JURNAL ISLAM DAN MASYARAKAT KONTEMPORARI
© PENERBIT UNIVERSITI SULTAN ZAINAL ABIDIN
ISSN 1985-7667 • e-ISSN: 2289-6325
https://doi.org/10.37231/ jimk.2015.11.1.134

Jurnal Islam dan Masyarakat Kontemporari
Journal of Islam and Contemporary Society JIMK

**https: / / journal.unisza.edu.my / jimk**

# [CYBER TYPES: NEW CRIME IN A CONTEMPORARY SOCIETY]

# INTIPAN SIBER: JENAYAH BARU DALAM MASYARAKAT KONTEMPORARI

ASIAH BIDIN[1*]
SHARIFFAH NURIDAH AISHAH SYED NONG MOHAMAD[1]
AKMAL MOHAMAD[1]

[1] Fakulti Undang-Undang, Perakaunan dan Hubungan Antarabangsa
Universiti Sultan Zainal Abidin, Malaysia

*Corresponding author: aishah@unisza.edu.my

Received Date: 9 Januari 2015 • Accepted Date: 9 April 2015

***Abstract***

*Innovation and technological advancement nowadays had produced several web-based products. These include social networking sites (SNS) which are dominating Internet usage among consumers. Although the site is able to connect friendship without limits and become a very effective means of communication in cyberspace, the negative impact should not be under-estimated. This article concludes that the use of social networking sites gives the risk of the crime of cyber stalking. An analysis on the legislative framework in Malaysia in relation to the crime shows that there is lacuna in legal provisions pertaining to the issue.*

*Keywords: social networking sites, cyber stalking, crimes, Malaysian law*

**Abstrak**

Inovasi dan kemajuan teknologi masa kini telah menghasilkan beberapa produk berasaskan web. Antaranya ialah laman rangkaian sosial yang sedang mendominasi penggunaan Internet dalam kalangan pengguna. Walaupun laman ini mampu menghubungkan persahabatan tanpa batasan dan merupakan alat komunikasi di dunia maya yang sangat efektif, kesan negatifnya juga tidak boleh dipandang ringan. Artikel ini membincangkan penggunaan laman rangkaian sosial dan risiko terhadap jenayah intipan siber (cyber stalking). Selain itu, bagaimana jenayah intipan siber berlaku turut dibincangkan. Akhir sekali kerangka perundangan di Malaysia berkaitan jenayah intipan siber diutarakan bagi menilai sama ada ia sudah memadai dalam menangani jenayah ini.

**Kata kunci**: Laman rangkaian sosial, intipan siber, jenayah, undang-undang Malaysia.

**Cite as:** Asiah Bidin, Shariffah Nuridah Aishah Syed Nong Mohamad & Akmal Mohamad. 2015. Intipan Siber: Jenayah Baru Dalam Masyarakat Kontemporari. *Jurnal Islam dan Masyarakat Kontemporari* 11(1):10-21.

## PENGENALAN

Perkembangan teknologi maklumat masa kini meletakkan kita dalam dunia tanpa sempadan. Semua maklumat dapat diakses dalam sekelip mata. Jika dahulu, pengguna Internet didedahkan dengan medium komunikasi e-mel, namun dewasa ini, laman rangkaian sosial amat mendapat tempat dalam kalangan masyarakat seantero dunia kerana jaringan sosialnya yang luas tanpa batasan. Tidak dapat dinafikan, banyak manfaat yang wujud daripada penciptaan laman rangkaian sosial ini atau lebih dikenali sebagai SNS (social networking sites) seperti penjimatan kos dan kuasa akses tanpa had waktu. Secara ringkasnya, laman rangkaian sosial merujuk kepada penggunaan laman web sosial bagi memudahkan komunikasi dan mengembangkan persahabatan sosial di alam maya. Laman web rangkaian sosial umpama satu komuniti dalam talian pengguna Internet. Tertakluk kepada syarat sesebuah laman web rangkaian sosial, ahli-ahli dalam komuniti tersebut akan berkongsi hampir semua maklumat seperti hobi, agama, alam sekitar mahupun politik. Keahlian kepada sesuatu laman sosial adalah penting bagi membolehkan ahlinya bersosial di alam maya dengan komuniti laman tersebut seperti membaca profil atau halaman profil ahli-ahli yang lain ataupun menghubungi mereka secara langsung menerusi ruangan sembang (chat). Pada masa kini kemudahan capaian atau akses kepada laman web ini boleh dilakukan di mana sahaja baik di rumah, pejabat, cybercafé, kiosk Internet, malah di restoran-restoran asalkan terdapat kemudahan Internet. Banyak premis awam dan persendirian menyediakan kemudahan Internet secara percuma bagi menarik pelanggan ke premis mereka. Laman rangkaian sosial ini digunakan secara meluas bukan hanya dalam kalangan pelajar universiti, tetapi juga remaja sekolah, golongan profesional dan ahli politik (Rosen, 2007). Lambakan laman web sosial pada hari ini dapat diumpamakan bagaikan cendawan tumbuh selepas hujan. Dianggarkan terdapat 170 laman web sosial interaktif yang terkenal dan aktif di seluruh dunia untuk pelayar-pelayar Internet (Syahrir & Fatin, 2012). Sesetengahnya hanya popular di negara-negara tertentu sahaja seperti QQ di China, V Kontakte di Brazil dan Cyworld di Korea Selatan (Megat Ishak, 2010). Di sekitar tahun 2005-2006, MySpace, laman web sosial muzik dikatakan mengalahkan kedudukan Google dari segi halaman yang dilihat (page viewed), manakala Friendster pula yang dilancarkan pada tahun 2002 lebih banyak digunakan oleh pengguna bagi tujuan perhubungan sosial atau persahabatan maya (Megat Ishak, 2010). Di antara kesemua aplikasi rangkaian sosial yang sedia ada masa kini, walaupun baru diperkenalkan pada tahun 2004, Facebook menduduki tempat pertama daripada senarai 15 teratas laman rangkaian sosial yang paling popular, diikuti dengan Twitter dan LinkedIn (eBizMBA Guide, 2014). Facebook juga dikatakan memiliki sejumlah 350 juta pengguna dan menyimpan 10 billion gambar yang dikongsi oleh pengguna-pengguna dari segenap pelosok dunia (Syahrir & Fatin, 2012).

## PENGGUNAAN LAMAN RANGKAIAN SOSIAL DI MALAYSIA

Laman web rasmi Persatuan Penolong Pegawai Teknologi Maklumat Sektor Awam Malaysia mendedahkan bahawa mengikut perangkaan rasmi, kira-kira 16.5 juta rakyat Malaysia menggunakan Internet dan jika mengambil kira secara keseluruhan termasuk pengguna melalui rangkaian telefon bimbit, jumlahnya adalah lebih tinggi. Sementara itu pengguna Facebook di

negara ini pula mencecah angka melebihi daripada 2 juta dan berada di tangga ke-18 di dunia sebagai negara aktif memperbaharui status masing-masing dalam laman web sosial itu (Harian Metro, 2009). Laman web Monster & Critics.com pula mendapati, dengan 17 juta pengguna di atas talian setiap hari, mereka secara puratanya meluangkan masa selama 20 jam seminggu untuk mengakses Internet.

Di Malaysia, nama-nama seperti Xanga, Classmates.com, Bebo, Blackplanet.com dan Orkut mungkin kurang diketahui atau jarang didengari (Social Networking Web Sites, 2006) walaupun kesemua aplikasi tersebut merupakan sebahagian daripada laman web rangkaian sosial yang disajikan untuk kemudahan pelayar Internet masa kini. Walau bagaimanapun, antara aplikasi yang mendapat tempat di hati masyarakat Malaysia ialah Facebook, Friendster, Skype, MySpace dan juga Twitter. Selain itu, terdapat juga beberapa aplikasi rangkaian sosial tempatan seperti eKawan, Ruumz, GoEatOut, Circles99, FriendX, eMeiMei serta Pacmee (Syahrir & Fatin, 2012) di mana setiap produk ini mempunyai ciri-ciri dan kelebihan masing-masing. Penggunaan jenis laman rangkaian sosial di negara ini berbeza mengikut kategori masyarakat. Facebook mungkin lebih digemari oleh golongan remaja manakala golongan selebriti seperti artis dan ahli politik lebih selesa menggunakan Twitter bagi memaklumkan perkembangan terkini aktiviti mereka. Dalam satu tinjauan yang dijalankan, 85 peratus responden di Malaysia menggunakan laman web sosial diikuti oleh India (83%), Singapura (82%) dan Amerika Syarikat (75%) (Social Networking Watch, 2010). Menurut sumber dari Alexa dan Google Ad Planner pula, seramai 6.2 juta pengguna Internet di Malaysia mengunjungi laman sosial Facebook, diikuti Friendster dengan 4.2 juta, MySpace 2.1 juta dan Twitter 750 ribu orang (Syahrir & Fatin, 2012).

## JENAYAH INTIPAN SIBER: APA DAN BAGAIMANA BERLAKU

Penggunaan laman sosial boleh memberi kesan terhadap perlakuan jenayah. Laman sembang sosial merupakan syurga bagi pengintip siber kerana tidak terdapat had perkongsian maklumat dalam kalangan pengguna laman ini, termasuklah maklumat-maklumat peribadi. Dari segi takrifan, sehingga kini tidak ada satu definisi yang disepakati secara universal mengenai maksud intipan siber (Harvey, 2012). Secara literal, menurut Kamus Dewan Edisi Keempat, intipan bermaksud "usaha mengintip, mengintai atau mencari-cari rahsia". Mengikut Kamus Besar Bahasa Melayu Utusan (Zainal Abidin, 1995) pula, mengintip ertinya "menyamar, meninjau, mengawasi, menyiasat atau mencari rahsia".

Menurut Manitoba Justice Victim Services, secara asasnya intipan atau hendapan siber bermaksud perbuatan mengintip yang dilakukan melalui teknologi komunikasi atau alat komunikasi elektronik khususnya Internet (). Berbeza dengan intipan biasa, intipan siber (cyber stalking) merujuk kepada beberapa siri perbuatan dan tingkah laku secara atas talian yang dilakukan oleh seseorang terhadap orang lain yang menyebabkannya merasa takut dan bimbang. Intipan pada mulanya mungkin tidak menimbulkan sebarang gangguan sehinggakan mangsa tidak menyedarinya di peringkat awal. Walau bagaimanapun, apabila tindakan intipan tersebut semakin menjadi-jadi, ia akan menghasilkan ancaman dan meletakkan mangsa dalam ketakutan terhadap keselamatan diri (Ogilvie, 2010). Ia mungkin berlaku pada waktu yang sebenar di alam nyata dan kebiasaannya menyebabkan konfrontasi fizikal di antara pengintip

dan mangsa. Ia meliputi satu siri pengulangan tindakan mengganggu yang kerap, mengancam dan menakutkan penerimanya. Pengulangan gangguan terhadap privasi seseorang yang menyebabkan ketakutan oleh mangsa itulah yang dikatakan sebagai intipan. Justeru itu intipan akan menjadi intipan siber apabila ianya dilakukan bukan secara nyata tetapi secara atas talian. Mengikut Webster's New World Law Dictionary, intipan siber ditakrifkan sebagai:

i. "using the Internet through chat rooms and e-mail, to find, identify and arrange to meet a person whom one intends to criminally victimize"

ii. "Sending multiple e-mails, often on a systematic basis to annoy, embarrass, intimidate or threaten a person or to make the person fearful that she or a member of her family or household will be harmed"

Kebanyakan statut di seluruh dunia memperuntukkan intipan sebagai satu jenayah tetapi memberi definisi yang berbeza mengenai istilah tersebut (Ellison & Akdeniz, 1998). Walau apa pun definisi yang diberikan, secara umumnya perbuatan intipan siber ialah di mana pengganggu mengintip dan mengikuti semua aktiviti mangsa melalui atas talian dan membuat ancaman seperti ugutan untuk mencederakan atau intimidasi lisan (Paulett, Rota & Swan, 2009). Lebih membahayakan apabila selepas intipan dan ancaman di alam maya dilakukan, penyerang atau pelaku tersebut meneruskan dengan melakukan jenayah di alam yang sebenar.

Intipan siber mempunyai banyak persamaan dengan gangguan siber (cyber harassment). Berdasarkan kepada bentuk perbuatan dan medium yang digunakan oleh pengganggu terhadap mangsa, adakalanya kedua-dua istilah ini digunakan bersilih ganti. Walau bagaimanapun menurut Hakim David Harvey (2012), kedua-dua perbuatan ini adalah sebenarnya berbeza di mana gangguan siber boleh berlaku hanya sekali manakala intipan siber pula berlaku secara berterusan untuk suatu tempoh yang lebih lama, mungkin daripada beberapa minggu hingga beberapa tahun. Satu lagi perbezaan adalah dari aspek motif asal tindakan di mana gangguan siber dilakukan untuk mengganggu mangsa bagi tujuan suka-suka atau memaksa mangsa bertindak mengikut kehendaknya manakala intipan siber dilakukan untuk menakutkan atau mencederakan mangsa sama ada fizikal, emosi atau reputasi.

Menerusi laman web National Conference of State Legislatures, definisi kedua-dua istilah ini dibezakan dengan jelas di mana intipan siber merujuk kepada perbuatan ugutan atau sebarang perbuatan yang mempunyai niat jahat melibatkan penggunaan medium Internet, e-mel atau alat komunikasi elektronik manakala gangguan siber merujuk kepada penghantaran e-mel berbentuk gangguan semata-mata untuk menyeksa seseorang individu (mangsa).

Dalam jenayah intipan siber, apabila seseorang mengintip orang lain, dia sebenarnya sedang menyerang mangsa secara mental dan psikologi secara berterusan, tidak diingini dan menimbulkan gangguan dengan memecah masuk ke dalam kehidupan seharian mangsa. Walaupun tindakan-tindakan tersebut tidak menyebabkan kecederaan atau kesakitan fizikal terhadap mangsa, tetapi sekiranya ianya dilakukan sekali gus dalam tempoh yang berpanjangan, ia akan menyebabkan penderaan mental kepada mangsa.

Kebiasaannya intipan siber tidak membawa kepada keganasan fizikal selagi mana ia dilakukan di alam maya tetapi sekiranya pengintip mengambil keputusan untuk bertindak di

alam nyata maka kesannya mungkin boleh membawa kepada jenayah yang lebih kejam seperti membunuh. Menurut Bocij (2002), intipan siber meliputi penghantaran ugutan dan tuduhan palsu, kerosakan data, kecurian data dan identiti, memujuk kanak-kanak di bawah umur untuk tujuan seks dan sebarang bentuk keganasan atas talian.

Dalam intipan siber, tindakan mengintip adalah lebih terbuka kerana pengintip menggunakan Internet untuk mengugut mangsa. Ia merupakan komunikasi global menerusi Internet. Pengintip siber mengguna pakai papan buletin Internet atau ruang borak, dengan menghantar mesej yang bersifat kontroversi atau lucah di bawah nama, nombor telefon atau alamat e-mel mangsa. Pengguna-pengguna Internet yang lain akan tertipu untuk mengganggu atau mengugut mangsa berdasarkan maklumat palsu yang diberikan oleh pengintip siber. Setiap mesej atau maklumat palsu sama ada daripada pengintip siber atau pengguna lain, akan menghasilkan kesan yang diingini oleh pengintip siber ke atas mangsa. Ketiadaan hubungan langsung di antara pengintip siber dan mangsa boleh menyebabkan kesulitan kepada penguat kuasa undang-undang untuk mengenal pasti, menjejaki dan menangkap pengintip siber.

Perlakuan intipan siber boleh menjangkau ke dunia nyata. Daripada hanya mengintip, ia disusuli dengan panggilan telefon yang mengancam, kemusnahan harta benda, surat ugutan atau serangan fizikal. Melalui cara ini, pengintip siber juga mungkin akan menggunakan pihak ketiga sama ada saudara mara, rakannya atau orang asing untuk mengganggu mangsa melalui kaedah intipan secara perwakilan. Contoh yang biasa ialah apabila pengintip menipu mangsa di Internet, dengan memberikan mesej palsu bahawa mangsa berminat untuk mengadakan hubungan seks di mana pengguna-pengguna internet yang berminat akan menghubungi mangsa dengan mesej yang lucah. Lebih parah lagi, ia boleh melangkaui ke dunia nyata apabila mereka mula mengetuk pintu rumah mangsa.

Kesimpulannya, walaupun intipan siber boleh berlaku dalam pelbagai bentuk, ia memiliki satu ciri penting yang sama dengan intipan di alam nyata iaitu keinginan untuk mengawal mangsa dan melibatkan jenis tindakan yang sama untuk mencapainya.

## INTIPAN SIBER DI MALAYSIA

Kewujudan Cyber Security Malaysia yang ditubuhkan di bawah Kementerian Sains Teknologi dan Inovasi adalah antara lain bertujuan bagi mengawasi keselamatan atas talian pengguna di Malaysia, menangani dan mengendalikan kes-kes berkaitan siber. Ia bukanlah sebuah agensi penguatkuasaan, tetapi ia memberi perkhidmatan dan sokongan kepada pihak-pihak yang terlibat seperti badan penguatkuasaan dan juga mangsa jenayah siber (Cyber Security Malaysia, 2015). Contohnya penggunaan Forensic Digital bagi pemeriksaan dan analisis ke atas bahan storan digital yang terlibat dalam siasatan kes di mahkamah (Khairunnisa, 2010). Begitu juga dari aspek teknikal di mana Cyber Security berperanan memberikan bantuan terhadap pihak berkuasa tempatan dalam menjalankan analisis terhadap bahan bukti digital seperti komputer, telefon bimbit dan pemain digital mudah alih.

Walaupun pihak Cyber Security tidak mengumpul statistik jenayah siber, ia menyimpan maklumat dan statistik bagi kes-kes yang dirujuk kepada badan ini melalui perkhidmatan Pusat Bantuan Cyber999. Menurut laporan yang dimuatkan di dalam penerbitannya, e-Security, istilah yang digunakan ialah gangguan siber (harassment) yang juga merangkumi intipan siber.

Dari tahun 2005 hingga 2008, kes melibatkan gangguan siber sememangnya masih rendah berbanding dengan jenayah-jenayah lain seperti pencerobohan dan penipuan.

Jadual 1: Pecahan insiden kes yang dilaporkan ke Cyber Security 2005-2008

| Jenis ancaman | Tahun | | | |
|---|---|---|---|---|
| | 2005 | 2006 | 2007 | 2008 |
| Pencerobohan (*intrusion*) | 467 | 897 | 385 | 766 |
| Penipuan (*fraud*) | 149 | 287 | 364 | 907 |
| Penggodam (*hacker*) | 87 | 68 | 182 | 277 |
| Gangguan siber (*harassment*) | **43** | **51** | **31** | **72** |
| Lain-lain | 119 | 69 | 76 | 101 |
| Jumlah kes | **865** | **1372** | **1038** | **2123** |

Sumber: Mustapha, 2009

Jadual di atas yang dipetik daripada Mustapha (2009) menunjukkan berlaku penurunan kes pada tahun 2007 iaitu sebanyak 31 kes berbanding 51 pada tahun sebelumnya. Walau bagaimanapun, angka ini melonjak kepada 72 pada tahun 2008. Pada tahun 2009 pula (sehingga Oktober) terdapat 151 kes gangguan siber yang dilaporkan. Walau bagaimanapun, menurut laporan oleh MYCERT dalam buletin e-Security, berlaku peningkatan kes yang mendadak pada tahun 2010 dan 2011. Menurut laporan Cyber Security Malaysia (Jadual 2), walaupun laporan mengenai kes gangguan siber masih menduduki tempat di belakang kes pencerobohan dan penipuan, jumlah kes yang dilaporkan menunjukkan peningkatan yang sangat tinggi berbanding dengan tahun-tahun berikutnya. Jika trend ini didapati berlarutan untuk beberapa tahun lagi, maka gangguan siber berpotensi menjadi salah satu jenayah siber yang utama di masa hadapan.

Jadual 2: Jumlah Kes Gangguan Siber Suku Tahunan 2010-2011

| Laporan Suku Tahunan | Tahun | |
|---|---|---|
| | 2010 | 2011 |
| Pertama | 57 | 146 |
| Kedua | 62 | 128 |
| Ketiga | 129 | 80 |

Kebanyakan kes gangguan siber yang berlaku di Malaysia sebagaimana yang dilaporkan oleh Cyber Security Malaysia melibatkan gangguan yang dilakukan melalui laman blog atau forum di mana maklumat palsu atau salah dihantar ke blog dan laman forum organisasi atau individu tertentu. Pihak Cyber Security Malaysia, selepas menerima aduan daripada mangsa akan bertindak memaklumkan kepada penyedia perkhidmatan internet (ISP) yang berkenaan untuk penyingkiran maklumat tersebut. Lain-lain tindakan yang turut dianggap sebagai mengganggu adalah seperti ancaman, ugutan atau e-mel yang berbau fitnah dan pesanan ringkas (SMS) yang dihantar kepada mangsa dengan niat jahat. Meskipun Cyber Security Malaysia bertindak sebagai badan pemantau untuk mengesan ancaman yang mungkin berlaku di dunia siber, ia tidak dilengkapi dengan peruntukan undang-undang (Cybersecurity Malaysia, 2015). Sebarang

aduan yang dilaporkan akan diuruskan oleh Cyber Security Malaysia dengan kerjasama ISP dan agensi penguatkuasaan undang-undang yang lain. Pihak Cyber Security Malaysia hanya bertindak sebagai pihak ketiga di mana laporan yang dibuat kepadanya boleh digunakan bagi menyokong penyiasatan yang dilakukan oleh polis.

## UNDANG-UNDANG MENGENAI JENAYAH INTIPAN SIBER

Beberapa negara telah mewujudkan undang-undang khusus bagi menangani kes-kes berkaitan intipan siber. Kebanyakan daripada negara-negara membangun (di mana penggunaan teknologi maklumat dan komunikasi adalah sesuatu yang lumrah) telah mengisytiharkan undang-undang anti intipan bagi menyelesaikan isu-isu intipan siber sama ada yang berlaku secara langsung atau tidak langsung. Amerika Syarikat misalnya, di samping undang-undang di peringkat persekutuan, iaitu Interstate Anti-Stalking Punishment & Prevention Act 1996, juga mempunyai undang-undang intipan di kesemua 50 wilayahnya menjelang tahun 1999. Walau bagaimanapun, memandangkan akta ini merupakan satu-satunya undang-undang persekutuan mengenai anti intipan siber, setiap negeri perlu mentakrifkan perlakuan jenayah. Disebabkan undang-undang berbeza mengikut bidang kuasa masing-masing, maka pentakrifan juga berbeza. Kebanyakan negeri memasukkan perlakuan-perlakuan yang biasa digunakan oleh pengintip siber dalam undang-undang anti pengintipan mereka. Sesetengah negeri telah menyemak semula undang-undang untuk mengawal selia gangguan berasaskan komputer manakala yang lain mentakrifkan undang-undang anti intipan dengan cukup luas untuk menampung tindakan dalam talian dan luar talian (Miller, 2006). Violent Crime Control & Law Enforcement Act 1994 digubal bagi mewujudkan satu undang-undang yang standard bertujuan melindungi mangsa merentasi semua wilayahnya. Penggubalan ini dibuat kerana masalah yang dihadapi oleh pihak penguatkuasaan atau pendakwaan apabila melibatkan perbezaan wilayah antara pengintip siber dan mangsa (U.S Department of Justice, 2001).

Begitu juga di England di mana di bawah Human Rights Act 1998, Hak terhadap Diri dan Hak Privasi Diri dan Keluarga boleh digunakan selain daripada Protection Against Harassment Act 1997. Akta ini mempunyai peruntukan berkaitan kesalahan jenayah dan sivil dalam intipan siber dan merangkumi semua jenis komunikasi termasuk komunikasi melalui elektronik. Akta ini mempunyai kedua-dua peruntukan iaitu jenayah dan sivil berhubung tindakan dari pengintip siber.

Di Malaysia, undang-undang siber yang terdiri daripada Akta Jenayah Komputer 1997, Akta Tandatangan Digital 1997 dan Akta Teleperubatan 1997 digunakan bagi menangani isu-isu perundangan yang khusus terhadap jenayah siber di samping undang-undang yang berkaitan dengan dunia siber iaitu Akta Komunikasi dan Multimedia 1998.

Akta Jenayah Komputer Malaysia 1997 telah diluluskan di Parlimen pada bulan Mac 1997 dan dikuatkuasakan pada 30 Jun 2000. Tujuan utamanya adalah untuk mengadakan peraturan-peraturan berkaitan dengan penyalahgunaan komputer. Ianya berdasarkan Akta Penyalahgunaan Komputer United Kingdom 1990 dengan beberapa pengubahsuaian. Walau bagaimanapun sebahagian besar akta ini berkait dengan jenayah yang melibatkan akses atau capaian tanpa kuasa atau yang menyalahi undang-undang kepada data dalam komputer dan penyalahgunaannya (Zaiton, 2004). Jenayah-jenayah tertentu seperti phishing dan kecurian

identiti diperkatakan secara khusus di bawah seksyen 3(1) Akta tersebut. Walau bagaimanapun kesalahan-kesalahan di dalam Bahagian II akta ini tidak memperuntukkan sebarang peruntukan mengenai intipan siber. Dalam konteks ini, seksyen 3 (1) memperuntukkan:

Seseorang adalah melakukan suatu kesalahan jika;

i. dia menyebabkan suatu komputer melaksanakan apa-apa fungsi dengan niat untuk mendapat capaian kepada mana-mana atur cara atau data yang disimpan dalam mana-mana komputer;
ii. capaian yang dia berniat untuk didapati adalah tanpa kuasa; dan
iii. dia tahu semasa dia menyebabkan komputer itu melaksanakan fungsi itu, demikian berlakunya.

Akta Tandatangan Digital 1997 pula direka bentuk dan digubal untuk menyediakan keselamatan dan jaminan kepada mereka yang menggunakan transaksi secara elektronik. Ia menyediakan peraturan-peraturan mengenai perantara yang bertindak sebagai pihak berkuasa perakuan dan pengiktirafan tandatangan digital (Ding, 1999).

Sementara itu, Akta Teleperubatan 1997 digubal untuk memudahkan dan membolehkan pemakaian teleperubatan ke kawasan luar bandar. Dengan ini komunikasi audio, visual dan data digunakan sepenuhnya dalam amalan perubatan. Ia membolehkan pengamal perubatan menggunakan teknologi maklumat dan komunikasi dalam mengubati pesakit setelah mendapat persetujuan pesakit terlebih dahulu.

Akta Komunikasi dan Multimedia 1998 pula mengawal selia industri telekomunikasi yang sedia ada dan membolehkan penumpuan yang lancar dalam industri komunikasi dan multimedia. Ia adalah sebahagian daripada rangka kerja undang-undang dan mengawal selia infrastruktur undang-undang siber di Malaysia. Suruhanjaya Komunikasi dan Multimedia telah dibentuk untuk melaksanakan Akta ini yang berperanan untuk menyelia dan mengawal aktiviti-aktiviti komunikasi dan multimedia di Malaysia merangkumi aspek teknikal, ekonomi, kepenggunaan, sosial, penguatkuasaan dan pematuhan. Walau bagaimanapun, akta ini tidak membincangkan isu intipan siber secara khusus. Sebagai contoh, seksyen 211(1) menyentuh berkenaan larangan terhadap pemberian kandungan jelik seperti berikut:

> *Tiada pemberi perkhidmatan aplikasi kandungan, atau orang lain yang menggunakan perkhidmatan aplikasi kandungan, boleh memberikan kandungan yang sumbang, lucah, palsu, mengancam atau jelik sifatnya dengan niat untuk mengacau, mendera, mengugut atau mengganggu mana-mana orang.*

Hukuman bagi mereka yang melanggar peruntukan ini dengan memiliki kandungan yang tidak senonoh atau menyalahi undang-undang diperuntukkan di bawah seksyen yang sama iaitu denda maksimum tidak melebihi RM50,000 atau penjara tidak melebihi setahun atau kedua-duanya sekali jika disabitkan kesalahan. Peruntukan ini seharusnya dapat mencegah pengintip siber yang berniat untuk memanipulasi sebarang kandungan untuk tujuan mengganggu mangsanya, akan tetapi dari sudut realitinya memerlukan pembuktian terlebih dahulu.

Selain itu, seksyen 233 akta yang sama melarang penggunaan tidak wajar kemudahan rangkaian atau perkhidmatan rangkaian dan sebagainya. Subseksyen 2 memperuntukkan bahawa adalah satu kesalahan bagi seseorang yang secara sedar membuat sebarang komunikasi lucah bagi maksud komersial kepada orang lain atau membenarkan perkhidmatan rangkaian atau aplikasi di bawah kawalan orang itu untuk digunakan bagi tujuan yang disebut di atas. Hukuman yang diperuntukkan adalah sama sebagaimana yang diperuntukkan dalam seksyen 211(2) akta yang sama.

Selain daripada peruntukan-peruntukan di atas, oleh kerana sifat intipan siber merupakan suatu tindakan jenayah, maka undang-undang yang mungkin boleh dirujuk ialah Kanun Keseksaan. Perlu disebut di sini bahawa tidak seperti Amerika Syarikat dan Australia, Malaysia masih tidak mempunyai undang-undang anti intipan yang khusus dalam undang-undang keseksaan. Walaupun begitu, pengganggu atau pengintip boleh didakwa di bawah seksyen 503 Kanun Keseksaan Malaysia atas kesalahan melakukan jenayah intimidasi (ugutan atau ancaman) atau di bawah seksyen 507 kanun tersebut di mana jenayah intimidasi dilakukan melalui komunikasi tanpa nama. Seksyen 503 memperuntukkan:

> *Sesiapa sahaja yang mengugut seseorang dengan apa jua kecederaan terhadap tubuh, nama baik atau harta, atau tubuh atau nama baik sesiapa sahaja orang yang kena ugut itu mempunyai kepentingan, dengan niat mengakibatkan kecemasan terhadap seseorang yang diugut, atau menyebabkan orang itu melakukan apa jua perbuatan yang ia tidak terikat di sisi undang-undang untuk melakukannya, atau menyebabkan orang tersebut meninggalkan daripada melakukan apa jua perbuatan yang ia berhak di sisi undang-undang melakukannya sebagai cara untuk mengelakkan pelaksanaan ugutan tersebut, dikatakan telah melakukan intimidasi jenayah.*

Di bawah peruntukan tersebut, syarat utama yang perlu dibuktikan ialah ancaman yang menyebabkan ketakutan kepada mangsa sama ada terhadap badan, harta atau maruah dan ia juga termasuk ancaman yang dilakukan melalui atas talian. Walau bagaimanapun, agar sukar untuk membuktikan bahawa ancaman atas talian boleh menyebabkan ketakutan kepada mangsa menyamai dengan keadaan seseorang yang melakukan konfrontasi secara fizikal. Justeru, ia bergantung kepada fakta dalam setiap kes. Sekiranya jenayah ugutan atau ancaman dilakukan tanpa nama, penjenayah boleh didakwa di bawah seksyen 507 kanun tersebut di mana hukuman bagi perbuatan tersebut (di bawah seksyen 506) ialah penjara sehingga 2 tahun dengan denda, atau sekiranya ia menyebabkan kesakitan atau kerosakan harta benda mangsa, membuat tuduhan tentang kesucian wanita, tempoh penjara dinaikkan hingga 7 tahun dengan denda.

Secara ringkasnya dapat disimpulkan bahawa undang-undang sedia ada dan rangka kerja perundangan tidak mempunyai peruntukan khusus untuk menyelesaikan isu intipan siber. Hakikatnya, sekiranya undang-undang perlu dirujuk untuk memerangi jenayah, rujukan perlu dibuat kepada peruntukan Kanun Keseksaan untuk mencari hukuman yang berkaitan. Walaupun undang-undang tradisional telah disemak semula atau dipinda untuk memanjangkan pemakaiannya termasuk perlakuan jenayah siber dan persekitaran atas talian, Malaysia masih memerlukan masa untuk menyelesaikan jenayah siber secara efektif berbanding dengan negara-negara seperti Australia dan United Kingdom. Jika dibandingkan dengan negara-negara maju

lain, di samping kewujudan akta berkaitan intipan, penggubalan akta lain khususnya mengenai intipan siber menunjukkan wujud keperluan untuk mengadakan dua akta yang berbeza disebabkan oleh sifat perlakuan dan medium pelaksanaan kesalahan yang berbeza.

## KESIMPULAN

Malaysia sememangnya berbangga jika rakyatnya celik IT tetapi pada masa yang sama mereka juga perlu menjadi celik keselamatan berkaitan IT. Teknologi akan terus berkembang dan penjenayah akan sentiasa mencari cara baru untuk melakukan jenayah dengan bantuan teknologi tersebut. Kadang-kadang jenayah yang berlaku disebabkan oleh tindakan individu itu sendiri. Pengguna Facebook dapat mengelakkan diri daripada menjadi mangsa intipan siber dalam kalangan rakan siber mereka sekiranya mereka bijak dalam menggunakan laman rangkaian sosial ini. Antara tindakan yang boleh diambil oleh mereka ialah mengelakkan daripada menggunakan identiti asal semasa mendaftar diri di Facebook kerana pendedahan identiti sebenar boleh menyebabkan mereka mudah dikenali oleh pengintip siber, tidak meletakkan gambar sendiri atau maklumat lengkap diri, mengelakkan pertemuan secara bersemuka dengan rakan siber yang baru dikenali, menggunakan laman sosial untuk tujuan yang bermanfaat sahaja dan memilih rakan sosial dengan mengawal lingkungan rakan siber yang dikehendaki. Sesungguhnya penggunaan secara bijak oleh pengguna laman sosial mampu menjadi pendinding kepada kejadian jenayah intipan siber. Adalah diharapkan agar kejadian jenayah yang berlaku di negara-negara luar tidak berlaku di Malaysia akibat kealpaan sendiri. Jenayah intipan siber sebenarnya dapat dielakkan.

Lantaran kesan negatif daripada penggunaan laman sosial ini, para ibu bapa perlu memperlengkapkan diri mereka dengan ilmu yang secukupnya supaya anak-anak mereka tidak menjadi mangsa kecanggihan teknologi masa kini. Ibu bapa boleh memainkan peranan bagi mengekang penyalahgunaan laman sosial oleh anak-anak mereka dengan cara melakukan pemantauan ke atas anak-anak. Kekurangan pemantauan oleh ibu bapa ke atas anak-anak akan mengundang masalah yang tidak dijangkakan di kemudian hari seperti lari dari rumah dengan mengikut teman sosial dan sebagainya. Dalam konteks penggunaan laman web sosial di kalangan remaja kini, ibu bapa boleh memainkan peranan yang berkesan dalam mengelakkan mereka daripada menjadi mangsa jenayah baru ini. Ibu bapa disarankan supaya menjadi rakan di Facebook anak-anak mereka. Secara tidak langsung, mereka akan mengetahui sejauh mana anak-anak mereka melibatkan diri dalam hubungan di alam maya ini. Selain itu, mereka juga boleh mengetahui siapakah rakan-rakan anak-anak mereka. Walaupun begitu, ia agak sukar dilaksanakan sekiranya anak-anak menggunakan nama lain selain dari nama sebenar dan mereka tidak menginginkan ibu bapa menjadi rakan siber mereka.

Peranan dan keperluan undang-undang dalam menangani perbuatan jenayah tidak dapat diketepikan. Penelitian terhadap peruntukan dalam undang-undang siber menunjukkan bahawa Malaysia tidak mempunyai undang-undang menangani jenayah siber khususnya intipan siber. Buat masa ini, Malaysia cuba memanfaatkan peruntukan-peruntukan yang berselerakan dalam pelbagai akta yang secara tidak langsung juga meliputi jenayah siber. Memandangkan sifat dunia maya yang menjadikan beban pembuktian elemen jenayah dari sudut niat (mens rea) dan perlakuan jenayah (actus reus) seorang penjenayah, adalah dirasakan perlu digubal satu

undang-undang yang khusus untuk mengawal setiap kategori jenayah siber yang dilakukan terhadap orang ramai, sama ada terhadap diri manusia, harta atau untuk keselamatan orang ramai. Ini adalah kerana undang-undang tradisional digubal bagi menangani kes-kes jenayah yang dilakukan secara nyata. Oleh itu, kemungkinan terdapat peruntukan-peruntukan di dalam Kanun Keseksaan yang tidak terpakai kepada ke-kes yang melibatkan atas talian. Hakikatnya ialah kita memerlukan satu mekanisme untuk membendung peningkatan jenayah siber melalui infrastruktur undang-undang yang sesuai dengan sifat jenayah siber itu sendiri. Adalah penting untuk kita memastikan bahawa undang-undang yang digubal mencukupi untuk menyelesaikan isu-isu intipan siber. Undang-undang khusus ini penting bagi memastikan penjenayah siber dapat didakwa dengan sempurna dan proses pembuktian jenayah yang dilakukan di alam maya dapat dijalankan dengan baik dengan hukuman yang setimpal. Tidak dinafikan bahawa undang-undang akan sentiasa dicabar untuk menangani jenis jenayah baru yang dicipta oleh alam maya. Justeru, undang-undang perlu diperbaharui bagi memenuhi keperluan keunikan dunia siber. Adalah diharapkan dengan gabungan pelbagai faktor seperti kesedaran keselamatan IT di pihak remaja, pemantauan di pihak ibu bapa, kewujudan undang-undang khusus berkaitan jenayah siber serta agensi-agensi penguatkuasaan, kejadian intipan siber dapat ditangani dengan lebih berkesan.

## RUJUKAN

(22 Februari 2012).

(25 Februari 2012).

(26 Februari 2012).

"Cyberstalking legal definition." Webster's New World Law Dictionary.

"Cyberstalking: A new challenge for law enforcement and industry: A report from the attorney agensi teknikal keselamatan siber bantu organisasi penguat kuasa undang-undang di Malaysia, h.1-3 http://www.cybersecurity.my/data/content_files/44/1493.pdf?.diff=1422844505 (27 Julai 2015).

April 2014. http://www.ebizmba.com/articles/social-networking-websites (27 Julai 2015).

Bocij, P. (2002). "Corporate cyberstalking: An invitation to build theory." dalam First Monday. Jilid 7 Bil 11. http://firstmonday.org/ojs/index.php/fm/article/view/1002/923 (27 Julai 2015).

Crimes Act 1997". dalam UiTM Law Review. Jilid 2, h 210-234.

Cyber Security Malaysia. (2015). Selasa 2 Jun. Siaran akhbar: Cybersecurity Malaysia sebuah

dictionary.com/cyberstalking (22 Februari 2012).

Ding, J. (1999). E-Commerce: Law & Practice. Malaysia: Sweet & Maxwell Asia.

eBizMBA Guide. (2014). Top 15 most popular social networking sites

Ellison, L & Akdeniz, Y. (1998). "Cyber-Stalking: The regulation of harassment on the general to the vice president." New York: US Department of Justice.

Harvey, D. (2012). "Cyberstalking and Internet harassment: What the law can do."

http://www.netsafe.org.nz/Doc_Library/netsafepapers_davidharvey_cyberstalking.pdf

http://drcoop.pbworks.com/f/Social%20Networking%20Web%20Sites.pdf

Internet. www.cybersecurity.my/data/content_files/13/615.pdf (22 Februari 2012).

Internet." dalam Criminal Law Review. December Special Edition: Crime, Criminal Justice and the Internet. h. 29-48.
Jerat Internet (2009). Khamis 26 November. Harian Metro, www.cybersecurity.my/en/knowledge_bank/news/2009/main/detail/1810/index.html Journal of Technology & Society. Summer 2007. h. 15-31.
jurisdictions". dalam Trends & Issues in Crime & Criminal Justice. No 76, h. 1-6. Justice.https://www.ncjrs.gov/pdffiles1/ojp/186157.pdf (22 Februari 2012).
Kamus Dewan Edisi Keempat. (2007). Kuala Lumpur: Dewan Bahasa dan Pustaka.
Khairunnisa Sulaiman. (2010). Khamis 7 Januari. Kaedah canggih kesan jenayah. Utusan Law Enforcement Technology. Jilid 33 Bil 4, h. 1-6.
Manitoba Justice Victim Services. "Stalking is a crime".
Megat Ishak. (2010). The impact of social networking. h. 50-54. http://woulibrary.wou.edu.my/weko/eed502/The_Impact_of_Social_Networking.pdf (27 Julai 2015).
Miller, C. (2006). Cyber stalking & bullying – What law enforcement needs to know. dalam
Ogilvie, E. (2010). "Stalking: Policing & prosecuting practices in three Australian
Online,http://ww1.utusan.com.my/utusan/info.asp?y=2010&dt=0107&pub=utusan_malaysia&sec=Sains_% 26_Teknologi&pg=st_01.htm&arc=hive (27 Julai 2015).
Paulett, K.L., Rota, D.R. and Swan, T.T. (2009). Cyberstalking: An exploratory study of Publication & Distributors Sdn. Bhd.
rights.org/documents/cyberstalkingreport.htm (26 Februari 2012).
Rosen, C. (2007). "Virtual Friendship and New Narcissism." dalam The New Atlantis: A
Social Networking Watch. (2010). "Malaysia the Most SN Active Country." http://www.socialnetworkingwatch.com/2010/04/malaysia-the-most-sn-active-country.htm (22 Februari 2012).
Social Networking Web Sites. (2006).
Stalking and domestic violence report to Congress. (2001). New York: U.S Department of students at a Mid-Atlantic University. dalam Issues in Information Systems. Jilid X No 2, h. 640-649.
Syahrir Mat Ali & Fatin Hasnan. (2012). Kesan aplikasi rangkaian sosial terhadap pengguna www.gov.mb.ca/justice/domestic/pdf/stalkingweb.pdf (26 Februari 2012).
Zainal Abidin Safarwan (1995). Kamus Besar Bahasa Melayu Utusan. Kuala Lumpur: Utusan
Zaiton Hamim. (2004). "The legal response to computer misuse in Malaysia: The Computer