Jurnal Komunikasi:
Malaysian Journal of Communication
Jilid 35(1) 2019: 103-119

Dasar Keselamatan Siber Malaysia: Tinjauan Terhadap Kesedaran Netizen dan Undang-Undang

MUHAMMAD ADNAN PITCHAN
Universiti Kebangsaan Malaysia

SITI ZOBIDAH OMAR
Universiti Putra Malaysia

ABSTRAK

Undang-undang merupakan salah satu dasar kerajaan yang diwujudkan untuk kebaikan negara. Hal ini kerana melalui undang-undang kita dapat mengatur dan mengawal masyarakat. Walau bagaimanapun, kebanyakan masyarakat tidak menyukai undang-undang kerana mereka beranggapan hidup mereka tidak bebas. Dalam konteks Internet pula, undang-undang siber dicipta bagi memastikan netizen menggunakan ruang siber dengan baik dan berhemah. Antara langkah yang baik dalam menangani isu ancaman siber adalah melalui penguatkuasaan undang-undang siber. Walau bagaimanapun, netizen masih tidak menyedari tentang kewujudan undang-undang siber dan peningkatan angka kes jenayah siber setiap tahun. Justeru, kajian ini bertujuan untuk mengetahui kesedaran informan terhadap kewujudan undang-undang siber dan menganalisis pelaksanaan undang-undang ancaman keselamatan siber di Malaysia. Dari segi metodologi, kajian ini menggunakan pendekatan kualitatif iaitu kumpulan fokus, temu bual mendalam dan analisis dokumen untuk mendapatkan data kajian yang berkualiti. Jumlah informan kumpulan fokus ialah seramai 35 orang pengguna Internet manakala jumlah informan temu bual mendalam adalah seramai 6 orang pegawai kerajaan. Antara dokumen utama yang dianalisis ialah akta dan perundangan, laporan tahunan dan siaran media. Hasil kajian mendapati informan kumpulan fokus tidak mengetahui kewujudan undang-undang siber kerana mereka merasakan undang-undang tersebut tidak penting, selain informan kurang peka dan mengamalkan sifat sambil lewa. Hasil analisis dokumen juga mendapati terdapat beberapa undang-undang siber yang boleh digunakan untuk mengatasi masalah ancaman siber seperti Akta Komunikasi dan Multimedia 1998, Akta Jenayah Komputer 1997, Akta Perdagangan Elektronik 2006, Akta Perlindungan Data Peribadi 2010 dan Akta Perlindungan Pengguna 1999 (Pindaan 2010).

Kata Kunci: *Undang-undang siber, keselamatan siber, netizen, media sosial, kesedaran.*

Cyber Security Policy: Review on Netizen Awareness and Laws

ABSTRACT

Law is one of the government policies created for the good of the state. The law is believed to control and regulate society. However, in the name of freedom many dislike it. In the context of the Internet, cyber laws are created to ensure netizens use cyber space well and prudently. Among the steps to address cyber threats is through cyber law enforcement. However, netizens are still unaware of the existence of cyber law and the increasing number of cyber crime cases in each year. Hence, this study aimed to uncover the informant's awareness on the existence of cyber laws and analysed the

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2019-3501-08

implementation of the law on cyber security threats in Malaysia. Qualitative methodology i.e. focus group, in depth interview and document analysis are used to get quality research data. The number of focus group informants is 35 Internet users while the number of in-depth interviewer is 6 people. Among the main documents analysed in this study are the legislation, annual reports, media releases and others. The findings suggest that focus group informants are unaware of the existence of cyber laws because they feel it least important, as well as informants are less sensitive and not practicing it. Document analysis results also found that several cyber laws could be used to address cyber threats such as the Communications and Multimedia Act 1998, Computer Crimes Act 1997, Electronic Trade Act 2006, Personal Data Protection Act 2010 and Consumer Protection Act 1999 (Amendment 2010).

Keywords: *Cyber law, cyber security, netizen, social media, awareness.*

PENGENALAN

Dalam era perkembangan teknologi terkini, memang tidak dapat dinafikan bahawa maklumat mengenai sesuatu isu di alam maya bergerak lebih cepat dan pantas berbanding dengan media yang lain. Sebagai contoh dalam insiden kes kematian Muhammad Adib Mohd Kassim pada 27 November 2018 maklumat lebih cepat diperoleh melalui media sosial berbanding dengan maklumat daripada media tradisional seperti TV, radio, mahupun surat khabar. Generasi muda kini dengan alam siber tidak boleh dipisahkan. Hal ini kerana warga muda di Malaysia lebih gemar menggunakan media sosial dalam proses penyampaian dan memperoleh maklumat (Ali Salman, 2018). Kesan daripada perkembangan dalam media baharu menyebabkan terdapat beberapa istilah popular turut wujud dan kerap digunakan dalam laman sosial oleh masyarakat seperti perkataan warganet, swafoto, *Instastory*, *hashtag*, dan *Tweet*. Pada 2014, Dewan Bahasa dan Pustaka (DBP) telah memberi takrifan kepada beberapa perkataan popular di alam maya dan bercadang akan dimasukkan ke dalam Kamus Dewan (Awang Sariyan, 2014). Antara definisi yang telah diberikan oleh DBP adalah, *Selfie* dan *Wefie* merujuk kepada perbuatan mengambil gambar sendiri dan juga mengambil gambar secara beramai-ramai serta memuat naik ke dalam media sosial seperti *Facebook, Instagram* dan lain-lain. Bagi istilah *hashtag* pula, penggunaan simbol "#" oleh pengguna *Twitter* bagi menandakan kata kunci atau topik hangat. Manakala *Tweet* merujuk kepada status yang diletakkan oleh pengguna *Twitter* dalam laman sosial. Selaras dengan perkembangan dan penggunaan istilah baru dalam dunia maya ini, syarikat *LG Electronics* turut mengambil peluang dengan melancarkan telefon pintar G3 yang khas direka untuk peminat *Selfie* (Marshal, 2014). Ini jelas menunjukkan syarikat teknologi turut menggalakkan netizen untuk berswafoto.

Media sosial kini bukan sahaja menjadi ejen sosialisasi malah turut digunakan dalam penyampaian pelbagai maklumat dan isu termasuk agama (Muhammad Adnan, Siti Nur Husna & Mohd Izhar Ariff, 2018). Apabila teknologi dalam dunia siber semakin berkembang dengan pantas sudah semestinya ia turut membawa kesan negatif kepada sesebuah negara terutamanya dalam kalangan pengguna teknologi tersebut. Contoh yang terdekat ialah buli siber yang dihadapi oleh warganet Malaysia di media sosial sehingga wujudnya istilah-istilah seperti "mak cik bawang" dan "pak cik bawang". Umumnya, istilah tersebut diberikan oleh netizen kepada individu yang suka bergosip atau mengata seseorang di laman sosial. Tambahan pula, istilah popular seperti "tentera bawang Malaysia" sering digunakan oleh netizen untuk merujuk kepada perbuatan serangan ke atas sesuatu akaun individu atau halaman media sosial.

Namun, masih ramai yang tidak tahu bahawa netizen sebenarnya lebih mudah terdedah kepada ancaman siber seperti menjadi mangsa penipuan dalam talian, maklumat peribadi diceroboh dan lain-lain. Selain itu, penguatkuasaan undang-undang juga turut penting dalam menangani isu keselamatan siber. Seperti yang telah dinyatakan di atas, akibat daripada tahap kesedaran dan penguatkuasaan undang-undang dalam kalangan masyarakat maka ia boleh memberi kesan ke atas kes jenayah siber Malaysia. Jadual 1 di bawah merupakan jumlah statistik insiden keselamatan siber dari 2016 hingga 2018. Laporan ini dikeluarkan secara rasmi oleh agensi MyCERT, CyberSecurity Malaysia pada 2019.

Jadual 1: Perangkaan Insiden Keselamatan Siber Tahun 2016-2018

Insiden	2016	2017	2018
Kandungan	50	46	111
Gangguan Siber	529	560	356
Penipuan	3921	3821	5123
Pencerobohan	2476	2011	1160
Kod Hasad	435	814	1700
Spam	545	344	342
Spam E-mel	732 818	1 217 423	1 555 848
Jumlah	**740 774**	**1 225 019**	**1 564 640**

Sumber: MyCERT, CyberSecurity Malaysia 2019.

Statistik ini dikeluarkan berdasarkan kepada beberapa kategori seperti kandungan, gangguan siber, penipuan dalam talian, pencerobohan, kod malisius atau hasad, spam dan spam e-mel. Berdasarkan Jadual 1 di atas, tahun 2018 merupakan antara tahun paling tinggi berlaku insiden yang melibatkan keselamatan siber iaitu sebanyak 1,564,640 berbanding tahun 2016 dan 2017. Insiden yang melibatkan spam e-mel adalah antara insiden yang mencatatkan angka paling tinggi dan ia meningkat setiap tahun dari tahun 2016 hingga 2018. Bagi tahun 2016 angka yang dicatatkan ialah sebanyak 732,818 dan angka ini meningkat sebanyak 823,030 dan menjadi 1,555,848 pada tahun 2018. Selain itu, kes kandungan juga menunjukkan angka yang meningkat dari tahun 2017 hingga 2018 iaitu 46 pada tahun 2017 dan menjadi 111 bagi tahun 2018. Selain itu, kes penipuan dalam talian juga turut mengalami peningkatan pada tahun 2018 iaitu sebanyak 5,123 kes.

Muhammad Adnan, Siti Zobidah, Jusang Bolong & Akmar Hayati (2017) berpendapat faktor kurangnya ilmu kefahaman tentang undang-undang siber turut menyumbang kepada peningkatan statistik jenayah siber di Malaysia. Justeru, antara langkah yang baik dalam mengurangkan statistik jenayah siber adalah melalui penguatkuasaan undang-undang. Hal ini kerana melalui hukuman yang diberikan pesalah berpeluang untuk menyedari kesalahan mereka dan tidak mengulangi perbuatan tersebut. Walaupun dunia maya tidak mempunyai sempadan, netizen masih berada di kawasan bidang kuasa secara fizikal dan masih tertakluk kepada undang-undang di mana mereka berada. Sebagai contoh orang Y berada di kawasan Malaysia dan melayari Internet dengan menggunakan pelayar Vietnam, orang Y masih tertakluk kepada undang-undang negara Malaysia dan tidak boleh menyalahgunakan rangkaian Internet. Terdapat pelbagai akta yang telah diwartakan oleh kerajaan Malaysia untuk diguna pakai bagi kesalahan dalam talian seperti Akta Komunikasi dan Multimedia 1998, Akta Fitnah 1957, dan

sebagainya. Namun, menurut Anita (2004) terdapat golongan netizen yang memang tidak sedar akan kewujudan akta-akta ini. Tambahan pula, netizen juga tidak mengambil kisah tentang undang-undang siber dan terus menyalahgunakan kemudahan Internet yang diberikan oleh kerajaan. Sebagai contoh, pada 2 Februari 2019 seorang peniaga ditangkap dan disiasat di bawah Akta Hasutan 1948 oleh pihak polis kerana mengeluarkan kata-kata yang menghina Yang di-Pertuan Agong, Al-Sultan Abdullah Ri'ayatuddin Al-Mustafa Billah Shah di *Facebook* (Amin Ridzuan, 2019). Persoalannya, adakah netizen masih tidak mengetahui bahawa perbuatan salah di alam maya boleh dihukum melalui undang-undang? Adakah netizen menyedari atau tidak menyedari tentang kewujudan undang-undang siber di Malaysia? Apakah undang-undang yang boleh diguna pakai untuk mengatasi ancaman keselamatan siber ini? Justeru bagi menjawab persoalan di atas, maka kajian ini bertujuan untuk mengetahui kesedaran khalayak terhadap kewujudan undang-undang siber serta menganalisis pelaksanaan undang-undang ancaman keselamatan siber di Malaysia.

METODOLOGI

Bagi menjawab persoalan kajian, kaedah kualitatif digunakan untuk mendapatkan data kajian ini. Data yang diperolehi adalah melalui kaedah kumpulan fokus, temu bual mendalam serta analisis dokumen. Kajian ini menggunakan tiga kaedah penyelidikan kerana penggunaan pelbagai kaedah dalam pengumpulan maklumat akan membantu penyelidik mendapatkan dapatan kajian yang tekal dan lebih tepat (Hasuria et al., 2009). Informan kumpulan fokus terdiri daripada pengguna Internet manakala informan temu bual mendalam ialah pegawai kerajaan. Jumlah informan pengguna Internet dalam kajian ini adalah sebanyak 35 orang. Dari segi umur pengguna Internet adalah 18 hingga 35 tahun. Seterusnya, pegawai kerajaan yang dipilih secara bertujuan ialah seramai 6 orang di mana seorang dari Suruhanjaya Komunikasi dan Multimedia Malaysia, tiga orang dari Polis Diraja Malaysia dan dua orang dari CyberSecurity Malaysia. Antara dokumen yang dianalisis dalam kajian ini ialah akta dan perundangan Malaysia, laman sesawang rasmi dan media sosial rasmi agensi di atas, laporan tahunan serta siaran media kerajaan. Lokasi dalam kajian ini pula adalah di Lembah Klang iaitu Petaling Jaya, Kuala Lumpur, Shah Alam dan Klang. Hal ini kerana menurut laporan statistik kerajaan kawasan Lembah Klang mempunyai kadar penembusan jalur lebar yang paling tinggi iaitu sebanyak 115.7% (Suruhanjaya Komunikasi dan Multimedia Malaysia, 2016). Tambahan pula, kebanyakan daripada populasi di Malaysia yang menggunakan kemudahan Internet terutama dalam konteks kesedaran dan keselamatan siber tertumpu di Lembah Klang. Oleh itu, Lembah Klang menjadi satu persampelan yang paling dekat mewakili populasi Malaysia dalam konteks ini.

KESEDARAN INFORMAN TERHADAP KEWUJUDAN UNDANG-UNDANG SIBER

Dalam realiti kehidupan, secara amnya masyarakat memerlukan satu panduan kepada apa yang boleh mereka lakukan dan apa yang tidak boleh dilakukan dalam kehidupan mereka. Undang-undang adalah antara elemen penting dalam konteks ini di mana melalui undang-undang seseorang boleh hidup secara aman dan tanpa huru hara. Walau bagaimanapun, kerajaan terus menghadapi pelbagai cabaran dalam menguatkuasa sesuatu undang-undang (Muhammad Adnan, Wan Amizah, Shahrul Nazmi & Ali Salman 2015). Hal ini kerana undang-undang yang diwujudkan oleh pihak berkuasa tinggi sesebuah negara akan menyatakan apa yang boleh dan tidak boleh dilakukan oleh masyarakat. Justeru, bagi menangani masalah penyalahgunaan

Internet dan jenayah siber, maka kerajaan Malaysia telah mewujudkan pelbagai undang-undang dan akta yang berkaitan dengan penyalahgunaan Internet. Sebagai contoh Akta Komunikasi dan Multimedia 1998, Akta Hasutan 1948, Kanun Keseksaan, Akta Fitnah 1957 dan sebagainya. Dalam hal ini, seorang pengguna Internet perlu mengetahui tentang kewujudan undang-undang siber ini sebagai panduan kepada mereka untuk mengetahui perbuatan yang dilakukan itu betul atau salah di samping dapat melindungi diri mereka sekiranya menjadi mangsa siber. Umumnya, sesuatu masalah tidak boleh diselesaikan hanya melalui undang-undang malah masyarakat perlu ada kesedaran mengenai undang-undang dan perbuatan yang menyalahi undang-undang berkenaan.

Justeru, antara isu yang diutarakan oleh informan kajian ialah mengenai kesedaran informan tentang kewujudan undang-undang dan akta siber di Malaysia. Hasil temu bual menunjukkan bahawa informan kumpulan fokus tidak sedar dan tidak tahu mengenai kewujudan undang-undang siber. Terdapat juga informan menggunakan perkataan 'kot' di mana melalui perkataan itu sendiri telah jelas bahawa informan masih ragu-ragu dan tidak yakin dengan jawapan yang diberikan apabila ditanya tentang kewujudan undang-undang dan akta siber. Hal ini dibuktikan melalui kenyataan informan berikut:

> …tak tahu sebab banyak benda tak baca semua.
> …adalah kot tapi undang-undang apa saya tak tahu.
> …tak tahu sebab tak penting pun bagi saya.
> …tak tahu sebab memang tak amik kesah langsung.
> …saya tak tahu sebab saya cakap tadi saya tak ambil kisah pun pasal Internet ini semua.
> …tak tahu langsung pasal undang ini. Bila benda itu tak jadi dekat kita, kita tak nak ambil tahu pasal benda tu.
> …saya memang tak tahu undang-undang apa…lagi pun saya ini tak ambil kisah benda tu semua. Saya bab ICT memang *failed*, tahu setakat kalau orang tanya sosial media ok *Instagram, FB*, itu je, *WeChat* itu semua yang lain memang tidak ambil tahu langsung. Kesedaran tidak ada dalam diri la.

Antara sebab yang dikemukakan oleh informan mengenai ketidaksedaran tentang undang-undang siber ialah informan merasakan undang-undang berkenaan tidak penting bagi mereka. Selain itu, informan juga kurang peka dan mengamalkan sifat sambil lewa di samping itu merasakan mereka berada dalam keadaan selamat dan tidak akan menjadi mangsa siber. Berdasarkan kenyataan para informan di atas telah jelas punca utama informan kajian tidak sedar mengenai kewujudan undang-undang siber ialah faktor sikap diri mereka sendiri. Sebagai contoh, ada informan menyatakan bahawa beliau hanya tahu menggunakan media sosial seperti *Instagram*, *Facebook* tetapi aspek undang-undang siber beliau tidak ambil kisah kerana pada pandangan beliau hanya individu yang pandai dan mahir dalam bidang ICT sahaja perlu mengetahui dan mempunyai kesedaran keselamatan siber serta kewujudan undang-undang siber. Tanggapan beliau ini menyebabkan informan merasakan kewujudan undang-undang siber tidak penting dalam kehidupan beliau.

Seterusnya, hasil kajian menunjukkan terdapat juga informan yang tahu wujudnya undang-undang siber di Malaysia. Hal ini boleh dilihat dalam kenyataan informan-informan berikut:

> …ada, sebab memang pernah belajar sikit dulu so dapat tahu melalui pembelajaran la. Contohnya Akta Hasutan, Akta Fitnah dalam siber.
> …tahu sebab pernah baca dekat berita siapa yang provokasi yang melibatkan menteri ke raja ke memang dikenakan tindakanlah. Bawah Akta Hasutan. Saya biasa tengok kes dekat Malaysia melibatkan menteri atau raja polis cepat je tangkap dan jadi isu besar dekat media dan semua orang tahu. Banyak saya baca kes-kes raja dan menteri lah.
> …saya tahu undang-undang itu ada sebab kita tengok ek provokasi dekat *Facebook* macam contohnya gambar atau sultan johor dimalukan di sosial media then kena tangkap dengan polis. Saya pernah baca Akta Hasutan orang itu kena tangkap...ada juga kes Chinta Fina yang hina sultan Johor kan..pastu teringat saya lagi yang pekerja petronas tu hina najib...yang itu pun kena tindakan juga.

Berdasarkan kenyataan di atas, informan turut mengetahui kewujudan undang-undang siber melalui proses pembelajaran. Sebagai contoh salah seorang informan kajian ialah seorang pelajar di Universiti Awam Malaysia dalam bidang Sains Politik dan beliau mengetahui undang-undang siber melalui subjek demokrasi dan masyarakat sivil. Menurut pelajar berkenaan beliau pernah mempelajari mengenai undang-undang seperti Akta Hasutan dan Akta Fitnah apabila perlu menyiapkan tugasan yang melibatkan undang-undang Malaysia. Selain itu, informan A turut mengenali kewujudan undang-undang siber melalui pembacaan di media sosial. Ketika sesi temubual informan A turut menyatakan berminat dalam hal politik serta sentiasa mengikuti perkembangan politik di Malaysia dan banyak mendapatkan maklumat melalui media sosial. Berdasarkan pengalaman informan A, beliau mengetahui kewujudan Akta Hasutan kerana di Malaysia sesiapa sahaja yang menyuarakan pendapat yang tidak berhemah melibatkan menteri atau golongan raja maka tindakan segera diambil oleh pihak polis di bawah Akta Hasutan. Justeru, kesedaran informan A mengenai undang-undang siber wujud hasil daripada mengikuti isu semasa politik di media sosial.

Seterusnya, informan B turut menyedari kewujudan undang-undang siber di Malaysia dan pengalaman beliau hampir sama dengan informan A di mana beliau mengetahui undang-undang berkenaan melalui kes yang pernah dipaparkan di akhbar dan media sosial. Berdasarkan kenyataan informan B, beliau telah mengutarakan dua kes yang pernah dibaca oleh beliau yang melibatkan undang-undang siber iaitu kes Chinta Fina dan pekerja Petronas di mana pada bulan Februari 2016 seorang pelayan wanita GRO yang berasal dari Pontian ditahan oleh pihak polis kerana menghina Sultan Ibrahim Iskandar di *Facebook* dengan menggunakan akaun bernama Chinta Fina. Hal ini terjadi apabila pemilik akaun *Facebook* Chinta Fina memberi komen tentang pengharaman penjualan rokok elektronik di negeri Johor yang dititahkan oleh Sultan Johor pada tahun 2015. Suspek ditahan di bawah Akta Hasutan 1948, Seksyen 4(1)(c). Dalam kes lain pula seperti diutarakan oleh informan B, pada bulan Mac 2016 seorang jurutera Petronas turut ditahan oleh pihak SKMM kerana memuatnaik komen yang bersifat jelik serta

menghina bekas Perdana Menteri Malaysia, Datuk Seri Najib Tun Razak. Kesalahan ini dilakukan di akaun *Facebook* bernama Jalil Ismail. Pihak SKMM juga turut menyita telefon bimbit dan kad sim suspek untuk siasatan. Hal ini menunjukkan pemaparan kes-kes tangkapan siber di media sosial boleh membantu informan untuk mengetahui kewujudan undang-undang siber.

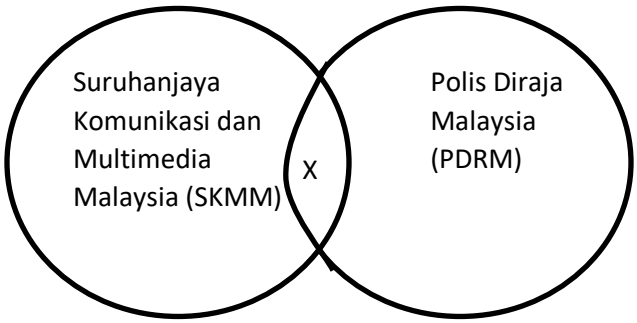
Justeru berdasarkan hasil dapatan di atas, boleh dirumuskan bahawa kesedaran para informan terhadap kewujudan undang-undang dan akta siber masih berada di tahap yang kurang memuaskan di mana informan kajian menyatakan mereka tidak sedar mengenai kewujudan undang-undang siber. Walaupun terdapat juga informan yang menyatakan mereka sedar tetapi mereka masih tidak jelas menyatakan undang-undang apakah yang terlibat secara langsung dan spesifik termasuk Seksyen-Seksyen undang-undang berkaitan.

PELAKSANAAN UNDANG-UNDANG MENGENAI ANCAMAN KESELAMATAN SIBER

Bahagian ini menghuraikan hasil dapatan kajian melalui analisis dokumen mengenai pelaksanaan undang-undang ancaman keselamatan siber. Analisis kajian mencakupi dua bahagian utama iaitu kuasa dan badan pelaksana serta undang-undang mengenai keselamatan siber Malaysia.

1. Kuasa dan Badan Pelaksana dalam Mengawal Keselamatan Siber Malaysia

Istilah kuasa sering dikaitkan dengan dunia politik dan pemerintahan. Dalam sesebuah negara kuasa adalah amat penting dalam menentukan dasar dan peraturan terhadap sesuatu perkara. Hal ini kerana dengan adanya kuasa seseorang individu boleh membuat keputusan serta mengawal tingkah laku orang lain. Kuasa juga menyebabkan seseorang individu atau organisasi menjadi lebih kuat. Secara umumnya, seseorang individu mahu pun organisasi akan memperoleh kuasa melalui peruntukan undang-undang sesebuah negara. Justeru, kuasa juga amat diperlukan oleh badan pelaksana keselamatan siber supaya peranan mereka lebih meluas dan boleh bertindak secara komprehensif dalam mengawal keselamatan siber. Oleh itu, hasil analisis dokumen mendapati terdapat dua badan pelaksana utama yang mempunyai kuasa dalam mengawal keselamatan siber (X) Malaysia iaitu SKMM dan PDRM. Sila rujuk Rajah 1 di bawah:



Rajah 1: Kuasa Badan Pelaksana.

a) Suruhanjaya Komunikasi dan Multimedia Malaysia

Hasil analisis dokumen menunjukkan SKMM memperoleh kuasa melalui dua akta iaitu Akta Suruhanjaya Komunikasi dan Multimedia Malaysia 1998 dan juga Akta Komunikasi dan Multimedia 1998. Dua punca kuasa ini menyebabkan badan berkenaan berdiri gagah dan mudah untuk melaksanakan tanggungjawab dan peranan mereka dalam mengawal keselamatan siber. Selaras dengan peruntukan di dalam Akta Suruhanjaya Komunikasi dan Multimedia Malaysia 1998 di bawah Seksyen 4 (1) maka badan SKMM telah ditubuhkan untuk menyelia, mengawal dan menguatkuasakan undang-undang berkaitan aktiviti komunikasi dan multimedia di Malaysia. Dapatan analisis dokumen mendapati, kini, SKMM dianggotai oleh seorang pengerusi iaitu Encik Al-Ishsal Ishak, dan seorang ahli suruhanjaya yang mewakili kerajaan iaitu Dato' Dr. Mohd Ali Mohamad Nor. Selain itu, SKMM mempunyai empat ahli suruhanjaya bukan kerajaan iaitu Dr. Chin Yoong Kheong, Puan Pushpa Nair, Prof. Dr. Tharek Abd Rahman dan Dato' Wei Chuan Beng.

Hasil analisis dokumen juga menunjukkan berdasarkan peruntukan Seksyen 16 (1) Akta Suruhanjaya Komunikasi dan Multimedia Malaysia 1998, antara fungsi dan peranan utama badan ini ialah untuk memberi nasihat kepada menteri mengenai dasar kebangsaan aktiviti komunikasi dan multimedia Malaysia, melaksanakan undang-undang komunikasi dan multimedia, mengawal selia segala perkara mengenai aktiviti komunikasi dan multimedia yang tidak diperuntukkan dalam undang-undang komunikasi, menimbang dan mengesyorkan reformasi undang-undang komunikasi, mengawasi dan memantau aktiviti komunikasi dan multimedia, menggalakkan dan meningkatkan pembangunan industri komunikasi serta pengawalan sendiri dan sebagainya. Berdasarkan dapatan analisis dokumen, SKMM telah mewujudkan pelbagai sektor dan antara sektor yang memainkan peranan penting dalam mengawal keselamatan siber ialah Bahagian Penguatkuasaan dan Siasatan di bawah sektor keselamatan rangkaian dan penguatkuasaan serta bahagian advokasi dan jangkauan di bawah sektor keselamatan rangkaian, pemantauan media baharu, pematuhan dan advokasi. Secara umumnya, fungsi bahagian penguatkuasaan dan siasatan ialah menjalankan siasatan apabila menerima laporan berkaitan dengan suruhanjaya yang merujuk kepada kesalahan di bawah Akta Komunikasi dan Multimedia 1998, Akta Perkhidmatan Pos 1991, Akta Tandatangan Digital 1997 serta perundangan subsidiari yang berkaitan. Manakala bahagian advokasi dan jangkauan mempunyai tanggungjawab dalam memberi kesedaran mengenai keselamatan siber kepada pengguna Internet serta menguruskan dan memberi tunjuk ajar mengenai cara membuat laporan dan aduan keselamatan siber. Hal ini turut disokong oleh informan menerusi temu bual mendalam, di mana bahagian advokasi turut membantu mangsa jenayah siber dengan memberi tunjuk ajar mengenai cara membuat aduan yang betul mengikut saluran sedia ada. Sebagai contoh, apabila seseorang mendapati wujudnya profil *Facebook* yang palsu, maka mangsa berkenaan boleh menghubungi pusat panggilan bahagian advokasi dan pegawai yang bertugas akan memberi bantuan mengenai cara melakukan aduan serta bagaimana untuk menghapuskan profil *Facebook* palsu. Berdasarkan kenyataan informan ini telah jelas bahawa bahagian advokasi SKMM sentiasa bersedia untuk membantu para mangsa jenayah siber. Hal ini dinyatakan oleh informan SKMM seperti berikut:

> ...kita memang promosi advokasi. Jadi kita ada bahagian lain yang lakukan pengawal seliaan dan penguatkuasaan....kita membantu mangsa. Contoh, *when, people* boleh telefon *call centre* atau dia boleh hantar aduan melalui e-mel, faks. Dia boleh *call this call centre* and katalah macam kes, *fake profile Facebook*, jadi bahagian ini boleh tolong, dia kata *okey* macam mana nak buat *report*, macam mana nak hapuskan *the fake profile* macam itu.

b) Polis Diraja Malaysia

Selepas SKMM, badan kedua yang memainkan peranan penting dalam mengawal keselamatan siber adalah PDRM. Menurut Perlembagaan Persekutuan di bawah Seksyen 140 (1) perlu mewujudkan sebuah Suruhanjaya Pasukan Polis bagi bertujuan pelantikan, pengesahan, kemasukan ke dalam perjawatan serta kawalan tatatertib terhadap anggota pasukan polis. Hasil analisis dokumen mendapati, selaras dengan peruntukan Perlembagaan Persekutuan Seksyen 140 (3), kini Suruhanjaya Pasukan Polis diterajui oleh seorang menteri merangkap pengerusi iaitu Tan Sri Dato' Haji Muhyiddin bin Haji Mohd Yassin. Selain itu, suruhanjaya ini terdiri daripada seorang Ketua Setiausaha Kementerian iaitu Dato' Seri Alwi bin Haji Ibrahim. Seterusnya terdiri daripada Tan Sri Dato' Sri Mohamad Fuzi bin Harun selaku Ketua Polis Negara merangkap ahli suruhanjaya dan wakil Suruhanjaya Perkhidmatan Awam, Dato' Seri Zoal Azha bin Yusof dan seorang ahli suruhanjaya wakil badan kehakiman iaitu Tan Sri Dato' Sri Azahar bin Mohamed. Selain itu, suruhanjaya ini juga terdiri daripada lima orang ahli iaitu Tan Sri Mohd Bakri bin Mohd Zinin, Dato' Wahab bin Mohd Yasin, Datuk Zaleha binti Abd. Rahman, Dato' Sri Mortadza bin Nazarene dan Encik Sidin bin Abdul Karim.

Dapatan analisis dokumen menunjukkan punca kuasa pasukan PDRM ialah melalui peruntukan-peruntukan Akta Polis 1967. Berdasarkan akta berkenaan di bawah Seksyen 20(3) terdapat 13 tugas utama PDRM yang disenaraikan. Berdasarkan peruntukan Seksyen ini pasukan PDRM mempunyai kuasa untuk menyiasat dan menangkap penjenayah siber dengan menggunakan kaedah forensik digital melalui Unit Forensik PDRM. Menurut kenyataan informan temu bual mendalam, di bawah forensik digital terdapat empat unit iaitu Unit Siasatan Jenayah Komputer, Internet dan Harta Intelek; Unit Siasatan Jenayah Telekomunikasi; Unit Siasatan Cakraoptik; dan Unit Pemantauan CCRC untuk memantau kegiatan orang awam mengenai penggunaan Internet.

2. Pelaksanaan Undang-Undang Siber Di Malaysia

Secara umumnya, undang-undang merujuk kepada suatu norma dan sistem peraturan yang digunakan untuk mengawal tingkah laku sesebuah masyarakat. Kebiasaannya undang-undang terdiri daripada hukuman dan seksaan mengikut sesuatu kesalahan yang dilakukan oleh seseorang individu. Manakala siber merujuk kepada satu perbuatan atau aktiviti komunikasi yang menggunakan komputer dan Internet. Justeru, undang-undang siber merujuk kepada peraturan dan hukuman yang berkaitan dengan aktiviti komunikasi melalui Internet dengan menggunakan sesuatu peralatan komputer. Hasil analisis dokumen mendapati di Malaysia belum ada istilah undang-undang siber kerana perkataan undang-undang siber adalah hanya nama yang diberikan oleh masyarakat, kerajaan mahupun pihak media kerana ia tidak wujud di

dalam statut negara. Walau bagaimanapun, ia bukan bermaksud tiada undang-undang yang mengawal dan menjamin keselamatan siber di Malaysia. Hal ini kerana, hasil kajian menunjukkan terdapat beberapa undang-undang tradisional yang sedia ada boleh diguna pakai untuk mengawal ancaman keselamatan siber. Terdapat undang-undang sedia ada boleh digunakan untuk melaksanakan hukuman ke atas pesalah kerana Internet merupakan satu medium atau platform yang digunakan untuk tujuan berkomunikasi.

a) Akta Komunikasi dan Multimedia 1998

Hasil analisis dokumen mendapati akta ini dikuatkuasakan oleh badan pelaksana seperti SKMM. Akta yang mengandungi sejumlah 282 Seksyen ini turut memperuntukkan dua Seksyen yang berkaitan dengan keselamatan siber iaitu Seksyen 211 dan Seksyen 233. Berdasarkan Seksyen 211 (1) seseorang individu atau pemberi perkhidmatan aplikasi kandungan tidak boleh memberikan kandungan yang berunsurkan sumbang, lucah, palsu, mengancam atau bersifat jelik untuk tujuan dan niat mengganggu, mengacau, mendera atau mengugut mana-mana orang. Berdasarkan peruntukan ini telah jelas bahawa aktiviti seperti buli siber, pornografi, menghantar virus, menyebarkan fitnah mahupun berita palsu adalah satu kesalahan di bawah Seksyen ini dan sekiranya melanggar Seksyen 211 (1) maka boleh dikenakan denda dan hukuman penjara di bawah Seksyen 211(2) iaitu denda tidak melebihi lima puluh ribu ringgit atau penjara tidak melebihi tempoh satu tahun. Seterusnya, di bawah Seksyen yang sama seseorang pentadbir atau ahli kumpulan *WhatsApp, Telegram* atau *WeChat* boleh dikenakan tindakan sekiranya mereka melakukan kesalahan seperti diperuntukkan dalam Seksyen ini. Selain itu, berdasarkan Seksyen ini juga seseorang individu telah melakukan satu kesalahan jika individu tersebut berkongsi, *retweet*, *forward* kandungan yang menyalahi Seksyen ini yang dibekalkan oleh individu lain. Sebagai contoh Ali membuat kenyataan palsu mengenai sesuatu perkara di *Facebook* miliknya, dan Abu selaku pengikut *Facebook* Ali turut berkongsi atau *share* maklumat tersebut di laman *Facebook* Abu. Dalam hal ini, berdasarkan Seksyen 211 Ali telah menyalahi peraturan kerana membekalkan kandungan palsu melalui *Facebook* dan Abu juga telah melakukan kesalahan yang sama kerana Abu berkongsi kandungan asal yang dibekalkan oleh Ali dengan menggunakan rangkaian Internet.

Selain itu, hasil analisis dokumen mendapati Seksyen 233 memperuntukkan kesalahan mengenai penyalahgunaan kemudahan rangkaian mahupun perkhidmatan rangkaian. Berdasarkan Seksyen ini seseorang itu tidak boleh menggunakan rangkaian untuk membuat atau menghantar apa-apa komen, permintaan, cadangan atau komunikasi lucah, palsu, sumbang, dan mengancam dengan niat mengganggu orang lain serta boleh dikenakan denda tidak melebihi RM 50,000 atau penjara tidak melebihi 1 tahun atau kedua-duanya.

Walaupun terdapat dua Seksyen yang berkaitan dengan keselamatan siber, tetapi berdasarkan hasil analisis dokumen akta ini masih memerlukan penambahbaikan bagi mengukuhkan aspek keselamatan siber. Antaranya ialah, tiada mana-mana peruntukan di dalam akta ini yang membenarkan pihak SKMM untuk menangkap penjenayah siber. Hal ini menyebabkan pihak SKMM hanya bertindak sebagai tempat untuk menerima aduan, menyiasat dan menyekat laman-laman yang melanggar peraturan di bawah Seksyen 211 dan 233. Sekaligus SKMM perlu bergantung kepada bantuan daripada pihak PDRM kerana PDRM mempunyai kuasa untuk menangkap. Selain itu, ia juga mengambil masa yang agak lama untuk membawa pesalah ke muka pengadilan. Di samping itu, akta ini juga tidak menggariskan

tempoh masa simpanan sesuatu rekod pengguna Internet oleh pembekal perkhidmatan rangkaian. Hal ini kerana, amalan yang sedia ada, pembekal hanya menyimpan rekod pengguna Internet bagi tempoh tiga bulan sahaja dan ia menyukarkan pihak pendakwaan untuk mendapatkan maklumat-maklumat penting seperti alamat IP dan sebagainya sekiranya melebihi tempoh masa tiga bulan. Hal ini turut disokong oleh informan PDRM berikut:

> ...rekod yang disimpan oleh *service providers*, macam rekod penggunaan Internet. *Nowadays service providers* macam *Maxis, Celcom* dan sebagainya *they keep the record for 3 months. So* bila orang report, kita akan minta butir-butir pengguna macam *IP Address* ke dia akan simpan dan boleh simpan tempoh 3 bulan je. So, kita kena minta dalam tempoh masa ni. Jadi kita hadapi dalam kebanyakan kes, nak kesan suspek itu mungkin kena ambil masa lama. *You know, maybe* orang yang buat report pun mungkin buat report bukan *immediate*, dia *realised*, dia sedar bahawa dia telah ditipu mungkin *2 months later, 3 months later*, baru buat report *so* memang susah. *I want to trace the record, so they will keep the record for three months. So if you go on to the fourth month no more record. So how to trace?* Kita punya siasatan akan gagal.

Seterusnya, hasil analisis dokumen juga mendapati, akta ini perlu dilihat dari segi penggunaan istilah "dengan niat" di dalam Seksyen 211 dan 233 kerana berdasarkan kedua-dua Seksyen tersebut seseorang individu hanya bersalah jika melakukan sesuatu gangguan, mengugut atau mendera mana-mana orang dengan niat. Sekiranya beliau melakukan perbuatan tersebut tetapi tidak mempunyai niat maka di bawah Seksyen ini individu tersebut tidak melakukan satu kesalahan. Sebagai contoh, Kumar meletakkan gambar lucah di dalam profil *WhatsApp* beliau dengan niat tidak menganggu mana-mana orang lain kerana gambar lucah tersebut diletakkan di *WhatsApp* peribadi beliau. Justeru, mengikut peruntukan Seksyen ini maka Kumar tidak melakukan kesalahan kerana elemen gangguan tidak wujud secara kasarnya. Walau bagaimanapun, adakah Kumar yakin dan boleh memastikan perbuatan tersebut tidak mengganggu orang lain kerana profil *WhatsApp* Kumar masih boleh dilihat oleh orang lain dan sudah semestinya ia mengganggu individu yang melihat gambar lucah berkenaan di profil *WhatsApp* Kumar. Justeru, elemen peruntukan dengan niat dalam Seksyen ini perlu dipinda dan kedua-dua Seksyen ini perlu dijadikan sebagai *straight liability* di mana kesalahan tidak perlu dibuktikan. Hal ini bermaksud sekiranya Kumar meletakkan gambar lucah di profil *WhatsApp* peribadi beliau telah dianggap melakukan satu kesalahan dan tidak perlu membuktikan niatnya. Tambahan pula, Seksyen ini juga perlu dipinda kerana peruntukan Seksyen ini agak bercanggah dengan peruntukan di dalam Kanun Keseksaan. Hal ini kerana menurut Seksyen 292 Kanun Keseksaan sesiapa yang memiliki sahaja bahan lucah telah melakukan satu kesalahan di bawah Kanun Keseksaan sedangkan di dalam Akta Komunikasi dan Multimedia 1998 di bawah Seksyen 211 dan 233 perlu membuktikan dahulu niat seseorang yang memiliki bahan lucah tersebut.

b) Akta Jenayah Komputer 1997

Hasil analisis dokumen menunjukkan akta ini merupakan adaptasi daripada *Computer Misuse Act 1990* United Kingdom yang telah disesuaikan dengan situasi di Malaysia. Tujuan penggubalan akta ini adalah untuk memberi peruntukan mengenai kesalahan dalam penyalahgunaan komputer (Anita & Nazura 2004). Akta ini terdiri daripada tiga bahagian utama dan 12 Seksyen. Menurut Seksyen 3(1) ia lebih menekankan mengenai kesalahan berkaitan penyalahgunaan komputer dengan niat untuk melakukan capaian tanpa kuasa. Sebagai contoh seseorang yang tidak mempunyai keizinan daripada pemilik komputer telah menghidupkan sistem komputer dan memuat turun beberapa maklumat dari sistem tersebut ke dalam disket (Anita & Nazura 2004). Menurut Seksyen 3, seseorang telah dikatakan melakukan sesuatu kesalahan sekirannya:

(i) menyebabkan sesuatu komputer melaksanakan apa-apa fungsi dengan niat mendapatkan capaian kepada mana-mana aturcara atau data yang disimpan dalam mana-mana komputer;
(ii) capaian yang dia berniat untuk didapati adalah tanpa kuasa;
(iii) dia tahu semasa dia menyebabkan komputer itu melaksanakan fungsi itu demikian berlakunya.

Jelas sekali *mens rea* bagi Seksyen ini terdiri daripada dua perkara penting iaitu perlu ada niat untuk mendapat capaian kepada mana-mana program atau data yang disimpan di dalam komputer dan kedua capaian tersebut adalah tanpa kuasa (Anita & Nazura 2004). Jika disabitkan kesalahan boleh dikenakan denda tidak melebihi RM50,000 atau dipenjarakan selama tempoh tidak melebihi 5 tahun atau kedua-duanya. Selain itu, hasil analisis dokumen mendapati, terdapat juga Seksyen 4 yang menyatakan kesalahan mengenai capaian tanpa kuasa bagi melakukan kesalahan seterusnya atau lanjut. Walau bagimanapun, Seksyen 4 ini hanya terpakai apabila terdapat kesalahan di bawah Seksyen 3 di atas. Justeru, hal ini menyukarkan pemakaian Seksyen 4 untuk proses pendakwaan. Sebagai contoh, Ali menghantar virus kepada laman web Ahmad yang terbuka kepada umum dengan menggunakan komputer sendiri. Dalam hal ini, walaupun Ahmad mengalami kerugian disebabkan oleh virus berkenaan tetapi Ali tidak boleh didakwa kerana elemen pencapaian tanpa kuasa tidak wujud di situ kerana Ali menggunakan komputer peribadi sendiri. Kelemahan dalam Seksyen ini perlu diperbaiki seperti mana yang dicadangkan oleh Anita Abdul Rahim dan Nazura Abdul Manap (2004) seperti berikut:

Seseorang adalah melakukan suatu kesalahan di bawah Seksyen ini jika dia:

a. melakukan suatu kesalahan yang melibatkan *fraud* atau kecurangan atau yang menyebabkan kecederaan sebagaimana yang ditakrifkan dalam Kanun Keseksaan; atau
b. memudahkan berlakunya suatu kesalahan itu sama ada olehnya sendiri atau oleh mana-mana orang lain.

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2019-3501-08

c) Akta Perdagangan Elektronik 2006

Analisis dokumen mendapati akta ini turut melindungi pengguna dalam urusan perniagaan secara dalam talian. Di bawah Seksyen 5 tafsiran, urus niaga perdagangan bermaksud suatu komunikasi sehala atau komunikasi pelbagai yang bersifat perdagangan, sama ada berbentuk kontraktual atau tidak, termasuklah apa-apa perkara yang berhubung dengan pembekalan atau pertukaran barang-barang atau perkhidmatan, agensi, pelaburan, kewangan, perbankan dan insurans. Dengan adanya akta ini pengguna menjalankan transaksi elektronik dalam persekitaran yang lebih terjamin. Walau bagaimanapun, hasil kajian mendapati, akta ini melalui Seksyen 3(1) menyatakan bahawa penggunaan adalah tidak mandatori seperti berikut:

> 3. (1) Tiada apa pun dalam Akta ini boleh menjadikannya mandatori bagi seseorang untuk menggunakan, memberi atau menerima apa-apa mesej elektronik dalam mana-mana urus niaga perdagangan melainkan jika orang itu mengizinkan penggunaan, pemberian atau penerimaan mesej elektronik itu.

Hal ini bermaksud, berdasarkan kenyataan informan, urusan membeli barangan adalah di bawah tindakan sivil dan Akta Perdagangan Elektronik 2006 tidak termasuk tindakan jenayah. Ini bererti peniaga masih mempunyai pilihan sama ada peniaga berkenaan masih ingin tertakluk di bawah Akta Perdagangan Elektronik 2006 atau di bawah Akta Kontrak 1950. Hal ini kerana mengikut peruntukan Akta Perdagangan Elektronik 2006 dalam kalangan peniaga adalah tidak wajib. Justeru peruntukan tidak mandatori di dalam Akta Perdagangan Elektronik 2006 ini perlu dilihat semula kerana jika seseorang peniaga menggunakan urusan perniagaannya melalui elektronik tetapi peniaga berkenaan membuat pilihan tidak mengikuti Akta Perdagangan Elektronik 2006 maka ia menimbulkan masalah sabitan di mahkamah sekiranya berlaku unsur-unsur penipuan dan sebagainya.

> …hal beli barang adalah tindakan sivil dan akta ini adalah tidak wajib. Contoh bila saya berniaga saya boleh pilih sama ada saya nak berada di bawah akta ini atau tidak atau pun saya nak guna Akta Kontrak 1950 biasa sahaja. Maksudnya saya sebagai peniaga boleh nyatakan dengan jelas bahawa perniagaan saya tidak termasuk di bawah Akta Perdagangan Elektronik 2006.

d) Akta Perlindungan Data Peribadi 2010

Dengan dunia yang bergerak pantas dan ledakan ICT di mana privasi seseorang tidak terjamin lagi. Segelintir syarikat tempatan atau orang tidak bertanggungjawab sering menyalahgunakan data peribadi seseorang terutama secara komersial. Oleh itu, hasil analisis dokumen mendapati pada 10 Jun 2010 Akta Perlindungan Data Peribadi 2010 diperkenalkan. Dapatan menunjukkan tujuan utama penggubalan akta ini adalah untuk mengawal selia pemprosesan data peribadi individu yang terlibat dalam transaksi komersial dan ini termasuk transaksi dalam talian. Hasil analisis dokumen menunjukkan akta yang mengandungi sebanyak 11 bahagian ini mempunyai tujuh prinsip yang perlu dipatuhi oleh seseorang. Pertama, prinsip am di mana seseorang pengguna tidak dibenarkan memproses data peribadi seseorang lain tanpa kebenarannya.

Kedua, prinsip notis dan pilihan di mana pengguna data perlu memaklumkan tujuan awal kepada subjek data. Ketiga penzahiran. Hal ini bermaksud tujuan data peribadi seseorang subjek itu demi mengenal pasti maksud yang baginya data peribadi itu hendaklah dizahirkan. Prinsip keempat adalah keselamatan di mana dalam memproses mana-mana data, perlu mengambil langkah supaya data tersebut selamat, tidak diubahsuai, disalahguna atau diberikan kepada pihak yang tidak berkenaan. Seterusnya prinsip penyimpanan iaitu sesuatu data peribadi tidak dibenarkan disimpan di dalam sesuatu pemprosesan lebih daripada had masa yang diperlukan. Keenam adalah prinsip integriti data di mana setiap data peribadi dipastikan tepat, lengkap, tidak mengelirukan dan terkini. Ketujuh adalah prinsip akses di mana seseorang hendaklah diberi hak akses kepada data peribadinya yang dipegang oleh seseorang pengguna data dan juga boleh membetulkan datanya itu supaya terkini.

Selain itu, hasil kajian mendapati seseorang individu mempunyai hak untuk melarang data peribadi mereka digunakan untuk tujuan komersial atau pemasaran melalui pemberian notis bertulis kepada pengguna data dan ini terbukti di bawah peruntukan Seksyen 43(1). Menurut Seksyen 43(2) sekirannya pengguna data masih enggan mematuhi notis maka individu tersebut boleh membuat permohonan kepada Pesuruhjaya untuk menghendaki pengguna data itu mematuhi notis itu. Sekiranya pengguna data masih gagal mematuhi notis tersebut maka boleh disabitkan kesalahan di bawah Seksyen 43 ini dan mengikut Seksyen 43(4) boleh membawa denda tidak melebihi RM 200,000 atau dipenjarakan selama tempoh tidak melebihi dua tahun atau kedua-duanya. Selain di atas, menurut Seksyen 129(1)(2)(3) data peribadi seseorang juga tidak boleh dipindahkan ke tempat di luar Malaysia kecuali mendapat persetujuan individu tersebut atau melibatkan kontrak. Sekiranya gagal mematuhi peraturan ini maka mengikut Seksyen 129(5) boleh didenda tidak melebihi tiga ratus ribu ringgit atau dipenjarakan selama tempoh tidak melebihi dua tahun atau kedua-duanya.

Walau bagaimanapun, berdasarkan kenyataan informan temu bual mendalam satu perkara yang perlu dilihat di dalam akta ini ialah tujuan komersial. Hal ini bermaksud pihak yang menjalankan urusan komersial sahaja perlu mendaftar di Jabatan Perlindungan Data Peribadi dan sekiranya urusan berkenaan bukan bertujuan komersial tidak perlu mendaftar di jabatan berkenaan. Sebagai contoh sebuah organisasi NGO yang memiliki data peribadi pelajar seluruh Universiti Awam di Malaysia, dan penggunaan data berkenaan bukan untuk komersial maka organisasi berkenaan tidak perlu mendaftar di Jabatan Perlindungan Data Peribadi. Walau bagaimanapun, dalam keadaan ini akan timbul persoalan bagaimanakah sekiranya data yang dimiliki oleh organisasi NGO telah diceroboh atau dicuri oleh pihak lain? Sudah tentu data yang banyak tersebut akan jatuh ke tangan individu yang tidak bertanggungjawab dan menimbulkan pelbagai masalah. Justeru, di dalam akta ini perlu dimasukkan sekali bukan komersial supaya data yang diperoleh dapat diuruskan dengan selamat. Hal ini boleh dilihat melalui kenyataan informan temu bual mendalam berikut:

> …dia terpakai kepada pihak yang melakukan urusan komersial sahaja kalau bukan komersial dia tak perlu daftar. Contohnya, saya satu organisasi NGO. Saya simpan data peribadi semua pelajar IPTA yang itu saya tak perlu daftar dengan Jabatan Perlindungan Data Peribadi sebab saya bukan komersil.

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2019-3501-08

e) *Akta Perlindungan Pengguna 1999 (Pindaan) 2010*

Hasil analisis dokumen menunjukkan akta ini melindungi hak pengguna secara keseluruhan seperti dalam proses jual beli, barangan, perkhidmatan, kontrak dan lain-lain termasuk urusan dalam talian serta melindungi pengguna dari segi mendapatkan maklumat terutamanya melalui iklan yang ditayangkan atau disiarkan melalui talian internet. Iklan dalam media cetak dan elektronik masih boleh dikawal oleh pihak kerajaan berbanding dengan iklan dalam talian. Pengguna mudah tertipu dengan iklan yang ditawarkan dalam Internet kerana tidak tahu kesahihannya selain tiada agensi yang memantau secara keseluruhan. Selain kesahihan, iklan di Internet juga tidak mematuhi garis panduan iklan yang sedia ada dan kebanyakan iklan adalah palsu dan mengelirukan pengguna. Di bawah pindaan 2010, hasil analisis dokumen menunjukkan terdapat peruntukan Bahagian baru iaitu XI_A Jawatankuasa Pengiklanan dan di bawah Seksyen 84_A bahagian ini menteri boleh menubuhkan satu Jawatankuasa Pengiklanan untuk meneliti aduan berhubung iklan, menguar-uarkan maklumat mengenai hak pengguna dan lain-lain. Di bawah jawatankuasa ini maka wujudnya garis panduan mengelakkan iklan palsu atau mengelirukan. Dalam garis panduan ini iklan ditafsirkan sebagai apa-apa bentuk iklan berupa ucapan, tulisan, bunyian, lakaran atau gambar yang diterbitkan melalui (i) pameran atau penyiaran notis; (ii) penggunaan media cetak seperti surat khabar, majalah atau bahan-bahan bercetak seperti katalog, senarai harga, pekeliling, label, kad atau dokumen atau bahan lain; (iii) pertunjukan filem, gambar atau gambar foto; (iv) penggunaan medium elektronik seperti radio, televisyen atau telekomunikasi dalam talian dan juga apa-apa cara yang lain. Garis panduan ini amat menekankan iklan-iklan palsu dan mengelirukan pengguna. Selain panduan ini, Akta Perlindungan Pengguna (Pindaan 2010) 1999 turut memberi peruntukan larangan mengenai perlakuan palsu atau mengelirukan di bawah Seksyen 9 dan 10.

Oleh itu, sesiapa yang melanggar Seksyen-Seksyen ini boleh dikenakan hukuman denda dan penjara di bawah Seksyen 25. Sekiranya ia melibatkan suatu pertubuhan perbadanan boleh didenda tidak melebihi RM 250,000 dan kesalahan berikutnya denda tidak melebihi RM 500,000. Manakala, melibatkan bukan suatu pertubuhan perbadanan maka denda tidak melebihi RM 100,000 atau penjara selama tempoh tidak melebihi 3 tahun atau kedua-duanya. Selain iklan, hasil analisis dokumen menunjukkan akta ini turut melindungi pengguna dalam urus niaga perdagangan elektronik. Pada 20 Disember 2012, di bawah peruntukan Seksyen 150 (2)(*a*) akta ini menteri telah membuat suatu peraturan baru yang dikenali sebagai Peraturan-Peraturan Pelindungan Pengguna (urus niaga perdagangan elektronik) 2012. Peraturan ini mula berkuat kuasa pada 1 Julai 2013. Di bawah peraturan ini, pasar dalam talian membawa maksud urus niaga atau perdagangan menggunakan tapak web di mana barang atau perkhidmatan dipasarkan oleh pihak ketiga dan manakala pengendali pasar dalam talian bermaksud seseorang yang menyediakan pasar dalam talian. Berdasarkan definisi di atas telah jelas bahawa peniaga yang menjual barangan di media sosial turut terikat dengan peraturan ini. Justeru, berdasarkan peraturan ini peniaga dalam talian perlu mengemukakan nama, nombor pendaftaran perniagaan, alamat e-mel, nombor telefon, alamat perniagaan, ciri-ciri barang dan perkhidmatan, harga penuh barangan, kaedah pembayaran, terma dan syarat serta anggaran masa penghantaran. Sekiranya seseorang peniaga tidak mengikuti peratutan ini maka peniaga tersebut telah melakukan suatu kesalahan dan ia boleh dilihat di bawah peraturan 3(1) (2).

KESIMPULAN

Secara ringkasnya, dari aspek kesedaran informan mengenai undang-undang siber, kajian mendapati para informan kajian tidak sedar dan tidak tahu mengenai kewujudan undang-undang siber. Antara sebab yang dikemukakan oleh informan kajian mengenai ketidaksedaran tentang undang-undang siber ialah informan merasakan undang-undang berkenaan tidak penting bagi mereka, tidak berkaitan dan informan mengamalkan sifat sambil lewa. Selain itu, informan juga merasakan mereka berada dalam keadaan selamat dan hal ini bermaksud informan beranggapan mereka tidak akan menjadi mangsa siber. Justeru, dalam proses memberi kesedaran keselamatan siber oleh kerajaan elemen peruntukan undang-undang perlu dimasukkan dan diterangkan secara jelas, mudah dan sistematik melalui kempen-kempen yang sedia ada. Sebagai contoh, dalam buku panduan keselamatan melayari Internet (SKMM, 2014), perkara mengenai undang-undang siber diceritakan secara ringkas dengan hanya memberitahu nama akta berkenaan tanpa ada sebarang petikan kesalahan atau rujukan kes. Hal ini perlu dilihat semula kerana peruntukan undang-undang merupakan antara kaedah yang baik dalam memberi kesedaran keselamatan siber kepada pengguna Internet. Justeru penjelasan dan perhatian yang baik amat diperlukan dalam proses penyampaian maklumat sesuatu kempen sekaligus meningkatkan kesedaran pembaca mengenai undang-undang siber. Selain itu, kajian mendapati terdapat beberapa undang-undang tradisional dan sedia ada yang boleh diguna pakai untuk mengawal ancaman keselamatan siber di Malaysia. Antara undang-undangnya ialah seperti Akta Komunikasi dan Multimedia 1998 di bawah Seksyen 211 dan 233. Selain itu, Akta Jenayah Komputer 1997 juga boleh diguna pakai di bawah Seksyen 3(1). Kewujudan Akta Perdagangan Elektronik 2006 turut membantu kerajaan dalam mengurangkan jenayah siber di Malaysia. Seterusnya, Akta Perlindungan Data Peribadi 2010 telah dilaksanakan di Malaysia bagi melindungi data peribadi yang digunakan secara komersial oleh pihak-pihak tertentu. Di bawah akta ini terdapat beberapa peruntukan Seksyen yang mengawal penyalahgunaan data peribadi seperti Seksyen 43(1)(2)(3) serta Seksyen 129 (5). Di samping itu pelaksanaan Akta Perlindungan Pengguna 1999 (Pindaan 2010) turut melindungi pengguna Internet dari segi kekeliruan iklan dan maklumat mengenai sesuatu perniagaan melalui peruntukan Seksyen 9, 10 dan 25 akta berkenaan.

BIODATA

Muhammad Adnan Pitchan merupakan Pensyarah Kanan di Pusat Komunikasi dan Masyarakat Digital, Fakulti Sains Sosial dan Kemanusiaan, UKM. Bidang kajian beliau adalah media baharu, undang-undang siber, dan dasar keselamatan siber. Email: adnan86@ukm.edu.my

Siti Zobidah Omar merupakan Profesor Madya di Jabatan Komunikasi, Fakulti Bahasa Moden dan Komunikasi, Universiti Putra Malaysia. Bidang Kepakaran beliau ialah Penggunaan ICT dan teknologi komunikasi serta e-komuniti. Email: zobidah@upm.edu.my

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2019-3501-08

RUJUKAN

Ali Salman, Mohammad Agus Yusoff, Mohd Azul Mohamad Salleh, & Mohd Yusof Hj Abdullah. (2018). Pengunaan Media Sosial Untuk Sokongan Politik di Malaysia. *Journal of Nusantara Studies,* 3(1), 51-63.

Amin Ridzuan. (2019, Februari 2). Peniaga Hina Yang Di-Pertuan Agong Disiasat Mengikut Akta Hasutan 1948. *Berita Harian Online*. Diambil daripada https://www.bharian.com.my

Anita, A. R., & Nazura, A. M. (2004). *Jenayah Berkaitan dengan Komputer: Perspektif Undang-Undang Malaysia*. Kuala Lumpur: Dewan Bahasa dan Pustaka.

Awang Sariyan. (2014). *DBP Guna Pakai Perkataan Popular dalam Kamus Dewan*. Diambil September 28, 2018, daripada http://www. bharian.com.my/bharian/ articles/DBPgunapakaiperkataanpopulardalamKamusDewan/Article/

CyberSecurity Malaysia. (2019). MyCERT Incident Statistics. Diambil Februari, 2019, daripada https://www.mycert.org.my/statistics/2018.php

Hasuria Che Omar, Rokiah Awang, Syed Zainal Ariff Syed Jamaluddin, & Noriah Mohamed (pnyt.). (2009). *Bahasa Verbal dan Bukan Verbal I*. Kuala Lumpur: Institut Terjemahan Negara Malaysia Berhad.

Marshal, J. (2014). LG Lancar Telefon Pintar untuk Peminat 'Selfie'. Diambil September 28, 2018, daripada http://www.bharian.com.my/bharian/articles/LGlancar telefonpintaruntukpeminat_selfie_/Article/?mutakhir=1

Muhammad Adnan, Siti Nur Husna, & Mohd Izhar Ariff. (2018). Teori Al-Daruriyyat dan Penggunaan Media Sosial: Satu Perbincangan Konsep. *Jurnal Komunikasi: Malaysian Journal of Communication*, 34(4), 75-92.

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), 016-029.

Muhammad Adnan, Wan Amizah, Shahrul Nazmi, & Ali Salman. (2015). Control and Freedom of the Internet: Challenges Face by the Government. *Journal of Asia Pacific Communication,* 25(2), 243-252.

SKMM. (2016). Internet Users Survey 2016. Diambil Julai 28, 2018, daripada https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/IUS2016.pdf