian Cross (2013), media sosial ini telah menyediakan satu pendekatan baru untuk pelbagai fungsi perusahaan dan perniagaan. Misalnya, berkenalan, berkomunikasi, mengumpul maklum balas pelanggan (*Facebook, Instagram, Ning*), mencari kepakaran (*Google Scholar*, *LinkedIn*), menyediakan platform komunikasi (*Mis., Twitter*) dan bekerjasama dengan pelbagai komuniti.

Media sosial menjadi alat utama untuk individu, pekerja atau organisasi agar dapat bekerjasama antara satu sama lain, berkomunikasi dengan pelanggan, pembekal atau pihak berkepentingan lain dengan cara yang lebih cepat dan lebih peribadi dari sebelumnya. Walau bagaimanapun, penggunaan media sosial turut membawa risiko besar dan boleh menjadi masalah kepada kehidupan manusia apabila keadaan menjadi salah daripada aturan sebenarnya seperti berlaku penipuan, jenayah siber, *scam*, kebocoran maklumat, fitnah, buli dan sebagainya. Media sosial mempunyai banyak risiko dan ancaman terhadap keselamatan peribadi individu, komuniti atau organisasi.

Pertubuhan Bangsa-bangsa Bersatu telah mengenalpasti tujuh kategori keselamatan insan iaitu merangkumi i) ekonomi, ii) makanan, iii) kesihatan, iv) persekitaran, v) peribadi, vi) masyarakat dan vii) politik (UNDP 1994). Sekiranya salah satu daripada kategori ini terancam maka keselamatan insan turut terancam. Konsep keselamatan insan mula mendapat perhatian selepas Pertubuhan Bangsa-Bangsa Bersatu (PBB) melakarkan satu rangka isu keselamatan dengan menegaskan keselamatan bukan sahaja mengenai peperangan atau mempertahankan negara dari ancaman musuh namun perlu melibatkan keselamatan insan iaitu individu atau manusia kerana ia boleh mengancam keselamatan negara dan kestabilan global (McGrew & Poku, 2007). Kajian ini membincangkan bentuk-bentuk ancaman keselamatan peribadi melalui *Facebook* serta langkah-langkah penyelesaiannya.

SOROTAN KAJIAN

a. Keselamatan Insan

Menurut UNDP (2009), agenda global berkaitan isu keselamatan bukan tradisional adalah terdiri daripada isu-isu seperti terrorisme, jenayah terancang seperti penyeludupan manusia dan pemerdagangan orang, masalah alam sekitar, konflik antara pertumbuhan dan pembangunan ekonomi, isu kesihatan serta penyakit berjangkit seperti HIV, AIDS, dan selsema burung. Selain itu, pembangunan senjata nuklear, migrasi penduduk atau buruh adalah tergolong dalam isu-isu yang boleh mengancam keselamatan insan, negara dan antarabangsa. Manakala Miranda (2003) menegaskan keselamatan insan boleh diancam melalui pemberontakan bersenjata, bantahan awam, agenda politik dan keganasan rumah tangga. Isu keselamatan kini telah bertukar daripada agenda yang memberi keutamaan

terhadap campur tangan tentera dan kekerasan kepada mempromosikan penyertaan penguatkuasaan undang-undang bagi menjamin keselamatan insan (McGrew & Poku, 2007).

Menurut Bajpai (2003) dalam kajian bertajuk *Human Security: Concept and Measurement* menyatakan keselamatan insan merujuk kepada kawalan keselamatan peribadi serta bebas daripada ancaman sama ada secara langsung atau tidak langsung. Justeru, keselamatan insan ini amat penting untuk mencapai keadilan sosial, politik, alam sekitar, keadaan ekonomi yang konduksif untuk kehidupan yang lebih bebas dan bermaruah iaitu hak seseorang individu terus terjamin (Anne, 2000). Manakala Fukuda-Parr (2003) mendefinisikan keselamatan insan sebagai melindungi kesemua kepentingan asas atau hak manusia iaitu kebebasan, kehendak serta membuka ruang kepada manusia untuk membina ketahanan hidup dan mempertahankan hak-hak peribadi.

b. Keselamatan Peribadi

Keselamatan peribadi atau individu adalah salah satu konsep yang berada dalam keselamatan insan dan telah diperkenalkan oleh UNDP pada tahun 1994. Ancaman keselamatan tradisional sering dikaitkan dengan ancaman daripada politik serta ketenteraan dan bukannya individu. Sistem tradisional adalah berdasarkan kepada pendekatan berpusatkan negara untuk keselamatan. Idea keselamatan insan atau manusia sebaliknya berbeza dengan sistem tradisional yang telah memperluaskan definisi ancaman keselamatan. Keselamatan manusia menggabungkan keselamatan individu dengan negara.

Menurut penyelidikan Gasper dan Gomez (2015), terdapat tiga bentuk ancaman terhadap keselamatan peribadi iaitu pertama, ancaman daripada konflik luar atau konflik dalaman (konflik senjata). Kedua, ancaman dalam negara iaitu cabaran kepada pihak polis dan penguatkuasa seperti jenayah kekerasan, jenayah harta benda dan jenayah siber. Ketiga, ancaman terhadap diri sendiri iaitu yang berkaitan dengan penggunaan dadah atau bunuh diri. Keselamatan peribadi bertujuan memastikan keselamatan orang, individu atau manusia terjamin dari sebarang bentuk ancaman (UNDP, 2009). Keamanan insan adalah hak asas yang dijamin oleh *Universal Declaration of Human Rights* dan diterima pakai oleh Pertubuhan Bangsa-Bangsa Bersatu pada tahun 1948. Perkara ini telah dinyatakan secara jelas dan dilindungi oleh *European Convention on Human Rights, Constitution of Canada, Constitution of South Africa* dan undang-undang lain di seluruh dunia.

Keselamatan peribadi adalah melindungi individu daripada sebarang bentuk keganasan fizikal, sama ada dari dalam atau luar negara, individu ganas, keganasan rumah tangga dan ancaman daripada orang dewasa yang bersifat pemangsa atau berniat jahat (United Nations, 2009). Sumber kecemasan atau ketakutan yang paling besar dihadapi oleh setiap manusia atau insan adalah jenayah terutamanya jenayah kekerasan. Konsep keselamatan peribadi yang digunakan dalam kajian ini adalah bertujuan menganalisis bentuk-bentuk ancaman keselamatan peribadi individu melalui *Facebook*.

Menurut Gierszewski (2017), keselamatan peribadi mula mendapat perhatian pada tahun 1970an. Ini terjadi apabila carian semula dilakukan bertujuan untuk membentuk susunan dunia yang stabil berasaskan isu keselamatan dari aspek individu. Merujuk laporan *Club of Rome* 1960, kewujudan isu-isu yang berkaitan dengan semua bahagian dunia seperti kemiskinan, pengangguran, urbanisasi, penghakisan nilai-nilai tradisional, pertumbuhan penduduk, kekurangan zat makanan dan masalah alam sekitar dan sumber alam yang tidak diperbaharui telah mempunyai banyak kajian khusus. Namun belum ada kajian yang melihat

daripada aspek keselamatan individu atau peribadi dengan lebih meluas iaitu memfokuskan ancaman kepada diri manusia yang bersifat non-tradisional.

c. Media Sosial

Media sosial adalah saluran media komunikasi yang digunakan secara dalam talian dengan membolehkan para pengguna mudah untuk menyertai, berkongsi, dan mencipta isi kandungan meliputi blog, rangkaian sosial (*Facebook*), wikipedia, forum dan dunia virtual. Blog, rangkaian sosial dan wikipedia merupakan bentuk media sosial yang paling umum digunakan oleh masyarakat di seluruh dunia (Ahlqvist et al., 2008). Rangkaian sosial dalam talian atau *Online Social Networks* (OSN) adalah sangat popular dan telah diterima secara meluas oleh masyarakat dunia kerana dianggap logik dan mempunyai satu entiti tunggal yang memiliki koleksi data peribadi tersusun serta ianya tidak pernah berlaku sebelum ini dari segi jumlah, kepelbagaian, merentasi geografi, penghebahan sumber dan maklumat secara terperinci (Bahri et al., 2018).

Secara umumnya media sosial seperti *Facebook*, *Twitter* dan *Instagram* digunakan untuk medium berkomunikasi dalam masyarakat, bersosial serta sebagai sumber maklumat kepada pengguna (Quan-Haase & Young, 2010; Ezumah, 2013; Basilisco & Jin, 2015). Namun begitu, perkembangan dunia media sosial pada masa kini telah menyebabkan fungsi asal media sosial mengalami pelbagai perubahan, cabaran dan berkembang ke arah fungsi-fungsi yang baharu bersifat lebih rencam (Nurul & Mohd Azul, 2015). Demikian itu, *Facebook* adalah salah satu media sosial yang sangat tinggi penggunaannya dalam urusan peribadi atau perniagaan. Melalui *Facebook* para peniaga dapat menghubungkan perniagaan mereka secara dalam talian dan kaedah ini telah terbukti mampu meningkatkan jumlah jualan serta tahap pengetahuan pengguna terhadap sesuatu produk yang dijual (Lombardi, 2012). *Facebook* juga amat membantu mempercepatkan proses suai kenal, urusan jual beli dan membina jaringan komunikasi berkesan antara penjual dan pembeli atau pengguna (Lorrie, 2010).

Perkembangan media sosial telah membantu banyak pihak menempa kejayaan khususnya syarikat dan organisasi perniagaan dalam merancang dan mengurus strategi pemasaran mereka. Menurut Fallerton (2011), komunikasi melalui Facebook yang berlaku di antara pelanggan dan pemasar atau penjual di era globalisasi ini telah memudahkan interaksi dalam memperkenalkan jenama yang dijual dengan lebih meluas. Media sosial juga menjadi agen perantara kepada pemasar untuk membangunkan produk atau jenama sendiri dengan lebih kukuh melalui ruang pasaran yang besar dan percuma (Cross, 2013). Kewujudan jaringan media sosial *Facebook* ini turut mengubah konsep ikatan kemanusiaan, perkenalan, persahabatan, wujudnya *public figure* serta membawa kepada pembentukan penumpuan dalam komuniti jaringan maya (Basilisco 2015). Laman sosial boleh meningkatkan kebolehpercayaan atau mempengaruhi persepsi individu atau masyarakat kerana media ini membolehkan orang ramai dapat melihat prestasi, identiti diri dan gaya hidup tokoh, pemimpin masyarakat, ahli politik atau kenalan mereka di profil laman sosial yang diikuti seperti *Facebook* dan Instagram (Siti Ezaleila, 2016).

d. Ancaman Keselamatan Peribadi di Facebook

Dengan peningkatan penggunaan media sosial, risiko ancaman keselamatan peribadi semakin meningkat. Menurut penyelidikan Kumar et al. (2013) dan Kumar et al. (2012), antara contoh ancaman keselamatan peribadi adalah kecurian identiti, *phishing*, penipuan dan pembuli siber. Lazimnya orang ramai akan mempamerkan maklumat peribadi mereka pada media

sosial seperti *Twitter, Facebook, LinkedIn* dan sebagainya. Maklumat atau data peribadi ini disimpan dalam laman rangkaian media sosial atau *Social Networking Sites* (SNSs). Rangkaian ini juga mempunyai kelemahan tersendiri dari aspek keselamatan iaitu penyimpanan data dan maklumat pengguna. Menurut Croteau dan Hoynes (2003), kemunculan Internet telah membawa perubahan dalam penggunaan media komunikasi. Kemunculan teknologi digital baharu dengan pelbagai aplikasi media sosial di era globalisasi ini telah membawa perubahan radikal terhadap pengawalan maklumat dan sumber serta telah wujudnya pelbagai cabaran baru melalui penggunaan media sosial ini.

Berdasarkan kajian Mohd Azul dan Nurul Madiha (2017), media sosial yang mempunyai ciri-ciri laman sesawang dinamik dapat menyediakan satu ruang sebenar terhadap pengguna yang gemar berkongsi pelbagai maklumat peribadi serta aktiviti-aktiviti harian mereka kepada ahli keluarga, rakan-rakan dan masyarakat umum. Ciri-ciri ini diakui memudahkan pengguna media sosial untuk menjalinkan hubungan, interaksi dan membina rangkaian secara dalam talian. Keadaan ini membuka peluang kepada sesiapa sahaja untuk berhubung secara maya antara satu dengan yang lain. Di medium media sosial, pengguna dibenarkan untuk berkomunikasi dan berjumpa secara maya dengan kenalan yang baru dikenali atau kenalan sedia ada dalam pelbagai jaringan sosial.

METODOLOGI

Kajian ini menggunakan kaedah kualitatif bagi mendapatkan data dan maklumat. Tiga pendekatan penyelidikan telah digunapakai iaitu temubual bersama responden elit, kutipan data statistik daripada Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dan analisis kandungan melalui kajian kepustakaan. Maklumat diperolehi adalah melalui tembual mendalam bersama responden elit iaitu tujuh pegawai polis dari beberapa daerah di Lembah Klang, dua orang pegawai polis dari IPD Perlis dan IPD Perak. Namun begitu, dalam kajian ini nama responden tidak dinyatakan atas faktor permintaan dan kerahsiaan daripada pihak tersebut. Antara dokumen yang dianalisis dalam kajian ini ialah akta dan perundangan Malaysia, maklumat daripada laman portal rasmi SKMM dan PDRM, laporan akhbar serta siaran media kerajaan. Kajian kepustakaan dilakukan melalui analisis buku dan jurnal yang telah dibuat oleh penyelidik lain supaya dapat membina sorotan literatur dan memperkukuhkan kajian. Data sekunder penyelidik lain turut digunakan iaitu hasil penyelidikan mereka diperolehi melalui akses umum daripada koleksi data yang tersedia.

HASIL KAJIAN DAN PERBINCANGAN

a) Kes Jenayah di Media Sosial

Pada masa kini, media sosial sering digunakan oleh berbilion pengguna untuk berinteraksi dan ianya juga merupakan platform utama untuk masyarakat mendapatkan maklumat, mengutarakan pendapat, memperluaskan rangkaian sosial dan profesional, memberi cadangan, kesedaran serta kempen politik. Penggunaan media sosial seperti *Facebook* dan *Twitter* telah menjadi fenomena kebudayaan, sosial dan ekonomi yang menyeluruh. Media sosial boleh mengeksploitasikan masyarakat untuk mencipta isi kandungan dan kerjasama bersama. Selain itu, perkembangan peranti peribadi mudah alih iaitu telefon pintar dan tablet yang meluas telah meningkatkan penggunaan media sosial. Hal ini telah menggalakkan lebih banyak reka bentuk perkhidmatan rangkaian sosial yang berteraskan mobiliti pengguna sebagai ciri-ciri utama. Media sosial dilihat mewakili persekitaran yang mencabar bagi saintis

computer, akademik dan industri untuk membangunkan idea-idea inovatif, membina reka bentuk platform komunikasi generasi baru dan perkhidmatan terkini.

Perkembangan aplikasi media sosial di Malaysia adalah seiring dengan pembangunan peralatan dan perkakasan teknologi komunikasi semasa seperti rangkaian telekomunikasi, telefon pintar, komputer peribadi dan sebagainya (Mohd Azul & Nurul Madiha, 2017). Aplikasi media sosial yang boleh dicapai melalui perkakasan sebegini dilihat sebagai satu medium baharu untuk berinteraksi dan berkomunikasi dalam kalangan pengguna. Ianya merupakan ciri-ciri yang ada pada Web 2.0 dan telah berkembang sejak 2008 iaitu suatu platform yang membenarkan pengguna bertukar maklumat secara dalam talian pada bila-bila masa dan di mana sahaja. Perkembangan teknologi yang sangat canggih pada era masa kini telah menggalakkan pelbagai pertumbuhan rangkaian sosial melalui internet. Masyarakat dilihat lebih gemar berkomunikasi, berinteraksi dan berkongsi hal-hal peribadi melalui laman sosial kerana beberapa faktor utama iaitu mudah, pantas, murah dan mesra (PDRM, 2019). Individu atau masyarakat dapat berkomunikasi dengan individu lain di serata dunia pada bila-bila masa dalam waktu yang singkat (Murugan, 2018 & SKMM, 2019).

Sejak beberapa tahun kebelakangan ini rangkaian media sosial semakin popular dan telah digunakan oleh masyarakat daripada semua peringkat umur. Malangnya, dengan perkembangan kemajuan ini terdapat risiko ancaman keselamatan baru dan timbulnya pelbagai masalah jenayah siber terhadap pengguna (PDRM, 2019). Misalnya, pencurian identiti adalah salah satu masalah besar yang terjadi kesan daripada penggunaan *Facebook*. Oleh kerana *Facebook* adalah salah satu laman media sosial yang paling popular, terdapat beberapa risiko keselamatan yang jelas telah dikenalpasti. Sehubungan itu, media sosial seperti *Twitter, Instagram*, dan *LinkedIn* juga mempunyai risiko tertentu dan hampir semua platform media sosial berpontensi menyebabkan banyak risiko ancaman keselamatan peribadi.

Rangkaian media sosial *Facebook* merupakan satu laman sesawang rangkaian sosial dimiliki oleh *Facebook Inc.* yang ditubuhkan pada tahun 2006. *Facebook* merupakan sebuah syarikat media sosial dan teknologi dari negara Amerika yang berpusat di Menlo Park, California. Sesiapa yang berumur 13 tahun ke atas dan memiliki akaun emel yang sah boleh menjadi pengguna *Facebook*. *Facebook* lebih menyasarkan kepada golongan belia berbanding dewasa. *Facebook* digunakan untuk mencari rakan, berkomunikasi, bertukar mesej, berkongsi cerita dan aktitivi semasa, berkongsi profil peribadi dan gambar (Brown & Cefaratti, 2019). Selain itu, pengguna juga boleh menyertai rangkaian yang dianjurkan oleh tempat kerja, sekolah, atau kolej dengan tujuan membantu masyarakat setempat mahupun dunia saling mengenali dan berkongsi maklumat harian di tempat masing-masing.

Rangkaian media sosial adalah suatu kemajuan komunikasi dan perhubungan manusia yang unik berbanding dengan komunikasi tradisional melalui telefon. Antara rangkaian media sosial yang popular ialah *Facebook, Instagram, Twitter, Google+* dan *YouTube* (eMarketer, 2020). Menurut eMarketer iaitu merupakan salah sebuah firma analisis pemasaran digital, *Facebook* merupakan rangkaian paling utama yang digunakan oleh masyarakat dunia dan diikuti dengan *Google+* dan *YouTube.* Walaupun *Facebook* jatuh ke tempat kedua di belakang *Twitter* untuk rangkaian sosial yang paling popular dalam kalangan remaja, namun secara global tidak dapat dinafikan bahawa *Facebook* masih menjadi saluran komunikasi paling popular dalam kalangan semua peringkat umur iaitu dengan anggaran sebanyak 1.1 bilion orang pengguna di seluruh dunia melayarinya setiap hari.

Melalui dapatan kajian daripada Kementerian Komunikasi & Multimedia (2019), terdapat lebih dari 10 juta rakyat Malaysia telah mempunyai akaun *Facebook*. Ia berkembang dengan sangat pantas namun tanpa kita sedari, ia mempunyai bahaya terselindung yang tidak disedari oleh pengguna. Melalui kajian kepustakaan dan temubual yang telah dijalankan bersama pegawai PDRM, berikut merupakan jenis-jenis ancaman keselamatan peribadi yang berlaku di *Facebook di Malaysia*.

i. Jenayah Siber

Menurut hasil dapatan dari Jabatan Siasatan Jenayah Komersial (JSJK) Bukit Aman (2019), telah merekodkan kerugian kira-kira RM250 juta membabitkan kes jenayah siber bagi tempoh enam bulan pertama tahun 2019 dengan penerimaan sebanyak 5,069 aduan kes. Terdapat tiga jenis penipuan siber paling popular di Malaysia iaitu membabitkan penipuan telekomunikasi (termasuk *Macau scam*), pembelian dalam talian (e-dagang) dan '*love scam'* (didalangi warga Afrika). Dapatan kajian juga menunjukkan kebanyakan jenayah penipuan siber ini turut melibatkan saluran *Facebook* sebagai titik pertemuan atau mendpatkan maklumat seseorang individu yang hendak ditipu (PDRM, 2019).

Manakala bagi jenayah penipuan telekomunikasi, terdapat kebocoran data membabitkan penggunaan jenis kad debit dan kad kredit pengguna berikutan suspek mempunyai maklumat individu ketika membuat panggilan palsu. Demikian itu, bagi pengguna yang menggunakan e-dagang, mereka perlu lebih berhati-hati sewaktu membeli barangan dalam talian seperti *Facebook.* Pengguna disaran mengamalkan kaedah pembayaran secara tunai ketika menerima barangan untuk mengelak ditipu dalam urusan pembelian (PDRM, 2019).

Jadual 1: Perangkaan jenayah siber tahun 2017-2018

Kes	2017	2018
Gangguan siber	560	356
Penipuan dalam talian	3821	5123
Pencerobohan maklumat	2011	1160
Spam	344	342
Spam emel	1,217,423	1,555,848
Jumlah	**1,224,159**	**1,562,829**

Sumber: MyCERT, Cyber Security Malaysia (2020)

Berdasarkan Jadual 1, tahun 2018 merupakan antara tahun paling tinggi berlakunya jenayah siber iaitu sebanyak 1,562,829 kes mengikut lima kumpulan utama yang telah dikenalpasti iaitu *spam* emel, penipuan dalam talian, pencerobohan maklumat dan spam. Ancaman keselamatan peribadi yang melibatkan *spam* emel adalah kes yang paling banyak berlaku dan dilaporkan serta jumlahnya meningkat dari 1,217,423 kes pada tahun 2017 kepada 1,555,848 kes pada tahun 2018. Justeru, antara langkah terbaik dalam mengurangkan jenayah siber adalah melalui penguatkuasaan undang-undang yang lebih tegas seperti hukuman penjara atau denda terhadap pesalah agar memberi ketakutan dan mencegah jenayah berulang. Walaupun dunia maya tidak mempunyai sempadan, pengguna masih berada dalam kawasan bidang kuasa secara fizikal dan masih tertakluk kepada undang-undang di mana mereka berada (Muhd Adnan & Siti Zobidah, 2019).

ii. Penipu *atau Scammer*

Berdasarkan temubual bersama pegawai PDRM (2019), penipu atau *scammer* mula mengalihkan modus operandi mereka kepada media sosial seperti *Facebook* untuk mencari mangsa. Mereka berusaha mengenali mangsa dan akan menipu secara perlahan-lahan dengan mengikuti *Facebook* sebagai teman baru, memberikan komen, tawaran hadiah atau diskaun barangan jualan. Ia bermula dengan mengambil perhatian, meraih keyakinan dan juga kepercayaan mangsa sebelum menipu.

iii. Kecurian Data, Eksploitasi & Kebocoran Maklumat Peribadi

Menerusi *Facebook*, para pengguna boleh membangunkan perisian masing-masing untuk akaun sendiri. Sesetengah daripada pemaju atau organisasi menggunakan kod sumber yang boleh dieksploitasi oleh pembangun perisian untuk mencuri data penting daripada akaun *Facebook* mangsa. Data penting seperti alamat emel dan *password* boleh dicuri menerusi *malware* yang diselitkan menerusi aplikasi *Facebook*. Manakala bagi kebocoran maklumat peribadi dikenalpasti dicuri melalui perincian yang ditulis pada akaun *Facebook*, status semasa, gambar yang dimuat naik, alamat emel, nombor telefon dan alamat rumah atau pejabat yang di nyatakan di *Facebook*. Ianya adalah mengundang ancaman secara tersirat dan ancaman yang diluar jangkaan.

Sehubungan itu, melalui *Facebook*, kecurian identiti dilaporkan telah berlaku. Ini adalah kerana *hacker* atau penggodam boleh menyamar sebagai diri orang lain dan melakukan jenayah. *Hacker* akan melakukan jenayah dengan menghantar mesej kepada rakan atau kenalan dan meminta wang yang kononnya mangsa berada dalam kesusahan dan memerlukan sejumlah wang dalam kadar segera (PDRM, 2019). Inilah antara bahaya *Facebook* yang perlu diambil perhatian.

iv. Love Scam

Bagi penipuan *love scam* atau turut dikenali dengan panggilan '*romance scam'*, suspek akan mencari mangsa dengan berkenalan melalui laman sosial seperti *Facebook* dan *Instagram*. Golongan *scammer* ini mensasarkan golongan yang dibelenggu kesunyian seperti orang bujang berusia, ibu tunggal dan duda. *Scammer* akan menggunakan kata-kata manis untuk memikat mangsa sehingga wujud perasaan percaya dan sayang kepada mereka (PDRM 2018, SKMM 2019 & Bernama 2019).

Apabila tiba masa yang sesuai, *scammer* akan memperdaya mangsa dengan menjanjikan satu barangan bungkusan akan tiba ke dalam negara. Contohnya, ketibaan bungkusan barang kemas dari luar negara namun menghadapi masalah untuk membawa masuk barangan tersebut dengan membuat helah ianya tersangkut di pihak kastam. Untuk mendapatkan barang tersebut, mangsa perlu mendahulukan sejumlah wang bagi membayar caj untuk mengeluarkan barang tersebut daripada simpanan pihak kastam. Tanpa usul periksa, lazimnya mangsa yang sudah percaya dengan kata-kata manis suspek dan bersetuju menjelaskan bayaran tersebut. Mangsa hanya sedar ditipu apabila mendapati barang yang dijanjikan tidak kunjung tiba. Sehingga awal bulan Oktober 2018, jumlah wang yang dilaporkan ditipu melalui sindiket ini adalah seperti jadual 2.

Jadual 2: Kes penipuan *scam* di Malaysia

Tahun	Kes/ ditipu	Kerugian
2017	1,774	RM67,199,064.00
2018	1,398	RM80,086,530.15
Jumlah		**RM147,285,594.15**

Sumber: Kementerian Komunikasi & Multimedia (2018)

Jadual 2 memperlihatkan jumlah kerugian bagi jenayah penipuan *scam* semakin meningkat iaitu dari RM67,199,064.00 pada tahun 2017, meningkat kepada RM80,086,530.15 pada tahun 2018. Keadaan ini disebabkan oleh sindiket jenayah terancang berkembang pesat di dalam dan luar negara yang melibatkan ramai mangsa dalam kalangan wanita tempatan. Menurut statistik *Malaysia Computer Emergency Response Team* (MyCERT) 2019, aduan insiden penipuan siber adalah paling tinggi diterima berbanding jenayah siber lain. Antaranya berkaitan kes '*phishing*', penipuan pekerjaan, Nigerian *scam,* penipuan dalam talian dan penipuan loteri. Maklumat-maklumat peribadi mangsa lazimnya diketahui melalui laman sosial seperti *Facebook* dan pendedahan maklumat peribadi sewaktu menggunakan aplikasi atau kemaskini maklumat dalam talian.

v. Fitnah

Fitnah, pengaiban atau tohmahan boleh disebarkan dengan cukup mudah. Dengan "kuasa" viral yang ada pada *Facebook*, ianya boleh menyebabkan sebarang bentuk penyebaran fitnah atau aib disebarkan dengan cukup pantas (SKMM 2019). Bagi mereka yang melalui keadaan ini akan berasa malu, tertekan, kemurungan dan depresi (PDRM, 2019). Hal ini akan mengganggu gugat emosi, tingkah laku dan suasana kerja yang tidak aman dalam kehidupan seharian.

vi. Buli siber

Hargeet Kaur (2013) menjelaskan buli siber adalah perbuatan manusia mengancam, memalukan atau menakutkan seseorang manusia atau masyarakat lain. Buli siber boleh berlaku melalui telefon pintar dan medium elektronik seperti mesej teks (SMS) dan *WhatsApp*, chatting, emel, *Facebook*, atau permainan internet (*games*). Jenis-jenis buli siber adalah seperti mesej yang mengganggu dan mengancam, menyalahgunakan kata laluan, menyamar sebagai nama individu lain atau menyamar sebagai orang lain, memanjangkan emel, foto atau video fitnah/aib kepada orang lain, memuat naik komen atau gambar yang tidak senonoh atau berunsur seksual atau memulaukan individu tertentu daripada sesuatu kumpulan internet dengan sengaja.

Istilah buli siber atau *cyberbully* ini merujuk kepada perlakuan. Bagi individu yang suka memuat naik gambar diri sendiri sesuka hati di *Facebook* mempunyai risiko menjadi mangsa buli siber seperti *body shaming* iaitu perbuatan menghina bentuk fizikal seseorang. Malah ada yang memberikan gambar bogel mereka kepada kenalan baru dikenali daripada *Facebook* sehingga menjadi mangsa ugutan atau *black mail* untuk mendedahkan gambar tersebut jika tidak melakukan apa yang dimahukan seperti seks atau wang tebusan (PDRM 2016). Pembuli akan terus membuli mangsa sehabis-habisnya sehingga mangsa menjadi ketakutan, menyerahkan sejumlah wang atau menghadapi tekanan emosi.

vii. Pendorong masalah sosial remaja

Facebook boleh mendedahkan remaja kepada risiko gejala sosial yang serius. Bermula dengan cinta siber, kemudian ia berubah kepada dunia luar seperti seks di luar perkahwinan dan rogol. Selain itu, *Facebook* berpontensi memberi pengaruh terhadap berlakunya aktiviti gangsterisme iaitu kelakuan memusnahkan atau merosakkan yang dilakukan secara berkumpulan (Portal Rasmi MyHealth, 2012). Pengaruh ini akan berlaku apabila remaja yang tidak matang, kurang didikan moral atau kasih sayang terpengaruh dengan video-video keganasan dari *youtube* dan permainan *game extreme* yang dikongsi melalui *Facebook* dan dilayari oleh mereka. Ibu bapa seharusnya mengambil serius tentang perkembangan dan pergaulan anak-anak setiap hari seperti membuat pantauan penggunaan internet, mengambil tahu dengan siapa mereka berkawan di *Facebook* dan mengetahui laman sosial yang sering mereka layari.

viii. Pasangan curang

Perkahwinan merupakan ikatan suci yang mengikat lelaki dan perempuan dalam satu ikatan sah untuk menjadi suami isteri dan membentuk keluarga. Melalui *Facebook*, individu dan masyarakat sentiasa berinteraksi dan berhubung. Individu boleh mencari kembali rakan lama, kekasih lama atau kenalan baru untuk memulakan sesuatu perhubungan. Justeru, salah satu ancaman institusi perkahwinan adalah isu pasangan curang. Hal ini akan mengancam keamanan dan keharmonian institusi kekeluargaan suami, isteri dan begitu juga anak-anak. Menurut kajian Mariam dan Mohammad Syafirul (2017), penyalahgunaan kecanggihan ICT seperti penggunaan *Facebook* kini dikenalpasti sebagai salah satu punca timbulnya masalah keretakan rumah tangga dan perceraian.

Selain itu, penggunaan aplikasi *Facebook* dan *Instagram* dalam kalangan pasangan yang sudah berkahwin boleh membawa kepada kerenggangan hubungan dalam institusi keluarga. Hal ini kerana masing-masing sibuk dengan media sosial yang dilayari dan banyak kes telah dilaporkan, pasangan tidak menjaga sensitiviti perhubungan mereka misalnya dengan memuat naik status dan gambar masing-masing yang tidak bersesuaian untuk tatapan umum (*Bernama*. 2016, Januari 14).

b) Cabaran Semasa Negara

Keselamatan peribadi bermaksud selamat dari keganasan fizikal, jenayah dalam kehidupan, jenayah harta benda, kemalangan, penyalahgunaan terhadap diri seperti dadah dan bunuh diri serta berlaku pengabaian dalam ekonomi, seperti peluang pekerjaan, pendapatan dan hak perumahan. Kategori peribadi juga meliputi kesihatan, akses kepada makanan, pendapatan dan pekerjaan, keselamatan politik, kebebasan awam seperti boleh memilih dan pilihan dihormati serta menjadi ahli dalam komuniti. Ancaman dan cabaran keselamatan negara yang dihadapi ketika ini adalah berkait rapat dengan kegiatan domestik yang berbentuk subversif, pelampau perkauman dan agama, sabotaj, keganasan dan gangguan keharmonian kehidupan manusia adalah dilakukan oleh individu, organisasi atau pihak yang mempunyai kepentingan tertentu. Polis Diraja Malaysia terus berusaha gigih untuk memastikan keamanan dan ketenteraman awam terus terpelihara.

Proses globalisasi semakin diterima masyarakat sehingga mendorong mereka melihat dan menilai sesuatu isu yang timbul berdasarkan ukuran sejagat dan bukan lagi berdasarkan kepada faktor sejarah, sensitiviti dan nilai-nilai tempatan. Misalnya, isu-isu yang dibangkitkan di *Facebook* dan *WhatsApp* tanpa usul periksa sesuatu perkara, masyarakat mudah

menyebarkan walaupun perkara tersebut tidak diketahui kesahihannya. Ini akan menimbulkan pelbagai ancaman kepada individu atau masyarakat terbabit seperti fitnah, diaibkan, buli, dimalukan serta ianya akan mengancam emosi dan rutin harian. Senario yang berlaku ini menyebabkan pelbagai isu kontroversi akan timbul dari semasa ke semasa dan boleh menggugat kestabilan serta perpaduan negara.

Masyarakat Malaysia masa kini tidak lagi menjadikan nilai-nilai moral, budaya dan sejarah pembangunan bangsa sebagai ukuran untuk memperkatakan sesuatu di media sosial. Sensitiviti dalam konteks masyarakat berbilang kaum tidak lagi menjadi perkiraan sewaktu menulis di ruangan *Facebook* serta secara lantang menuntut hak dan kepentingan masing-masing yang bukan diperuntukkan dalam undang-undang. Masyarakat lebih suka menuntut kebebasan tanpa sebarang had iaitu bebas sehingga mendorong mereka melanggar peruntukan undang-undang negara, menceroboh hak peribadi orang lain dan hilang nilai saling menghormati sesama manusia.

Dalam perkembangan yang sama, elemen *'information warfare'* turut memberi kesan negatif terhadap keselamatan negara kerana terdapat pihak yang menyalahgunakan kecanggihan sistem teknologi maklumat dan media sosial ini untuk melakukan pelbagai aktiviti '*disinformation*' dan '*misinformation*' yang bermatlamat membentuk persepsi dan menimbulkan kekeliruan masyarakat atau rakyat. Perlu diakui bahawa ancaman *'war of perception'* ini adalah suatu yang nyata dan boleh memberikan kesan buruk kepada keselamatan negara.

Menurut kajian Bahdri (2018), dengan memuatnaik butiran atau maklumat peribadi di *Facebook* ianya adalah berpontensi menjadi salah satu ancaman kepada privasi pengguna itu sendiri dan hak peribadi mereka. Hasil kajian mendapati terdapat lebih banyak cabaran semasa yang akan dihadapi oleh individu atau masyarakat apabila kerap memuatnaik butiran atau maklumat peribadi di *Facebook*. Penggunaan media sosial dan tahap kesedaran masyarakat terhadap ancaman siber memerlukan perhatian sewajarnya. Masyarakat perlu sentiasa peka dengan persekitaran semasa supaya terhindar daripada ancaman keselamatan peribadi yang dimulai oleh diri sendiri.

c) Langkah Penyelesaian

Pada tahun 2018, bank-bank di Malaysia telah memulakan Strategi Keselamatan Siber bagi memperkukuhkan perlindungan aset maklumat kritikal organisasi (Wan Azizah & Ann Teck, 2019). Usaha ini disokong oleh struktur tadbir urus dan operasi yang telah diwujudkan bagi memacu mengawasi pengurusan risiko siber di seluruh bank. Bank-bank di Malaysia telah menubuhkan unit Keselamatan Siber dan Perlindungan Data di Jabatan Digital dan Teknologi untuk mengurus keselamatan siber di peringkat organisasi. Di samping itu, Kumpulan Kerja Keselamatan Siber dan Maklumat juga ditubuhkan bagi memacu pelaksanaan inisiatif keselamatan siber dan maklumat bank. Hal ini bertujuan menjamin keselamatan penyimpanan maklumat organisasi bank dan menjaga keselamatan peribadi pengguna bank iaitu masyarakat Malaysia. Ini merupakan salah satu usaha kerajaan melalui kerjasama dengan bank-bank di Malaysia dalam membanteras jenayah siber seperti *scam* dan penipuan.

Selain itu, Kementerian Komunikasi dan Multimedia Malaysia (KKMM) telah mengambil tindakan segera dengan menggerakkan kempen kesedaran dan pencegahan jenayah komunikasi pada tahun 2019. Agensi serta jabatan di bawah KKMM seperti MCMC, Bernama, RTM, Jabatan Penerangan (JaPen), Perbadanan Kemajuan Filem Nasional Malaysia (Finas) dan Bahagian Komunikasi Strategik KKMM turut menggalas tanggung jawab bersama

untuk mempromosi dan mengadakan program khas masing-masing bagi menyokong kempen kesedaran yang bertujuan membanteras jenayah siber.

Menurut kajian Muhd Adnan et al. (2017), antara punca berlakunya jenayah siber ini adalah faktor kurangnya ilmu kefahaman tentang undang-undang siber dan tidak peka dengan hak asasi individu lain menyebabkan peningkatan statistik jenayah siber di Malaysia. Justeru penguatkuasaan undang-undang sedia ada dan menghebahkan kepentingan undang-undang ini terhadap masyarakat awam adalah tindakan yang wajar diambil oleh kerajaan Malaysia. Terdapat pelbagai akta yang telah diwartakan oleh kerajaan Malaysia untuk diguna pakai bagi kesalahan dalam talian (media sosial) seperti Akta Komunikasi dan Multimedia 1998, Akta Hasutan 1948, dan Akta Fitnah 1957 (Muhd Adnan & Siti Zobidah, 2019). Kesemua akta ini bertujuan melindungi hak asasi manusia dan menjaga keamanan negara.

Penguatkuasaan Akta Suruhanjaya Komunikasi dan Multimedia Malaysia 1998 adalah langkah terbaik dalam menyelesaikan isu jenayah siber di media sosial (Undang-undang Malaysia). Akta ini merupakan suatu peruntukan bagi penubuhan Suruhanjaya Komunikasi dan Multimedia Malaysia untuk mempunyai kuasa mengawasi dan mengawal selia aktiviti komunikasi dan multimedia di Malaysia, menguatkuasakan undang-undang komunikasi dan multimedia Malaysia serta perkara-perkara yang berkaitan.

Sehubungan itu, KKMM turut melakukan kerjasama strategik dengan agensi penguatkuasa lain iaitu PDRM, rangkaian media swasta, pelbagai kementerian, badan-badan bukan kerajaan (NGO) dan pemimpin masyarakat untuk meningkatkan keberkesanan kempen ini. Sebagai contoh PDRM membantu dari aspek penguatkuasaan dan bahan kempen, sementara stesen tv dan radio swasta pula membantu menyebar luas bahan kempen serta penglibatan kementerian lain membenarkan penyebaran kempen tersebut di tempat awam. Kempen ini adalah mensasarkan kepada masyarakat awam terutamanya pesara, wanita berkerjaya dan golongan pertengahan umur kerana golongan ini yang dilaporkan mudah terpedaya dengan jenayah siber (Syamsiah & Rozlin, 2019). Kempen membanteras jenayah siber ini turut mensasarkan golongan muda termasuk pelajar sekolah menengah dan institusi pengajian tinggi. Masyarakat diseru supaya sentiasa mendapatkan maklumat terkini serta mengikuti perkembangan kempen pencegahan dengan melayari media sosial dengan kata kunci #BeSmart #JanganTerpedaya dan #Scammers (Portal Rasmi Kementerian Komunikasi & Multimedia, 2019).

Kementerian Komunikasi & Multimedia juga telah menyediakan perkhidmatan bantuan kepada masyarakat dengan menegaskan bahawa jika ada individu-indvidu merasa diri telah menjadi mangsa jenayah siber adalah disarankan untuk membuat aduan kepada Pusat Bantuan Cyber999. Aduan boleh dilaporkan melalui borang dalam talian, emel, khidmat pesanan ringkas (SMS), panggilan telefon, faksimili, memuat turun Aplikasi Mudah Alih 'Cyber999' atau datang sendiri ke Kementerian Komunikasi & Multimedia Malaysia (Portal Rasmi Kementerian Komunikasi & Multimedia, 2019). Antara tindakan yang akan dilakukan oleh Pusat Bantuan Cyber999 adalah membuat laporan, siasatan teknikal dan analisis berdasarkan insiden yang dilaporkan oleh pengguna Internet. Manakala semua aduan berkaitan jenayah siber juga boleh diadukan ke talian 1-300-88-2999, faks (03-80087000), talian kecemasan mudah alih 24 jam (019-2665850) atau SMS ke CYBER999 REPORT dan hantar ke 15888 serta emel ke cyber999@cybersecurity.my (Kementerian Komunikasi & Multimedia, 2019).

Bagi menangani ancaman keselamatan peribadi dari aspek buli siber, masyarakat disarankan mengamalkan keselamatan penggunaan internet seperti didik anak-anak tentang keselamatan dan etika ketika melayari internet serta menggunakan telefon dengan

berhemah. Ajari anak-anak agar tidak berkongsi butiran peribadi di internet, awasi setiap penulisan dan makna mesej yang ditulis agar tidak disalah tafsir serta tidak menghantar atau memanjangkan mesej yang mempunyai kata-kata kesat atau berunsurkan ancaman, fitnah dan boleh menyalahi undang-undang negara (Hargeet Kaur, 2013). Seterusnya bagi mengekang kebocoran maklumat peribadi, masyarakat dinasihatkan tidak sesekali memasukkan maklumat peribadi penting seperti nombor kad pengenalan, nombor telefon dan alamat rumah dalam profile *Facebook*. Hal ini bagi mengekang penyalahgunaan maklumat peribadi pengguna *Facebook* digunakan untuk tujuan tidak baik. Sekiranya menerima SMS atau emel yang mengatakan telah memenangi sesuatu hadiah, barangan, baucer percutian dan sebagainya hendaklah membuat pengesahan dan semakan terlebih dahulu dengan syarikat yang dinamakan dalam sms atau emel yang diterima (PDRM, 2019). Sekiranya sms atau maklumat tersebut tidak dapat disahkan dan diragui adalah perlu untuk mengabaikannya. Jangan balas atau hantar sms atau memanjangkan emel kepada orang lain kerana ianya berfungsi untuk menyebarkan lagi penipuan.

Sehubungan itu, langkah terbaik yang perlu diambil peduli sekiranya merasakan diri telah menjadi mangsa penipuan, hubungi pihak bank dan laporkan transaksi yang terlibat dan kemudian membuat laporan kepada pihak polis. Seterusnya, masyarakat diingatkan agar tidak memberikan maklumat peribadi seperti nama pengguna, kata laluan atau nombor '*tac*' perbankan internet dan butiran-butiran peribadi kepada orang yang tidak dikenali sama ada melalui *Facebook*, mesej, emel mahupun *WhatsApp*.

KESIMPULAN

Melalui perbincangan yang telah diutarakan, kajian ini mendapati ancaman keselamatan peribadi adalah melibatkan Individu dan organisasi. *Facebook* mempunyai potensi risiko ancaman keselamatan peribadi melalui jenayah siber, penipu/ *scammer*, kecurian data, eksploitasi, kebocoran maklumat peribadi, *love scam*, fitnah, buli siber, pendorong masalah sosial remaja dan isu pasangan curang.

Selari dengan perkembangan pesat teknologi komunikasi semasa di seluruh dunia, paradigma keselamatan mula berubah ke arah keselamatan insan iaitu keselamatan individu, masyarakat atau manusia sebagai keutamaan dalam mengekalkan kesejahteraan mahupun kestabilan negara. Demikian itu, dalam usaha mengekalkan kestabilan negara, tumpuan tidak lagi memfokuskan keselamatan negara sahaja namun ianya perlu berkait rapat dengan keselamatan masyarakat dalam negara seperti terhindar daripada jenayah-jenayah kemajuan ICT dan media sosial.

Kajian ini membantu individu, masyarakat dan organisasi memahami dan menyedari risiko yang ada melalui penggunaan *Facebook.* Hal ini bagi mengurangkan risiko ancaman terhadap diri masyarakat melalui penyebaran data dan maklumat peribadi di media sosial dan menjamin keselamatan peribadi. Apabila memilih untuk menggunakan *Facebook*, masyarakat perlu mengetahui dan memahami risiko serta langkah-langkah terbaik yang boleh diambil untuk melindungi diri daripada beberapa bentuk ancaman yang telah dibincangkan. Selain itu, kita perlu menentukan amalan terbaik sewaktu menggunakan *Facebook*, berfikir dahulu sebelum memberi maklumat peribadi dan menggunakan media sosial dengan cara yang betul supaya dapat mengurangkan risiko ancaman keselamatan peribadi.

Sudah tiba masanya konsep keselamatan negara diperkukuhkan dengan pelbagai elemen keselamatan untuk menjaga hak individu dan masyarakat. Tanpa menidakkan peranan kekuatan ketenteraan dan pengaruh kerajaan sebagai elemen penting dalam

menegakkan sistem keselamatan negara, keselamatan insan perlu diaplikasi demi kelangsungan dan masa depan negara. Masyarakat juga perlu terus berusaha untuk mengekalkan keamanan, perpaduan, menjadi masyarakat yang baik, saling menghormati sesama manusia, menjaga kedaulatan undang-undang dan keamanan negara Malaysia.

BIODATA

Intan Suria Hamzah, Pensyarah Kanan Jabatan Pengajian Kemasyarakatan dan Kewarganegaraan, Fakulti Sains Kemanusiaan, Universiti Pendidikan Sultan Idris. Kepakaran dalam bidang Sains Politik dan Keselamatan Insan. E-mel: intan.hamzah@fsk.upsi.edu.my

RUJUKAN

Ahlqvist, T., Back, A., Halonen, M., & Heinonen, S. (2008). *Social media roadmaps: Exploring the futures triggered by social media*. Julkaisija- Utgivare.

Bajpai, K. (2000). *Human security: Concept and measurement*. Kroc Institute Occasional Paper.

Bahri, L., Carminati, B., & Ferrari, E. (2018). Decentralized privacy preserving services for online social networks. *Online Social Networks and Media*, *6*, 18-25.

Basilisco, R., & Jin, C. K. (2015). Uses and gratification motivation for using Facebook and the impact of Facebook usage on social capital and life satisfaction among Filipino users. *International Journal of Software Engineering and Its Applications, 9*(4),191-194.

Bernama. (2016, Januari 14). Media sosial boleh jadi medium penyumbang kes cerai. *Astro Awani*. http://www.astroawani.com/berita-malaysia/

Brown, F., & Cefaratti, T. (2019). *Big tech tyrants: How Silicon Valley's stealth practices addict teens, silence speech and steal your privacy*. Post Hill Press.

Croteau, D., & Hoynes, W. (2003). *Media society: Industries, images, and audiences* (3rd ed). Pine Forge Press.

Cross, M. (2013). *Social media security: Leveraging social networking while mitigating risk*. Elsevier Inc.

Cyber Security Malaysia. (2019, Januari 2). MyCERT incident statistics 2018.

eMarketer. (2019, September 9). Data and research on digital for business. https://www.emarketer.com/

Ezumah, B. A. (2013). College students' use of social media: Site preferences, uses and gratifications theory revisited. *International Journal of Business and Social Science*, *4*(5),27-34.

Fullerton, R. (2011). *The impact of social media on marketing strategy*. http://www.academia.edu/3719601/The_Impact_of_Social_Media_on_Marketing

Faris Fuad. (2019, Ogos 7). JSJK rekod kerugian RM250 juta jenayah siber. *Berita Harian*. https://www.bharian.com.my/berita/kes/2019/08/593732/jsjk-rekod-kerugian-rm250-juta-jenayah-siber

Fukuda-Parr, S. (2003). New threats to human security in the era of globalisation. *Journal of Human Development, 4*(2), 167-180.

Gasper. D., & Gomez, O. (2015). Human security thinking in practice: Human security thinking in practice: 'Personal security', 'citizen security' and comprehensive mappings. *Journal Contemporary Politics, 21*(1), 100-116.

Gierszewski, J. (2017). *Personal* security within the human security paradigm. *Security Dimensions International & National Studies, 23,* 51–66.

Hargeet Kaur. (2013, Julai 9). Buli siber: Apakah buli siber?. *Kementerian Kesihatan Malaysia.* http://www.myhealth.gov.my/cyberbullying/

Ilyas, S., & Khushi, Q. (2012). *Facebook* status updates: A speech act analysis. *Academic Research Internasional, 3*(2), 500-507.

Kumar, A., Gupta, S.K., Rai, A. K., & Sinha, S. (2013). Social networking sites and their security issues. *International Journal of Scientific and Research Publications*, *3*(4),1-5.

Lachenicht, L. G. (1980). Aggravating language: A study of abusive and insulting language. *International Journal of Human Communication, 13*(4), 607–688.

Lombardi, G. (2012). How to map out the perfect, integrated, online marketing strategy for your practice. *Dental Economics, 102*(61).

Lorrie, T. (2010). *McGraw-Hill 36-hour course: Online marketing*. McGraw-Hill Professional Publishing.

Mariam Abd. Majid, & Mohammad Syafirul Zarif Saleh Hudin. (2017). Perceraian rumah tangga di negeri Selangor Darul Ehsan dan pendekatan menanganinya. *e-Jurnal Penyelidikan dan Inovasi, 4*(2), 285-303.

Murugan Krishnan. (2018). *Strategi ketidaksantunan bahasa dalam komen malaysiakini*. Universiti Malaya.

Muhammad Adnan Pitchan, & Siti Zobidah Omar. (2019). Dasar keselamatan siber malaysia: Tinjauan terhadap kesedaran netizen dan undang-undang. *Jurnal Komunikasi: Malaysian Journal of Communication, 35*(1), 103-119.

Muhammad Adnan, Siti Zobidah, Jusang Bolong, & Akmar Hayati. (2017). Analisis keselamatan siber dari perspektif persekitaran sosial: Kajian terhadap pengguna internet di Lembah Klang. *Journal of Social Sciences and Humanities*, *12*(2), 16-29.

Mohd Azul Mohamad Salleh, & Nurul Madiha Mohd Ilham. (2017). Pengalaman dan kesedaran pengguna dewasa terhadap isu pengawasan di media sosial. *Jurnal Komunikasi*: *Malaysian Journal of Communication, 33*(1), 502-514.

McGrew, A., & Poku, N. K. (2007). *Globalization, development and human security*. Polity Press.

MyCert. (2019, Disember 2). Langkah dan panduan pencegahan penipuan. Kementerian Komunikasi & Multimedia. https://www.mycert.org.my/portal/index

Portal Rasmi MyHealth. (2012, April 27). Gengsterisme. Kementerian Kesihatan Malaysia http://www.myhealth.gov.my/en/gengsterisme/

Nurul Madiha Mohd Ilham, & Mohd Azul Mohamad Salleh. (2015). Isu privasi dan keselamatan dalam kalangan pengguna aplikasi media sosial. *E-Bangi: Journal of Social Sciences & Humanities, 10*(2), 203-216.

Polis Diraja Malaysia. (2016). *Statistik kes jenayah warga Malaysia tahun 2014-2015*. Bahagian Rekod Jenayah (D4), Jabatan Siasatan Jenayah, Bukit Aman Kuala Lumpur.

Polis Diraja Malaysia. (2019, Disember 20). *Kesedaran masyarakat tentang pencegahan jenayah.* Ketua Jabatan Pencegahan Jenayah dan Keselamatan Komuniti, Ipoh Perak.

Polis Diraja Malaysia. (2014, November 4). *Jenayah warga Malaysia* (temubual). Ibu Pejabat Daerah Ampang Jaya, Kuala Lumpur.

Polis Diraja Malaysia. (2019, November 9) Langkah Pencegahan jenayah siber (Temubual menerusi telefon).

Portal Rasmi Suruhanjaya Komunikasi dan Multimedia Malaysia. (2019, November 16). Elakkan diri daripada menjadi statistik jenayah siber. https://www.mcmc.gov.my/ms/media/press-clippings/statistik

Portal Rasmi Kementerian Komunikasi & Multimedia. (2020, Januari 22). https://www.kkmm.gov.my/

Quan-Haasn, A., & Young, A. L. (2010). Uses and gratifications of social media: A comparison of Facebook and instant messaging. *Bulletin of Science, Technology & Society*, *30*(5), 350-361.

Siti Ezaleila Mustafa. (2016). Penggunaan laman sosial dan impaknya terhadap hubungan persahabatan dalam talian. *Jurnal Komunikasi: Malaysian Journal of Communication*, *32*(2), 65-81.

Syamsiah Sahat, & Rozlin Rusharmeen Rosmin. (2019, Ogos 13). Jangan biar hati anda di Godam. *Bernama*. KKMM. https://www.kkmm.gov.my/index.php/awam/berita-terkini/15578 bernama-13-ogos-2019-jangan-biarkan-hati-anda-digodam

Undang-Undang Malaysia. (2020, Februari 11). Akta Suruhanjaya Komunikasi dan Multimedia Malaysia 1998. *AGC Portal Governance.* http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/MY/Akta.pdf

UNDP. (1994). *Human development report*. Oxford University Press.

United Nations. (2009). *Human security in theory and practice: Application of the human security concept and the united nations trust fund for human security*. Human Security Unit Office for the Coordination of Humanitarian Affairs United Nations. http://hdr.undp.org/en/media/HS_Handbook_2009.pdf

Wan Azizah Wan Omar, & Lim Ann Teck. (2019). *Malaysia baharu 2018* (Buku rasmi tahunan Jabatan Penerangan Malaysia). Jabatan Penerangan Malaysia.