(2022) 4 CLI 54 – 68

Kesahan Identiti dalam Perdagangan Elektronik

(Authentication of Identity in Electronic Commerce)

JOSLYN YEO YI TIAN

ABSTRAK

Kesahan identiti merupakan kaedah yang berkesan untuk memastikan identiti pihak-pihak bertransaksi adalah sah dan sebenar seperti dikemukakan dalam perdagangan elektronik. Di Malaysia, Akta Tandatangan Digital 1997 dan Akta Perdagangan Elektronik 2006 merupakan undang-undang siber yang mengiktiraf penggunaan tandatangan digital dan tandatangan elektronik. Walau bagaimanapun, Akta Tandatangan Digital 1997 dan Akta Perdagangan Elektronik 2006 perlu dikaji semula kerana terdapat masalah kekaburan dari segi pemakaiannya. Antara isu-isu perundangan ialah sama ada identiti pelanggan dan penjual adalah sah dan sebenar seperti dikemukakan dan sama ada kontrak terbentuk dan sah timbul kepercayaan salah sangka terhadap identiti suatu pihak. Selain itu, terdapat juga isu berkenaan pemakaian sistem kripto tidak simetri yang terlalu spesifik dan kesukaran membuktikan identiti pesalah dan pengecualian liabiliti apabila kunci persendirian hilang atau disalahgunakan. Oleh itu, artikel ini akan mengenal pasti konsep dan kaedah-kaedah kesahan identiti, menganalisis isu-isu perundangan dan memberi cadangan untuk memantapkan pemakaian Akta Tandatangan Digital 1997 dan Akta Perdagangan Elektronik 2006. Pengumpulan data dilakukan dengan merujuk sumber primer dan menggunakan kaedah kualitatif . Hasil perbincangan menunjukkan bahawa perakuan yang dipasang dalam rangkaian laman sesawang dan kunci persendirian dapat mengesahkan identiti suatu pihak; sistem kripto tidak simetri adalah elemen penting bagi menjana tandatangan digital yang unik; perjanjian yang dimasuki disebabkan frod atau khilaf unilateral tidak akan mempunyai kesan undang-undang dan pelanggan bertanggungjawab untuk menjaga kunci persendirian dan kesan perundangan tandatangan tandatangan tidak boleh dinafikan jika terdapat tiada niat jahat untuk mengelak daripada tanggungan ganti rugi. Penulis mencadangkan untuk menyatukan Akta Tandatangan Digital 1997 dengan Akta Perdagangan Elektronik 2006; meratifikasikan konvensyen ECC dan; pihak-pihak bebas memilih teknologi dan akta lebih bersifat berteknologi neutral; mengkaji semula peruntukan berkenaan pembentukan kontrak elektronik dan meningkatkan kesedaran awam.

Kata kunci: kesahan identiti; perdagangan elektronik; Akta Tandatangan Digital 1997; Akta Perdagangan Elektronik 2006; Akta Transaksi Elektronik 2010.

ABSTRACT

Authentication of identity is an effective method to ensure the identity of the transacting parties is valid and true as represented in electronic commerce. In Malaysia, Digital Signature Act 1997 and Electronic Commerce Act 2006 are the cybers laws which recognize the digital signature and electronic signature. However, Digital Signature Act 1997 and Electronic Commerce Act 2006 need to be reviewed because there are several ambiguities. Among the legal issues are whether the identity of the buyer and the seller is valid and true as represented, and whether the contract is created and valid if there is a mistaken identity. There is another issue on asymmetric cryptosystem which is too specific and the difficulty to prove the identity of the wrongdoers and the exemption from liability when the private keys are missing or being misused. Therefore, this paper will identify the concept and method of authentication of identity, analyze the legal issues and provide several suggestions to improve the application of the Act. Data collection is done by referring to primary data and qualitative method. The findings show that the certificate on the website and the digital signature can authenticate the identity of the parties; asymmetric cryptosystem is important to generate unique digital signature; the contract will not have legal effect if entered upon fraud or unilateral mistake. and the subscribers are responsible to take care of their private keys and the legal effect of the signature shall not be denied if maliciously intended to avoid any claim for damages. The author suggests to combine the Digital Signature Act 1997 with the Electronic Commerce Act 2006; widen the scope of the Digital Signature Act 1997, ratify ECC and MLETR; give freedom to the parties to choose the technology and to make the Act more technologically neutral; review provisions regarding electronic contract and to increase public awareness.

Keywords: authentication of identity; electronic commerce; Digital Signature Act 1997; Electronic Commerce Act 2006; Electronic Transactions Act 2010.

PENGENALAN

Internet merupakan medium yang penting untuk memacu perkembangan ekonomi, teknologi, sosial, politik dan pelbagai bidang serta industri. Ia membantu proses komunikasi tanpa mengira sempadan negara, mengembangkan perdagangan elektronik dan memudahkan sistem pembayaran atau transaksi elektronik. Industri perdagangan elektronik di Malaysia dijangka akan menyumbang sebanyak 20.8% iaitu RM211 bilion kepada Keluaran Dalam Negeri Kasar (KDNK) menjelang tahun 2020 berdasarkan Laporan Separuh Penggal Rancangan Malaysia Ke-11 (RMK-11) 2016-2020. Pasaran jualan produk dan servis melalui platform perdagangan elektronik yang berpotensi dapat dibuktikan semasa pelaksanaan perintah Kawalan Pergerakan (PKP) pada 18 Mac 2020. Norma baharu telah meningkatkan aktiviti jual beli dalam platform perdagangan elektronik tertentu sebanyak 28.9% dalam tempoh PKP. [1]

Menurut *Oxford Dictionary of Computer Science, 7th Edition*, kesahan bermaksud suatu proses sesuatu subjek atau pengguna mewujudkan identiti mereka dalam sistem dengan menggunakan kata kunci atau pemilikan peranti yang fizikal. Identiti pula didefinisikan sebagai siapakah orang tersebut dalam *Oxford Advanced Learner's Dictionaries, 8th Edition.*

Perdagangan elektronik secara umumnya bermaksud komunikasi secara komersial antara individu atau entiti yang berlaku dalam Internet[2] (Chris Reed dan John Angel, 2011). Perdagangan elektronik terbahagi kepada *Business-to-Business* ("B2B"), *Business-to-Customer* (B2C) dan *Government-to-Citizen* (G2C). Misalnya, antara kaedah-kaedah kesahan yang dipakai untuk menegaskan sifat yang diwujudkan ialah PINs, *smartcards, biometrics*, tandatangan digital dan lain-lain. Dalam pada itu, penggunaan tandatangan digital digunakan dalam perdagangan elektronik melalui *E-invoice, E-mail Security services*[3]dan perbankan internet[4], kontrak pekerjaan, perjanjian jual beli, perjanjian pengguna dalam pembukaan akaun baru, dan lain-lain.

Di Malaysia, Akta Tandatangan Digital 1997 yang dikuatkuasakan pada 1 Oktober 1998 merupakan akta yang mengawal tandatangan digital dan tertakluk di bawah Undang-undang Siber. Jadi, peruntukan undang-undang berkenaan tandatangan digital perlu merujuk akta ini. Sebelum itu, Akta Tandatangan Digital Utah 1995 (*Utah Digital Signature Act 1995*) merupakan undang-undang pertama yang mengiktiraf tandatangan digital, merangka peruntukan undang-undang tentang pelesenan dan peraturan pihak berkuasa pemerakuan. Pada tahun 2006, Akta Perdagangan Elektronik 2006 dikuatkuasa pada 19 Oktober 2006 bagi mengiktiraf dan mempermudah transaksi komersial dan kontrak dalam perdagangan elektronik.

Seksyen 2 Akta Tandatangan Digital 1997 mendefinisikan tandatangan digital berasaskan identiti dan kesahannya. Ini boleh dilihat dalam klausa (a) yang menerangkan bahawa kunci persendirian yang digunakan perlu berpadanan dengan kunci awam penandatangan manakala klausa (b) berkait dengan mesej yang asli. Sebaliknya, Seksyen 5 Akta Perdagangan Elektronik 2006 menyatakan bahawa tandatangan elektronik boleh dalam bentuk apa-apa huruf, aksara, nombor, bunyi atau apa-apa simbol lain atau apa-apa gabungannya yang dicipta dalam suatu bentuk elektronik yang diterima pakai oleh seseorang sebagai suatu tandatangan.

Seksyen 66 Akta Tandatangan Digital 1997 yang bertajuk pengesahan tandatangan digital turut menerangkan bahawa perakuan yang dikeluarkan oleh pihak berkuasa pemerakuan berlesen merupakan pengakuterimaan tandatangan digital yang telah disahbetulkan berdasarkan kata kunci awam yang dinyatakan dalam perakuan, jika tandatangan digital tersebut dapat disahbetulkan oleh perakuan tersebut serta ditambahkan ketika perakuan tersebut sah.

Antara pihak berkuasa pemerakuan berlesen yang diiktiraf bawah Akta Tandatangan Digital 1997 untuk mengeluarkan perakuan ialah Pos Digicert Sdn Bhd, Telekom Applied Business Sdn Bhd, MSC Trustgate.Com Sdn Bhd, dan Raffcomm Technologies Sdn Bhd. Jadi, tidak ada sesiapa boleh mengemukakan diri sebagai pihak berkuasa pemerakuan melainkan ada lesen sah yang dikeluarkan bawah akta ini.

Kesahan identiti dalam perdagangan elektronik amat penting untuk dikaji untuk memastikan pihak-pihak bertransaksi yang menjalankan urus niaga atas talian memang orang seperti dikemukakannya. Dengan itu, kajian ini akan membincangkan konsep serta kaedah-kaedah untuk mengesahkan identiti dan mengenal pasti isu-isu perundangan yang timbul dari segi pemakaian Akta Tandatangan Digital 1997. Akta Transaksi Elektronik 2010 di Singapura akan dibandingkan dengan peruntukan Akta Tandatangan Digital 1997 dan Akta Perdagangan Elektronik 2006 di Malaysia kerana Singapura telah meminda aktanya selepas meratifikasikan dan menguatkuasakan ECC. Ini boleh dijadikan rujukan semasa Malaysia meminda peruntukan undang-undang. Kajian ini juga akan mencadangkan langkah penyelesaian bagi memantapkan pemakaian Akta Tandatangan Digital 1997 dan Akta Perdagangan Elektronik 2006.

KAEDAH-KAEDAH KESAHAN IDENTITI PIHAK-PIHAK BERTRANSAKSI

a. Tandatangan Digital

Tandatangan digital yang digunakan bukan sahaja mewakili tandatangan tetapi juga identiti seseorang individu. Ia diaplikasikan melalui sistem kripto tidak simetri atau lebih kerap dikenali sebagai PKI yang bermaksud suatu algoritma atau siri algoritma yang memberikan suatu pasangan kunci yang selamat.

Tandatangan digital digunakan bagi memastikan individu yang menghantar mesej memang orang seperti dikemukakannya. Antara ciri-ciri utama tandatangan digital ialah ia disokong dengan perakuan yang bermaksud “suatu rekod berasas komputer yang mengenal pasti pihak berkuasa pemerakuan yang mengeluarkannya, menamakan atau mengenal pasti pelanggannya, mengandungi kunci awam pelanggan itu; dan ditandatangani secara digital oleh pihak berkuasa pemerakuan yang mengeluarkannya” berdasarkan Seksyen 2 Akta Tandatangan Digital 1997. Perakuan sah pula ialah “suatu perakuan yang dikeluarkan oleh pihak berkuasa pemerakuan berlesen, diterima oleh pelanggan yang disenaraikan di dalamnya, tidak dibatalkan atau digantung; dan tidak habisnya tempoh. Dengan syarat bahawa suatu perakuan transaksi merupakan suatu perakuan sah hanya berhubungan dengan tandatangan digital yang digabungkan dalamnya secara rujukan menurut Seksyen 2 Akta Tandatangan Digital 1999.

Selain daripada itu, penanda masa ialah ciri yang penting bagi tandatangan digital. Ia ditakrifkan sebagai “untuk menambahkan atau menggabungkan kepada sesuatu mesej, tandatangan digital atau perakuan suatu catatan yang ditandatangani secara digital yang menyatakan sekurang-kurangnya tarikh, masa dan identiti orang yang menambahkan atau menggabungkan catatan itu; atau catatan yang ditambahkan atau digabungkan sedemikian” menurut Seksyen 2 Akta Tandatangan Digital 1997. Dengan kata lain, fungsi penanda tarikh atau masa adalah untuk menunjukkan tarikh dan masa selepas tandatangan digital dihasilkan. Peraturan 58 hingga Peraturan 70 dalam Peraturan-Peraturan Tandatangan Digital 1998 telah menjelaskan penggunaan, kesan, peringkat dan kelayakan perkhidmatan penanda masa. Kelayakan autoriti-autoriti penanda masa, juga telah diterangkan dalam dokumen yang dikeluarkan oleh SKMM iaitu

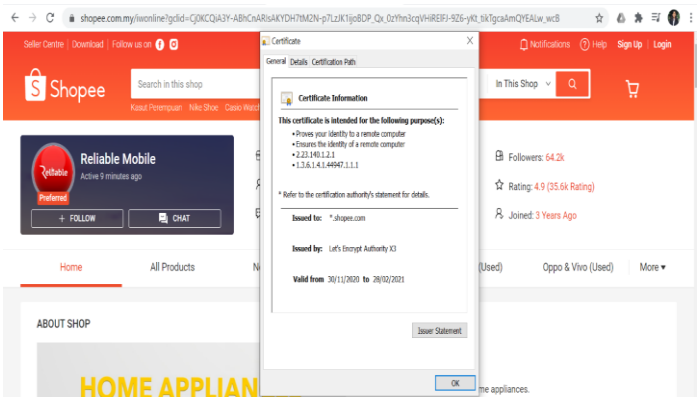
Requirements for Certification Authority (CA) to be Recognised as a Time Stamping Authority (TSA) yang dikuatkuasakan pada 1 Februari 2018. Di Malaysia, antara autoriti-autoriti penanda masa yang menawarkan perkhidmatan penanda tarikh atau masa ialah MSC Trustgate Sdn. Bhd., Pos Digicert Sdn. Bhd., dan Raffcomm Technologies Sdn. Bhd.[5]

Abu Bakar Munir (1999)[6] telah menjelaskan bahawa kunci persendirian adalah unik dan perlu disimpan dengan berhati-hati manakala kunci awam boleh diketahui oleh ramai orang. Tandatangan digital ini dimeterai di atas mesej digital melalui kriptografi. Sistem kripto tidak simetri pula bertindak sebagai skema berunsur matematik bagi mengatur data komputer. Selepas proses keselamatan yang mengesahkan pasangan kunci awam dan kunci persendirian ini, dokumen akan ditandatangani. Kesannya, ia akan berkuat kuasa di sisi undang-undang. Dalam pada itu, pihak pemerakuan berlesen akan mengeluarkan kunci persendirian tersebut selepas mengesahkan maklumat identiti pemilik kunci awam adalah sah.

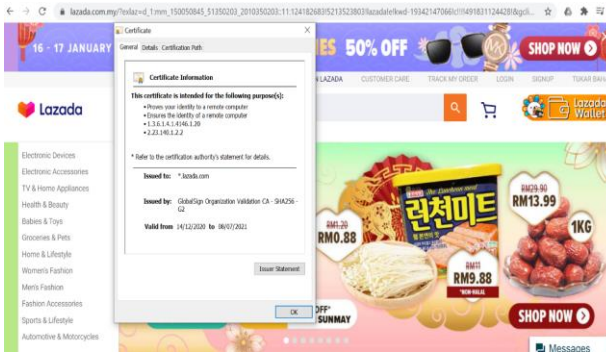
Di samping itu, pihak berkuasa pemerakuan mengeluarkan pemerakuan yang menghasilkan identiti digital. Identiti digital di sini bukan hanya terpakai untuk seseorang pelanggan, malahan ia juga terpakai untuk sistem rangkaian komputer. Sistem ini berjalan melalui *Secure Sockets Layer* (SSL) yang sebelum ini dikenali sebagai *Transport-Level Security* (TLS) untuk menyulit (*encrypt*) maklumat peribadi dalam internet, bertujuan untuk memastikan transaksi adalah selamat. Sehubungan itu, kedua-dua pihak bertransaksi akan dikenal pasti dan mereka masing-masing akan mengetahui sumber asal maklumat transaksi dari mana serta maklumat transaksi ini akan dihantar kepada siapa.[7]

Sebagai contoh, Shopee memasang sistem rangkaian komputer dengan SSL yang berjalan berdasarkan modul PKI untuk mewujudkan ia adalah sah dan sebenar. Modul PKI diguna pakai sebab pemerakuan sah berkait rapat dengan SSL. Pemerakuan sah ini kemudiannya dipasang ke dalam sistem rangkaian komputer. Pemerakuan sah yang dikeluarkan Let's Encrypt ini akan menjadi bukti bahawa Shopee memang sah, benar dan wujud. Beberapa perniagaan perdagangan elektronik di Malaysia turut mengaplikasi cara kesahan identiti ini. Contohnya, Lazada memasang pemerakuan sah yang dikeluarkan oleh GlobalSign dan sistem rangkaian komputer Zalora yang memasang pemerakuan sah yang dikeluarkan oleh Pos Digicert Sdn. Bhd.

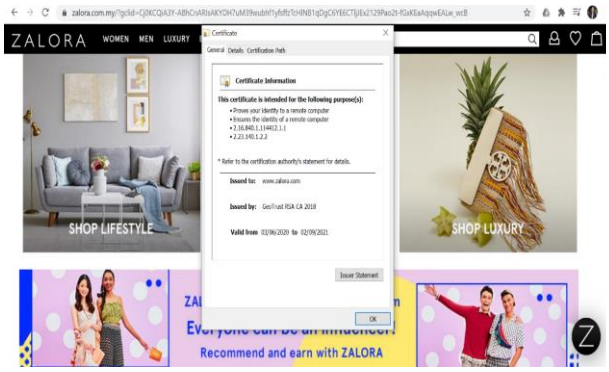
Selain daripada mengesahkan identiti sistem rangkaian komputer, ia dapat membantu menghalang pancingan laman sesawang. Jika ia tidak menunjukkan pemerakuan sah, ini membantu untuk mengingati dan menyedari pelanggan bahawa ia mungkin tidak selamat untuk dilanggan dan bukan sah serta sebenar seperti dikemukakan, secara tidak langsung mengelakkan pelanggan ditimpa kerugian kewangan.



Rajah 1.1 Gambar Pemerakuan Sah Shopee Dikeluarkan Let's Encrypt.



Rajah 1.2 Gambar Pemerakuan Sah Lazada Dikeluarkan GlobalSign



Rajah 1.3 Gambar Pemerakuan Sah Zalora Dikeluarkan GeoTrust RSA.

b. Tandatangan Elektronik

Bawah Akta Perdagangan Elektronik 2006 (Akta 658), Seksyen 5 menjelaskan bahawa tandatangan elektronik bermaksud "apa-apa huruf, aksara, nombor, bunyi atau apa-apa simbol lain atau apa-apa gabungannya yang dicipta dalam suatu bentuk elektronik yang diterima pakai oleh seseorang sebagai suatu tandatangan. Dengan kata lain, ia bermaksud sesuatu data dalam bentuk elektronik, ditambah atau dikaitkan secara logik dengan data elektronik, bertujuan untuk menunjukkan persetujuan penandatangan terhadap maklumat dalam mesej menurut Artikel 2 UNICITRAL Model Law on Electronic Signatures (2001).

Tandatangan elektronik boleh dalam pelbagai bentuk mengikut teknologi yang berbeza. Biasanya, antara jenis-jenis ialah kata kunci atau nombor PIN (*Personal Identification Number*), tandatangan dalam e-mel, dan tandatangan dalam bentuk gambar (Faye Fangfei Wang, 2010).[8]

Artikel 6 UNICITRAL Model Law on Electronic Signatures (2001) menerangkan bahawa antara ciri-cirinya adalah pertama, ia berhubung kait dengan penandatangan; kedua, ia dicipta bawah kawalan penandatangan; ketiga, ia adalah telus; dan keempat, mesej adalah telus, begitu juga dengan tandatangannya. Tidak seperti tandatangan digital, tandatangan elektronik tidak perlu dicipta dengan teknologi yang spesifik bawah undang-undang.

Seksyen 9(2) Akta Perdagangan Elektronik 2006 telah menyenaraikan syarat-syarat yang perlu dipenuhi iaitu (a) cara menghasilkan tandatangan elektronik itu dikaitkan dengan dan di bawah kawalan orang itu sahaja; (b) apa-apa perubahan yang dibuat kepada tandatangan elektronik itu selepas masa penandatanganan itu boleh dikesan; dan (c) apa-apa perubahan yang dibuat kepada dokumen itu selepas masa penandatangan itu boleh dikesan.

Secara perbandingan, tandatangan elektronik tidak seperti tandatangan digital yang berfungsi melalui sistem kripto tidak simetri. Tandatangan elektronik boleh diguna pakai dengan mudah dan harganya kurang mahal. Ia boleh dalam bentuk tulisan pendek atau gambar. Sebagai ilustrasi, Microsoft Word membenarkan pengguna menambah kata kunci kepada dokumen yang ingin dilindungi. Kata kunci yang ditambah dikenali sebagai PIN atau tandatangan dokumen (*word documented signature*).[9]

Pengguna boleh mencipta tulisan pendek atau imej sebagai tandatangan. Sebagai contoh, pengguna boleh menggunakan alat pengimbas untuk mengimbas tandatangan yang ditulis dalam kertas ke dalam komputer dalam format "*electronic bitmap*" atau "JPEG". Kemudiannya, ia akan ditambah ke dalam dail dokumen sebagai tandatangan elektronik. Tandatangan dalam e-mel sebenarnya merupakan antara kaedah

kesahan yang digunakan secara luas. Ia termasuk tulisan atau imej atau kedua-duanya.

c. Biometrik

UNICITRAL, Promoting Confidence in Electronic Commerce (2009) telah menyenaraikan biometrik sebagai antara kaedah-kaedah mengesahkan identiti seseorang. Secara amnya, biometrik dikatakan sebagai proses automatik yang mengiktiraf seseorang melalui ciri-ciri tubuh badan dan tingkah lakunya. Contoh ciri-ciri tubuh badan yang asli ialah muka, cap jari, tangan dan iris manakala ciri-ciri tingkah laku yang boleh dikenal pasti atau diukur termasuk keystroke, tandatangan dan suara.

Di Malaysia, teknologi biometrik telah diterima pakai dalam industri perbankan dengan lebih sistematik ekoran pengeluaran polisi Electronic Know-Your-Customer (e-KYC) (2020) oleh Bank Negara Malaysia. Polisi ini menerangkan bahawa biometrik merujuk penampilan fizikal seseorang dari segi biologi, termasuk penampilan muka, cap jari atau corak retina. Data berkenaan akan diambil dengan alat untuk dimasukan kepada pangkalan data. Suatu borang juga dilampirkan untuk mengesahkan identiti pelanggan berdasarkan biometrik. Jadi, institusi kewangan perlu mengisi borang tersebut sama ada *False Positive, False Negative, True Positive* atau *True Negative*. Kemudiannya, ia perlu dihantar kepada Bank Negara Malaysia melalui laman sesawang yang diberikan berdasarkan Lampiran 5. Selepas menghabiskan setiap peringkat, pelanggan baru akan dibenarkan menggunakan perkhidmatan kewangan.

Sreela Sasi (2004)[10] berpendapat bahawa corak retina adalah relevan dan sesuai diguna pakai dalam perdagangan elektronik. Hal ini dikatakan demikian kerana corak retina setiap orang berbeza dan sedikit perubahan tidak akan mengubah keputusan. Beliau turut mencadangkan cara pelaksanaan yang dimulakan dengan menggunakan imej iris yang standard, perisian penyulitan dan kamera.

Walau bagaimanapun, antara kelemahan-kelemahan biometrik adalah kemungkinan berlaku pencurian serta penggantian data biometrik dalam pangkalan data (UNICITRAL, Promoting Confidence in Electronic Commerce, 2009).

Electronic Know-Your-Customer (e-KYC) (2020) mengatakan institusi kewangan yang menerima pakai kombinasi faktor kesahan perlu mengenal pasti identiti pelanggan menggunakan konsep e-KYC dan perlu mematuhi tiga faktor kesahan iaitu sesuatu yang dimiliki oleh pelanggan seperti kad pengenalan dan nombor telefon; sesuatu yang diketahui pelanggan seperti nombor PIN dan maklumat peribadi; dan sesuatu berkenaan pelanggan sendiri seperti penampilan biometrik berdasarkan Perkara 7.6. Polisi ini secara tidak langsung mengiktiraf penggunaan biometrik dalam bidang institusi kewangan.

d. Kata Kunci dan Kaedah Kacukan

Kata kunci merupakan kaedah kesahan yang hampir dipakai oleh sebuah institusi kewangan. Biasanya, pelanggan perlu menaip kata kunci atau dikenali sebagai nombor PIN (*personal identification number*) ke dalam mesin ATM bagi megeluarkan duit atau menaip kata kunci ke dalam sistem rangkaian komputer bagi memindah duit ke akaun lain. Masalahnya, kira-kira 25% pelanggan telah lupa terhadap kata kunci atau nama pengguna dalam 6 bulan dan hanya 19% pelanggan menukar kata kunci dalam masa tertentu. Jadi, ini menimbulkan masalah kecurian identiti dan salah gunaan oleh orang lain berdasarkan Global Fraud and Identity Report (2018).

APEC Telecommunications and Information Working Group (2002) mendapati pelbagai teknologi digunakan dalam satu transaksi seperti kaedah kacukan iaitu tandatangan dan kriptografi di mana kata kunci diturunkan melalui SSL,

kaedah biometrik diaplikasikan untuk mencetuskan tandatangan digital melalui sistem kripto tidak simetri yang seterusnya disahkan melalui pemerakuan yag dikeluarkan oleh pihak berkuasa pemerakuan. Dalam pada itu, tiket Kerberosaan dihasilkan untuk mengakses kepada fail.

Secara keseluruhannya, pada masa dulu, penggunaan SSL digunakan untuk mengenal pasti kesahan identiti sistem rangkaian komputer, kemudiannya kegunaannya menjadi semakin luas sehingga digunakan untuk mengesahkan identiti seseorang pelanggan. Ini menunjukkan apabila teknologi semakin berkembang, kehidupan manusia semakin dipermudahkan. Teknologi juga mampu memberikan perubahan yang besar dalam kualiti hidup manusia (Zhang, M., Lin, L. & Chen, Z., 2021). Kita dapat memanfaatkan teknologi seperti tandatangan digital, tandatangan elektronik dan sebagainya untuk menguruskan transaksi dan pelbagai perkara lagi dalam kehidupan seharian. Pada masa yang sama, ia berperanan afdal bagi memastikan keselamatan transaksi dan urusan lain untuk mengelakkan ditimpa kerugian kewangan.

ISU-ISU PERUNDANGAN YANG TIMBUL DARI SEGI PEMAKAIAN UNDANG-UNDANG BERKAITAN KESAHAN IDENTITI DALAM PERDAGANGAN ELEKTRONIK

Perdagangan elektronik menjadi sebahagian daripada aktiviti masyarakat (Shiyu Wang, 2021). Walau bagaimanapun, terdapat banyak risiko keselamatan dalam membincangkan tentang perdagangan elektronik, termasuklah dalam hal berkaitan transaksi-transaksi perdagangan (Cai Baoyu, 2020). Dalam sektor awam, bagi memodenkan transaksi di agensi kerajaan, tandatangan digital diperlukan semasa menggunakan sistem e-perolehan. Tandatangan digital dalam sistem ini akan dijalankan dengan menggunakan token USB yang dibekalkan oleh Unit Permodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU). Ini adalah bagi mengelakkan masalah berlakunya pertikaian berkenaan obligasi kontrak, masalah pelaksanaan urusan perolehan dan pembayaran (Perbendaharaan Malaysia 2018). Bagi menggalakkan pembayaran cukai pendapatan secara elektronik, pengguna boleh menggunakan sijil digital yang dikeluarkan oleh Pos Digicert Sdn Bhd bagi mengesahkan capaian pengguna untuk menggunakan sistem e-Filing dan menandatangani Borang Nyata Cukai Pendapatan (BNCP) secara dalam talian. Tambahan pula, bagi memohon ePermit STA bagi barang-barang sensitif atau barang-barang bawah Akta Perdagangan Strategik 2010 (Akta 708), setiap permohonan akan dibekalkan dengan Token Tandatangan Digital bagi mengesahkan identiti pengguna selepas diluluskan oleh Dagang Net Technologies Sdn. Bhd. (DNT).

Dalam sektor persendirian seperti sektor perbankan, bagi membuka akaun di Bursa Malaysia Securities Berhad, pengguna boleh melakukannya melalui penggunaan tandatangan digital merujuk laman sesawangnya. Selain daripada itu, pembukaan akaun boleh didaftarkan secara digital oleh pelanggan tanpa mengira waktu dan tempat menerusi dokumen dasar yang dikeluarkan oleh Bank Negara Malaysia, iaitu mengenali Kenali Pelanggan Anda Menerusi Platform Digital atau lebih dikenali sebagai e-KYC (*Electronic Know-Your-Customer*) yang berkuat kuasa pada 30 Jun 2020. Jadi, institusi kewangan boleh mengenal pasti dan mengesahkan identiti pelanggan melalui pengecaman wajah, menyambung kepada pangkalan awam, swasta atau panggilan video dengan bantuan perkhidmatan daripada vendor pihak ketiga seperti pihak berkuasa pemerakuan berlesen. Berdasarkan pegawai operasi dari Innov8tif Solutions Sdn Bhd, Encik Tien Soon (2021), National Digital Identity (NDI) dapat meningkatkan penggunaan tandatangan digital seterusnya

menyambung kepada pangkalan data MyKAD yang merupakan kunci penerima pakaian e-KYC dengan lebih meluas.

Menjelang tahun 2020, berita yang menarik perhatian ramai rakyat ialah NDI yang disebut dalam rangka tindakan MyDIGITAL. MyDIGITAL merupakan pelan negara untuk memajukan Malaysia sebagai pemimpin ekonomi digital. Ia dihasilkan bagi merealisasikan Pelan Malaysia ke-12, 2021-2025 (RMKe-12) dan menuju ke Wawasan Kemakmuran Bersama 2030 kerana ekonomi digital ialah antara kunci bidang perkembangan ekonomi (KEGA). Berdasarkan rangka tindakan ini, penggunaan tandatangan digital diharap dapat ditingkatkan melalui inisiatif yang dipimpin oleh KKMM. Misalnya, inisiatif yang memastikan pekerja kerajaan berkemahiran untuk menggunakan tandatangan digital dan inisiatif yang menjamin keselamatan bagi mengelakkan penipuan dalam ruang siber dan juga inisiatif yang meningkat transaksi digital perkhidmatan sektor awam dari mula hingga akhir dalam Fasa 1 hingga Fasa 2 (2021-2025). Dengan itu, suatu ruang siber akan menjadi lebih selamat untuk menjalankan urus niaga secara maya kerana meterai yang dicap pada dokumen tidak dapat dipalsukan. Pada masa yang sama, pengguna dapat menggunakan tandatangan digital dengan kos yang lebih murah.

Sehubungan itu, tandatangan digital diperlukan untuk ditetapkan dalam MyKAD kerana ia dapat menyimpan perakuan digital yang dikeluarkan oleh pihak berkuasa pemerakuan berlesen, seterusnya menjana tandatangan digital dengan menggunakan pembaca dan perisian (Dr Shawn Tan, 2021). Namun begitu, masalah yang akan ditimbulkan ialah masalah kebebanan. Hal ini dikatakan demikian kerana inisiatif tandatangan digital diasingkan dari *National Digital Identity*. Kesannya, kos pembelian pembaca kad, pembaharuan perakuan digital dan pengeluaran perakuan digital dari pihak berkuasa pemerakuan berlesen tertentu bawah Akta Tandatangan Digital 1997 merupakan antara masalah-masalah yang akan ditimbulkan (Shawn Tan, 2019). Ini secara tidak langsung memperlahan penerimaan penggunaan perakuan digital dan tandatangan digital menurut pendapat Dr Shawn Tan (2021).

Akta Tandatangan Digital 1997 sebenarnya telah dipinda lebih daripada 20 tahun sejak 1997. Walaupun ia telah dipinda pada 27 September 2001, tetapi sebahagian besar peruntukan undang-undang masih dikekalkan. Hal ini menimbulkan kebimbangan kerana terdapat masih sebahagian isu-isu perundangan yang perlu dikaji semula dalam Akta Malaysia.

Masalah utama semasa mengesahkan identiti pengguna ialah bagaimanakah untuk memastikan identiti pelanggan dan penjual adalah sah dan sebenar seperti yang telah dikemukakan? Misalnya, ketika sesuatu dokumen telah ditandatangani, ini tidak semestinya menyebabkannya sah. Hal ini dikatakan demikian kerana tandatangan mungkin sah namun kandungan dokumen mungkin tidak sah. Sebaliknya, sesuatu dokumen mungkin sah namun tandatangan sebenarnya telah ditiru. Walaupun terdapat Sistem 1 Faktor yang bergantung kepada pengetahuan tentang kata kunci atau nombor PIN tetapi kekurangannya ialah ia kurang selamat manakala Sistem 2 atau 3 Faktor lebih selamat tetapi kekurangannya ialah ia lebih mahal dan ia kompleks untuk diaplikasikan oleh pengguna, ini boleh menyebabkan tahap kepuasan pengguna terjejas. Maka, pihak kerajaan perlu memandang berat isu perundangan ini yang boleh membawa masalah pemalsuan dan kecurian identiti dalam perdagangan elektronik.

Selain itu, ketika terwujud kepercayaan salah sangka terhadap identiti pihak tersebut akibat seseorang membentangkan diri sebagai X kepada pemilik barangan secara menipu dan penerimaan dibuat, adakah kontrak terbentuk dan sah?[11]

Di Malaysia, Akta Tandatangan Digital 1997 telah diperuntukkan untuk mengawal tandatangan digital tetapi telah dikritik bahawa terdapat beberapa kekurangan dan pindaan perlu dilakukan kerana pindaan terakhir telah lama dilakukan pada tahun 2001. Seksyen 2 Akta Tandatangan Digital 1997 hanya menyatakan sistem kripto tidak simetri boleh digunakan. Ini mungkin dapat memberi perlindungan secara spesifik dari segi undang-undang. Hakikatnya, ini boleh menyekat perkembangan dan penggunaan teknologi lain kerana teknologi baru telah dipakai di negara lain (Abu Bakar Munir, 1999)[12]. Jadi, sama ada peruntukan undang-undang tentang teknologi tandatangan digital yang ditetapkan sebelum ini patut dipinda seiring dengan perkembangan teknologi perlu dikaji secara terperinci.

Selain daripada itu, apabila kunci pengguna hilang dan kemudiannya disalahgunakan, kesannya adalah sukar untuknya membuktikan identiti pesalah dan dikecualikan daripada liabiliti[13]. Ini meningkatkan risiko ketika menandatangani dokumen digital kerana status kunci persendirian mesti selamat. Kesannya, liabiliti tidak terhad perlu ditanggung sekiranya kunci persendirian hilang atas kecuaian dan menyebabkan kerugian atau kerosakan (Susanna Frederick Rischer, 2001).[14]

RUMUSAN

Di bawah subtopik ini, penulis akan mencadangkan beberapa langkah penambahbaikan untuk memantapkan pemakaian Akta Tandatangan Digital 1997 dan Akta Perdagangan Elektronik 2006.

Sebenarnya, masalah-masalah yang ditimbulkan dalam urus niaga dalam perdagangan elektronik lebih rumit berbanding dengan urus niaga yang dijalankan secara bersemuka. Masalah yang paling utama ialah bagaimanakah memastikan identiti pihak-pihak bertransaksi adalah sah dan sebenar dalam perdagangan elektronik. Dalam pada ini, kita perlu memahami terlebih dahulu bahawa PKI merupakan suatu siri algoritma yang memberikan suatu pasangan kunci yang selamat. Ia merupakan infrastruktur yang berasaskan kepada SSL. PKI ini bukan sahaja berfungsi untuk menjana kunci awam dan kunci persendirian sehingga perakuan sah dikeluarkan. Dengan kata lain, penjelmaan mesej dihasilkan dengan menggunakan sistem kripto tidak simetri dan hanya pemegang kunci awam boleh menentukan dengan tepat, sama ada penjelmaan itu telah dihasilkan dengan menggunakan kunci persendirian yang berpadanan dengan kunci awamnya dan sama ada mesej itu telah diubah. Di sini, tandatangan digital dihasilkan.

Bagi menunjukkan kesahan, kebenaran dan kewujudan sistem rangkaian komputer seperti laman sesawang institusi perbankan dan perdagangan elektronik yang lain, perakuan sah yang dikeluarkan oleh pihak berkuasa pemerakuan berlesen akan dipasang di dalam rangkaian komputer. Sehubungan itu, pihak berkuasa pemerakuan berlesen akan mengenal pasti identiti pihak-pihak bertransaksi seperti pelanggan, syarikat, organisasi atau sistem rangkaian komputer. Perakuan ini turut memberi rujukan kepada pengguna supaya tidak menggunakan laman sesawang yang palsu. Kemudiannya, kunci persendirian dapat mengesahkan identiti pihak seperti dikemukakan kerana hanya dia mempunyai kunci persendirian tersebut. Program e-mel akan memberi makluman sekiranya telah ditandatangani secara digital dan sama ada tandatangan itu adalah sah.

Secara ringkasnya, infrastruktur PKI membolehkan pengguna menjana tandatangan digital yang unik. Selepas kunci persendiriannya dihantar bersama-sama dengan mesej, sesiapa yang memegang kunci awam dapat menentukan integriti tandatangan seterusnya mengenal pasti sama ada mesej asal itu telah diubah. Bagi menjamin kesahan identiti pihak-pihak bertransaksi, pihak berkuasa

pemerakuan berlesen perlu mengenal pasti identiti pemegang kunci tersebut ialah orang sebenar dengan mengeluarkan perakuan sah yang mengandungi identiti pihak-pihak bertransaksi, pasangan kunci dan penggunaan kunci menjana tandatangan digital. Justeru itu, tandatangan digital dikategorikan dalam Tahap Kepastian Alat Pengesahan (AAL) yang paling kuat dan selamat.

Seterusnya, sesetengah pengguna mungkin risau bahawa rangkaian komputer tidak selamat sepenuhnya kerana boleh dicapai tanpa kuasa. Ini turut menimbulkan isu yang kedua iaitu kepercayaan salah sangka terhadap identiti pihak tersebut disebabkan niat tipuan pihak satu lagi. Dengan itu, perayu harus merujuk Akta Kontrak 1950 kerana kontrak elektronik sama seperti kontrak tradisional. Misalnya, kontrak elektronik juga boleh terjejas dengan unsur-unsur negatif seperti paksaan, pengaruh tidak berpatutan, salah nyataan, frod atau tipuan dan khilaf.

Sekiranya seseorang dikatakan telah mengenakan unsur frod ke atas pihak satu lagi apabila berniat untuk mendorong orang lain membuat kontrak dengannya. Seksyen 17 Akta Kontrak 1950 telah memperuntukkan jenis-jenis perbuatan yang boleh dikatakan sebagai frod. Jenis-jenis perbuatan yang relevan dengan penipuan identiti adalah apabila seseorang menyatakan identitinya tersebut sebagai benar walaupun mengetahui fakta ini adalah tidak benar di sebaliknya. Selain daripada itu, apabila seseorang sengaja membunyikan identiti yang akan memudaratkan pihak itu dan mendorong pihak lain memasuki kontrak dengannya. Seseorang juga boleh melakukan frod dengan memperdaya untuk menipu dan difikirkan oleh mahkamah sesuai untuk diisytiharkan sebagai tipuan atau memang jelas dinyatakan sebagai tipuan di bawah undang-undang.

Di bawah *Common Law*, istilah frod merujuk salahnyataan tipu muslihat. Ia merujuk kepada kenyataan salah yang telah dibuat dengan sengaja dan mengetahui ketidakbenarannya atau tanpa mempercayai kebenarannya atau secara cuainya membuat kenyataan yang salah. Prinsip ini dipakai oleh Lord Herschell dalam kes *Derry v Peek (1889) 14 App Cas 337.*

Sekiranya seseorang silap terhadap identiti satu pihak lagi dalam perdagangan elektronik, ini boleh dikategorikan sebagai khilaf unilateral kerana suatu pihak telah melakukan kesilapan dan pihak satu lagi mempengaruhi berlakunya kesilapan ini sedar akan kesilapan yang dilakukan oleh pihak sebelah (Sakina Shaik Ahmad Yusoff & Azimon Abdul Aziz, 2003)[15].

Di bawah *Common Law*, khilaf unilateral akan mengakibatkan kontrak terbatal tetapi khilaf mengenai sifat pihak yang satu lagi tidak memberi kesan terhadap kesahan kontrak, dan dengan itu kontrak adalah sah (Sakina Shaik Ahmad Yusoff & Azimon Abdul Aziz, 2003). Dalam kes *Cundy v Lindsay (1878) 3 App Cas 459,* si penipu membuka perniagaan dengan nama Blenkarn di No.37, Wood Street dan menghantar pesanan barangan kepada perayu. Pesanan itu ditandatangani oleh si penipu yang mirip seperti firma, iaitu Blenkarn di No. 123, Wood Street yang dihormati oleh perayu. Si penipu menjualnya semula kepada defendan setelah menerima barangan itu. Perayu cuba mendapatkan semula barangan daripada defendan. House of Lords memutuskan bahawa perayu berjaya dalam tuntutan mereka kerana mereka hanya ingin berkontrak dengan Blenkiron and Co bukannya orang lain dan identiti pihak yang akan berkontrak adalah amat penting. Dengan itu, kontrak adalah terbatal. Dalam kes *Ingram v Little [1961] 1 QB 31,* plaintif menyaman defendan iaitu pihak ketiga dan menghujahkan bahawa kontrak adalah terbatal kerana wujud khilaf identiti. Sallers LJ bersetuju bahawa khilaf identiti wujud. Plaintif menjual kereta untuk cek semasa membuat cadangan dan mempercayai mereka sedang berurusan dengan Encik P.G.M Hutchinson dari Caterham yang jujur itu. Secara ringkasnya, perayu perlu

membuktikan kepada mahkamah bahawa beliau telah mengambil langkah-langkah dengan berhati-hati untuk mengenal pasti identiti pihak satu lagi dan identiti pihak yang satu lagi adalah secara fundamentalnya afdal.

Bagi masalah penipuan identiti, perayu boleh membawa tindakan di bawah frod atau khilaf identiti bergantung kepada keadaan dan fakta kes. Namun begitu, kedua-dua unsur frod dan khilaf akan menyebabkan perjanjian tidak mempunyai kesan undang-undang seperti diperuntukkan dalam Seksyen 2. Kesannya, frod dan khilaf yang dilakukan oleh suatu pihak merupakan unsur negatif yang dinyatakan dalam Seksyen 14 dan akan menjejaskan kesahihan sesuatu kontrak. Hal ini dikatakan demikian kerana pihak-pihak berkontrak tidak mempunyai kerelaan bebas semasa memasuki kontrak. Sekiranya kontrak dimasuki tanpa kerelaan bebas pihak-pihak berkontrak maka ia adalah kontrak boleh batal atas pilihan untuk meneruskan atau membatalkan kontrak ini sebagaimana diperuntukkan dalam Seksyen 19.

Bagi kes penipuan identiti yang melibatkan frod, remedi yang terpakai bagi pihak teraniaya ialah Seksyen 65 yang memperuntukkan bahawa jika kontrak menjadi batal, segala faedah yang didapati daripada perjanjian perlu dikembalikan. Selain itu, pembatalan kontrak dan pampasan boleh dituntut di bawah Seksyen 34(1) dan Seksyen 37. Sebaliknya, orang teraniaya yang membawa tindakan bawah khilaf boleh menuntut remedi seperti diperuntukkan di bawah Seksyen 65 dan remedi kedua yang boleh digunakan ialah restitusi di bawah Seksyen 66. Peruntukan ini menerangkan bahawa apabila suatu perjanjian didapati batal, atau menjadi batal, sesiapa yang telah menerima sebarang faedah daripada perjanjian harus memulangkannya atau memberi pampasan untuk orang diambil faedah.

Di samping itu, Akta Tandatangan Digital 1997 menimbulkan persoalan bahawa tantangan digital yang menggunakan sistem kripto tidak simetri akan menyekat perkembangan dan penggunaan teknologi lain. Penulis berpandangan bahawa penggunaan sistem yang spesifik ini adalah munasabah untuk diperuntukkan sebegini dalam Akta Tandatangan Digital 1997. Hal ini dikatakan demikian kerana ia sebenarnya merupakan infrastruktur yang menghasilkan tandatangan digital.

Masalah seterusnya ialah kesukaran membuktikan identiti pesalah dan dikecualikan daripada liabiliti apabila berlaku kehilangan atau penyalahgunaan kunci persendirian. Apabila mentafsir tandatangan digital, kita perlu memahami bahawa ia dijana dengan menggunakan pasangan kunci iaitu kunci awam dan kunci persendirian. Selain daripada itu, tandatangan digital dikaitkan dengan pasangan kunci, bukan identiti pengguna secara fizikal. Penjelmaan mesej hanya dapat dihasilkan dengan menggunakan kunci persendirian yang berpadanan dengan kunci awam. Sesiapa yang memegang kunci persendirian dapat menjana tandatangan digital. Jadi, kunci persendirian merupakan elemen amat penting dalam perihal kesahan identiti.

Penulis mendapati pelanggan bertanggungjawab menjaga kunci persendirian dan mengelakkan ia terdedah kepada pihak ketiga yang tidak diberi kuasa berdasarkan Seksyen 43. Ini kelihatan seolah-olah mengalihkan tanggungan liabiliti kepada pelanggan tetapi ini adalah bagi memastikan pelanggan menanggung tanggungjawab untuk menyimpan kunci persendirian dengan selamat dan mengelakkan ketidakadilan kepada pihak lain. Ketidakadilan yang dimaksudkan ialah penafian pengguna terhadap kesan undang-undang tandatangan dan niat jahat untuk mengelakkan daripada tanggungan ganti rugi. Beliau juga menyatakan bahawa sekiranya kunci persendirian pelanggan disalahgunakan atau dicuri, mereka digalakkan melapor kepada polis kerana kunci persendirian merupakan harta persendirian. Malahan, hanya pihak polis

berkuasa menjalankan siasatan apabila berlaku kehilangan harta persendirian.

CADANGAN PENAMBAHBAIKAN TERHADAP PERUNTUKAN UNDANG-UNDANG YANG SEDIA ADA

Terdapat beberapa kekaburan dari segi pemakaiannya Akta Tandatangan Digital 1997 dan Akta Perdagangan Elektronik 2006. Jadi, beberapa langkah penambahbaikan telah dicadangkan seperti berikut.

Penulis berpandangan bahawa Akta Tandatangan Digital 1997 boleh disatukan dengan Akta Perdagangan Elektronik 2006. Walaupun konsep tandatangan digital dalam Akta Perdagangan Elektronik sama dengan tandatangan digital dalam Akta Tandatangan Digital, tetapi ia tidak terpakai kepada transaksi bukan komersial. Ini merupakan aspek yang perlu diberi perhatian. Justeru itu, penulis mencadang supaya peruntukan dalam Akta Tandatangan Digital 1997 bersama-sama dengan Peraturan-Peraturan Tandatangan Digital 1998 dimuatkan ke bahagian belakang Akta Perdagangan Elektronik. Akta Transaksi Elektronik 2010 di Singapura merupakan model peruntukan undang-undang yang mengasingkan jenis transaksi secara jelas dalam Bab 4.

Justeru itu, penulis juga mencadang supaya Malaysia wajar meratifikasikan konvensyen UNICITRAL iaitu ECC. Sebab utama adalah skopnya yang luas kerana konvensyen ini mencadangkan ahli negara untuk menerima pakai peruntukan yang berbunyi, "penggunaan komunikasi elektronik yang berkaitan dengan pembentukan atau pelaksanaan kontrak antara pihak-pihak yang berniaga di negara berlainan." Merujuk peruntukan undang-undang ini, boleh dikatakan perkataan "kontrak" boleh ditafsirkan secara meluas kerana terpakai juga untuk kontrak yang dibentuk di peringkat antarabangsa walaupun negara tersebut telah menerima pakai konvensyen ini. Selain daripada itu, konvensyen ini terpakai tertakluk kepada undang-undang antarabangsa persendirian, dengan syarat pihak-pihak kepada kontrak tidak memilih untuk menerima pakainya. Pendek kata, jika Malaysia menerima pakai konvensyen ini, ini membantu melicinkan urus niaga dalam perdagangan elektronik Malaysia dari perspektif undang-undang perdagangan antarabangsa dan komunikasi elektronik dianggap sah dan boleh dikuatkuasakan. UNCITRAL Model Law on Electronic Transferable Records (MLETR) juga bermanfaat untuk melicinkan perdagangan elektronik dengan menambahbaik kelajuan dan keselamatan penghantaran. Tandatangan dalam rekod elektronik boleh dipindah yang bertujuan mengesahkan identiti seseorang turut disebut. Ini membolehkan rekod elektronik boleh dipindah dan secara tidak langsung memastikan banyak salinan dokumen dihasilkan dan menyebabkan pelaksanaan obligasi dilakukan oleh pihak-pihak lain. Sebagai contoh, Akta Singapura berjaya mendapat pengiktirafan kerana Aktanya setaraf dengan standard di peringkat global. Ia secara jelasnya menerangkan undang-undang berkenaan kontrak dan transaksi elektronik dan memberi kebebasan kepada pihak-pihak berkontrak.

Kerajaan Malaysia berhasrat supaya penggunaan tandatangan digital dalam transaksi digital dari mula hingga akhir (*end-to-end transactions*) dengan agensi awam dapat ditingkatkan antara tahun 2021 hingga 2025 berdasarkan rangka kerja MyDIGITAL. Namun begitu, penulis berpendapat bahawa inisiatif ini memerlukan masa yang lebih panjang. Misalnya, kita perlu mengambil kira masa untuk melatih semua pendaftar atau pegawai agensi awam berkenaan pengetahuan dan kemahiran yang relevan, terutamanya pegawai Jabatan Pendaftaran Negara (JPN) sekiranya dipertanggungjawab dalam perkara ini kerana jabatan ini mengawal selia pangkalan data peribadi rakyat Malaysia. Sebaliknya, sekiranya pihak berkuasa pemerakuan berlesen dipertanggungjawab, masa yang diambil akan dipendekkan. Hal

ini dikatakan demikian kerana mereka mempunyai kepakaran dalam bidang ini dalam menggunakan kaedah kesahan iaitu tandatangan digital bagi mengenal pasti identiti pengguna dan memastikan orang tersebut merupakan orang seperti yang dikemukakan melalui e-KYC.

Selain itu, penggunaan token kriptografi harus dipakai dalam pelaksanaan MyDIGITAL. Ia bukan sahaja memudahkan para pengguna malahan sangat selamat untuk digunakan kerana kunci akan dijana dalam token dan tidak boleh dikeluarkan atau disalin kemudiannya. Token ini akan diberi selepas mendaftar identiti digital dan identiti seseorag disahkan sama ada secara fizikal atau melalui e-KYC. Prosedurnya mesti selaras dengan panduan BNM. Berdasarkan panduan BNM, USB token boleh dipos kepada pengguna, kemudiannya pengguna melayari laman sesawang untuk mengaktifkan token tersebut. Pada masa itu, perakuan sah dan token dapat dijana seterusnya menghasilkan kunci persendirian. Sekiranya token ini dipakai, maka pembaca kad tidak diperlukan, ini secara tidak langsung menjimatkan kos pengguna.

Di samping itu, penulis mencadangkan supaya penggubal undang-undang boleh mengkaji peruntukan undang-undang dalam Akta Transaksi Elektronik 2010 di Singapura yang bersifat berteknologi neutral. Ini adalah untuk memberi kebebasan kepada pihak-pihak berkontrak memilih teknologi yang dirasakan sesuai selagi mengikut kehendak undang-undang. Teknologi neutral patut dipertimbangkan dan digantikan dengan konsep tandatangan digital dalam Akta Malaysia yang sedia ada. Hal ini dikatakan demikian kerana inovasi teknologi semakin berkembang dan pematuhan kepada standard antarabangsa yang ditetapkan oleh PBB melalui MLEC dan ECC. Jadi, peruntukan undang-undang yang sesuai tidak sepatutnya menyekat penggunaan kaedah teknologi lain dan tidak boleh terlalu luas dan kabur.

Penulis juga menyeru supaya Akta Perdagangan Elektronik dikaji semula dengan mencontohi Akta Transaksi Elektronik Singapura. Misalnya, pelawaan cadangan merupakan elemen penting dalam pembentukan kontrak elektronik tetapi tidak diperuntukkan dalam Akta yang sedia ada. Penulis juga berpandangan bahawa peruntukan 22 dan 23 mengelirukan kerana tidak menetapkan secara tegas dan jelas mengenai tempat pengiriman dan penerimaan, tetapi memberi perhatian terhadap isu ketiadaan tempat perniagaan dan kelebihan tempat perniagaan. Kedua-dua peruntukkan ini sebenarnya boleh digabungkan.

Akhirnya, kerajaan terutamanya SKMM bertanggungjawab untuk meningkatkan kesedaran dan pengetahuan rakyat Malaysia mengenai manfaat penggunaan tandatangan digital termasuk menjimatkan masa untuk mengesahkan identiti dan menjimatkan kertas untuk membuktikan identiti sendiri di kaunter agensi kerajaan dan institusi kewangan.

PENUTUP

Tandatangan digital sebenarnya telah digunakan oleh agensi kerajaan tetapi bolehlah ditingkatkan lagi untuk melicinkan urusan secara atas talian. Selan itu, tandatangan digital amat diperlukan untuk mencapai sasaran pihak kerajaan dalam MyDIGITAL.

Walau bagaimanapun, isu-isu perundangan dalam Akta Tandatangan Digital 1997 dan Akta Perdagangan Elektronik 2006 harus diselesaikan secepat mungkin. Penggubal undang-undang boleh mengambil iktiraf dari negara Singapura dengan mengkaji kerangka undang-undang negara Singapura untuk mengetahui bagaimanakah Singapura menambah baik aktanya melalui pindaan pada tahun 2010 dan sama adakah Malaysia boleh menyesuaikannya dengan Akta Tandatangan Digital 1997 dan Akta Perdagangan Elektronik 2006.

Akhirnya, penulis berpendapat bahawa tandatangan digital berkesan untuk mengesahkan identiti pihak-pihak bertransaksi dalam perdagangan elektronik. Ia juga berpotensi besar kerana kerajaan Malaysia sedang bergiat berusaha untuk menggunakan tandatangan digital semasa menjalankan urus niaga dengan orang awam. Artikel ini diharapkan dapat memberi kesedaran kepada pihak-pihak bertransaksi semasa menggunakan tandatangan digital dan meningkatkan pemahaman masyarakat berkenaan penggunaan tandatangan digital dan kaedah-kaedah kesahan identiti lain.

NOTA

[1] Rafidah Mat Ruzki, 'Jualan dalam talian meningkat 28.9 peratus pada April', Berita Harian, pada 18 Oktober 2020.

[2] Chris Reed dan John Angel, *Computer Law* 7th Edn, Oxford University Press, United States, 2011, hlm 198.

[3] APEC Telecommunications and Information Working Group (TEL), PKI/E-Authentication Advancement: Evaluation Report, 3 April 2020, hlm 175.

[4] Hartini Saripan, 'The role of the 'law of the horse' in the governance of electronic signatures: lessons from Malaysia' [2009] 2 MLJ clxxxvi, hlm 248.

[5] Suruhanjaya Komunikasi dan Multimedia, *Certifications,* https://www.mcmc.gov.my/en/commons/print?printpath=/Legal/Registers/DSARegisters&classname=CMS.MenuItem (25 February 2022).

[6] Abu Bakar Munir, *Policies and Challenges*, Butterworths Asia, Malaysia, 1999, hlm 186.

[7] Abu Bakar Munir, *Policies and Challenges*, Butterworths Asia, Malaysia, 1999, hlm 186.

[8] Faye Fangfei Wang, *Law of Electronic Commercial Transactions, Contemporary Issues in the EU, US and China,* Routledge, Kuala Lumpur, 2010, hlm 79-80.

[9] Faye Fangfei Wang, *Law of Electronic Commercial Transactions, Contemporary Issues in the EU, US and China,* Routledge, Kuala Lumpur, 2010, hlm 80.

[10] Sreela Sasi, *Biometric authentication for e-commerce transaction*, International Workshop on Imaging Systems and Techniques, Italy, 2004, hlm 113-114.

[11] Eliza Mik, 'Mistaken identity, identity theft and problems of remote authentication in e-commerce', (2012) *Computer Law and Security Review* 28 (4) hlm 397.

[12] Abu Bakar Munir, Policies and Challenges, Butterworths Asia, Kuala Lumpur, Malaysia, 1999, hlm 192.

[13] Roger Clarke, 'Module 4- message security, cryptography, identification and authentication', 1 November 1996, http://www.rogerclarke.com/BEG9673/module4.html, (3 April 2020).

[14] Susanna Frederick Rischer, 'Saving rosencrantz guildenstern in a virtual world? A comparative look at recent global electrnonic signature legislation' 2001, hlm 235.

[15] Sakina Shaik Ahmad Yusoff & Azimon Abdul Aziz, *Mengenali Undang-undang Kontrak Malaysia,* Internasional Law Book Services, Malaysia, 2003, hlm 118.

RUJUKAN

Akta Kontrak 1950 (Akta 136).

Akta Perdagangan Elektronik 2006 (Akta 658).

Akta Tandatangan Digital 1997 (Akta 562).

Akta Tandatangan Digital Utah 1995.

Abu Bakar Munir. 1999. *Cyber Law Policies and Challenges*. Kuala Lumpur. Butterworths Asia.

Anwarul Yaqin.2007. Legal Research and Writing. Malaysia: Lexis Nexis, Malaysia.

APEC Telecommunications and Information Working Group. 2002. Electronic Authentication: Issues Relating to its Selection and Use. Singapore: 1-207.Cai Baoyu. 2020. Application of computer network

security technology in e-commerce [J]. Computer products and circulation. (05): 18.

Chris Reed & John Angel. 2011. Computer Law 7th Edn. New York: Oxford University Press.

Eliza MIK. 2012. Mistaken identity, identity theft and problems of remote authentication in e-commerce. Computer Law and Security Review. 28 (4): 396-402.

Faye Fangfei Wang. 2010. *Law of Electronic Commercial Transactions, Contemporary Issues in the EU, US and China.* United Kingdom: Routledge.

Hartini Saripan. 2009. The role of the 'law of the horse' in the governance of electronic signatures: lessons from Malaysia. Malayan Law Journal.

Rafidah Mat Ruzki. 2020. Jualan dalam talian meningkat 28.9 peratus pada April. Berita Harian, 18 Oktober 2020.

Roger Clarke. 1996. Module 4- message security, cryptography, identification and authentication. http://www.rogerclarke.com/BEG9673/module4.html [1 November 1996].

Sakina Shaik Ahmad Yusoff & Azimon Abdul Aziz. 2003. *Mengenali Undang-undang Kontrak Malaysia. Petaling Jaya*: Internasional Law Book Services.

Shiyu Wang. 2021. Study on the Application of Computer Security Technology in E-commerce. Journal of Physics: Conference Series. 1915. 042044. doi:10.1088/1742-6596/1915/4/042044.

Sreela Sasi. 2004. Biometric authentication for e-commerce transaction. International Workshop on Imaging Systems and Techniques. Italy: Stresa 113-116.

Susanna Frederick Rischer. 2001. Saving rosencrantz guildenstern in a virtual world? A comparative look at recent global electrnonic signature legislation 229-242.

Suruhanjaya Komunikasi dan Multimedia. 2022. Certifications. https://www.mcmc.gov.my/en/commons/print?printpath=/Legal/Registers/DSARegisters&classname=CMS.MenuItem [25 February 2022].

Zhang, M., Lin, L. & Chen, Z. 2021. Lightweight security scheme for data management in E-commerce platform using dynamic data management using blockchain model. Cluster Comput. Springer. https://doi.org/10.1007/s10586-021-03373-6.

Joslyn Yeo Yi Tian
Fakulti Undang-Undang
Universiti Kebangsaan Malaysia (UKM).
E-mel: joslynyeoyitian@gmail.com