ISU DAN CABARAN DALAM USAHA MENGHADAPI JENAYAH SIBER DI MALAYSIA
(*Issues and Challenges in Addressing Cybercrime in Malaysia*)

Mahyuddin Daud
mahyuddin@iium.edu.my

Kulliyyah Undang-undang Ahmad Ibrahim, Universiti Islam Antarabangsa Malaysia, 50728 Kuala Lumpur, Malaysia.

Rujukan makalah ini (*To cite this article*): Mahyuddin Daud. (2025). Isu dan cabaran dalam usaha menghadapi jenayah siber di Malaysia. *Kanun*: *Jurnal Undang-undang Malaysia, 37*(1), 1–28. https://doi.org/10.37052/kanun.37(1)no1

Peroleh: *Received*:	21/2//2024	Semakan: *Revised*	27/11/2024	Terima: *Accepted*:	9/12/2024	Terbit dalam talian: *Published online*	28/1/2025

Abstrak

Keadaan jenayah siber di Malaysia makin membimbangkan dengan pelbagai kes yang melibatkan penggodaman, penipuan dalam talian, serangan perisian hasad dan kebocoran data. Walaupun terdapat lebih daripada 30 undang-undang yang berkaitan dengan aktiviti siber, pelaksanaan undang-undang ini masih kurang berkesan untuk menangani ancaman yang makin kompleks. Dalam kajian ini, analisis data dilakukan secara kualitatif. Oleh itu, pengkaji menganalisis isu dan cabaran untuk mengatasi jenayah siber di Malaysia. Antara cabaran utama yang ditemukan termasuklah perubahan pesat teknologi, definisi jenayah siber yang terus berkembang, isu bidang kuasa dalam siasatan rentas sempadan dan kekurangan keterangan digital. Di samping itu, kesukaran untuk mengenal pasti lokasi sebenar penjenayah siber dan masalah pemeliharaan data digital turut menjadi penghalang utama bagi siasatan dan pendakwaan yang berkesan. Menerusi kajian ini, pengkaji mencadangkan penambahbaikan terhadap undang-undang siber sedia ada, termasuklah pindaan Akta Komunikasi dan Multimedia 1998, Akta Jenayah Komputer 1997 dan Akta Perlindungan Data Peribadi 2010 untuk memperkukuh penguatkuasaan dan penyiasatan jenayah siber. Dengan adanya pendekatan yang lebih dinamik, undang-undang ini menjadi lebih responsif ke arah mengurangkan risiko terhadap ancaman siber yang berkembang pesat.

e-ISSN: 2682-8057

Kata kunci: Jenayah siber, definisi jenayah siber, penyiasatan rentas sempadan, forensik digital, rangka kerja undang-undang, keselamatan digital

Abstract

Cybercrime in Malaysia has become increasingly alarming, with various cases involving hacking, online fraud, malware attacks, and data breaches. Although there are more than 30 laws related to cyber activities, the enforcement of these laws remains ineffective in addressing increasingly complex threats. This study employs qualitative data analysis to examine the issues and challenges in combating cybercrime in Malaysia. Key challenges identified include the rapid advancement of technology, the evolving definition of cybercrime, jurisdictional challenges in cross-border investigations, and inadequate digital evidence. Additionally, difficulties in pinpointing the exact location of cybercriminals and issues related to the preservation of digital data pose significant obstacles to effective investigation and prosecution. This study proposes improvements to existing cyber laws, including amendments to the Communications and Multimedia Act 1998, the Computer Crimes Act 1997, and the Personal Data Protection Act 2010, to enhance the enforcement and investigation of cybercrimes. With more dynamic approaches, these laws can become more responsive in reducing the risks posed by the rapidly evolving cyber threats.

Keywords: *Cybercrime, cybercrime definition, cross-border investigation, digital forensics, legal framework, digital security*

PENDAHULUAN

Pertubuhan Polis Jenayah Antarabangsa (Interpol) mendefinisikan jenayah siber sebagai kesalahan yang dilakukan terhadap data komputer, media penyimpanan data komputer, sistem komputer dan penyedia perkhidmatan. Konsep ini biasanya merangkumi kategori kesalahan, seperti capaian haram, gangguan terhadap sistem data dan komputer, penipuan dan pemalsuan, pemintasan data secara haram, peranti haram, eksploitasi kanak-kanak dan pelanggaran harta intelek (Interpol, 2021).

Terdapat dua jenis jenayah siber yang mesti diketahui perbezaannya. Pertama, jenayah yang bergantung pada siber (juga dikenali sebagai jenayah siber tulen). Kedua, jenayah yang dibolehkan siber. Pejabat dalam Negeri United Kingdom (UK) menjelaskan bahawa jenayah

yang bergantung pada siber ialah kesalahan yang hanya dapat dilakukan menggunakan komputer, rangkaian komputer, atau lain-lain bentuk teknologi maklumat dan komunikasi (TMK). Contohnya, penyebaran virus atau perisian hasad, penggodaman dan serangan penafian perkhidmatan teragih (DDoS). Jenayah ini ditujukan terutamanya kepada komputer atau sumber rangkaian, seperti data yang dikumpulkan, dengan menggodam akaun e-mel yang digunakan untuk melakukan penipuan (Home Office UK Government, 2013).

Sebaliknya, jenayah yang dibolehkan siber ialah jenayah tradisional yang dapat dilakukan secara lebih meluas atau ditingkatkan dengan menggunakan komputer dan internet. Tidak seperti jenayah yang bergantung pada siber, jenayah yang dibolehkan siber dapat dilakukan tanpa penggunaan komputer, seperti penipuan dan kecurian. E-mel penipuan yang dihantar untuk menipu penerima supaya memindahkan wang kepada orang yang tidak dikenali termasuk dalam jenis jenayah siber ini.

Pada era digital ini, pengautomasian dan penyampaian perkhidmatan dalam talian menjadi pemangkin perkhidmatan yang lebih cepat, stabil dan mudah. Di balik kemudahan tersebut, cabaran dalam bentuk ancaman dan serangan siber juga makin canggih. Antara ancaman ini termasuklah ancaman berterusan lanjutan (*advanced persistent threats*), penggodaman sistem kritikal dan serangan penafian perkhidmatan (*denial of service attacks*). Hal ini menyebabkan kerugian yang besar, serta pelanggaran hak data individu dan syarikat. Pandemik COVID-19 dan perintah kawalan pergerakan tidak menghalang penjenayah siber daripada menjalankan aktiviti jenayah siber terhadap pengguna di 10 negara yang menyasarkan hampir 330 juta orang (Norton, 2021). Firma keselamatan siber Norton Life Lock menyatakan bahawa lebih daripada 27 juta orang dewasa India mengalami kecurian identiti pada tahun 2021.

Pada tahun 2016, tujuh penggodam Iran melancarkan serangan siber yang diselaraskan kepada berpuluh-puluh bank Amerika Syarikat (AS) sehingga mengakibatkan kehilangan berjuta-juta dolar dalam sektor perniagaan. Kerajaan AS menuduh individu berkenaan dengan tuduhan cuba mengganggu infrastruktur kritikal, seperti cubaan menutup empangan New York (Dustin Volz, 2016). Singapura juga mengalami serangan siber terburuk pada tahun 2018 apabila pangkalan data SingHealth yang merupakan kumpulan terbesar institusi penjagaan digodam. Maklumat peribadi 1.5 juta pesakit terjejas, termasuklah preskripsi ubat, Perdana Menteri, Lee Hsien Loong dan beberapa menteri telah dibocorkan (Irene

Tham et al., 2018). Malaysia berada pada kedudukan ke-17 dalam senarai negara yang berisiko tinggi untuk terdedah pada serangan siber melalui internet. Di samping itu, CyberSecurity Malaysia melaporkan kerugian lebih kurang RM2.75 bilion dalam tempoh lima tahun lalu yang melibatkan jenayah siber terhadap sektor kewangan di Malaysia. (Prasad Jayabalan et al., 2014).

Ancaman keselamatan siber di Malaysia makin meningkat dari segi tahap kekerapan dan keseriusan. Pada tahun 2022, negara mengalami serangan siber yang serius, termasuklah serangan perisian hasad, percubaan pengintipan siber, kebocoran data dan penipuan siber. CyberSecurity Malaysia melaporkan bahawa terdapat 4,741 kes ancaman siber pada tahun 2022, manakala 456 kes penipuan direkodkan setakat Februari 2023. Polis Diraja Malaysia (PDRM) melaporkan bahawa sebanyak 68 peratus daripada 71,833 kes penipuan yang dilaporkan antara tahun 2020 hingga 2022 ialah penipuan dalam talian (Maleen Balqish Salleh, 2023).

Malaysia dan negara ASEAN yang berjiran mengalami peningkatan ancaman siber yang amat ketara pada tahun 2023. Kebanyakan kes jenayah siber melibatkan kebocoran data dalam pelbagai sektor. Peningkatan ini disebabkan oleh pelbagai faktor, seperti kecanggihan penjenayah siber yang makin meningkat dari segi taktik, teknik dan prosedur. Bentuk serangan siber baharu, seperti *Malware as a Service* atau Perisian Hasad sebagai Perkhidmatan (MaaS) dan *Ransomware* sebagai Perkhidmatan (RaaS) telah muncul. Serangan licik terhadap syarikat besar kelihatan berjaya walaupun syarikat tersebut dilengkapi infrastruktur keselamatan siber yang mantap. Modus operandi jenayah siber yang dijalankan di forum web tertutup (*darkweb*) turut diperhebat melalui saluran media sosial, seperti Telegram. Terdapat perubahan ketara dalam fokus serangan *ransomware* sejak belakangan ini. Sebelum ini, penyerang menyasarkan sektor biasa, seperti kewangan dan penjagaan kesihatan. Kini, penyerang beralih kepada industri, seperti pendidikan, automotif dan logistik. Sektor ini mengalami serangan ransomware berskala besar yang menyebabkan kerosakan yang ketara dan datang dengan permintaan tebusan yang lebih besar (CyberSecurity Malaysia, 2023).

Kedinamikan ancaman dan serangan siber menuntut setiap pihak berkepentingan untuk melaksanakan langkah yang lebih proaktif dan berkesan bagi melindungi ruang siber. Banyak faktor mesti dipertimbangkan, termasuklah keselamatan sistem berasaskan siber, keselamatan rangkaian, keselamatan maklumat, pemulihan bencana

dan kesedaran keselamatan pengguna akhir. Oleh itu, pihak berwajib dan pihak berkepentingan perlu segera melaksanakan usaha melindungi teknologi, data dan rangkaian masing-masing dari pelbagai ancaman dalam operasi harian.

KAJIAN LEPAS

Jenayah siber suatu bentuk perlakuan jenayah yang menyasarkan data komputer, sistem komputer dan penyedia perkhidmatan. Kesalahan ini merangkumi capaian haram, gangguan sistem, penipuan, pemalsuan, eksploitasi kanak-kanak dan pelanggaran harta intelek (Interpol, 2021). Home Office UK pula membahagikan jenayah siber kepada dua kategori utama. Pertama, jenayah bergantung pada siber dan jenayah dibolehkan siber. Jenayah bergantung pada siber melibatkan serangan yang hanya dapat berlaku menggunakan teknologi maklumat, seperti penggodaman dan serangan penafian perkhidmatan teragih (DDoS), manakala jenayah dibolehkan siber, termasuklah penipuan dan kecurian, diperkukuh dengan penggunaan teknologi (Home Office UK Government, 2013).

Malaysia menyaksikan peningkatan ketara ancaman keselamatan siber sejak beberapa tahun belakangan ini. Pada tahun 2022, CyberSecurity Malaysia melaporkan lebih 4,741 kes ancaman siber, termasuklah serangan perisian hasad dan kebocoran data, sementara 456 kes penipuan siber direkodkan pada awal tahun 2023 (CyberSecurity Malaysia, 2023). Penipuan dalam talian menjadi ancaman utama apabila 68% daripada 71,833 kes penipuan yang dilaporkan antara tahun 2020 hingga 2022 diklasifikasikan sebagai penipuan dalam talian (Maleen Balqish Salleh, 2023).

Walaupun terdapat lebih 30 undang-undang yang berkaitan dengan aktiviti siber, hanya beberapa undang-undang khusus yang menangani jenayah siber, termasuklah Akta Jenayah Komputer 1997 dan Akta Komunikasi dan Multimedia 1998 (Janaletchumi Appudurai & Chitra L. Ramalingam, 2007; Donna, 1998; Duryana Mohamed, 2012). Akta Komunikasi dan Multimedia 1998 mengawal selia industri komunikasi dan multimedia, termasuklah rangka kerja pelesenan dan kawal selia kandungan, tetapi tidak mengawal selia jenayah siber secara langsung. Walaupun memerlukan pemegang lesen untuk memastikan keselamatan rangkaian, akta ini tidak memperuntukkan rangka kerja yang komprehensif bagi menangani jenayah siber (Mahyuddin Daud & Ida Madieha Abd Ghani Azmi, 2021; Mahyuddin Daud, 2021). Walaupun menggalakkan kawal selia kendiri internet, Akta Komunikasi dan Multimedia 1998

didapati tidak lagi mencukupi dan memerlukan kawal selia bersama yang membabitkan pelibatan semua pihak (Mahyuddin Daud & Ida Madieha Abd Ghani Azmi, 2021; Mahyuddin Daud, 2021). Akta Jenayah Komputer 1997 pula digubal untuk menangani penyalahgunaan komputer dan dilihat sebagai perundangan utama untuk memerangi jenayah siber.

Terdapat keperluan untuk meminda akta ini agar selaras dengan perubahan teknologi dan ancaman siber yang makin kompleks (Donna, 1998; Duryana Mohamed, 2012, 2013). Walaupun Seksyen 114A Akta Keterangan 1950 cuba menangani isu ini dengan cara meletakkan beban pembuktian kepada defendan jika nama atau identifikasinya dikaitkan dengan sesuatu penerbitan di internet, perkara ini perlu diperhalusi dengan kewujudan akaun palsu yang makin membimbangkan (Nazli Ismail Nawang, 2017).

METODOLOGI

Kajian ini dijalankan secara kualitatif yang menumpukan kajian literatur dan analisis undang-undang terhadap sumber perundangan primer dan sekunder. Sebagai contoh, Akta Komunikasi dan Multimedia 1998 dan Akta Jenayah Komputer 1997. Antara perundangan sekunder, termasuklah rujukan terhadap buku dan artikel ilmiah yang berkaitan. Perundangan semasa yang berkaitan dianalisis untuk mengenal pasti isu dan cabaran yang wujud dalam aspek pemakaian dan penguatkuasaan. Di samping itu, pengkaji turut menjalankan sesi temu bual dengan beberapa agensi kerajaan dan badan berkanun yang relevan yang melaksanakan fungsi yang berkaitan dengan penyiasatan dan penguatkuasaan jenayah siber di Malaysia. Antara agensi tersebut termasuklah Agensi Keselamatan Siber Negara (NACSA), Majlis Keselamatan Negara, Polis Diraja Malaysia (PDRM) dan Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM). Hal ini dilakukan supaya isu dan cabaran yang dilaporkan dalam kajian ini datang daripada sumber yang sahih dan terkini. Perkara ini dibincangkan secara lebih lanjut dalam bahagian selanjutnya. Sungguhpun begitu, oleh sebab isu yang diperhalusi melibatkan isu keselamatan negara dan jenayah siber yang amat sensitif terhadap kedaulatan negara, pengkaji tidak menyatakan pandangan agensi berkenaan sesuatu isu secara khusus atas permintaan agensi tersebut dan untuk menghormati etika kajian. Segala dapatan dan pandangan daripada mana-mana agensi hanya dinyatakan secara umum bagi menyokong kajian dan berkongsi ilmu dan manfaat.

DAPATAN DAN PERBINCANGAN

Dengan berdasarkan kajian yang dilakukan, pengkaji membincangkan dapatan kajian dalam dua aspek utama. Bahagian pertama membincangkan kerangka undang-undang yang mengawal selia jenayah siber di Malaysia. Bahagian kedua kertas kerja ini menganalisa isu dan cabaran untuk memerangi jenayah siber, termasuklah isu berkaitan takrifan, bidang kuasa, dan cabaran dalam penyiasatan dan pendakwaan.

Kerangka Undang-undang yang Mengawal Selia Jenayah Siber di Malaysia

Malaysia mempunyai lebih 30 undang-undang yang berkaitan dengan aktiviti siber. Walau bagaimanapun, hanya beberapa undang-undang yang menangani jenayah siber secara khusus dan diwujudkan sebelum tahun 2000. Bahagian ini menganalisis undang-undang Malaysia yang berkaitan yang membentuk rangka kerja undang-undang untuk memerangi jenayah siber. Selain itu, bahagian ini turut meneliti isu perundangan yang menjadi cabaran bagi pengawalseliaan dan penguatkuasaan jenayah siber yang khusus bagi peruntukan tersebut. Bahagian ini juga melaporkan sebahagian hasil temu bual dengan agensi berkepentingan yang berkaitan dengan penyiasatan dan penguatkuasaan jenayah siber.

Akta Komunikasi dan Multimedia 1998

Akta Komunikasi dan Multimedia 1998 mengawal selia industri komunikasi dan multimedia dan berkuatkuasa pada 1 April 1999. Akta Komunikasi dan Multimedia 1998 mewujudkan rangka kerja pelesenan dan kawal selia, menentukan kuasa dan fungsi SKMM, dan menubuhkan kuasa dan prosedur bagi pentadbiran akta tersebut. Malangnya, pandemik COVID-19 menyebabkan lonjakan penyebaran maklumat yang salah dan mengelirukan di internet. Akibatnya, mangsa mengalami gangguan emosi, seperti kebimbangan, keraguan dan kekurangan keyakinan. Hal ini membuktikan bahawa pengawalseliaan kendiri (*self-regulation*) tidak mencukupi, sebaliknya internet memerlukan kawal selia bersama yang membabitkan pelibatan semua pihak (*co-regulation*) (Mahyuddin Daud & Ida Madieha Abd Ghani Azmi, 2021; Mahyuddin Daud, 2021).

Bagi jenayah siber, Akta Komunikasi dan Multimedia 1998 tidak mempunyai sebarang peruntukan berkenaan rangka kerjanya. Seksyen 3

dan 263 meletakkan tanggungjawab kepada pemegang lesen SKMM untuk mengambil langkah yang perlu bagi memastikan keselamatan rangkaian dan membantu penguatkuasaan undang-undang. Dengan berdasarkan Perintah Fungsi-fungsi Menteri 2023, MCMC bukan agensi yang bertanggungjawab dalam hal jenayah siber dan keselamatan siber (Malaysian Communications and Multimedia Commission, 2020). Walaupun mempunyai talian penting (hotline) untuk melaporkan sebarang pelanggaran undang-undang siber, MCMC merujuk sebarang perkara yang berkaitan dengan keselamatan siber dan jenayah siber kepada Agensi Keselamatan Siber Negara, Polis Diraja Malaysia atau Cybersecurity Malaysia berdasarkan keperluan. Hal ini sering disalah erti oleh masyarakat yang beranggapan bahawa MCMC ialah agensi tunggal yang bertanggungjawab terhadap apa-apa perkara yang berkaitan dengan internet. Apabila perkara ini diperjelaskan, masyarakat perlu memahami bahawa tugas MCMC tertakluk pada peruntukan dalam Akta Komunikasi dan Multimedia 1998 yang secara amnya terhad untuk beberapa skop yang melibatkan kawal selia pemegang lesen MCMC. Dari aspek peningkatan kadar jenayah siber, akta ini tidak mengawal selia jenayah siber secara langsung kerana tertakluk di bawah skop akta yang berbeza, iaitu Akta Jenayah Komputer 1997.

Akta Jenayah Komputer 1997

Akta Jenayah Komputer 1997 digubal bagi memperuntukkan kesalahan yang berkaitan dengan penyalahgunaan komputer, khususnya yang berkaitan dengan jenayah siber dan jenayah yang dibolehkan siber. Sebahagian besar daripada Akta Jenayah Komputer 1997 dimodelkan daripada Computer Misuse Act 1990. Walaupun undang-undang UK dipinda beberapa kali, terutamanya untuk memperkenalkan kesalahan baharu pada tahun 2007 dan 2015, Akta Jenayah Komputer 1997 tidak pernah disemak atau dipinda. Dalam era serangan siber yang makin meningkat dan mengganas, sudah tiba masanya untuk mempertimbangkan pindaan Akta Jenayah Komputer 1997. Walaupun merupakan perundangan khusus bagi jenayah siber di Malaysia, Akta Jenayah Komputer 1997 tidak mentakrifkan terma jenayah siber secara khusus.

Jika dibandingkan dengan undang-undang United Kingdom (UK), Seksyen 3A Akta Penyalahgunaan Komputer UK 1990 melarang sebarang tindakan membuat, membekal atau mendapatkan bahan untuk digunakan dalam kesalahan penyalahgunaan komputer. Bahagian ini

menyasarkan penciptaan, pembekalan dan penggunaan alat penggodaman, seperti perisian penggodaman. Pembaharuan ini menjadikan undang-undang UK lebih selaras dengan Konvensyen Budapest mengenai Jenayah Siber 2001. Tambahan pula, Seksyen 3ZA Akta Penyalahgunaan Komputer UK 1990 diperkenalkan dengan mewujudkan satu kesalahan baharu. Sebarang perbuatan yang dapat mewujudkan risiko kerosakan yang serius terhadap komputer boleh dihukum setimpal dengan kerugian yang ditanggung oleh mangsa. Perubahan ini sebahagian daripada pembaharuan yang dibawa oleh pengenalan Serious Crime Act 2015.

Kedinamikan yang sama juga berlaku terhadap Akta Penyalahgunaan Komputer Singapura yang dipinda beberapa kali untuk menampung perkembangan baharu dalam undang-undang yang berkaitan dengan jenayah siber dan keselamatan siber. Pada masa ini, Akta Jenayah Komputer 1997 Malaysia tidak mempunyai peruntukan khusus berkenaan langkah yang perlu diambil oleh penyedia infrastruktur kritikal untuk menangani insiden atau krisis keselamatan siber (Donna, 1998). Hal ini menunjukkan keperluan perundangan khusus bagi mengawal selia isu keselamatan siber negara, sama ada melalui akta yang khusus atau pindaan Akta Jenayah Komputer 1997, dengan penambahan peruntukan yang berkaitan dengan insiden atau krisis keselamatan siber.

Di Malaysia, Akta Jenayah Komputer 1997 digubal untuk melengkapkan undang-undang jenayah sedia ada yang masih terpakai untuk pelbagai aktiviti jenayah lain melalui Internet dan sekitaran komputer. Kesalahan substantif di bawah Akta Jenayah Komputer 1997 ini, termasuklah; (1) capaian tanpa kebenaran terhadap bahan komputer (Seksyen 3), (2) capaian tanpa kebenaran dengan niat untuk melakukan atau memudahkan pelakuan kesalahan selanjutnya (Seksyen 4), (3) pengubahsuaian kandungan komputer yang tidak dibenarkan (Seksyen 5), dan (4) komunikasi yang salah (Seksyen 6).

Selain kesalahan substantif yang dinyatakan ini, akta ini juga memperuntukkan peruntukan sampingan dan am. Antaranya termasuklah peruntukan skop wilayah kesalahan di bawah akta, kuasa pencarian, penyitaan dan penangkapan, kesalahan menghalang pencarian, serta keperluan persetujuan daripada pendakwa raya untuk membuat pendakwaan bagi kesalahan yang diperuntukkan di bawah akta tersebut.

Sebagai undang-undang utama dalam jenayah siber, penguatkuasaan Akta Jenayah Komputer 1997 memerlukan ketangkasan untuk memastikan jenayah dapat ditangani dengan segeranya dan pelaku dapat didakwa dengan berkesannya. Oleh itu, Akta Jenayah Komputer 1997 terpakai

untuk semua orang, tanpa mengambil kira status kewarganegaraannya, serta terpakai di luar dan di dalam Malaysia. Jika suatu kesalahan dilakukan oleh mana-mana orang di mana-mana tempat di luar Malaysia di bawah akta ini, orang tersebut boleh diambil tindakan berkenaan dengan kesalahan itu, seolah-olah kesalahan itu dilakukan di mana-mana tempat di Malaysia. Peruntukan ini mengambil kira jenayah siber yang bersifat rentas sempadan dan kesalinghubungan digital yang kian canggih.

Subseksyen (2) Seksyen 9 Akta Jenayah Komputer 1997 (2) menyatakan bahawa akta ini terpakai jika komputer, program atau data yang terlibat dalam melakukan kesalahan berada di Malaysia, atau jika dapat disambungkan atau digunakan dengan komputer di Malaysia pada masa kesalahan berlaku. Sebagai contoh, jika seseorang menggodam sistem komputer di Singapura, tetapi menggunakannya untuk mencuri data dari pelayan yang terletak di Malaysia, atau menghantar perisian berbahaya kepada komputer di Malaysia, akta ini dapat digunakan untuk mengambil tindakan terhadap orang tersebut. Hal ini memberikan impak yang sangat meluas terhadap mana-mana komputer di luar Malaysia yang mempunyai capaian terhadap internet dan dapat berhubung dengan komputer di Malaysia kerana tertakluk di bawah akta ini.

Seksyen 10 Akta Jenayah Komputer 1997 memperuntukkan kuasa penggeledahan, penyitaan dan penangkapan kepada pegawai polis berpangkat inspektor atau lebih tinggi untuk memasuki premis dengan waran untuk "menggeledah, menyita dan menahan apa-apa keterangan sedemikian dan dia berhak mendapat capaian terhadap mana-mana program atau data yang disimpan dalam mana-mana komputer, atau mendapat capaian kepada, memeriksa atau menyemak pengendalian, mana-mana komputer dan apa-apa radas atau bahan yang berkaitan yang dia mempunyai sebab yang munasabah untuk mengesyaki digunakan atau telah digunakan berkaitan dengan apa-apa kesalahan di bawah akta ini."

Walau bagaimanapun, waran mahkamah tidak diperlukan sekiranya terdapat sebab yang munasabah untuk mempercayai bahawa terdapat apa-apa keterangan perlakuan kesalahan disembunyikan atau didepositkan di mana-mana premis di bawah Akta Jenayah Komputer 1997, dan pegawai polis mempunyai alasan yang munasabah untuk mempercayai bahawa kelewatan untuk mendapatkan waran geledah menyebabkan objek carian mungkin gagal. Dalam hal ini, masa ialah elemen yang amat penting kerana kelewatan mungkin menyebabkan keterangan gagal diperoleh, seterusnya, berisiko menggagalkan sebarang tindakan undang-undang.

Selain penipuan, Serangan Nafi Khidmat Teragih atau *Distributed Denial of Service* (DDOS) ialah sejenis serangan siber yang mengeksploitasikan had kapasiti sumber rangkaian, seperti laman web. Serangan ini menyebabkan isu prestasi rangkaian, seperti prestasi rangkaian yang perlahan secara luar biasa, ketiadaan laman web tertentu, ketidakupayaan untuk mencapai mana-mana laman web, peningkatan dramatik dalam bilangan e-mel spam yang diterima, pemotongan sambungan internet tanpa wayar atau berwayar, dan penafian jangka panjang mencapai terhadap web atau mana-mana perkhidmatan internet. Dalam sesetengah kes, seluruh kawasan geografi sambungan internet dapat terjejas kerana peralatan infrastruktur rangkaian yang salah dikonfigurasikan. Walaupun serangan DDoS ialah jenayah yang bergantung pada siber, insiden yang dilaporkan tidak dapat dibicarakan di mahkamah kerana kekurangan keterangan, terutamanya untuk mencari penjenayah sebenar.

Oleh itu, serangan DDoS dipertahankan melalui kaedah teknologi. Sebagai contoh, penggunaan tembok api (*firewall*) dan Sistem Pengesanan Pencerobohan (IDS) dapat menyekat trafik yang mencurigakan dengan menganalisis alamat IP, menyekat trafik daripada sumber berniat jahat yang diketahui atau menapis serangan berdasarkan jenis trafik. Sistem Pengesanan Pencerobohan (IDS) memantau trafik rangkaian untuk corak luar biasa dan memberikan amaran kepada pentadbir jika potensi ancaman dikesan. Perkhidmatan Mitigasi DDoS, seperti Cloudflare, Akamai atau AWS Shield, direka untuk mengesan dan memesongkan serangan DDoS. Perkhidmatan ini mengenal pasti trafik berniat jahat dan mengalihkannya daripada pelayan sasaran, serta memastikan trafik yang sah dapat terus mengalir. Dengan menggunakan gabungan teknologi ini, organisasi dapat mencipta pertahanan yang teguh terhadap serangan DDoS dan memastikan masa henti dan kehilangan data minimum (Cloudfare, 2024).

Dari aspek undang-undang, Seksyen 233 Akta Komunikasi dan Multimedia 1998 dapat digunakan untuk mendakwa apa-apa kesalahan yang melibatkan penggunaan kemudahan rangkaian secara tidak wajar, termasuklah DDoS. Namun begitu, pendakwa raya perlu membuktikan bahawa tertuduh melakukan DDoS dengan niat jenayah untuk "menyakitkan hati, menganiayai, mengugut atau mengganggu orang lain". Walau bagaimanapun, masih belum ada kes yang menunjukkan bahawa pelaku DDoS berjaya didakwa di bawah peruntukan tersebut

setakat ini kerana isu keterangan yang tidak kukuh untuk digunakan di mahkamah. Dalam masa yang sama, Seksyen 233 hanya tertumpu pada kesalahan yang berkaitan dengan kandungan digital. Hal ini menyebabkan seksyen ini tidak pernah digunakan bagi pendakwaan dalam konteks kes yang berkaitan dengan DDoS. Selain itu, pegawai penyiasat amat sukar untuk menjejaki identiti sebenar penjenayah yang melakukan serangan DDoS kerana jejak digitalnya telah dipadamkan.

Walaupun Akta Jenayah Komputer 1997 digubal dan dikuatkuasakan lebih sedekad yang lalu, perkembangan teknologi menjadikan serangan siber makin berleluasa. Oleh hal yang demikian, selain cadangan pindaan undang-undang, tiba masanya untuk pihak berwajib melihat semula sebab di balik perlakuan jenayah siber oleh individu tertentu.

Kanun Keseksaan

Selain jenayah siber yang berkaitan dengan capaian tanpa kuasa di bawah Akta Jenayah Komputer 1997, kes penipuan dalam talian makin menjadi kebimbangan umum di Malaysia. Dari aspek perundangan substantif, tindakan menipu seseorang untuk mendapatkan harta ialah kesalahan jenayah di bawah Seksyen 420 Kanun Keseksaan. Beberapa kes dapat menjadi contoh penguatkuasaan Seksyen 420 Kanun Keseksaan, terutamanya bagi kes yang berkaitan dengan penipuan. Antaar contoh jenayah tersebut, termasuklah menipu orang melalui skim palsu yang menawarkan keuntungan kewangan atau produk diskaun melalui laman web atau e-mel (Mohamad Rizal Abd Rahman, 2020).

Dalam kes *Pendakwa Raya* lwn *Mohamad Azmil Mohd Diah* [2017] 1 *LNS* 1376, seorang penganggur didakwa dan disabitkan kesalahan di bawah Seksyen 420 kerana mengiklankan iPhone 6 kepada penyelia kedai makanan segera secara palsu melalui WeChat pada bulan Mac 2016. Hal yang sama berlaku dalam kes *Pendakwa Raya* lwn *Siti Latifah Mohd* [2016] 1 *LNS* 1376 apabila seorang jurutera aplikasi komputer sambilan didakwa dan disabitkan kesalahan di bawah seksyen yang sama kerana menyamar sebagai seseorang di media sosial dan menipu seorang doktor berusia 28 tahun sebanyak RM75,750. Dalam kes ini, *Pendakwa Raya* lwn *Peace Okotie* [2009] 1 *LNS* 1759, seorang pelajar Pengurusan Perniagaan Nigeria didakwa dan disabitkan kesalahan di bawah Seksyen 420 kerana menipu seorang pegawai tadbir awam melalui e-mel mengenai hadiah kemenangan palsu $1 juta (RM3.6 juta) pada tahun 2008 (Mohamad Rizal Abd Rahman, 2020).

Sebagai peruntukan alternatif, Seksyen 424 Kanun Keseksaan biasanya digunakan terhadap pemegang akaun bank yang menerima wang daripada sindiket penipuan yang akaunnya dijadikan akaun keldai. Seksyen 424 menyatakan "barang siapa dengan curang atau secara penipuan menyembunyikan atau mengalihkan apa-apa harta miliknya atau milik orang lain, atau dengan curang atau secara penipuan membantu dalam penyembunyian atau pengalihan tersebut, atau dengan curang melepaskan apa-apa tuntutan atau hak yang dia berhak, hendaklah dihukum dengan penjara selama tempoh yang boleh sampai lima tahun atau dengan denda atau dengan kedua-duanya."

Dalam perihal ini, tertuduh secara umumnya akan membela diri dengan menyatakan bahawa dirinya tidak mengetahui bahawa wang itu berada dalam akaunnya. Walau bagaimanapun, dalam kes *Pendakwa Raya* lwn *Sabariah Adam* 1 *LNS* 1376 (Mahkamah Majistret Perbicaraan Jenayah No. 83RS – 206 – 08/2016), tertuduh mendakwa bahawa dirinya ialah mangsa penipuan dalam talian dan bukan penjenayah sebenar, serta tidak mempunyai kawalan terhadap akaun bank miliknya. Sebaliknya, mahkamah berpendapat bahawa pemegang akaun mesti bertanggungjawab untuk semua transaksi yang dimulakan atau dibenarkan menggunakan nombor akaunnya, termasuklah transaksi yang dilakukan oleh orang lain.

Seksyen 414 melibatkan larangan bersubahat dalam penyembunyian harta curi, manakala Seksyen 130J berkaitan dengan keganasan internet, termasuklah tindakan keganasan siber yang mengganggu sistem kritikal atau perkhidmatan kecemasan.

Selain itu, Seksyen 424 banyak digunakan untuk mendakwa kes yang berkaitan dengan akaun keldai. Terdapat sindiket apabila penjenayah siber memperdaya pemilik akaun bank supaya menerima sejumlah wang dalam akaun banknya untuk digunakan sebagai akaun keldai dalam cubaan untuk mengelakkan pengesanan pihak berkuasa. Seksyen ini memperuntukkan niat jenayah dengan curangnya atau dengan tipuan yang perlu dibuktikan oleh pendakwaan.

Cabaran berlaku apabila tertuduh perlu dibuktikan, iaitu mempunyai niat jenayah tersebut seperti yang dapat dilihat dalam kes *Pendakwa Raya* lwn *Sarimah Peri* [2019] 12 *MLJ* 468. Kes ini melibatkan pertuduhan di bawah Seksyen 424 Kanun Keseksaan apabila defendan dituduh, iaitu membuka akaun bank yang digunakan untuk wang penipuan. Majistret di mahkamah majistret mendapati bahawa defendan bersalah, tetapi

keputusan ini diterbalikkan oleh mahkamah tinggi. Hakim mahkamah tinggi mendapati bahawa tiada niat tidak jujur yang dibuktikan oleh pihak pendakwaan dan majistret telah terkhilaf apabila bergantung pada keterangan yang tidak boleh dipercayai. Hakim mahkamah tinggi juga mendapati bahawa pertuduhan itu ditulis secara cacat, seterusnya melepaskan dan membebaskan tertuduh.

Hal ini mendorong cadangan pemindaan Seksyen 424 untuk menganggap kesalahan semata-mata berdasarkan penggunaan akaun dalam jenayah akaun keldai (*actus reus*) tanpa mengambil kira elemen niat (*mens rea*) pemilik akaun. Walau bagaimanapun, pendekatan ini mungkin berpotensi untuk melanggar hak asasi manusia dengan menganggap seseorang itu bersalah tanpa perlu membuktikan niat, seperti kesalahan liabiliti ketat (*strict liability*).

Sebagai tindak balas terhadap kesukaran untuk membuktikan niat tidak jujur, tertuduh didakwa dengan peruntukan kesalahan kecil yang menyebabkan dirinya dikenakan penalti minimum walaupun telah menyebabkan kerugian kewangan yang ketara. Seksyen 424 meletakkan ambang yang sangat tinggi terhadap pendakwaan dalam menetapkan *mens rea* yang tinggi untuk dibuktikan. Pada pemerhatian penulis, perkara ini wajar diselaraskan dengan standard pembuktian mana-mana kesalahan jenayah dan dalam perkara yang berkaitan dengan akaun keldai, mana-mana tertuduh wajar diberi hak untuk didengari.

Akta Perlindungan Data Peribadi 2010

Akta Perlindungan Data Peribadi 2010 diperkenalkan untuk mengawal selia pemprosesan data peribadi dalam transaksi komersial. Undang-undang ini tidak terpakai untuk kerajaan persekutuan dan kerajaan negeri. Undang-undang terpakai untuk entiti, seperti badan berkanun, syarikat, industri dan organisasi swasta. Akta 709 dimodelkan berdasarkan undang-undang perlindungan data peribadi di Kesatuan Eropah dan telah diuji ketika pandemik COVID-19. Pengumpulan data peribadi menjadi kritikal dalam pengawalan dan pengehadan penyebaran virus.

Di bawah Seksyen 9 Akta 709, pengguna data yang memproses data peribadi secara komersial, seperti bank, syarikat telekomunikasi, penyedia perkhidmatan internet atau penyedia perkhidmatan aplikasi, diberi mandat untuk mengambil langkah praktikal untuk melindungi data peribadi daripada kehilangan, capaian atau pendedahan, serta pengubahan

atau pemusnahan yang tidak dibenarkan atau tidak disengajakan. Sebarang pengumpulan atau pendedahan data yang menyalahi undang-undang boleh menjadi kesalahan di bawah Seksyen 131 Akta 709, dengan hukuman denda hingga RM500,000 atau penjara hingga tiga tahun, atau kedua-duanya sekali. Peruntukan ini peruntukan tunggal yang menggariskan tanggungjawab untuk memastikan keselamatan data bagi subjek akta ini.

Dalam Seksyen 3 Akta 709, dinyatakan bahawa akta ini tidak mengikat kerajaan persekutuan dan kerajaan negeri. Hal ini bermaksud, kerajaan tidak terikat dengan keperluan dan tanggungjawab di bawah Akta 709 walaupun terdapat peningkatan insiden serangan siber dan pelanggaran data dalam sektor kerajaan Malaysia. Apabila PDPA tidak terpakai untuk kerajaan, adalah tidak keterlaluan jika dikatakan bahawa ketidakpatuhan terhadap prinsipnya tidak memberikan kesan terhadap kerajaan. Hal yang sama tidak berlaku bagi sektor komersial kerana PDPA jelas terpakai untuk sektor tersebut. (Nurkhairina Noor Sureani et al., 2021). Dalam pengendalian data peribadi dan data sensitif, kerajaan mempunyai tatacara dan polisi dalaman yang khusus bagi jabatan tertentu yang secara umumnya mematuhi prinsip perlindungan data peribadi di bawah Akta 709 atau Akta Rahsia Rasmi 1972 [Akta 88] bagi rahsia rasmi.

Dalam hal ini, entiti komersial dan kerajaan perlu memahami dan mematuhi peruntukan yang ditetapkan di bawah PDPA. Hal ini memastikan bahawa data peribadi dilindungi secukupnya dan langkah yang diperlukan disediakan untuk mencegah pengumpulan atau pendedahan data yang menyalahi undang-undang, seterusnya mengelakkan pendakwaan jenayah dan melindungi data subjek.

Isu dan Cabaran untuk Memerangi Jenayah Siber

Walaupun wujud kerangka perundangan sedia ada bagi mendepani jenayah siber, kajian ini mendapati bahawa terdapat kelompangan dan kelonggaran dalam kerangka dan peruntukan undang-undang yang berkaitan dengan prinsip substantif jenayah siber dan pelaksanaan dan penguatkuasaan undang-undang. Kelemahan perundangan ini merumitkan usaha untuk memerangi jenayah siber di Malaysia. Perkara ini dirangkumkan dalam aspek yang berikut: (1) definisi jenayah siber yang sentiasa berubah; (2) isu bidang kuasa, dan (3) cabaran dalam penyiasatan dan pendakwaan jenayah siber. Bahagian ini turut melaporkan hasil temu bual dengan agensi berkepentingan yang berkaitan dengan penyiasatan dan penguatkuasaan jenayah siber.

Konteks Jenayah Siber yang Sentiasa Berubah

Dalam landskap digital pada masa ini, evolusi pesat teknologi, kepelbagaian kesalahan, isu bidang kuasa dan pertindihan dengan jenayah tradisional menyebabkan kesukaran dalam penentuan definisi dan konteks jenayah siber yang jelas dan diterima secara universal. Penciptaan teknologi baharu pula seolah-olah memberikan peluang baharu kepada penjenayah siber untuk melakukan jenayah. Sebagai contoh, kemunculan mata wang kripto membentuk jenayah kewangan yang unik, seperti serangan *cryptojacking* dan *ransomware* yang tidak wujud sedekad yang lalu. Evolusi berterusan ini menuntut keperluan definisi jenayah siber yang fleksibel dan boleh disesuaikan, yang merangkumi perkembangan teknologi masa hadapan dan neutral teknologi.

Pelbagai aktiviti jenayah yang terangkum dalam jenayah siber menambahkan kerumitan untuk menentukan istilah tersebut. Antara contoh jenayah siber termasuklah jenayah bergantung pada siber, seperti penggodaman. Jenayah siber boleh meliputi buli siber, gangguan dalam talian, penggodaman dan pelanggaran data. Kepelbagaian ini bukan sahaja menjadikannya mencabar untuk mewujudkan definisi yang komprehensif, tetapi juga merumitkan tindak balas undang-undang dan pemahaman masyarakat tentang maksud jenayah siber.

Banyak jenayah siber yang hanya aktiviti jenayah tradisional yang diperkembangkan melalui medium internet atau komputer. Beberapa bentuk jenayah siber sangat khusus untuk teknologi atau platform tertentu, seterusnya menyukarkannya untuk dimasukkan dalam definisi yang luas yang dapat difahami merentasi kecekapan teknologi dan bidang kuasa undang-undang yang berbeza-beza. Sebagai contoh, jenayah yang melibatkan platform media sosial tertentu atau teknologi baharu, seperti kecerdasan buatan yang digunakan untuk membentuk *deepfakes*, memerlukan pemahaman dan tafsiran undang-undang yang khusus. *Deepfakes* digunakan untuk membuat video atau gambar kelihatan asli dengan memalsukan wajah seseorang dalam video dan audio bagi memperdaya mangsa dengan menyebarkan maklumat palsu atau melakukan penipuan (Majlis Keselamatan Negara, 2024). *Deepfakes* dapat menukar muka orang dalam video dengan muka figura terkenal dengan hasrat untuk mencemarkan imej dan memberikan impak negatif terhadap individu tersebut. Sekiranya figura terkenal itu merupakan pemimpin negara, sudah tentu perkara ini memberikan kesan negatif terhadap negara itu.

Tidak seperti jenayah tradisional, jenayah siber sering melibatkan aset tidak ketara dan keterangan berbentuk digital yang lebih mencabar untuk dijejaki, diukur dan didakwa. Sifat tidak ketara ini merumitkan penetapan definisi jenayah siber kerana memerlukan pemahaman yang nuansa tentang sekitaran digital dan cara jenayah dilakukan.

Negara dan budaya yang berbeza-beza mempunyai sudut pandangan yang berbeza-beza mengenai apa-apa yang menjadi jenayah dalam alam digital. Sesetengah aktiviti yang dianggap menyalahi undang-undang atau tidak beretika dalam satu-satu bidang kuasa mungkin dibenarkan di bidang kuasa lain. Pornografi merupakan contoh yang ideal bagi perkara ini. Perbezaan ini amat ketara dalam kes yang melibatkan penapisan kandungan, pelanggaran privasi dan kebebasan bersuara dalam talian.

Perbezaan cara pelbagai negara dan budaya melihat dan menggubal undang-undang siber dapat dilihat dalam beberapa bidang utama. Sebagai contoh, dalam hal penapisan kandungan, China terkenal dengan undang-undang penapisan internet yang ketat (OpenNet Initiatives, 2012), sementara Amerika Syarikat (AS) menawarkan kebebasan perlindungan kebebasan bersuara yang luas di bawah Pindaan Pertama Perlembagaan Amerika Syarikat (Caral, 2004; Freedom House, 2016; Marsden et al., 2020). Dari segi pelanggaran privasi, Kesatuan Eropah (EU) mempunyai Peraturan Perlindungan Data Umum (GDPR) yang menyediakan perlindungan privasi yang komprehensif, termasuklah hak untuk dilupakan, keperluan persetujuan yang ketat untuk pengumpulan data dan penalti berat untuk pelanggaran. Sebaliknya, pendekatan AS secara amnya kurang ketat berbanding dengan GDPR, dengan lebih banyak menekankan peraturan kendiri oleh syarikat, bukannya mandat yang dikuatkuasakan oleh kerajaan.

Mengenai kebebasan bersuara dalam talian, Arab Saudi mempunyai undang-undang yang ketat yang mengawal ekspresi dalam talian, manakala Piagam Hak dan Kebebasan Kanada melindungi kebebasan bersuara, termasuklah kandungan dalam talian (Freedom House, 2014; Helmi Noman, 2013; Joli-Coeur, 2014). Walau bagaimanapun, kebebasan ini tertakluk pada had yang munasabah dan tidak meliputi ucapan kebencian yang boleh dihukum oleh undang-undang. Dalam hal fitnah, Korea Selatan mempunyai undang-undang yang ketat terhadap fitnah dalam talian, manakala Amerika Syarikat mempunyai undang-undang fitnah yang meletakkan beban pembuktian yang lebih tinggi kepada plaintiff yang merupakan tokoh dalam masyarakat (Caragliano, 2013).

Pada dasarnya, pentakrifan jenayah siber dalam era digital ialah tugas yang kompleks yang memerlukan pertimbangan pelbagai faktor,

termasuklah kemajuan teknologi, kepelbagaian kesalahan, kepelbagaian bidang kuasa dan sifat unik jenayah digital. Definisi jenayah siber yang berkesan mestilah dinamik dan inklusif, serta dapat disesuaikan untuk menampung landskap digital yang terus berkembang. Dengan teknologi yang terus maju, rangka kerja undang-undang dan kerjasama antarabangsa perlu berkembang untuk memerangi landskap jenayah siber yang sentiasa berubah dengan berkesannya.

Isu Bidang Kuasa

Ciri Internet yang bersifat terbuka dan tanpa sempadan turut memberikan cabaran terhadap bidang kuasa (*jurisdiction*) tradisional sesebuah negara untuk mengambil tindakan yang sewajarnya bagi membendung jenayah siber dan menguatkuasakan undang-undang. Internet tidak dimiliki atau dikawal oleh satu-satu organisasi atau kerajaan. Secara konsepnya, Internet atau alam maya ialah kawasan tanpa sempadan geografi (Nehaluddin Ahmad & Norulaziemah Zulkiffle, 2022; Wimmer & Pogoriler, 2006). Hal ini bermakna, ketika seseorang itu berada dalam talian, dirinya boleh berada di beberapa tempat sekali gus.

Dunia tanpa sempadan ini membolehkan seseorang itu melakukan perjalanan dari satu lokasi ke lokasi lain dengan satu klik butang. Sebagai contoh, Internet membolehkan dua orang berkomunikasi dari seberang kutub Bumi yang sempadan jarak geografi tidak lagi menjadi suatu halangan. Hal ini termasuklah melaksanakan kontrak dan transaksi kewangan secara dalam talian. Negara yang merdeka mempunyai bidang kuasa untuk mengiktiraf kedaulatan negara dan kuasa tersebut bertindak secara perundangan, eksekutif dan kehakiman. Namun begitu, Internet tidak mempunyai sempadan atau wilayah tetap yang membolehkan bidang kuasa sesebuah kerajaan atau mahkamah dikuatkuasakan dan dilaksanakan (Nehaluddin Ahmad & Norulaziemah Zulkiffle, 2022).

Apabila suatu jenayah siber berlaku, aktiviti jenayah sering melangkaui sempadan negara. Pelaku boleh melancarkan serangan dari mana-mana tempat. Sebagai contoh, National Cyber Security Agency (NACSA) melakukan siasatan yang berkaitan dengan insiden keselamatan siber yang berlaku di sesebuah agensi kerajaan di Malaysia. Ketika siasatan, di atas skrin, penjenayah mungkin kelihatan seperti sedang melakukan aktiviti jenayah di Kuala Lumpur. Siasatan lanjut mendedahkan penjenayah tersebut berada di Nigeria ketika jenayah itu dilakukan kerana penjenayah menggunakan teknik tertentu untuk mengaburi lokasi sebenarnya di

dunia nyata. Hal ini dapat merumitkan siasatan dan pendakwaan, dan yang lebih rumit adalah apabila melibatkan penyiasatan antara negara yang berbeza-beza (Brenner, 2006). Pihak berkuasa di negara lain mungkin mengenakan keperluan pematuhan terhadap proses siasatan yang merumitkan pihak berkuasa Malaysia yang perlu dipatuhi demi mendapat kerjasama untuk menyiasat sesuatu kes jenayah siber. Hal ini menyebabkan kelewatan penyiasatan jenayah siber sehingga menjadikan keterangan kes kurang atau lemah. Selain itu, perbezaan rangka kerja undang-undang dan tahap kecanggihan teknologi antara negara mewujudkan jurang yang dapat dieksploitasikan oleh penjenayah siber.

Sebelum mana-mana mahkamah Malaysia mempunyai bidang kuasa terhadap sesuatu pihak, pihak tersebut mesti mempunyai kaitan dengan Malaysia untuk mewujudkan *locus standi* dan sebab tindakan yang sesuai. Oleh sebab sifat Internet, iaitu identiti dan lokasi mungkin dipalsukan, isu sedemikian diseriuskan lagi dengan kekurangan sumber dan pengetahuan teknikal pada pihak badan kehakiman dan penguatkuasaan undang-undang.

Bagi memahami perkara ini, terdapat kes kegagalan pihak pendakwaan kerana Polis Diraja Malaysia (PDRM) tidak dapat menunjukkan rantaian keterangan (*chain of evidence*) yang berkaitan dengan komputer tertentu. Komputer itu tiada pada pihak PDRM sepanjang siasatan dilakukan. Oleh itu, ada kemungkinan bahawa komputer tersebut diganggu dan keterangan diubah. Jenis keterangan yang diperlukan untuk menyabitkan kesalahan penggodaman menimbulkan banyak cabaran dari aspek penguatkuasaan undang-undang (Janaletchumi Appudurai & Chitra L. Ramalingam, 2007).

Cabaran dalam Penyiasatan dan Pendakwaan Jenayah Siber

Malaysia berkongsi isu dan cabaran praktikal yang sama dengan negara lain mengenai isu pendakwaan jenayah siber. Perkara ini dijelaskan dalam subbahagian selanjutnya.

Kesukaran Pengenalpastian Identiti Sebenar Penjenayah di Alam Digital

Penjenayah siber menggunakan teknik tertentu untuk menyembunyikan identitinya. Hal ini menyukarkan siasatan bagi mengenal pasti suspek sebenar. Cabaran ini menuntut kemajuan dalam forensik digital, keupayaan memecahkan penyulitan dan kerjasama dengan agensi penguatkuasaan undang-undang antarabangsa untuk mengesan identiti sebenar penjenayah siber. Satu daripada halangan utama dalam pendakwaan penjenayah siber

ialah faktor kerahsiaan identiti atau ketanpanamaan (*anomymity*) dan nama samaran (*pseudonymity*) yang dibenarkan melalui ciri internet (Duryana Mohamed, 2012).

Penjenayah siber sering menggunakan pelbagai teknik, seperti pelayan proksi, rangkaian persendirian maya (*virtual private network*) dan web tertutup (*dark web*) untuk menyembunyikan identiti dan lokasinya (Wall, 2007). Hal ini secara signifikan menghalang keupayaan agensi penguatkuasaan undang-undang untuk mengesan aktiviti jenayah dan mengaitkannya dengan penjenayah tersebut. Penjenayah siber sering menggunakan taktik dan teknologi canggih. Penjenayah itu terus menyesuaikan kaedahnya untuk mengelakkan pengesanan, menggunakan penyulitan, perisian hasad dan mengeksploitasikan kelemahan dalam perisian dan rangkaian (McGuire & Dowling, 2013). Evolusi taktikal penjenayah yang berterusan ini menjadikannya lebih mencabar bagi penguatkuasa undang-undang untuk mengikuti perkembangan penjenayah siber.

Dalam perihal kawal selia kandungan internet, isu kesukaran untuk mengenal pasti penjenayah sebenar yang menyebarkan kandungan yang dilarang turut dihadapi oleh pihak berkuasa, seperti PDRM dan MCMC. Hal tersebut menyebabkan pindaan Seksyen 114A Akta Keterangan 1950 diluluskan di Parlimen pada 2012. Secara ringkasnya, peruntukan tersebut meletakkan beban pembuktian kepada defendan, iaitu sekiranya nama atau apa-apa bentuk identifikasi yang tertera pada sesuatu penerbitan dapat dikaitkan dengan defendan, maka defendan perlu membuktikan bahawa penerbitan itu tidak diterbitkan olehnya kepada mahkamah.

Setakat ini, peruntukan ini terpakai dalam beberapa kes mahkamah dan melalui pemantauan pengkaji, belum ada mana-mana kes yang mencabar keabsahan Seksyen 114A. Peruntukan ini menjadi senjata bagi pendakwa untuk mengatasi cabaran yang ditimbulkan daripada isu ketanpanamaan tersebut. Bagi menjamin keadilan bagi tertuduh, beban pembuktian tersebut perlu dibuktikan oleh tertuduh di atas imbangan kebarangkalian (*on the balance of probabilities*) dan pendakwa kekal perlu membuktikan standard beban pembuktian yang lebih berat, iaitu tanpa sebarang keraguan munasabah.

Keperluan Keterangan yang Mencukupi dalam Siasatan Jenayah Siber

Bagi memastikan siasatan dan pendakwaan kes jenayah siber dilakukan secara berkesan, cabaran praktikal ialah pengekalan dan pemeliharaan

data. Pembekal perkhidmatan mengekalkan data pelanggan untuk memudahkan pemasaran, pengebilan dan pematuhan peraturan. Walau bagaimanapun, beberapa cabaran timbul daripada pengesanan data dari peringkat pengumpulan sehingga pelupusannya. Pertama, privasi dan perlindungan data menjadi kebimbangan kerana data peribadi pelanggan tertentu berada di bawah Akta Perlindungan Data Peribadi 2010. Kedua, keadaan tersebut menjadi cabaran bagi syarikat untuk melindungi rekod pelanggan daripada risiko kebocoran data. Ketiga, penyimpanan data untuk tempoh yang panjang memberikan implikasi kewangan, sama ada di premis, di awan atau menggunakan alamat IPv4 atau IPv6 awam. Keempat, ketiadaan kepakaran yang diperlukan dalam siasatan forensik bakal meningkatkan kos aktiviti penguatkuasaan.

Dengan peningkatan jumlah data pada setiap saat di Internet, pengurusan dan penyimpanan sejumlah besar data menjadi suatu cabaran kerana memerlukan infrastruktur yang mantap, termasuklah sistem storan dan penyelesaian sandaran untuk mengendalikan peningkatan jumlah data dengan berkesannya. Pelaksanaan penyelesaian storan berskala, seperti storan awan atau sistem storan teragih, dapat menampung jumlah data yang makin meningkat dan mengoptimumkan penggunaan storan dan mengurangkan kos. Perkara ini mungkin perlu diteliti dengan lebih lanjut jika melibatkan jenis data berstatus rahsia di bawah Akta Rahsia Rasmi 1972 bagi melindungi keselamatan data tersebut daripada terbocor.

Oleh hal yang demikian, dalam konteks sektor penyedia perkhidmatan di bawah Suruhanjaya Komunikasi Multimedia Malaysia, adalah wajar sekiranya Akta Komunikasi dan Multimedia 1998 dipinda bagi memperuntukkan prinsip pengekalan data dan pemeliharaan data. Matlamatnya adalah untuk menyediakan pegawai polis dengan kuasa yang sesuai bagi memperkukuh siasatan.

Oleh sebab data tentang sekitaran rangkaian adalah dinamik dan selama-lamanya terkumpul, adalah penting untuk memelihara data tertentu untuk disiasat. Bagi menangani pemeliharaan data, menteri wajar diberi kuasa untuk menetapkan peraturan mengenai pengekalan data bagi tujuan siasatan.

Cabaran lain ialah pengekalan keselamatan dan privasi data sambil mengekalkan dan memelihara data (Koops & Goodwin, 2014). Bagi menangani cabaran ini, organisasi perlu memastikan privasi data, mencegah capaian yang tidak dibenarkan dan melaksanakan kawalan

penyulitan dan capaian yang sesuai. Bagi mencapai matlamat ini, organisasi boleh melaksanakan langkah keselamatan yang mantap, seperti penyulitan, kawalan capaian, pengesahan pengguna dan sistem pemantauan. Audit keselamatan yang kerap, penilaian kerentanan dan pematuhan peraturan perlindungan data, penting untuk keselamatan data dan privasi.

Cadangan

Dengan berdasarkan perbincangan dan analisis dapatan dalam bahagian sebelumnya, isu yang berkaitan dengan kerangka perundangan yang mengawal selia jenayah siber perlu ditambah baik.

Pada dasarnya, pentakrifan jenayah siber dalam era digital ialah tugas kompleks yang memerlukan pertimbangan pelbagai faktor, termasuklah kemajuan teknologi, kepelbagaian kesalahan, kepelbagaian bidang kuasa dan sifat unik jenayah digital. Definisi jenayah siber yang berkesan mestilah dinamik, inklusif dan dapat disesuaikan untuk menampung landskap digital yang terus berkembang.

Antara isu yang dikesan yang melibatkan Akta Komunikasi dan Multimedia 1998 termasuklah perundangan ini tidak mengawal selia jenayah siber secara khusus dan tidak mengandungi peruntukan yang berkaitan. Daripada hasil kajian ini juga, didapati bahawa jenayah siber berada di bawah bidang kuasa penyiasatan dan penguatkuasaan PDRM. Namun begitu, dari aspek praktikal, apabila jenayah siber berlaku, pihak berwajib akan melakukan siasatan secara bersama-sama. Pasukan ini terdiri daripada wakil PDRM, NACSA dan SKMM, bergantung pada keperluan kes tersebut. Namun begitu, berdasarkan kerangka perundangan dan konteks yang ditetapkan di bawah Akta Komunikasi dan Multimedia 1998, SKMM mempunyai bidang kuasa khusus terhadap pelesen yang mendapatkan lesen di bawah Akta Komunikasi dan Multimedia 1998.

Dalam aspek praktikal sesebuah penyiasatan, sekiranya terdapat keperluan untuk mendapatkan kerjasama daripada pihak syarikat telekomunikasi yang merupakan pemegang lesen SKMM, syarikat komunikasi mempunyai tanggungjawab di bawah Seksyen 263 Akta Komunikasi dan Multimedia 1998 untuk memberikan kerjasama sewajarnya demi menjamin kelancaran penyiasatan dan penguatkuasaan. Antara kerjasama ini termasuklah membantu mengenal pasti lokasi komputer yang digunakan untuk melakukan jenayah siber, membuat penyiasatan forensik dan perkara lain yang berada di bawah bidang

kuasa SKMM. Namun begitu, perluasan bidang kuasa SKMM sehingga mencakupi pihak yang bukan pemegang lesen SKMM wajar dipertimbangkan. Hal ini dikatakan demikian kerana ekosistem Internet itu meluas dan dapat dieksploitasikan oleh penjenayah siber yang mengetahui selok belok bidang kuasa yang terhad. Bagi jenayah siber, Akta Komunikasi dan Multimedia 1998 wajar dipinda bagi mempertimbangkan aspek jenayah siber yang lebih khusus.

Dalam perbincangan sebelum ini, terdapat isu, iaitu penyiasatan jenayah siber tertunda disebabkan oleh kekurangan keterangan untuk dibuktikan dan isu prosedur yang dibangkitkan oleh penguatkuasa negara luar. Hal ini menjadi cabaran yang besar dalam penguatkuasaan jenayah siber yang berkesan, bukan sahaja di Malaysia, malah di negara maju, seperti Amerika. Namun begitu, sekiranya undang-undang diperketat tanpa pertimbangan sewajarnya, dibimbangi bahawa undang-undang bersifat terlalu intrusif dan menyebabkan ketidakadilan. Oleh hal yang demikian, isu ini dicadangkan untuk diatasi secara teknologi melalui kerjasama erat antara agensi penguatkuasa di antara pelbagai negara. Malaysia hendaklah terus mempertingkatkan kemahiran yang berkaitan dengan digital, khususnya dalam aspek penyiasatan dan penguatkuasaan jenayah siber dengan menggunakan teknologi terkini.

Selain itu, kajian penulis mendapati bahawa terdapat keperluan untuk menambah baik aspek perjawatan penguatkuasa di Malaysia, terutamanya bagi penyiasatan jenayah siber. Pegawai yang melakukan penyiasatan wajar diberi pendedahan dan ilmu terkini yang berkaitan dengan forensik digital. Hal ini termasuklah penambahbaikan capaian terhadap teknologi penguatkuasaan dan menambah perjawatan yang berkaitan, serta meningkatkan capaian terhadap kemahiran yang berkaitan dengan keselamatan dalam talian. Apabila Parlimen meluluskan Akta Keselamatan Siber 2024 [Akta 854], akta tersebut dapat memperkasakan ekosistem keselamatan siber negara secara menyeluruh. Entiti infrastruktur kritikal maklumat negara mempunyai peranan kritikal dalam pelbagai aspek kerana sebarang gangguan terhadap perkhidmatannya dapat menyebabkan kesan yang besar terhadap negara. Bagi menyambut inisiatif baharu ini, aspek perundangan perlu disokong oleh modal insan yang utuh dan sentiasa berdaya saing. Hal ini secara langsung dapat memberikan kesan terhadap jenayah siber kerana pengukuhan aspek keselamatan siber negara membolehkan jenayah siber dikawal dengan lebih berkesan.

Oleh hal yang demikian, dalam konteks sektor penyedia perkhidmatan di bawah Suruhanjaya Komunikasi Multimedia Malaysia, Akta Komunikasi dan Multimedia 1998 sewajarnya dipinda bagi memperuntukkan prinsip pengekalan data dan pemeliharaan data. Matlamatnya adalah untuk menyediakan pegawai polis dengan kuasa yang sesuai bagi memperkukuh siasatan.

Bagi isu dan cabaran dalam penyiasatan dan pendakwaan disebabkan oleh kesukaran pengenalpastian penjenayah sebenar, aspek yang diperkenalkan melalui Seksyen 114A Akta Keterangan 1950 dapat dipertimbangkan untuk peluasan dalam akta lain yang berkaitan. Setakat ini, peruntukan ini terpakai dalam beberapa kes mahkamah dan berdasarkan pemantauan penulis, belum ada mana-mana kes yang mencabar keabsahan Seksyen 114A. Peruntukan ini menjadi suatu "senjata" pendakwaan untuk mengatasi cabaran yang ditimbulkan daripada isu ketanpanamaan tersebut. Bagi menjamin keadilan untuk tertuduh, beban pembuktian tersebut perlu dibuktikan oleh tertuduh di atas imbangan kebarangkalian (*on the balance of probabilities*) dan pendakwa perlu membuktikan kes tanpa sebarang keraguan yang munasabah. Pada masa yang sama, aspek teknikal dalam forensik digital perlu ditambah baik supaya pengesanan penjenayah siber dapat dilakukan dengan lebih berkesan, selaras dengan peruntukan undang-undang.

KESIMPULAN

Secara keseluruhan, Malaysia menghadapi cabaran besar dalam menangani jenayah siber yang semakin kompleks. Reformasi undang-undang, seperti pemodenan Akta Jenayah Komputer 1997 dan Akta Komunikasi dan Multimedia 1998, adalah penting untuk memastikan relevannya perundangan sedia ada dengan perkembangan teknologi. Selain itu, penguatkuasaan perlu diperkukuh melalui peningkatan keupayaan agensi berkaitan, termasuk akses kepada alatan forensik yang canggih, dasar pengekalan data, dan latihan khusus untuk pegawai penguatkuasa. Usaha ini juga perlu memberi perhatian kepada penyiasatan isu seperti anonymity, penyulitan, dan pemeliharaan bukti digital bagi memastikan keberkesanan pendakwaan dan pencegahan jenayah siber.

Pendekatan proaktif yang menggabungkan reformasi perundangan, peningkatan teknologi dan prinsip moral amat penting untuk membina

sekitaran digital yang lebih selamat. Selain itu, kerjasama antarabangsa, seperti Interpol dan negara anggota ASEAN, juga harus diperkukuh untuk menangani jenayah siber rentas sempadan. Dengan langkah ini, Malaysia dapat memperkukuh tindak balas terhadap ancaman siber dan menjadi model bagi negara lain yang menghadapi cabaran yang serupa.

NOTA

1 *Cryptojacking* sejenis jenayah siber yang melibatkan penggunaan peranti orang secara tidak sah dan tidak dibenarkan (komputer, telefon pintar, tablet atau pelayan) oleh penjenayah siber untuk melombong cryptocurrency.

PENGHARGAAN

Kajian ini dibiayai oleh geran The Harun M. Hashim Research Grant (HAREG) 2023 HAREG23-023-0023. Penulis merakamkan penghargaan kepada Universiti Islam Antarabangsa Malaysia atas sokongan yang diberikan terhadap penyelidikan ini.

SUMBANGAN PENGARANG

Selaku penulis tunggal, pengarang bertanggungjawab terhadap keseluruhan penulisan makalah ini.

PENDANAAN

Penerbitan makalah ini dibiayai oleh Dewan Bahasa dan Pustaka.

PERNYATAAN KETERSEDIAAN DATA

Data yang dinyatakan dalam kajian ini boleh dicapai secara terbuka tertakluk kepada polisi Dewan Bahasa dan Pustaka.

PERISYTIHARAN

Konflik kepentingan: Pengarang tidak mempunyai sebarang konflik kepentingan dari segi kewangan dan bukan kewangan untuk diisytiharkan.

RUJUKAN

Brenner, S. W. (2006). At light speed: Attribution and response to cybercrime/terrorism/warfare. *The Journal of Criminal Law & Criminology, 97*(2), 379–475.

Caragliano, D. A. (2013). Real names and responsible speech: The cases of South Korea, China and facebook. *Yale Journal of International Affairs*. https://www.yalejournal.org/publications/real-names-and-responsible-speech-the-cases-of-south-korea-china-and-facebook

Caral, J. (2004). Lessons from ICANN: Is self-regulation of the Internet fundamentally flawed? *International Journal of Law and Information Technology*, *12*(1), 1–31. https://doi.org/10.1093/ijlit/12.1.1

Cloudfare. (2024). *How to prevent DDoS attacks*. *Methods and tools*. Cloudfare. https://www.cloudflare.com/learning/ddos/how-to-prevent-ddos-attacks/

CyberSecurity Malaysia. (2023). *Mid-yearreportthreatlandscape2023*. CyberSecurity Malaysia. https://www.cybersecurity.my/data/content_files/26/2511.pdf

Donna L. B. (1998). Malaysia's "Computer Crimes Act 1997" gets tough on cybercrime but fails to advance the development of cyberlaws. *Pacific Rim Law and Policy*, *7*(2), 26.

Duryana Mohamed. (2012). Investigating cybercrimes under the Malaysian cyberlaws and the criminal procedure code: Issues and challenges. *Malayan Law Journal*, *6*, i--ix. http://irep.iium.edu.my/27926/

Duryana Mohamed. (2013). Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws. *Computer Law & Security Review*, *29*(1), 66–76. https://doi.org/10.1016/J.CLSR.2012.11.005

Dustin Volz, J. F. (2016, 24 Mac). *U.S. indicts Iranians for hacking dozens of banks, New York dam.* Reuters. https://jp.reuters.com/article/us-usa-iran-cyber-idUSKCN0WQ1JF

Freedom House. (2014). *Freedom on the Net*: *Canada*. https://freedomhouse.org/report/freedom-net/2014/canada

Freedom House. (2016). *Freedom on the Net 2015*. https://freedomhouse.org/sites/default/files/FOTN 2015 Full Report.pdf

Helmi Noman. (2013). *Saudi Arabia to impose restrictions on online content production, including on YouTube*. OpenNet Initiatives. https://opennet.net/blog/2013/12/saudi-arabia-impose-restrictions-online-content-production-including-youtube

Home Office UK Government. (2013). *Cyber crime*: *A review of the evidence.* Home Office UK Government. https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

Interpol. (2021). *National cybercrime strategy guidebook*. Interpol. https://www.interpol.int/content/download/16455/file/Cyber Strategy Guidebook.pdf

Irene Tham, Rachel Au-Yong, Tin May Linn & Rodolfo Pazos. (2018). SingHealth cyber attack: How it unfolded. *Strait Times*. https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html

Janaletchumi Appudurai & Chitra L. Ramalingam. (2007). Computer crimes: A case study of what Malaysia can learn from others? *Journal of Digital Forensics, Security and Law*, *2*(2).

Joli-Coeur, F. (2014). Canada's approach to intermediary liability for copyright infringement: The notice and notice procedure. *Berkeley Technology Law* Journal. http://btlj.org/2014/03/canadas-approach-to-intermediary-liability-for-copyright-infringement-the-notice-and-notice-procedure/

Mahyuddin Daud & Ida Madieha Abd Ghani Azmi. (2021). Digital disinformation and the need for Internet co-regulation in Malaysia. *Pertanika Journal of Social Sciences and Humanities*, *29*(S2), 169–183. https://doi.org/10.47836/pjssh.29.s2.12

Mahyuddin Daud. (2021). Freedom of Misinformation and the relevance of co-regulation in Malaysia: A cross-jurisdictional analysis. *IIUM Law Journal*, *29*(2), 27–54. https://doi.org/10.1016/j.clsr.2019.105373

Majlis Keselamatan Negara. (2024, 15 Mac). Deepfake dikesan semakin banyak digunakan dalam aktiviti penipuan. *Majlis Keselamatan Negara*. https://www.mkn.gov.my/web/ms/2024/03/15/deepfake-dikesan-semakin-banyak-digunakan-dalam-aktiviti-penipuan/

Malaysian Communications and Multimedia Commission. (2020). *FAQs on online content problems*. Malaysian Communications and Multimedia Commission. https://www.mcmc.gov.my/en/faqs/online-content-problems/what-are-the-steps-required-for-me-to-lodge-compla

Maleen Balqish Salleh. (2023, 17 Jun). *PDRM*: *Over RM5.2 billion lost to scams in two years*. *The Edge*. https://theedgemalaysia.com/article/pdrm-over-rm52-billion-lost-scams-two-years

Marsden, C., Meyer, T., & Brown, I. (2020). Platform values and democratic elections: How can the law regulate digital disinformation? *Computer Law & Security Review*, *36*, 105373. https://doi.org/10.1016/j.clsr.2019.105373

Mohamad Rizal Abd Rahman. (2020). Online scammers and their mules in Malaysia. *Jurnal Undang-undang dan Masyarakat*, *26*, 65–72. https://doi.org/10.17576/juum-2020-26-08

Nazli Ismail Nawang. (2017). Combating anonymous offenders in the cyberspace: An overview of the legal approach in Malaysia. *International Conference on Anti-Cybercrime (ICACC)*. https://doi.org/10.1109/Anti-Cybercrime.2017.7905255

Nehaluddin Ahmad & Norulaziemah Zulkiffle. (2022). Jurisdiction issues in cyberspace: An overview in respect of Brunei and Malaysia Compared to the United States' system. *Journal of Southeast Asian Research*, 1–12. https://doi.org/10.5171/2022.384427

Norton. (2021). *2021 Norton cyber safety insights report.* Norton Life Locks. https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report/

Nurkhairina Noor Sureani, Atikah Shahira Awis Qurni, Ayman Haziqah Azman, Mohd Bahrin Othman & Hariz Sufi Zahari. (2021). The adequacy of data protection laws in protecting personal data in Malaysia. *Malaysian Journal of Social Sciences and Humanities (MJSSH)*, *6*(10), 488–495. https://doi.org/10.47405/mjssh.v6i10.1087

OpenNet Initiatives. (2012). *ONI country profile*: *China*. OpenNet Initiatives.

Prasad Jayabalan, Roslina Ibrahim & Azizah Manaf. (2014). Understanding cybercrime in Malaysia: An vverview. *Sains Humanika*, *2*(2), 109–115. https://doi.org/10.11113/sh.v2n2.424

Wall, D. S.(2007). *Cybercrime*: *The transformation of crime in the information age*. https://ssrn.com/abstract=1066922

Wimmer, K., & Pogoriler, E. R. (2006). *International Jurisdiction and the Internet*. Covington & Burling LLP. http://euro.ecom.cmu.edu/program/law/08-732/Jurisdiction/InternationalJurisdiction.pdf