ULASAN PERUNDANGAN

PERANAN ATAU KEPENTINGAN AKTA KESELAMATAN SIBER 2024 (AKTA 854) UNTUK MENDEPANI JENAYAH SIBER: SATU ULASAN

Duryana Mohamed
mduryana@iium.edu.my

Kulliyyah Undang-undang Ahmad Ibrahim, Universiti Islam Antarabangsa Malaysia, 53100 Kuala Lumpur, Malaysia.

PENDAHULUAN

Perkembangan teknologi maklumat memberikan banyak kemudahan kepada manusia. Teknologi membolehkan manusia berkomunikasi dengan sesiapa sahaja di seluruh dunia, mempercepat urusan penghantaran maklumat antara satu dengan lain dan meningkatkan urusan pentadbiran, serta pengurusan negara. Pada masa ini, teknologi kecerdasan buatan menjadi satu keperluan bagi masyarakat (Ilah Hafiz Aziz, 2023). Namun begitu, banyak yang menyalahgunakan teknologi ini hingga wujud ancaman siber yang makin meningkat dan berleluasa (Bernama, 2024a). Ancaman jenayah siber, seperti jenayah intipan siber, pancingan data, jenayah atas talian, kecurian identiti, penggodaman, serangan perisian tebusan, penipuan kad kredit siber, keganasan siber dan peperangan siber terhadap infrastruktur keselamatan negara, institusi kewangan, kemudahan ketenteraan dan institusi kerajaan dapat menggugat kestabilan ekonomi dan politik negara ini. Oleh itu, negara perlu mengkaji semula undang-undang siber yang wujud sejak tahun 1997, di samping memperkukuh pelaksanaan undang-undang terkini, iaitu Akta Keselamatan Siber 2024 (Akta 854) (AKS 2024).

Makalah ini membincangkan undang-undang siber di Malaysia dan usaha yang dilakukan oleh kerajaan sebelum pelaksanaan Akta Keselamatan Siber 2024 atau Akta 854. Fokus utama makalah ini adalah untuk mengulas kandungan Akta 854, pelaksanaannya di Malaysia dan beberapa perkara yang perlu disemak dan ditambah baik.

Undang-undang Siber di Malaysia dan Usaha Kerajaan Menangani Isu Siber

Undang-undang siber di Malaysia wujud sejak tahun 1997. Antaranya termasuklah Akta Jenayah Komputer 1997 (Akta 563), Akta Tandatangan

Digital 1997 (Akta 562) dan Akta Komunikasi dan Multimedia 1998 (Akta 588). Akta Komunikasi dan Multimedia telah dipinda dan dijangka berkuat kuasa pada bulan Februari 2025 (Bernama, 2025). Selain itu, terdapat juga Akta Perlindungan Data Peribadi 2010 (Akta 709) yang dipinda melalui Personal Data Protection (Amendment) Act 2024 (2024). Akta lain yang turut berkaitan termasuklah Kanun Keseksaan dan Kanun Prosedur Jenayah (Agensi Keselamatan Siber Negara, t.t.). Namun begitu, akta ini masih belum mencukupi bagi menangani serangan siber yang mengancam keselamatan negara. Selain mewujudkan dan melaksanakan akta tersebut, kerajaan juga menggubal Akta Keselamatan Negara 2016, mengadakan sekatan terhadap penggunaan internet secara bebas melalui Kod Kandungan Internet dan merangka Dasar Keselamatan Siber yang diluluskan pada 14 Februari 2023 bagi mengawal serangan atau ancaman siber (PLANMalaysia, t.t.). Kod ini bertujuan untuk mengawal selia dan mewujudkan panduan kepada pihak industri dan semua rakyat Malaysia dalam penciptaan kandungan internet. Melalui kod ini, sesiapa sahaja dapat mencipta kandungan yang kreatif dan melakukan pelbagai inovasi mengikut peruntukan dalam Akta Komunikasi dan Multimedia 1998. Kod ini masih relevan dan dijadikan panduan penggunaan internet di Malaysia. SKMM ditubuhkan di bawah Akta Suruhanjaya dan Komunikasi Multimedia Malaysia 1998. Selain itu, beberapa agensi atau institusi juga ditubuhkan. Antaranya termasuklah Majlis Keselamatan Negara (MKN), Cybersecurity Malaysia dan Agensi Keselamatan Siber Negara (NACSA).

Agensi Keselamatan Siber Negara ditubuhkan secara rasmi pada bulan Februari 2017. Institusi ini ialah agensi kerajaan yang bertanggungjawab dalam usaha untuk mempertingkatkan tahap kesiapsiagaan keselamatan siber negara dengan cara memperkukuh tindakan bagi menangani ancaman siber yang merangkumi empat perkara yang antaranya termasuklah perlindungan terhadap sistem kritikal Negara (Jabatan Perdana Menteri, 2022).

Namun begitu, usaha ini masih belum mencukupi kerana akta yang lebih khusus masih diperlukan bagi mengawal keselamatan negara daripada ancaman siber. Dengan erti kata lain, undang-undang siber yang sedia ada tidak mampu menyelesaikan isu ancaman siber secara komprehensif. Sebagai contoh, perbuatan buli siber masih belum dapat ditangani sepenuhnya menerusi Akta Jenayah Komputer 1997 dan Akta Perlindungan Data Peribadi 2010 (Akta 709). Oleh itu, jika kes buli siber berlaku, mahkamah perlu merujuk akta yang berkaitan, seperti Kanun Keseksaan, Akta Keterangan 1950, Akta Komunikasi dan Multimedia 1998 dan beberapa akta lain.

Hal ini bermakna, penggunaan undang-undang siber perlu disokong oleh undang-undang lain yang berkaitan, dikaji semula dan dipinda dari semasa ke semasa mengikut perkembangan teknologi. Di samping itu, undang-undang keselamatan siber di negara lain dan undang-undang antarabangsa juga harus dirujuk dan dijadikan panduan.

SERANGAN SIBER DI MALAYSIA

Pada bulan Mei 2024, Ensign InfoSecurity (Ensign), penyedia penyelesaian keselamatan siber komprehensif terbesar di Asia melaporkan bahawa hampir 40 peratus serangan siber di Malaysia melibatkan akaun pembuatan dan sektor kerajaan pada tahun 2023. Dalam Laporan Landskap Ancaman Siber Ensign, tiga sektor sasaran utama ialah pembuatan (20 peratus), kerajaan (18.2 peratus), serta teknologi, media dan telekomunikasi (14.5 peratus) (Bernama, 2024b). Hal ini menunjukkan bahawa sektor yang tersenarai dalam 11 sektor Infrastruktur Maklumat Kritikal Negara (IMKN) berada dalam ancaman.

Sejajar dengan ancaman siber yang makin serius, pada 26 Ogos 2024, Akta Keselamatan Siber 2024 (Akta 854) dikuatkuasakan bagi meningkatkan perlindungan terhadap sistem keselamatan negara (Majlis Keselamatan Negara, 2024). Selain Malaysia, kepentingan penjagaan keselamatan siber turut dipertingkatkan di negara, seperti Amerika Syarikat, Britain dan Singapura. Jika akta ini dibandingkan dengan kandungan Akta 854 dan Akta Keselamatan Siber 2018 Singapura yang dipersetujui dan diluluskan oleh presidennya pada 2 Mac 2018, dapat disimpulkan bahawa kedua-dua akta ini mempunyai objektif yang hampir sama. Penekanan turut diberikan terhadap CII dan ancaman siber, kesan ancaman tersebut dan cara untuk menangani insiden siber atau serangan siber.

AKTA KESELAMATAN SIBER 2024 (AKTA 854) DAN PERATURAN YANG BERKAITAN

Akta 854 digubal dan dilaksanakan bagi tujuan mempertingkatkan tahap keselamatan siber negara. Akta ini mengandungi sembilan bahagian (I-IX) dan 64 seksyen. Bahagian 1 yang terdiri daripada Seksyen 1 hingga Seksyen 4 mengandungi penerangan terhadap aplikasi akta ini dan definisi beberapa terma. Bahagian II mengandungi penerangan tentang penubuhan Jawatankuasa Keselamatan Siber Negara (JKSN). Bahagian III memperuntukkan penentuan perihal tugas dan kuasa Ketua Eksekutif NACSA. Bahagian IV pula terkandung pelantikan peneraju sektor IMKN,

penyataan fungsi dan tugas peneraju sektor IMKN dan entiti IMKN, serta pengurusan ancaman keselamatan siber. Bahagian V mengandungi Kod Amalan. Dalam Bahagian VI diperincikan tentang kawal selia pembekal perkhidmatan keselamatan siber melalui pelesenan. Seterusnya, Bahagian VII mengandungi insiden keselamatan siber terhadap IMKN. Selanjutnya, Bahagian VIII terkandung penguatkuasaan. Akhir sekali, Bahagian IX mengandungi aspek umum, termasuklah rayuan, penyerahan dokumen dan lain-lain hal yang berkaitan.

Di samping akta ini, terdapat lima peraturan yang bertujuan untuk memperincikan pelaksanaan dan penguatkuasaan akta ini. Setiap peraturan merujuk seksyen yang berkaitan. Contohnya, dalam Seksyen 60 AKS, diterangkan kuasa menteri dan wang kompaun yang dimasukkan di bawah Wang Disatukan Kerajaan (Seksyen 60). Peraturan ini menurut National Cyber Security Agency (t.t.), diperincikan seperti yang berikut:

1. Peraturan Keselamatan Siber (Pengkompaunan Kesalahan) 2024 membolehkan NACSA mengeluarkan kompaun bagi kesalahan tertentu di bawah Akta 854 dan menerangkan tatacara mengkompaun (rujuk Seksyen 60).

2. Peraturan Keselamatan Siber (Pemberitahuan Insiden Keselamatan Siber) 2024 menetapkan keperluan bagi organisasi untuk melaporkan insiden keselamatan siber kepada NACSA secara elektronik (rujuk Seksyen 23 dan Seksyen 63). Menurut Peraturan 2(1), orang yang diberi kuasa bagi entiti infrastruktur maklumat kritikal negara hendaklah memberitahu dengan segeranya, melalui cara elektronik mengenai suatu insiden keselamatan siber yang telah atau mungkin telah berlaku sebagaimana yang diperuntukkan di bawah Seksyen 23 apabila insiden keselamatan siber itu diketahui oleh entiti infrastruktur maklumat kritikal negara. Laporan hendaklah disediakan dalam tempoh enam jam dari insiden tersebut diketahui.

3. Peraturan Keselamatan Siber (Tempoh bagi Penilaian Risiko Keselamatan Siber dan Audit) 2024 menetapkan keperluan bagi organisasi untuk melakukan penilaian risiko keselamatan siber atau risiko kerentanan dan audit secara berkala. (rujuk Seksyen 63). Peraturan ini juga menerangkan makna risiko keselamatan siber.

4. Peraturan Keselamatan Siber (Pelesenan Pemberi Perkhidmatan Keselamatan Siber) 2024 menetapkan keperluan pelesenan bagi penyedia perkhidmatan keselamatan siber, serta mentafsirkan maksud "kerentanan" dan lain-lain. (rujuk Seksyen 63).

5. Perintah Keselamatan Siber (Pengecualian) 2025 (rujuk Seksyen 61). Bermula pada 1 Februari 2025, Perintah no. 2 menyatakan bahawa menteri diberi kuasa untuk mengecualikan pihak yang berikut daripada semua peruntukan akta:

    i. Amazon Data Services Malaysia Sdn. Bhd.
    ii. Amazon Web Services Malaysia Sdn. Bhd.
    iii. Google Asia Pacific Pte. Ltd.
    iv. Google Cloud Malaysia Sdn. Bhd.
    v. Google Malaysia Sdn. Bhd.
    vi. Microsoft Knowledge Capital Centre Sdn. Bhd.
    vii. Microsoft (Malaysia) Sdn. Bhd.
    viii. Microsoft Payments (Malaysia) Sdn. Bhd.
    ix. Pearl Computing Malaysia Sdn. Bhd.

Secara umumnya, setiap syarikat perlu memohon lesen perkhidmatan, tetapi Akta 854 mengecualikan syarikat tersebut. Pengecualian dilakukan terhadap sembilan syarikat yang beroperasi di Malaysia kerana syarikat ini terlibat dalam pengendalian perkhidmatan awan, pengurusan data dan infrastruktur digital (Digital Policy Alert, 2025).

BAHAGIAN I (SEKSYEN 1 HINGGA SEKSYEN 4): PENDAHULUAN

Bahagian ini menyatakan bahawa Akta 854 ini juga dikenali sebagai Akta Keselamatan Siber 2024 selepas digazetkan. Akta ini mengikat Kerajaan Persekutuan dan Kerajaan Negeri, tetapi kedua-duanya tidak bertanggungjawab atau tidak boleh didakwa atas sebarang kesalahan di bawah akta ini (Seksyen 2 (2)). Pengecualian ini menimbulkan persoalan tentang kerasionalan di baliknya. Akta ini juga terpakai kepada sesiapa sahaja, sama ada rakyat Malaysia atau tidak, dan merangkumi kesalahan siber yang dilakukan di dalam atau di luar Malaysia (bidang kuasa luar wilayah) dan kesalahan terhadap IMKN yang sebahagiannya atau keseluruhan berada di Malaysia (Seksyen 3).

Seksyen 4 mengandungi definisi terhadap terma yang terdapat dalam Bahagian II hingga IX Akta 854. Antaranya termasuklah definisi komputer yang mempunyai banyak persamaan dengan maksud "komputer" dalam Akta Keterangan 1950 (AK) dan Akta Jenayah Komputer 1997 (AJK). Terdapat juga definisi pada terma "sistem komputer", "Ketua Eksekutif", "Sektor IMKN", "ancaman keselamatan siber", "keselamatan siber" dan

"entiti Kerajaan". "Ancaman keselamatan siber" bermaksud tindakan atau aktiviti terhadap komputer atau melalui komputer atau sistem komputer tanpa kuasa yang sah yang mungkin segera membahayakan atau mungkin memberikan kesan buruk terhadap keselamatan siber komputer tersebut atau sistem komputer atau komputer lain atau sistem komputer yang lain. Maksud ini tidak jauh berbeza daripada maksud "insiden keselamatan siber". Hanya terdapat sedikit perbezaan melalui penambahan kata "*may imminently*" dan "*may*" pada maksud "ancaman keselamatan siber".

"Keselamatan siber" pula bermaksud keadaan apabila sebuah komputer atau sistem komputer dilindungi daripada sebarang serangan atau capaian tanpa kebenaran disebabkan oleh: (a) Komputer atau sistem komputer tersebut terus tersedia dan beroperasi; (b) Integriti komputer atau sistem komputer dapat dikekalkan, dan (c) Integriti dan kerahsiaan informasi yang disimpan, diproses oleh atau dihantar melalui komputer atau sistem komputer dapat dikekalkan.

Menurut Nur Sarida Mohd Daud @ Mohd Fuad dan Ahmad Rizal Mohd Yusof (2022), keselamatan siber merujuk aspek perlindungan yang digunakan untuk melindungi perisian, perkakasan (peranti mudah alih, seperti telefon pintar) dan rangkaian internet daripada serangan penggodam, serta pihak yang tidak bertanggungjawab. Keselamatan siber juga dapat dijelaskan sebagai teknologi, proses dan amalan yang direka bentuk untuk melindungi rangkaian, peranti, program dan data daripada serangan, kerosakan atau capaian tanpa kebenaran yang dilakukan oleh pihak yang tidak bertanggungjawab, sama ada individu atau organisasi. Namun begitu, susunan terma yang diberikan maksud ini tidak mengikut abjad seperti dalam akta lain.

BAHAGIAN II (SEKSYEN 5 HINGGA SEKSYEN 9): JAWATANKUASA KESELAMATAN SIBER NEGARA

Bahagian ini mengandungi penerangan tentang pihak yang berkuasa dan peranannya dalam pengawalan keselamatan siber. Jawatankuasa Keselamatan Siber Negara (JKSN) terdiri daripada 13 orang anggota, iaitu perdana menteri (pengerusi), timbalan pengerusi (dalam kalangan menteri yang berkaitan, ketua setiausaha, ketua pasukan pertahanan, ketua polis negara, ketua pengarah keselamatan negara dan dua orang yang berpengalaman dalam keselamatan siber. Ketua eksekutif bertindak sebagai setiausaha jawatankuasa ini dan Ketua Eksekutif Agensi Keselamatan Siber Negara (NACSA).

Seksyen 6 hingga Seksyen 9 antara lain mengandungi penerangan fungsi atau tugas jawatankuasa, pengendalian mensyuarat dan perlantikan subjawatankuasa. Penggunaan video langsung atau televisyen dibenarkan ketika mensyuarat. Antara tugas jawatankuasa termasuklah merancang, merumuskan dan menentukan polisi yang berkaitan dengan keselamatan siber negara, menasihati dan memberikan cadangan kepada kerajaaan persekutuan mengenai polisi dan langkah strategik untuk mengukuhkan keselamatan siber negara dan mengawasi, serta memantau keberkesanan pelaksanaan akta ini dan lain-lain tugas.

BAHAGIAN III (SEKSYEN 10 HINGGA SEKSYEN 14): TUGAS DAN KUASA KETUA EKSEKUTIF

Bahagian ini menekankan tanggungjawab atau kewajipan yang perlu dilakukan oleh ketua eksekutif dan kuasa yang dimiliki sebagai Ketua Eksekutif NACSA dan seorang daripada Jawatankuasa Keselamatan Siber Negara.

Secara umumnya, ketua eksekutif mempunyai tujuh tanggungjawab. Antaranya termasuklah menasihati dan mencadangkan polisi, strategi dan langkah strategik yang berkaitan dengan keselamatan siber negara kepada jawatankuasa (Seksyen 10 (1)(a)). Jawatankuasa pula perlu melakukan tugasan yang sama dan melaporkan kepada Kerajaan Persekutuan (Seksyen 6(1)(d)).

Ketua eksekutif juga perlu menubuhkan Pusat Penyelarasan Siber Negara (NC4). Pusat ini ialah agensi di bawah NACSA dan bertanggungjawab memantau tahap ancaman siber terhadap negara (National Cyber Coordination and Command Centre, t.t.). Penubuhan NC4 amat penting dan sangat berfungsi untuk memberikan amaran tentang ancaman siber dan insiden siber terhadap masyarakat dan negara. Data yang disimpan di pusat ini dapat dicapai oleh sesiapa sahaja yang dibenarkan oleh ketua eksekutif (Seksyen 11).

Seksyen 12 hingga Seksyen 14 pula mengandungi penerangan tentang kuasa yang ada pada ketua eksekutif. Ketua eksekutif boleh melantik pakar yang berkelayakan dalam bidang keselamatan siber secara bertulis jika perlu (Seksyen 12); mengeluarkan arahan untuk memastikan pematuhan akta ini apabila perlu dan boleh membatalkan, mengubah, menyemak semula atau meminda arahan tersebut (Seksyen 13). Selain itu, ketua eksekutif juga berkuasa untuk mengumpulkan maklumat jika mempunyai alasan yang munasabah untuk mempercayai bahawa seseorang itu mempunyai

maklumat, butiran atau dokumen atau seseorang itu berkemampuan untuk memberikan keterangan atau bukti yang berdasarkan alasan munasabah yang berkaitan dengan tugasan dan kuasanya (Seksyen 14(1)(a)(b)).

Jika berpuas hati dengan perkara dalam Seksyen 14(1)(a) dan Seksyen 14(1)(b), ketua eksekutif boleh memberikan notis bertulis kepada individu tersebut untuk memberikan maklumat dalam tempoh yang dinyatakan, mengeluarkan dokumen secara fizikal atau elektronik dan membuat salinan dan menyerahkan kepada ketua eksekutif dalam tempoh yang ditetapkan. Ketua eksekutif juga boleh mengarahkan individu, syarikat atau rakan kongsi untuk tampil memberikan keterangan secara lisan atau bertulis atau menyerahkan dokumen seperti yang diarahkan dalam notis.

Jika dokumen tiada dalam jagaan atau milikan individu tersebut, ketua eksekutif boleh mengarahkan individu tersebut untuk menyatakan lokasi dokumen tersebut mungkin didapati sepanjang pengetahuan dan kepercayaannya dan mengenal pasti orang terakhir yang menjaga atau memiliki dokumen tersebut. Dokumen yang dikeluarkan ini mesti betul, tepat dan lengkap. Pihak yang mendedahkan maklumat atau dokumen seperti yang dinyatakan dalam notis tidak perlu didakwa atas sebarang kesalahan di bawah mana-mana prosiding atau apa-apa kontrak, perjanjian atau susunan/perancangan.

Pematuhan terhadap arahan ketua eksekutif ini wajib. Jika gagal, orang yang menerima arahan atau notis dianggap melakukan kesalahan dan boleh didenda tidak melebihi RM200,000 atau dipenjarakan dalam tempoh tiga tahun atau kedua-duanya sekali. Hukuman yang sama akan dikenakan bagi kesalahan memberikan kenyataan palsu atau mengemukakan dokumen palsu (Seksyen 14(2)(3)(7)). Bahagian lain akta ini juga menekankan kuasa ketua eksekutif.

Peruntukan ini menunjukkan bahawa ketua eksekutif mempunyai tugas yang agak mencabar dan perlu menggunakan kuasa yang ada secara berhemah dan teliti.

BAHAGIAN IV (SEKSYEN 15 HINGGA SEKSYEN 24): INFRASRTUKTUR MAKLUMAT KRITIKAL NEGARA (IMKN) – PENERAJU SEKTOR DAN ENTITI IMKN

Infrastruktur Maklumat Kritikal Negara (IMKN) merujuk sistem kritikal yang merangkumi aset maklumat (elektronik), rangkaian, fungsi, proses, kemudahan, dan perkhidmatan dalam sekitaran teknologi maklumat

yang penting untuk negara yang sebarang gangguan atau kemusnahan terhadapnya dapat memberikan impak terhadap pertahanan dan keselamatan negara, kestabilan ekonomi negara, imej negara, keupayaan kerajaan untuk berfungsi, kesihatan dan keselamatan awam, serta privasi individu (Jabatan Perdana Menteri, 2022). Bahagian ini merangkumi entiti kerajaan yang dinyatakan di bawah Seksyen 3.

Terdapat 11 sektor IMKN yang dinyatakan dalam jadual akta ini, iaitu: (1) Kerajaan; (2) Pertahanan dan Keselamatan Negara; (3) Perbankan dan Kewangan; (4) Informasi dan Komunikasi; (5) Tenaga; (6) Pengangkutan; (7) Perkhidmatan Kecemasan; (8) Air; (9) Perkhidmatan Kesihatan; (10) Pertanian dan Penanaman; (11) Perdagangan, Industri dan ekonomi.

Menerusi Seksyen 15, Menteri Komunikasi/Digital (atas rekomendasi Ketua Eksekutif) dibenarkan untuk melantik entiti kerajaan atau sesiapa sahaja untuk menjadi peneraju sektor IMKN bagi setiap sektor dalam IMKN. Nama peneraju sektor dipaparkan dalam laman NACSA (Seksyen 15). Entiti kerajaan bermaksud (Seksyen 4) mana-mana kementerian, jabatan, pejabat, agensi dan sesiapa yang berada di bawah kerajaan persekutuan dan negeri, termasuklah pihak berkuasa tempatan.

Dalam Seksyen 16 diterangkan fungsi peneraju sektor IMKN bagi memastikan semua yang berkenaan melaksanakan peranan masing-masing. Tindakan yang diambil masih tertakluk pada keputusan oleh ketua eksekutif. Antara fungsi peneraju sektor IMKN termasuklah menetapkan entiti IMKN (Seksyen 17 dan Seksyen 18), mengadakan Tataamalan (Seksyen 25), melaksanakan keputusan Jawatankuasa dan Arahan di bawah Akta 854, memantau entiti IMKN ketika melakukan tugasannya dan memastikan segala tanggungjawab yang diberikan dilaksanakan. Contohnya, entiti IMKN hendaklah memaklumkan secara notis bertulis kepada peneraju sektor IMKN tanpa berlengah jika komputer atau sistem komputernya berhenti beroperasi sebagai IMKN (Seksyen 17 (6)(a)).

Penetapan entiti merangkumi entiti kerajaan atau mana-mana pihak yang memiliki atau mengendalikan Infrastruktur Maklumat Kritikal Negara (IMKN) (Seksyen 17(1)). Peneraju sektor IMKN boleh membatalkan pelantikan sesuatu entiti IMKN melalui notis bertulis sekiranya entiti tersebut tidak lagi mengendalikan IMKN (Seksyen 19). Pembatalan ini harus dilaporkan kepada ketua eksekutif. Seksyen 20 hingga Seksyen 23 mengandungi penekanan terhadap tanggungjawab entiti IMKN untuk melaksanakan tugasan seperti yang berikut:

1. Memberikan maklumat mengenai sektor IMKN yang dimiliki atau dikendalikan olehnya kepada peneraju sektor IMKN jika diminta berbuat demikian. Entiti IMKN perlu mematuhi permintaan tersebut (Seksyen 20).

2. Melaksanakan langkah standard dan proses seperti yang dinyatakan dalam tata amalan bagi memastikan keselamatan siber terhadap IMKN yang dimiliki atau dikendalikan oleh entiti IMKN. Kegagalan untuk mematuhi peruntukan ini boleh mengakibatkan, jika disabitkan kesalahan, denda hingga RM500,000 atau hukuman penjara tidak melebihi 10 tahun, atau kedua-duanya sekali. Penggunaan langkah, standard atau proses alternatif dibenarkan jika ketua eksekutif berpuas hati (Seksyen 21).

3. Melakukan penilaian risiko keselamatan siber terhadap IMKN yang dimiliki atau di bawah operasinya mengikut tataamalan dan melakukan audit untuk memastikan entiti IMKN mematuhi akta ini. Laporan penilaian risiko dan audit perlu dihantar dalam tempoh 30 hari kepada ketua eksekutif. Jika terdapat perubahan pada rekaan, konfigurasi, keselamatan atau operasi IMKN, ketua eksekutif hendaklah memberikan notis bertulis kepada entiti IMKN untuk melakukan semula penilaian risiko dan audit (Seksyen 22). Entiti ini juga perlu memaklumkan kewujudan insiden keselamatan siber kepada ketua eksekutif jika ada. Jika Seksyen 23 gagal dipatuhi, entiti tersebut boleh didenda tidak melebihi RM500,000 atau dipenjarakan tidak melebihi 10 tahun atau kedua-duanya sekali (Seksyen 23).

Seksyen 24 pula membolehkan ketua eksekutif mengadakan latihan keselamatan siber untuk menguji kesediaan mana-mana entiti IMKN bagi menghadapi ancaman keselamatan siber dan insiden keselamatan siber. Notis harus diberikan terlebih dahulu sebelum mengadakan latihan. Ketua eksekutif juga boleh mengarahkan entiti IMKN jika diperlukan dan arahan tersebut mesti dipatuhi. Jika mana-mana entiti IMKN gagal mengikut arahan, denda tidak melebihi RM100,000 boleh dikenakan, tetapi tiada hukuman penjara diperuntukkan bagi kesalahan ini.

BAHAGIAN V (SEKSYEN 25 DAN SEKSYEN 26): TATAAMALAN

Seksyen 25 ini berkaitan dengan Seksyen 21 yang menekankan tanggungjawab untuk melaksanakan tataamalan yang disediakan oleh peneraju sektor IMKN. Beberapa perkara perlu dipertimbangkan termasuklah fungsi entiti IMKN dan peruntukan yang berkaitan dengan keselamatan siber dalam mana-mana undang-undang bertulis yang terpakai untuk peneraju sektor IMKN. Dalam Seksyen 26, sebarang bentuk arahan

oleh peneraju sektor IMKN terhadap entiti IMKN haruslah konsisten dan selaras dengan tataamalan. Tataamalan ini dapat menjadi panduan bagi peneraju sektor IMKN dan entiti untuk melaksanakan tanggungjawab dengan baiknya.

BAHAGIAN VI: PEMBEKAL PERKHIDMATAN KESELAMATAN SIBER

Seksyen 27 hingga Seksyen 34 mengandungi penerangan tentang keperluan untuk mendapatkan lesen oleh pembekal perkhidmatan keselamatan siber, kelayakan yang diperlukan oleh pemohon dan akibat daripada kegagalan berbuat demikian. Dalam hal ini, setiap pembekal perlu mendapatkan lesen. Keperluan ini adalah selaras dengan syarat yang dikenakan terhadap penyedia perkhidmatan internet di bawah Akta Komunikasi dan Multimedia 1998 (Seksyen 263), yang mewajibkan pemegang lesen untuk memastikan rangkaian atau perkhidmatan internet tidak disalahgunakan bagi tujuan jenayah. Namun begitu, tiada definisi atau penerangan tentang jenis perkhidmatan yang ditawarkan oleh pembekal. Jika gagal berbuat demikian, denda tidak melebihi RM500,000 atau dipenjarakan dalam tempoh 10 tahun atau kedua-duanya sekali akan dikenakan (Seksyen 27). Pemohon perlu memenuhi syarat yang ditentukan oleh ketua eksekutif dan tidak pernah disabitkan dengan kesalahan jenayah, seperti penipuan, tidak jujur atau pecah amanah atau kelakuan buruk atau tidak bermoral (Seksyen 28). Permohonan dan pembaharuan lesen boleh dihantar kepada ketua eksekutif dan pemohon perlu membayar yuran yang ditetapkan oleh ketua eksekutif. Namun begitu, lesen terbabit boleh dikeluarkan dengan bersyarat, ditukar, dibatalkan atau digantung (Seksyen 29, Seksyen 30, Seksyen 31 dan Seksyen 33).

Pemegang lesen diwajibkan untuk menyimpan rekod perkhidmatan yang disediakan, dan rekod tersebut perlu lengkap dan mempunyai maklumat terperinci seperti yang dikehendaki di bawah Seksyen 32. Lesen tersebut tidak boleh dipindahkan atau diserahkan kepada orang lain. Jika syarat ini gagal dipatuhi, pesalah tersebut didenda tidak lebih RM200,000 atau dipenjarakan dalam tempoh tiga tahun atau kedua-duanya sekali (Seksyen 34). Peruntukan ini memastikan penerima lesen melakukan tugas dengan jujurnya dan apa-apa sahaja masih tertakluk pada budi bicara atau kuasa ketua eksekutif.

BAHAGIAN VII: INSIDEN KESELAMATAN SIBER

Bahagian ini berkaitan dengan Seksyen 23 yang meletakkan tanggungjawab kepada entiti IMKN untuk melaporkan insiden keselamatan siber. Seksyen 35 memfokuskan penyiasatan terhadap insiden yang dilaporkan. Ketua eksekutif akan mengarahkan pegawai yang diberi kuasa untuk melakukan siasatan, sama ada wujud insiden tersebut atau sebaliknya. Laporan atau hasil siasatan akan dikaji, seterusnya ketua eksekutif akan mengeluarkan arahan kepada entiti IMKN yang memiliki atau mengendalikan IMKN terbabit untuk mengambil langkah sewajarnya bagi mencegah kejadian tersebut berulang pada masa hadapan.

Selain itu, Cybersecurity Malaysia turut mengeluarkan statistik insiden keselamatan siber yang menunjukkan bahawa terdapat sebanyak 5917 kes pada tahun 2023. Jumlah kes penipuan sebanyak 3705, manakala kes kecurian identiti meningkat kepada 1192 kes berbanding dengan hanya 50 kes pada tahun 2022. Penipuan internet turut melibatkan isu dadah dan penipuan cinta. Dalam kes seperti ini, pakar forensik yang berkaitan dengan keselamatan siber dipanggil untuk memberikan keterangan di mahkamah dalam kes *Maria Elvira Pinto Exposto* lwn *Pendakwa Raya* [2020] 3 *MLJ* 21 dan *Murugan a/l Manoharan* lwn *Pendakwa Raya* [2017] 6 *MLJ* 23. Pelanggaran data yang berkaitan dengan maklumat pengenalan peribadi (PII) sangat mudah berlaku kerana PII dapat diperoleh melalui laman sesawang dan disebarkan dan dijual secara terbuka (Opalyn Mok, 2024).

BAHAGIAN VIII: PELAKSANAAN

Bahagian ini amat penting untuk memastikan akta ini dilaksanakan dengan berkesannya dan mencukupi. Seksyen 36 hingga Seksyen 38 membenarkan pegawai kerajaan yang diberi kuasa oleh menteri sahaja untuk melakukan siasatan yang berkaitan dengan insiden keselamatan siber. Pegawai tersebut perlu menunjukkan kad kuasa kepada orang yang dikenakan tindakan dan dirinya mempunyai kuasa, seperti pegawai polis yang berpangkat sebagaimana yang dinyatakan dalam Kanun Prosedur Jenayah (KPJ) (Akta 593).

Seksyen 39 hingga Seksyen 44 mengandungi penerangan tentang proses penggeledahan dan penyitaan yang boleh dilakukan oleh pegawai yang diberi kuasa di bawah Seksyen 36. Contoh barang yang boleh disita ialah dokumen atau komputer yang dapat membantu pembuktian kes jenayah yang dilakukan. Menurut Seksyen 3 Akta Keterangan 1950 (Akta 56) dan Seksyen 2 Akta Jenayah Komputer 1997 (Akta 563), istilah "dokumen"

merangkumi peranti elektronik, magnet, optik, elektrokimia, atau peranti berbentuk pemprosesan data lain. Oleh itu, telefon bimbit, cakera padat dan sistem kamera litar tertutup juga tergolong sebagai dokumen dan boleh dijadikan bahan bukti yang sah untuk disita oleh pegawai berkuasa (Malaysia, 1950; Malaysia, 1997). Pembuktian melibatkan pakar forensik daripada Pusat Keselamatan Siber yang akan memberikan keterangan mengenai kes jenayah siber atau yang bukan melibatkan jenayah siber.

Majistret pula diberi kuasa untuk mengarah dan mengeluarkan waran kepada pegawai yang dinyatakan ini untuk melakukan penggeledahan dan penyitaan di tempat yang digunakan untuk melakukan jenayah di bawah akta ini atau di mana-mana tempat yang perlu dilakukan siasatan tanpa mengira waktu, sama ada siang atau malam. Tindakan ini dapat dilakukan dengan bantuan atau tanpa bantuan, dan pegawai tersebut boleh memasuki premis berkenaan secara paksa jika perlu. Penyitaan dan penggeledahan perlu dilakukan menurut prosedur yang dinyatakan dalam akta ini dan KPJ. Berdasarkan KPJ, majistret juga diberi kuasa untuk mengeluarkan perintah atau arahan. Seksyen 9 KPJ memperuntukkan bidang kuasa jenayah majistret. Antaranya termasuklah kuasa seperti yang berikut:

> Seksyen 9 (e) mengeluarkan waran untuk geledah atau menyebabkan digeledah tempat-tempat yang di dalamnya apa-apa barang curi atau apa-apa juga barang-barang, perkakas atau benda-benda yang dengannya atau bersangkut paut dengannya sebarang kesalahan telah dilakukan dikatakan ada disimpan atau disembunyikan, dan menghendaki orang-orang supaya memberi jaminan untuk keamanan atau supaya mereka berkelakuan baik menurut undang-undang.

Terdapat tiga bahagian atau bab yang berkaitan dengan pelaksanaan dalam KPJ, iaitu Bab IV – Bab VI. Bab IV berkenaan tangkapan, melepaskan diri dan menangkap semula (Seksyen 15 hingga Seksyen 33). Bab V tentang proses memaksa kehadiran (Seksyen 34 hingga Seksyen 50). Bab VI pula mengandungi proses pemaksaan penyerahan dokumen dan lain-lain harta alih dan penemuan orang yang dikurung secara salah (Seksyen 51 hingga Seksyen 65). Sebagai contoh, menerusi Seksyen 62 KPJ, penggeladahan tanpa waran dibenarkan dan peruntukan ini juga terdapat dalam Seksyen 40 Akta 854 atau AKS 2024. Hal ini termasuklah penutupan atau pemeteraian barang rampasan yang tidak boleh dibawa keluar atau digerakkan. Sesiapa yang didapati merosakkan atau membuka barang yang telah ditutup atau dimeterai ini boleh didenda tidak melebihi RM100,000 atau dipenjarakan dalam tempoh dua tahun atau kedua-duanya sekali (Seksyen 39).

Penggeledahan dan penyitaan juga boleh dilakukan tanpa waran jika pegawai yang diberi kuasa mempercayai bahawa kelewatan mengambil tindakan ini dapat memberikan kesan buruk terhadap proses penyiasatan atau bukti kesalahan jenayah berkemungkinan akan diusik, dibuang atau dirosakkan (Seksyen 40). Pegawai yang berkuasa perlu menyediakan senarai barang rampasan dan menunjukkannya kepada pemilik premis yang digeledah dan menandatangani senarai tersebut (Seksyen 41). Pihak yang disabitkan dengan kesalahan juga perlu membayar kos penyimpanan barang rampasan yang disimpan sehingga prosiding kes berakhir (Seksyen 42). Barang yang disita atau dirampas akan dilepaskan atau dikembalikan kepada orang yang layak, namun mana-mana pegawai yang diberi kuasa perlu merekodkan sebab pelepasan atau pengembalian barang tersebut dan rekod itu perlu dihantar kepada timbalan pendakwa raya seberapa segera yang praktikal (TPR @ DPP) (Seksyen 43).

Seterusnya, Seksyen 44 memperuntukkan bahawa apa-apa objek/ barang yang telah diambil atau dirampas akan diberikan perlucutan hak melalui perintah mahkamah. Akan tetapi, sesiapa yang mengakui bahawa dirinya pemilik barang tersebut perlu memberikan notis tuntutan kepada pegawai yang diberi kuasa. Kemudian, majistret yang menerima notis tersebut daripada pegawai berkenaan akan mengeluarkan saman untuk memanggil orang yang menuntut supaya hadir ke mahkamah bagi memeriksa kesahihan tuntutan tersebut. Jika barang tersebut terbukti digunakan untuk melakukan kesalahan di bawah akta, majistret meneruskan prosedur pelucutan hak dan barang terbabit akan diserahkan kepada ketua eksekutif untuk proses pelupusan. Barang rampasan yang dilucuti hak menjadi milik kerajaan persekutuan (Seksyen 45)

Selain itu, pegawai yang diberi kuasa boleh mengakses data di dalam komputer yang dirampas atau diambil. Pegawai ini hendaklah diberi kata kunci yang perlu dan lain-lain perkara yang berkaitan ketika melakukan siasatan kes (Seksyen 46). Pegawai ini juga dibenarkan untuk memberikan arahan bertulis kepada sesiapa yang berkenaan untuk hadir di hadapannya dan menjalani peperiksaan lisan atau soal jawab bagi membantu siasatan kes berkenaan (Seksyen 48 dan Seksyen 49). Namun begitu, sebarang kenyataan yang diberikan kepada pegawai ini oleh sesiapa yang berkenaan ketika proses siasatan tidak boleh digunakan sebagai keterangan atau bukti (Seksyen 50). Namun begitu, mahkamah boleh merujuk kenyataan yang dibuat oleh saksi kepada pegawai tersebut ketika siasatan kes. Seksyen ini menerangkan kepentingan dan perkaitan kenyataan yang dibuat oleh saksi dan tertuduh ketika proses siasatan

dilakukan. Pegawai tersebut juga diberi kuasa tambahan oleh akta ini (Seksyen 51).

Selain itu, tiada sebarang tuntutan kos, ganti rugi atau apa-apa relief boleh dilakukan terhadap prosiding di mahkamah yang berkaitan dengan barang rampasan, kecuali rampasan dilakukan tanpa sebab yang munasabah (Seksyen 47).

Perlu diingatkan bahawa sebarang serangan, halangan, sekatan, gangguan atau penolakan terhadap ketua eksekutif atau pegawai yang diberi kuasa ketika memasuki premis untuk membuat penggeledahan dan rampasan atau pengaksesan data komputer adalah dianggap sebagai suatu kesalahan yang jika disabitkan, pesalah boleh didenda tidak melebihi RM100,000 atau dipenjarakan dalam tempoh dua tahun atau kedua-duanya sekali (Seksyen 52).

BAHAGIAN IX: UMUM

Bahagian ini bermula daripada Seksyen 53 hingga Seksyen 64 dan merangkumi pelbagai perkara yang tidak dinyatakan dalam seksyen atau peruntukan terdahulu. Antaranya termasuklah rayuan untuk mendapatkan lesen, penggunaan medium elektronik dan perkongsian syarikat, serta liabiliti pengarah syarikat.

Seksyen 53 mengandungi rayuan oleh pihak yang gagal mendapatkan lesen atau lesennya dibatalkan atau digantung yang perlu dilakukan dalam tempoh 30 hari dari tarikh lesennya digantung. Dalam hal ini. menteri berhak untuk mengetepikan rayuan atau mengesahkan keputusan. Bagi Seksyen 54, dinyatakan bahawa medium elektronik dibenarkan untuk menghantar dokumen atau maklumat. Menerusi Seksyen 55, jawatankuasa, ketua eksekutif atau pegawai yang diberi kuasa perlu mengekalkan rahsia dan tidak berkongsi sebarang maklumat yang diperoleh ketika bertugas. Dalam Seksyen 56, pihak yang dinyatakan dalam Seksyen 55 tidak boleh disaman disebabkan oleh kecuaian atau kesalahan ketika melaksanakan tugas melainkan terdapat bukti bahawa kegagalan itu disebabkan oleh niat jahat dan tanpa sebarang kuasa tindakan yang munasabah. Melalui Seksyen 57, sebarang pendakwaan bagi kesalahan di bawah akta ini tidak dibenarkan untuk dimulakan melainkan dengan persetujuan bertulis daripada pendakwa raya. Seksyen 58 pula memperincikan tanggungjawab pengarah syarikat. Dalam kes ini, syarikat perkongsian, semua rakan kongsi sama-sama bertanggungjawab melainkan terbukti kesalahan itu dilakukan tanpa pengetahuan dan persetujuan mereka. Dalam Seksyen 59,

ditekankan tentang tanggungan atau liabiliti majikan terhadap pekerja yang melakukan kesalahan ketika bertugas atau ketika mewakili majikannya.

Seksyen 60 hingga Seksyen 63 memberikan kuasa kepada menteri untuk membuat peraturan, menetapkan sesuatu dan lain-lain. Antaranya termasuklah menteri dibolehkan, dengan kelulusan pendakwa raya untuk membuat peraturan, iaitu menetapkan apa-apa kesalahan di bawah akta ini sebagai kesalahan yang boleh dikenakan kompaun dan prosedur kompaun tersebut. Ketua eksekutif dibenarkan untuk mengenakan kompaun dan tindakan ini boleh dilakukan sebelum kesalahan tersebut didakwa dan dimulakan di mahkamah. Menerusi Seksyen 60, wang kompaun ini dimasukkan dalam Wang Disatukan Kerajaan. Dalam Seksyen 61 dikecualikan sesiapa daripada akta ini jika sesuai untuk berbuat demikian. Seksyen 62 mengandungi pemindaan jadual selepas penerimaan cadangan daripada ketua eksekutif. Melalui Seksyen 63, peraturan dan penetapan beberapa perkara dibenarkan, jika perlu dalam pelaksanaan akta ini. Contohnya, tempoh yang diperlukan untuk melakukan penilaian risiko keselamatan siber. Malaysia boleh melihat contoh peraturan yang dihasilkan di Singapura, iaitu Cybersecurity (Critical Information Infrastructure) Regulations 2018 (Attorney-General's Chambers, 2018) dan borang yang berkaitan sebagai panduan penambahbaikan akta ini dan peraturan yang berkaitan.

Dalam Seksyen 64, diperuntukkan kecualian yang berfungsi untuk mengekalkan keberkesanan apa-apa sahaja langkah, piawaian, tahap dan proses yang telah dilaksanakan untuk memastikan keselamatan siber terhadap IMKN. Antara langkah ini termasuklah langkah yang dikenakan terhadap entiti kerajaan atau individu di bawah Arahan Majlis Keselamatan Negara No 26 (National Security Council, t.t.). Peruntukan ini memastikan bahawa semua mekanisme keselamatan telah diwujudkan akan terus terpakai bermula dari tarikh penguatkuasaannya sehinggalah dibatalkan oleh Akta Majlis Keselamatan Negara 2016 (AMK) (Akta 776) (Akta Majlis Keselamatan Negara, 2016).

KESIMPULAN

Akta 854 dan peraturan yang diwujudkan sedikit sebanyak menjadikan garis panduan atau rangka kerja yang lebih sistematik untuk NACSA dan pihak yang berkenaan untuk melindungi IMKN yang merupakan sektor kritikal dan terpenting dalam negara. Pelaksanaan Akta 854 menunjukkan bahawa Malaysia bersiap siaga bagi mempertahankan benteng keselamatan negara

daripada serangan siber. Namun begitu, berdasarkan beberapa komen dan ulasan yang dibincangkan, akta ini masih perlu dikaji, ditambah baik dan dipantau sejajar dengan perkembangan teknologi. Pandangan daripada pelbagai pihak, terutamanya pakar IT dan perundangan, perlu diambil kira bagi mencapai keberkesanan pelaksanaan akta yang maksimum walaupun ada pihak yang menganggap akta ini mengancam kebebasan bersuara atau berekspresi kerana berdasarkan Perkara 10 Perlembagaan Persekutuan, setiap warganegara Malaysia berhak untuk bebas bercakap dan bersuara, termasuklah berhimpun secara aman dan tanpa senjata (Artikel 19, 2014). Namun begitu, rakyat harus memahami bahawa melalui Perenggan (2)(a) Perlembagaan Persekutuan, parlimen boleh mengenakan apa-apa sekatan terhadap hak yang diberikan ini melalui undang-undang demi keselamatan negara dan ketenteraman awam.

RUJUKAN

Akta Jenayah Komputer 1997 (Akta 563). (1997). International Law Book Services.

Akta Keterangan 1950 (Akta 56). (1950). International Law Book Services.

Akta Majlis Keselamatan Negara 2016 (Akta 776). (2016). Majlis Keselamatan Negara. https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/Akta-MKN-2016-BM.pdf

Article 19. (2014, 4 April). Malaysia: *The Cyber Security Bill is a threat to freedom of expression online*. https://www.article19.org/resources/malaysia-the-cyber-security-bill-is-a-threat-to-freedom-of-expression-online/

Attorney-General's Chambers. (2018). *Cybersecurity (Critical Information Infrastructure) Regulations 2018* (S 519/2018). Singapore Statutes Online. https://sso.agc.gov.sg/SL-Supp/S519-2018/Published/20180830?DocDate=20180830

Bernama. (2024a, 21 Februari). Ancaman serangan siber di Malaysia terus meningkat – Kaspersky. Astro Awani. https://www.astroawani.com/berita-malaysia/ancaman-serangan-siber-di-malaysia-terus-meningkat-kaspersky-459078

Bernama. (2024b, 16 Mei). Hampir 40 peratus serangan siber di Malaysia libatkan akaun pembuatan, sektor kerajaan pada 2023. Astro Awani. https://www.astroawani.com/berita-malaysia/hampir-40-peratus-serangan-siber-di-malaysia-libatkan-akaun-pembuatan-sektor-kerajaan-pada-2023-470731

Bernama. (2025, 11 Februari). CMA amendments come into force today. Malaysiakini. https://www.malaysiakini.com/news/734221

Digital Policy Alert. (2025). *Malaysia: Prime Minister signed Cyber Security (Exemption) Order*. https://digitalpolicyalert.org/event/26571-adoption-of-cyber-security-exemption-order-2025

Fuad Nizam. (2025, 26 Mac). Cyber attack on MAHB: Hackers yet to be identified. New Straits Times. https://www.nst.com.my/news/nation/2025/03/1193233/cyberattack-mahb-hackers-yet-be-identified

Ida Madieha Abdul Ghani Azmi. (2024). The salient features of the Cyber Security Act 2024. *INSAF: The Journal of the Malaysian Bar, 41*(1), 60–78.

Ilah Hafiz Aziz. (2023, 7 Ogos). AI langkau kemampuan manusia. BH Online. https://www.bharian.com.my/berita/nasional/2023/08/1129390/ai-langkau-kemampuan-manusia

Jabatan Perdana Menteri. (2022, 1 Ogos). *Pekeliling Am Bilangan 4 Tahun 2022: Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam*. https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/PEKELILING-Pengurusan-dan-Pengendalian-Insisden-Keselamatan-Siber-Sektor-Awam.pdf

Majlis Keselamatan Negara. (2024, 26 Ogos). *Penguatkuasaan Akta Keselamatan Siber 2024 (Akta 854)*. https://www.mkn.gov.my/web/ms/2024/08/26/penguatkuasaan-akta-keselamatan-siber-2024-akta-854/

Maria Elvira Pinto Exposto lwn *Pendakwa Raya*. (2020). [2020] 3 MLJ 21.

Mok, O. (2024, 13 April). CyberSecurity Malaysia reports a steep jump in data thefts last year. Malay Mail. https://www.malaymail.com/news/malaysia/2024/04/13/cybersecurity-malaysia-reports-a-steep-jump-in-data-thefts-last-year/128617

Murugan a/l Manoharan lwn *Pendakwa Raya* [2017] 6 *MLJ* 23

National Cyber Security Agency (NACSA). (t.t.). *Best practices on data breaches prevention*. https://www.nacsa.gov.my/advisory_data_breach.php

National Cyber Security Agency. (t.t.). *Legal*. https://www.nacsa.gov.my/legal.php

National Security Council. (t.t.). *National Security Council's Directive No. 26: National Cyber Security Management (NSC Directive No. 26)*. National Cyber Security Agency (NACSA). https://www.nacsa.gov.my/directive26.php

Nur Sarida Mohd Daud @ Mohd Fuad, & Ahmad Rizal Mohd Yusof. (2022). Memahami jenayah siber dan keselamatan siber di Malaysia: Suatu pemerhatian terhadap pandangan sarjana dan intelektual. *Asian Journal of Environment, History and Heritage, 6*(1), 11–26.

Opalyn Mok. (2024, 13 April). CyberSecurity Malaysia reports a steep jump in data thefts last year. Malay Mail. https://www.malaymail.com/news/malaysia/2024/04/13/cybersecurity-malaysia-reports-a-steep-jump-in-data-thefts-last-year/128617

Personal Data Protection (Amendment) Act 2024. (2024). *Act A1727*. Jabatan Perlindungan Data Peribadi Malaysia. https://www.pdp.gov.my/ppdpv1/wp-content/uploads/2024/11/Act-A1727.pdf

PLANMalaysia. (t.t.). *Dasar Keselamatan Siber (DKS)*. https://www.planmalaysia.gov.my/planmalaysia/resources/PLANMalaysia/MainPortal/STM/%5BPLANMalaysia%5DDasar_Keselamatan_Siber-V1.0_.pdf