PRIVASI DI TEMPAT KERJA: TINJAUAN DARI SUDUT PERUNDANGAN DI MALAYSIA

(*Workplace Privacy: The Legal Point of View in Malaysia*)

Zuryati Mohamed Yusoff
zuryati@uum.edu.my

Zainal Amin Ayub
z.amin@uum.edu.my

Pusat Pengajian Undang-undang,
Kolej Undang-undang, Kerajaan dan Pengajian Antarabangsa,
Universiti Utara Malaysia.

Published online: 1 January 2019
To cite: Zuryati Mohamed Yusoff and Zainal Amin Ayub. (2019). Privasi di tempat kerja: Tinjauan sudut perundangan di Malaysia. *Kanun: Jurnal Undang-undang Malaysia*, *31*(1), 55 – 84.

Abstrak

Pertumbuhan pesat teknologi maklumat dan komunikasi (TMK) menggesa pekerja mencari maklumat dan menjana kecekapan dalam pekerjaan. Perubahan ini berlaku akibat peningkatan kecanggihan teknologi pengawasan yang melibatkan kawalan data peribadi yang membolehkan majikan memantau prestasi pekerja, mengekalkan disiplin dan produktiviti pekerja. Antara teknologi pengawasan yang digunakan termasuklah aplikasi sistem penentududukan sejagat (*global positioning system*), pengawasan video, kad pintar, pengecaman wajah dan biometrik. Pengumpulan data ini juga amat berkait rapat dengan privasi. Tambahan pula, Perlembagaan Persekutuan Malaysia tidak mengiktiraf secara khusus privasi sebagai suatu hak asasi dan Akta Perlindungan Data Peribadi 2010 hanya melindungi data yang berkaitan dengan transaksi komersial sahaja. Oleh itu, artikel ini membincangkan sejauh manakah perlindungan privasi diberikan kepada pekerja di Malaysia menggunakan kaedah kajian doktrin. Kes Kesatuan Eropah dan

Amerika Syarikat dirujuk sebagai panduan dan perbandingan dengan keadaan di Malaysia. Dapatan kajian menunjukkan bahawa tiada perlindungan privasi secara khusus diberikan kepada pekerja di Malaysia.

Kata kunci: privasi, privasi tempat kerja, data peribadi, pengawasan, hak pekerja

Abstract

The rapid growth of information and communication technology has made it possible for everybody to search information and be more efficient in their work. Another shift taking place as a result of the advancement of surveillance technologies involves the control of personal data. Controlling personal data enables employers to monitor work performance as well as maintaining employee discipline and productivity. The new technology involved includes global positioning systems, video surveillance, smart cards, face recognition and biometrics. The collection of personal data has significant importance with regard to privacy. The Malaysian Federal Constitution does not specifically recognize privacy as a fundamental right, while the Personal Data Protection Act 2010 only protects the handling of personal data in commercial transactions. As such, this article discusses the extent to which protection is available to employees relating to privacy. The doctrinal methodology was employed in conducting this research. Cases from the European Union and the United States of America were used as guides and for comparison with the situation in Malaysia. The findings are that there is no protection of privacy at the workplace provided specifically to protect employees in Malaysia.

Keywords: privacy, workplace privacy, personal data, surveillance, employee rights

PENDAHULUAN

Definisi privasi dibezakan secara meluas mengikut konteks dan persekitaran, dan di kebanyakan negara, konsep ini digabungkan dengan perlindungan data yang mentafsirkan privasi dari segi pengurusan maklumat peribadi. Perlindungan privasi pada dasarnya

ialah had sejauh manakah masyarakat boleh mengganggu hal ehwal peribadi seseorang. Pada tahun 1890-an, Hakim Louis Brandeis Mahkamah Agung Amerika Syarikat menyatakan bahawa konsep privasi yang ditegaskan ialah individu mempunyai "hak untuk tidak diganggu (*right to be left alone*)".[1] Brandeis berhujah bahawa privasi yang paling dihargai ialah kebebasan dalam demokrasi yang harus digambarkan dalam perlembagaan. Menurut Bloustein,[2] privasi penting kerana melindungi personaliti seseorang dan tidak boleh menyentuh kebebasan, maruah dan integriti seseorang. Ellis[3] mentakrifkan privasi sebagai "keinginan setiap daripada kita untuk memiliki ruang fizikal yang bebas daripada gangguan, pencerobohan, rasa malu atau akauntabiliti dan percubaan untuk mengawal masa dan cara pendedahan maklumat peribadi tentang diri kita."

Privasi ialah jangkaan bahawa maklumat sulit peribadi yang didedahkan di tempat persendirian tidak akan didedahkan kepada pihak ketiga kerana pendedahan itu akan menyebabkan ada rasa malu atau tekanan emosi yang munasabah terhadap sensitiviti seseorang.[4] Hak privasi juga terbatas kepada individu yang berada di suatu tempat yang secara munasabahnya bersifat peribadi, contohnya di rumah, bilik hotel, pondok telefon, dan lain-lain. Tidak ada perlindungan terhadap maklumat sama ada maklumat tersebut merupakan catatan awam atau mangsa secara sukarela didedahkan di tempat awam.[5]

Hak privasi juga dianggap sebagai hak asasi manusia. Perkara 12 Perisytiharan Hak Asasi Manusia Pertubuhan Bangsa-Bangsa Bersatu (PBB) yang diterima pakai pada tahun 1948 menyatakan bahawa tidak seorang pun boleh diganggu sewenang-wenangnya dari

1 Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 193 – 220.

2 Bloustein, E. J. (1964). Privacy as an aspect of human dignity: An answer to Dean Prosser. *NYUL Rev.*, *39*, 962.

3 Smith, R. E. (2000). Ben Franklin's web site: Privacy and curiosity from Plymouth Rock to the Internet. *In Privacy journal*. (p. 6).

4 Standler, R. B. (1997). Privacy law in the USA. Retrieved from http://www.rbs2.com/privacy.htm.

5 Standler, R. B. (2004). Privacy law in the USA. Retrieved from http://www.rbs2.com/privacy.htm.

segi keadaan peribadi, keluarga, rumah tangga atau surat-menyurat, atau pencerobohan terhadap maruah dan nama baik. Setiap orang berhak mendapat perlindungan undang-undang daripada gangguan atau pencerobohan sedemikian.[6] Hak yang sama juga diberikan di bawah artikel 8 Konvensyen Hak Asasi Manusia Eropah atau *European Convention on Human Rights* (ECHR).[7]

Perlembagaan Persekutuan Malaysia tidak mengiktiraf secara khusus hak privasi, tetapi ada memperuntukkan beberapa hak yang berkaitan, termasuk hak kebebasan diri[8], hak kebebasan bergerak,[9] dan hak kebebasan berhimpun, bersuara dan berpersatuan[10]. Walau bagaimanapun, sekatan tertentu tentang hak tersebut boleh dikenakan oleh undang-undang untuk melindungi kepentingan dan keselamatan persekutuan dan mengekalkan ketenteraman awam. Dalam erti kata lain, hak yang diberikan di bawah Perlembagaan Persekutuan adalah tidak mutlak. Terdapat undang-undang yang mengehadkan hak yang dilindungi di bawah Perlembagaan Persekutuan. Contohnya Akta Rahsia Rasmi 1972 yang berkaitan dengan larangan pendedahan oleh penjawat awam yang bertujuan melindungi privasi kerajaan dan bukannya pekerja. Antara undang-undang lain yang mengehadkan hak privasi individu termasuklah seksyen 43 Akta Suruhanjaya Pencegahan Rasuah Malaysia 2009,[11] seksyen 245 sehingga seksyen 247 Akta Komunikasi dan Multimedia 1998,[12] seksyen 10(2) dan (3) Akta Jenayah Komputer

6 Artikel 12 *Universal Declaration of Human Rights*.

7 Artikel 8 ECHR memperuntukkan "*1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*."

8 Perkara 5 Perlembagaan Persekutuan.

9 Perkara 9 Perlembagaan Persekutuan.

10 Perkara 10 Perlembagaan Persekutuan.

11 Seksyen 43 – kuasa untuk memintas perhubungan, Akta Suruhanjaya Pencegahan Rasuah Malaysia 2009.

12 Seksyen 245 sehingga seksyen 247 Akta Komunikasi dan Multimedia 1998.

1997[13] dan beberapa akta lain. Peruntukan yang terkandung dalam akta ini menunjukkan bahawa hak privasi diiktiraf tetapi terhad dari segi perlindungannya.

PERMASALAHAN KAJIAN

Pekerja di seluruh dunia biasanya tertakluk pada beberapa jenis pemantauan oleh majikan mereka. Lazimnya atas sebab tertentu, majikan mengumpulkan dan mendapatkan maklumat peribadi daripada pekerja, seperti penjagaan kesihatan, cukai, dan pemeriksaan latar belakang, serta melakukan pemantauan dan pengawasan berterusan terhadap pekerja di tempat kerja dan ketika mereka bekerja.[14] Secara tradisinya, pemantauan dan pengumpulan maklumat di tempat kerja melibatkan beberapa bentuk campur tangan manusia sama ada dengan kebenaran, atau sekurang-kurangnya dengan pengetahuan pekerja. Walau bagaimanapun, perubahan struktur dan bentuk tempat kerja menyebabkan pengawasan dan amalan pemantauan yang dilakukan bersifat lebih invasif, kerap dan tersembunyi, serta berkait rapat dengan hak terhadap privasi dan maruah di tempat kerja.[15] Kemajuan teknologi dan perisian juga meningkatkan tahap pengawasan automatik.[16] Pada masa ini, pengawasan prestasi pekerja, tingkah laku, dan komunikasi boleh dijalankan melalui teknologi, dengan cara meningkatkan kemudahan dan kecekapan.[17] Teknologi yang sedang dibangunkan berkuasa dan boleh meliputi setiap aspek kehidupan pekerja. Program perisian tersebut boleh merakam butang yang ditekan pada komputer dan memantau imej skrin secara tepat, sistem pengurusan telefon boleh menganalisis corak penggunaan telefon dan

13 Seksyen 10(2) dan (3) Akta Jenayah Komputer 1997.

14 Smith-Butler, L. (2009). Workplace privacy: We'll be watching you. *Ohio NUL Rev.*, *35*, 53.

15 Smith, W. P., & Tabak, F. (2009). Monitoring employee e-mails: Is there any room for privacy? *The Academy of Management Perspectives*, *23*(4), 33 – 48.

16 Nord, G. D., McCubbins, T. F., & Nord, J. H. (2006). E-monitoring in the workplace: Privacy, legislation, and surveillance software. *Communications of the ACM*, *49*(8), 72 – 77.

17 Mishra, J. M., & Crampton, S. M. (1998). Employee monitoring: Privacy in the workplace? *SAM Advanced Management Journal*, *63*(3), 4.

destinasi panggilan, manakala kamera kecil dan kad pengenalan atau ID pintar boleh memantau bukan sahaja tingkah laku dan pergerakan, malahan orientasi fizikal pekerja.

Penggunaan internet, media sosial, laman web dan e-mel menyumbang kecekapan dan kecemerlangan dalam perniagaan[18] kerana alat tersebut murah, cepat dan mudah digunakan. Walau bagaimanapun, kewujudan media sosial, e-mel, dan pelbagai lagi bentuk teknologi komunikasi membuka ruang berlakunya penyalahgunaan.[19] Sebagai contoh, kajian yang dibuat terhadap 1439 pekerja oleh Vault.com mendapati 37 peratus mengaku melayari internet secara konsisten semasa bekerja, 32 peratus melayari beberapa kali sehari dan 21 peratus melayari beberapa kali seminggu. Kajian oleh Websense Inc. pula mendapati antara laman sesawang yang dilayari oleh pekerja termasuklah laman lucah (42%), perbualan online (13%), permainan dalam talian (12%), sukan (8%), pelaburan (7%), dan jual beli di tempat kerja (7%) merupakan penyebab tindakan disiplin dan pembuangan kerja diambil terhadap pekerja di Kesatuan Eropah[20] dan Amerika Syarikat.[21] Penyalahgunaan internet menyebabkan kehilangan produktiviti dan pendapatan, serta menyebabkan kerugian berjumlah berbilion,[22] iaitu sekitar USD$54 billion setahun mengikut anggaran Vault.com.[23] Kajian yang dijalankan juga mengesahkan penemuan penggunaan internet dan e-mel yang tidak berkaitan dengan kerja, iaitu 50 peratus melayari laman lucah, 92 peratus membeli barang secara dalam talian, 84

18 Leftheriotis, I., & Giannakos, M. N. (2014). Using social media for work: Losing your time or improving your work? *Computers in Human Behavior*, *31*, 134 – 142.

19 Turban, E., Bolloju, N., & Liang, T. P. (2011). Enterprise social networking: Opportunities, adoption, and risk mitigation. *Journal of Organizational Computing and Electronic Commerce*, *21*(3), 202 – 220.

20 *Bărbulescu* lwn *Romania* [2016] *ECHR* 61; [2017] *ECHR* 742.

21 Young, K. S., & Case, C. J. (2004). Internet abuse in the workplace: New trends in risk management. *CyberPsychology & Behavior*, *7*(1), 105 – 111.

22 Stewart, F. (2000). Internet acceptable use policies: Navigating the management, legal, and technical issues. *Information Systems Security*, *9*(3), 1 – 7.

23 Young, K. S., & Case, C. J. (2004). Internet abuse in the workplace: New trends in risk management. *CyberPsychology & Behavior*, *7*(1), 105 – 111.

peratus mencari pekerjaan dalam talian, dan 54 peratus melayari laman sembang semasa di tempat kerja.[24] Kajian Archambault dan Grudin[25] pula mendapati pekerja bersetuju bahawa media sosial ialah tempat yang baik bagi mereka untuk berhibur atau berseronok (83%) dan bersosial (90%). Bagaimanakah cara untuk menyeimbangkan antara hak majikan, hak pekerja dengan hak privasi pekerja? Walau bagaimanapun, artikel ini hanya membincangkan tahap perlindungan privasi semasa bekerja dan ketika berada di tempat kerja.

PERLAKUAN PENCEROBOHAN PRIVASI DI TEMPAT KERJA

Pengawasan Video dan Televisyen Litar Tertutup

Pengawasan menggunakan video di tempat kerja untuk memantau akiviti pekerja kerap dilakukan oleh majikan. Penggunaan video untuk tujuan pengawasan oleh majikan dibenarkan di Amerika Syarikat. Mahkamah di Amerika Syarikat mengambil kira jangkaan pekerja berhubung dengan privasi di tempat kerja yang diawasi. Mahkamah persekutuan memutuskan bahawa pengawasan menggunakan video rakaman tanpa suara adalah tidak dilarang di bawah Tajuk I Akta Privasi Komunikasi Elektronik 1986 yang dikenali sebagai *Title I Electronic Communications Privacy Act (ECPA) 1986*. Namun, video pengawasan yang boleh merakam perbualan atau suara melanggar *Title I ECPA 1986* seperti yang diputuskan dalam kes *Thompson* lwn *Johnson County Community College*.[26]

Keadaan yang sama diguna pakai di Kesatuan Eropah dan di bawah prinsip *common law* apabila pengawasan menggunakan video rakaman dibenarkan tertakluk pada pemberian notis yang jelas dan mencukupi berkenaan dengan pemantauan menggunakan

24 Hamin, Z. (2001). E-mail @ work: Its legal implication on employer's liability. *Malayan Law Journal*, *3*, xxviii.

25 Archambault, A., & Grudin, J. (2012, Mei). A longitudinal study of facebook, linkedin, & twitter use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2741 – 2750). ACM.

26 930 F. Supp. 501 (D. Kan. 1996).

video kamera tersebut. Dalam kes *Peck* lwn *The United Kingdom*[27], rakaman CCTV dianggap sebagai suatu pelanggaran privasi apabila identiti mangsa didedahkan kepada media. Penggunaan video pengawasan di tempat kerja dibenarkan sebagai langkah keselamatan untuk menghalang perbuatan seperti kecurian, salah laku dan perbuatan menceroboh, memantau pematuhan pekerja terhadap tatacara keselamatan pekerjaan dan keselamatan di tempat kerja, serta memantau penilaian prestasi pekerja secara umum. Namun begitu, pengawasan melalui CCTV secara rahsia adalah tidak dibenarkan seperti dalam kes *Kopke* lwn *Germany*.[28]

Penggunaan video kamera dan sistem televisyen litar tertutup adalah antara contoh lain yang biasa digunakan untuk memantau dan mengawasi pekerja di tempat kerja. Pengawasan di tempat kerja semakin meningkat berbanding dengan tempat yang biasanya pekerja menikmati atau mendapat lebih privasi seperti di tandas atau bilik persalinan. Pekerja pejabat pos di bandar raya New York, misalnya menjumpai kamera tersembunyi di dalam tandas. Pekerja Hotel Sheraton di Boston juga dirakam secara rahsia di dalam bilik persalinan mereka. Bagi pekerja yang sentiasa bergerak, syarikat menggunakan pelbagai teknologi yang boleh menjejaki dan mengetahui kedudukan pekerja mereka[29] seperti penggunaan Sistem Kedudukan Sejagat atau *Global Positioning System* (GPS). Sesetengah hospital mengarahkan jururawat memakai lencana pada baju seragam agar kedudukan mereka boleh ditentukan dengan segera.[30]

PEMANTAUAN TELEFON

Pemantauan penggunaan telefon merupakan suatu pencerobohan privasi terhadap pekerja sekiranya dilakukan oleh majikan tanpa asas. Majikan mempunyai budi bicara untuk memantau panggilan

27 [2003] *EHRR* 287.

28 [2010] *ECHR* 1725 Application No. 420/07.

29 Hartman, L. P., & Bucci, G. (1999). The economic and ethical implications of new technology on privacy in the workplace. *Business and Society Review*, *102*(1), 1 – 24.

30 Eric Auchard. (29 Mei, 2001). Monitoring shrinks worker privacy sphere. *Reuters* (p. 1).

telefon yang dibuat atas urusan rasmi oleh pekerja mereka.[31] Suatu program yang dipanggil "Watcall" dihasilkan oleh syarikat bernama Harlequin yang boleh menganalisis panggilan telefon dan mengkategorikan panggilan tersebut kepada "jaringan persahabatan" untuk menentukan corak penggunaan telefon.[32] Sistem pesanan suara juga tertakluk pada pemantauan secara sistematik atau secara rawak oleh majikan.[33] Kedudukan yang sama diterima pakai di bawah undang-undang Kesatuan Eropah dan United Kingdom seperti yang diputuskan dalam kes *Halford* lwn *the United Kingdom*[34] dan *Copland* lwn *United Kingdom*.[35] Dalam kes *Halford*, pemohon yang merupakan seorang polis wanita dinafikan hak kenaikan pangkat atas dasar diskriminasi yang dikenakan terhadapnya. Pemohon mendakwa panggilan telefon rumah dan pejabatnya dipintas bagi mendapatkan maklumat yang tidak memihak kepadanya. Mahkamah memutuskan panggilan telefon pejabat yang dipintas melanggar perlindungan yang diberikan di bawah artikel 8 ECHR. Hal yang sama juga diputuskan dalam *Copland* berkenaan dengan telefon pejabat yang diawasi tanpa pengetahuannya.

Di Amerika Syarikat, *Title III ECPA 1986* mempunyai pelbagai pengecualian. Bagi pengecualian di tempat kerja, dua pengecualian sering digunakan. Pengecualian pertama ialah "kebenaran" atau "keizinan" oleh satu pihak. ECPA 1986 memperuntukkan komunikasi sesuatu pihak boleh dipintas dan boleh memberikan kebenaran awal untuk memintas walaupun pihak yang dipintas perbualan itu tidak menyedari tentang pemintasan yang dibuat. Keizinan sesuatu pihak tidak semestinya secara nyata tetapi boleh berlaku secara tersirat berdasarkan keadaan sekitar atau

31 D'Urso, S. C. (2006). Who's watching us at work? Toward a structural – perceptual model of electronic monitoring and surveillance in organizations. *Communication Theory*, *16*(3), 281 – 303.

32 Van Meter, K. M. (2002). Terrorists/liberators: Researching and dealing with adversary social networks. *Connections*, *24*(3), 66 – 78.

33 Davies, S. (1997, April 29). Watch out for the Old Bill. *Daily Telegraph.*

34 [1997] *ECHR* 32 (20605/92).

35 [2007] *ECHR* 253.

"surrounding circumstances", termasuk pengetahuan tentang pemintasan tersebut. Pengecualian yang kedua ialah yang selalu dikatakan sebagai dalam "keadaan perjalanan biasa urusan" atau "ordinary course of business". Penggunaan pengecualian ini adalah berdasarkan peruntukan ECPA yang menyatakan:

> Apa-apa instrumen telefon, telegraf, peralatan, atau kemudahan, atau apa-apa komponen adalah sebahagian daripadanya,
>
> (i) yang diberikan kepada … pengguna dengan penyedia wayar atau perkhidmatan komunikasi elektronik dalam perjalanan biasa perniagaannya … atau
> (ii) yang digunakan oleh pemberi wayar atau perkhidmatan elektronik dalam perjalanan biasa perniagaannya.

Merujuk kes *Watkins* lwn *L. M. Berry & Co.*,[36] defendan, iaitu Berry Co. mengambil Carmie Watkins, iaitu plaintif sebagai pekerja untuk menjual iklan melalui telefon dari pejabat Berry & Co. Berry & Co. membuat suatu polisi yang dimaklumkan kepada semua pekerja bahawa semua panggilan telefon merupakan sebahagian daripada latihan kepada pekerja. Polisi tersebut membenarkan pekerja untuk membuat panggilan peribadi tetapi tidak dimaklumkan sama ada panggilan peribadi juga akan dipantau. Dalam kes ini, rakan Puan Watkins menelefonnya semasa di tempat kerja dan rakannya memberitahu Puan Watkins berhubung dengan peluang kerja yang baharu. Panggilan telefon tersebut sebenarnya dipantau oleh Berry & Co. Puan Watkins menyaman Berry & Co. tetapi mahkamah menolak saman tersebut dan membenarkan tindakan Berry & Co. kerana terdapat keizinan secara nyata dan tersirat berhubung dengan pemantauan panggilan telefon. Walau bagaimanapun, mahkamah rayuan menolak keputusan tersebut dan membenarkan rayuan Puan Watkins kerana keizinan memantau panggilan telefon tidak boleh diberikan secara tersirat. Menurut hakim mahkamah rayuan:

> *Consent is not to be cavalierly implied. Title III expresses a strong purpose to protect individual privacy by strictly limiting the occasion*

36 704 F.2d 577 (11th Cir. 1983).

on which interception may lawfully take place .... Knowledge of the capability of monitoring alone cannot be considered implied consent.[37]

Mahkamah juga menerangkan maksud pengecualian "keadaan perjalanan biasa urusan" sebagai:

It is not enough for Berry Co. to claim that its general policy is justifiable as part of the ordinary course of business. We have no doubt that it is. The question before us, rather, is whether the interception of this call was in the ordinary course of business. In the "ordinary course of business" cannot be expanded to mean anything that interests a company. We hold that a personal call may not be intercepted in the ordinary course of business . . . except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not. In other words, a personal call may be intercepted in the ordinary course of business to determine its nature but never its contents.[38]

Dalam kes *Deal* lwn *Spears*,[39] plantif yang bernama Sibbie Deal diambil bekerja di gudang yang dimiliki oleh Newell dan Juanita Spears. Tuan dan Puan Spears meminta Sibbie Deal untuk mengurangkan penggunaan telefon pejabat untuk membuat panggilan peribadi, dan Sibbie Deal juga diberitahu Spears bahawa pemantauan telefon mungkin akan dibuat. Gudang tersebut kemudiannya mengalami kecurian dan Tuan dan Puan Spears percaya bahawa perbuatan tersebut disebabkan oleh "kerja orang dalam" dan mengesyaki Deal. Tuan dan Puan Spears memasang pita rakaman telefon di gudang tersebut tanpa memaklumkan bahawa panggilan dan perbualan telefon dirakam. Setelah lebih dari tujuh minggu, Tuan dan Puan Spears merakam lebih dari 24 jam perbualan Deal termasuk perbualan yang berbaur seks dengan bukan pekerja gudang itu. Deal menyaman Spears tetapi Spears menggunakan alasan pengecualian, iaitu "keizinan" dan keadaan "perjalanan biasa urusan perniagaan".

37 *Watkins* lwn *L. M. Berry & Co*, p. 581.
38 *Watkins* lwn *L. M. Berry & Co.* p. 582, 583.
39 980 F.2d 1153 (8th Cir. 1992).

Dalam perbicaraan di mahkamah daerah, hujahan Spears ditolak dan USD40 000 diberikan kepada Deal sebagai pampasan. Mahkamah rayuan juga menyokong keputusan mahkamah daerah, serta menyatakan bahawa "keizinan" tidak boleh diterima kerana Tuan dan Puan Spears tidak memaklumkan tentang rakaman itu. Mereka hanya memaklumkan bahawa panggilan telefon Deal mungkin akan dirakam untuk tujuan pengurangan panggilan peribadi dengan menggunakan telefon pejabat. Pasangan Spears mengesaki Deal terlibat dalam kes kecurian yang berlaku dan mengharapkan agar Deal membuat pengakuan melalui panggilan yang dirakam.

Berhubung dengan keadaan "perjalanan biasa urusan perniagaan", mahkamah memutuskan:

> *The Spearses had a legitimate business reason for listening in: they suspected Deal's involvement in a burglary . . . and hoped she would incriminate herself. Moreover, Deal was abusing her privileges by using the phone for numerous personal calls . . . when there were customers in the store. The Spearses might legitimately have monitored Deal's calls to the extent necessary to determine that the calls were personal and made or received in violation of store policy. But, the Spearses recorded twenty-two hours of calls, and . . . listened to all of them…, Deal might have mentioned the burglary at any time during the conversations, but we do not believe that the Spearses' suspicions justified the extent of the intrusion. The scope of the interception in this case takes us well beyond the boundaries of the ordinary course of business.*[40]

Berdasarkan kes tersebut, terdapat beberapa prinsip yang diamalkan oleh mahkamah di Amerika Syarikat. Pertama, pemilikan majikan terhadap peralatan semata-mata tidak memberikan kuasa penuh kepada majikan untuk memintas perbualan telefon pekerjanya. Kedua, pengecualian keadaan "perjalanan biasa urusan perniagaan" selalunya menuntut pihak majikan (sebagai pemilik peralatan) untuk membuktikan:

40 *Deal* lwn *Spears*, p. 1158.

(a) majikan mempunyai sebab tertentu untuk memintas komunikasi yang tertentu, dan;

(b) majikan mengambil langkah yang munasabah untuk tidak melangkaui tujuan pemintasan itu.

Dengan kata lain, pengecualian ini tidak membenarkan pemintasan secara menyeluruh (*blanket*), terutama apabila melibatkan komunikasi peribadi pekerja. Ketiga, keizinan secara tersirat mestilah diketahui dengan jelas oleh pekerja bahawa komunikasi mereka akan dipantau, dirakam atau dipintas dan bukan sekadar memaklumkan bahawa perbualan mereka mungkin atau boleh dipintas kerana tindakan tersebut adalah tidak memadai.

E-mel dan Pemantauan Penggunaan Internet

Pencerobohan privasi juga amat mudah dilakukan terhadap komputer dan rangkaiannya kerana sifatnya yang sangat kondusif untuk diawasi. Kajian yang dijalankan oleh Yayasan Privasi[41] menunjukkan bahawa 14 juta pekerja di Amerika Syarikat tertakluk pada pengawasan ini secara berterusan. Majikan boleh memantau e-mel secara rawak melalui semakan penghantaran e-mel, mengkaji semula penghantaran e-mel oleh pekerja tertentu, atau menetapkan syarat penghantaran e-mel. Beberapa program boleh digunakan oleh majikan seperti penggunaan algoritma untuk menganalisis corak komunikasi dan menukarkannya kepada imej. Monitor kemudiannya boleh melihat imej tersebut berdasarkan pola lalu lintas dan mengesannya sama ada data tersebut sensitif dan berisiko.

Ramai majikan bergantung pada perisian bagi memantau mesej e-mel dari jarak jauh. Dengan beberapa klik sahaja mereka dapat melihat setiap mesej e-mel yang dihantar atau diterima oleh pekerja sama ada sah atau tidak. Majikan memberikan pelbagai sebab untuk memasang perisian tersebut. Antaranya termasuklah melindungi rahsia perdagangan atau mencegah insiden gangguan

41 Privacy Foundation. (2001). *The extent of systematic monitoring of employee e-mail and internet use*. Retrieved from http://www.sonic.net/~undoc/extent.htm.

seksual,[42] mengelak saiz mel yang besar yang boleh menyebabkan jaringan terganggu, dan penggunaan terlalu banyak lebar jalur (*bandwith*). Selain itu, syarikat juga tidak mahu pekerja membuang masa syarikat menggunakan e-mel untuk kegunaan peribadi dan syarikat tidak mahu menanggung liabiliti perundangan akibat kesalahan yang dilakukan oleh pekerja.[43]

Pencerobohan privasi melalui pemantauan e-mel dan internet pekerja berlaku di United Kingdom dan Kesatuan Eropah. Hal ini jelas dapat dilihat dalam kes *Bărbulescu* dan *Copland*. Mahkamah memutuskan bahawa berlaku pelanggaran artikel 8. Dalam kes *Copland*, mahkamah memutuskan:[44]

> *According to the Court's case-law, telephone calls from business premises are prima facie covered by the notions of "private life" and "correspondence" for the purposes of Article 8... It follows logically that e-mails sent from work should be similarly protected under Article 8 ... The applicant in the present case had been given no warning that her calls would be liable to monitoring, therefore she had a reasonable expectation as to the privacy of calls made from her work telephone ... The same expectation should apply in relation to the applicant's e-mail and internet usage.*

Sementara itu, dalam kes *Bărbulescu*, majikan mengenakan sekatan sepenuhnya terhadap peralatan pejabat termasuk internet bagi kegunaan peribadi. Pemohon atas permintaan majikan membuka akaun "Yahoo Messenger" bagi tujuan menghantar pesanan dan sebagai maklum balas kepada pelanggan syarikat. Walau bagaimanapun, pemohon menggunakan akaun ini untuk menghantar pesanan kepada saudaranya dan juga tunangnya. Akibat tindakan tersebut, pemohon dibuang kerja oleh majikannya. Mahkamah Hak Asasi Manusia Kesatuan Eropah memutuskan bahawa berlaku pelanggaran artikel 8 dalam kes ini.

---

42 Smith-Butler, L. (2009). Workplace privacy: We'll be watching you. *Ohio NUL Rev.*, *35*, 53.

43 Smith, W. P., & Tabak, F. (2009). Monitoring employee e-mails: Is there any room for privacy? *The Academy of Management Perspectives*, *23*(4), 33 – 48.

44 *Copland* lwn *UK* [2007] *ECHR* 253, perenggan 41 – 42.

Menurut Pengurusan Penyelidikan Amerika Syarikat,[45] hampir dua pertiga daripada semua pekerja syarikat dikenakan tindakan tatatertib dan 27 peratus daripadanya dipecat atas alasan penyalahgunaan e-mel atau penyambungan internet. Contohnya, Dow Chemical Company memecat 50 pekerja Amerika Syarikat dan mengugut untuk menggantung kerja 200 orang pekerjanya selepas membuka e-mel peribadi lebih daripada 7000 e-mel pekerjanya dan dapat mengesan bahan yang menjelikkan. New York Times juga memecat 23 kakitangannya pada tahun 1999 kerana menghantar mesej lucah.[46]

Di Hong Kong, Pejabat Pesuruhjaya Privasi Data Peribadi pada tahun 2000 ditugaskan menjalankan kajian untuk memeriksa pengawasan majikan di tempat kerja. Menurut kaji selidik tersebut, 64 peratus daripada majikan memasang sekurang-kurangnya sejenis alat pemantauan pekerja tetapi hanya 18 peratus daripada majikan mempunyai dasar bertulis tentang pemantauan pekerja. Di samping itu, 35 peratus responden tidak tahu kewujudan polisi tersebut.[47]

Sebaliknya, Perancis mewujudkan dasar yang ketat untuk melindungi privasi penggunaan e-mel pekerja. Mahkamah Agung Perancis dalam kes *Nikon* lwn *Onof*[48] menyatakan bahawa majikan tidak mempunyai hak untuk membuka apa-apa mesej pekerja mereka. Mahkamah memutuskan dalam kes antara Nikon dengan bekas pekerja, syarikat itu tidak mempunyai hak automatik untuk membuat carian melalui peti masuk e-mel.

Walaupun sistem perundangan di Amerika Syarikat tidak secara khusus memperuntukkan persoalan hak dan tanggungjawab berhubung dengan penggunaan e-mel di tempat kerja, namun mahkamah di Amerika Syarikat secara konsisten menyokong hak

45 American Management Association. (2001). *Annual survey on workplace monitoring and surveillance 2001*, 18 April.

46 Young, K. S., & Case, C. J. (2004). Internet abuse in the workplace: New trends in risk management. *CyberPsychology & Behavior*, *7*(1), 105 – 111.

47 Chung, W., & Paynter, J. (2002, Januari). Privacy issues on the Internet. In *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on* (p. 9). IEEE.

48 Decision No. 4164, 2 Oktober 2001 (99 – 42, 942)

majikan untuk memantau dan mengawasi e-mel pekerja.[49] Dalam kes *Smyth* lwn *Pillsbury Co*,[50] mahkamah mendapati bahawa seseorang pekerja tidak akan mempunyai jangkaan privasi yang munasabah dalam kandungan e-melnya yang secara sukarela dihantar melalui e-mel majikan, walaupun majikan memberikan jaminan kepada pekerjanya bahawa komunikasi e-mel akan kekal sebagai rahsia dan istimewa. Mahkamah memberikan alasan bahawa apabila pekerja menyampaikan komen kepada orang yang kedua menerusi e-mel yang digunakan oleh seluruh syarikat, mana-mana jangkaan privasi yang munasabah akan hilang. Dan jika pekerja mempunyai jangkaan privasi yang munasabah dalam kandungan e-mel, seseorang yang munasabah tidak akan menganggap pemintasan komunikasi oleh majikan itu sebagai suatu kesalahan besar yang menyakitkan hati.

Dalam satu lagi kes *United States of* America lwn *Simons*,[51] diputuskan bahawa majikan yang mempunyai dasar untuk "kegunaan perniagaan sahaja" dalam penggunaan internet boleh menjalankan audit rangkaian komputer untuk mengenal pasti, menamatkan, dan mendakwa aktiviti yang tidak dibenarkan. Mahkamah mendapati bahawa walaupun pekerja mungkin mempunyai jangkaan privasi yang sah terhadap peralatan komputer mereka, beberapa amalan pejabat, peraturan atau prosedur boleh mengurangkan jangkaan tersebut.

Title III ECPA dalam takrifannya terhadap "komunikasi elektronik" merangkumi e-mel dan internet. Walau bagaimanapun, definisi *Title III* mengandungi kelompangan utama, "komunikasi elektronik" tidak merangkumi komunikasi dalam storan elektronik. Dalam kes *Steve Jackson Games Inc.* lwn *United States Secret Service*,[52] plaintif Steve Jackson Games Inc (SJGI) mempunyai papan buletin elektronik yang "menawarkan kepada pelanggan keupayaan untuk menghantar dan menerima e-mel peribadi. E-mel peribadi disimpan buat sementara waktu sehingga penutur 'dipanggil' (menggunakan komputer dan modem mereka) dan membaca e-mel

49 Smith, W. P., & Tabak, F. (2009). Monitoring employee e-mails: Is there any room for privacy?. *The Academy of Management Perspectives*, *23*(4), 33 – 48.

50 914 F. SUPP. 97 (ED Pa. 1996).

51 206 F.3d 392 (4 Cir. 2000).

52 36 F.3d 457 (5 Cir. 1994).

mereka." Defendan, United State Secret Service (USSS) membaca "162 item belum dibaca, e-mel peribadi". Walau bagaimanapun, SJGI menyaman USSS. Mahkamah daerah memberikan penghakiman yang memihak kepada USSS dan memutuskan bahawa e-mel tersebut tidak diperoleh oleh USSS kerana e-mel tersebut hanya diperoleh secara serentak ketika transmisi komunikasi dilakukan (*contemporaneous with the transmission of these communications*). Mahkamah juga memutuskan tidak seperti definisi "komunikasi wayar", definisi "komunikasi elektronik" tidak termasuk dalam storan elektronik komunikasi itu.

Keputusan yang sama juga diputuskan dalam kes *Bohach* lwn *City of Reno*[53] kerana jabatan polis di bandar tersebut mempunyai sistem "Alphapage". Seorang pegawai polis boleh berkomunikasi dengan pegawai lain dengan menaip pada papan kekunci yang disambungkan ke komputer. Ketua polis boleh memberikan amaran kepada semua pengguna bahawa setiap mesej akan "logged" pada rangkaian. Walau bagaimanapun, ketua tersebut tidak memberikan amaran kepada pegawai bahawa mesej disimpan secara automatik dan perkara ini tidak diketahui oleh pegawai terbabit. Akhirnya, pesanan tersebut disimpan untuk digunakan dalam prosiding hal ehwal dalaman. Berdasarkan *Title III,* dua pegawai menyaman City of Reno tetapi mahkamah menolak permohonan saman tersebut dan menyatakan:

> *All messages are recorded and stored not because anyone is "tapping" the system, but simply because that's how the system works. It is an integral part of the technology… E-mail messages are, by definition, stored in a routing computer. An electronic communication may be put into electronic storage, but the storage is not itself part of the communication. The statutes therefore distinguish the "interception" of an electronic communication at the time of transmission from the retrieval of such a communication after it has been put into "electronic storage*.[54]

53 932 F.Supp. 1232, 1236 (D. Nev. 1996).
54 *Bohach* lwn *City of Reno*, pp. 1234 – 1236.

Dalam kes *Garrity* lwn *John Hancock Mutual Life Insurance Co.*,[55] dua pekerja syarikat insurans didapati mengedarkan e-mel yang menjelikkan dan lucah dengan menggunakan sistem elektronik syarikat. Seorang rakan sekerja yang menerima e-mel tersebut membuat aduan kepada pihak pengurusan dan aduan tersebut mendorong penyiasatan dilakukan serta-merta mengakibatkan semua e-mel pekerja diperiksa. Kedua-dua pekerja terbabit mendakwa bahawa mereka menggunakan e-mel dan kata laluan peribadi sejak bekerja dengan syarikat itu. Di sebalik pertikaian itu, mahkamah mendapati bahawa jangkaan privasi yang berlaku tidak munasabah atas beberapa sebab. Antara sebab terpenting di sebalik keputusan mahkamah termasuklah perincian syarikat, dasar penerbitan e-mel syarikat yang menyatakan bahawa pekerja diberitahu tentang larangan penggunaan e-mel syarikat dan pelanggaran dasar ini mengakibatkan tindakan disiplin diambil, termasuk pemberhentian kerja. Mahkamah juga bergantung pada beberapa siri kes dari negara lain yang menyatakan bahawa dalam ketiadaan apa-apa dasar syarikat, penyerahan sukarela komen peribadi terhadap sistem yang digunakan oleh seluruh syarikat menafikan sebarang kepentingan privasi dalam komunikasi tersebut. Selain itu, mahkamah menolak sebarang tanggapan bahawa dengan mencipta kata laluan peribadi atau fail, majikan kehilangan hak pemeriksaan fail e-mel yang digunakan oleh pekerja tetapi diselenggarakan oleh syarikat tersebut. Akhir sekali mahkamah memutuskan bahawa jangkaan privasi yang munasabah diperoleh kerana majikannya secara sah melindungi pekerja daripada gangguan. Selain itu, tindakan syarikat membenarkan pekerja menggunakan sistem e-mel syarikat untuk mengedarkan bahan yang menjelikkan atau mengganggu rakan sekerja menyebabkan majikan boleh tertakluk pada liabiliti atau tanggungan yang berpotensi untuk diganggu atau menghadapi pelbagai bentuk diskriminasi.

Oleh itu, majikan perlu mencegah penyebaran bahan tersebut. Kes *Garrity* boleh dijadikan sebagai panduan kepada majikan dan mahkamah, terutama sejak ramai majikan di sektor swasta

55 18 *IER* Kes 981 (Mass. Dist. Ct. 2002).

mewujudkan polisi syarikat yang mengehadkan jangkaan privasi pekerja, walaupun privasi mungkin dianggap perkara biasa.

Berdasarkan kes yang dinyatakan, timbul persoalan undang-undang dan etika yang kompleks tentang hak asasi pekerja berhubung dengan privasi dan proses yang sewajarnya, seperti bagaimanakah jika seorang pekerja menghantar e-mel yang menjelikkan secara tidak sengaja atau dengan niat jahat kerana e-mel tersebut akan kekal dan tidak sewenang-wenangnya dihapuskan. Tindakan ini bukan sahaja boleh menjejaskan hubungan, malahan menggugat kepercayaan pekerja terhadap pihak pengurusan. Masalah ini juga timbul apabila syarikat memantau semua aktiviti internet yang melayari laman yang "tidak sesuai". Pengawasan tersebut menyamai pengawasan terhadap bahan pornografi yang memberikan kesan negatif kepada pekerja. Seseorang pekerja secara tidak sengaja boleh melawat laman web lucah apabila membuka e-mel spam yang menghubungkannya dengan apa-apa laman web atau laman web yang tidak sengaja dilawati apabila dipaparkan sebagai "hit" sebagai tindak balas terhadap "perfectly innocent search query". Walau bagaimanapun, teknologi pengawasan tidak membezakan antara pihak yang melayarinya secara tidak sengaja dengan pihak yang melayarinya dengan sengaja.

Pemantauan terhadap tindakan pekerja yang melayari ruangan sembang juga memberikan tekanan di tempat kerja. Terdapat peningkatan trend dalam kalangan syarikat untuk memecat atau mendakwa pekerja kerana mendedahkan "rahsia perdagangan" syarikat atau memfitnah syarikat di laman sembang[56] seperti kes *John Doe*. Keadaan ini berlaku kerana apabila syarikat mendapati ada pihak tertentu yang melayari laman sembang tanpa nama dan seterusnya memerhatikan pihak tertentu dalam laman sembang terdapat ucapan "tidak sah", syarikat perlu bertindak menghantar sapina kepada perkhidmatan mesej-*board* seperti *Yahoo*! atau *America Online* untuk mendapatkan identiti penulis tersebut. Pembekal perkhidmatan yang sering bertukar ganti

56 Kaupins, G., & Minch, R. (2005, Januari). Legal and ethical implications of employee location monitoring. In *System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on* (p. 133a). IEEE.

akan mengenal pasti maklumat tersebut berdasarkan sapina yang dihantar tanpa sebarang notis kepada individu. Bilangan kes ini semakin meningkat dengan pesat dan tidak hanya mengancam privasi pekerja tetapi juga hak mereka untuk tidak mahu dikenali dan kebebasan bersuara.

Oleh itu, tidak hairanlah jika pihak majikan prihatin terhadap penggunaan komputer di tempat kerja kerana bimbang pekerja akan banyak membuang masa untuk berbual atau membeli-belah secara dalam talian. Lebih merisaukan jika pekerja menimbulkan liabiliti[57] dengan melayari dan mengedarkan bahan berunsur porno, perkauman, atau bahan lain yang tidak wajar atau menyalahi undang-undang.

Geledahan di Tempat Kerja

Geledahan di tempat kerja juga merupakan suatu bentuk pencerobohan privasi terhadap pekerja. Dalam kes *Libert* lwn *France,*[58] pemohon merupakan pekerja syarikat keretapi Perancis, iaitu French National Railway Company (SNCF). Komputer syarikat yang digunakannya dirampas semasa ketiadaannya. Dalam komputer tersebut, ditemukan fail pornografi dan sijil palsu, dan kemudiannya pemohon dibuang kerja oleh syarikatnya. Mahkamah Hak Asasi Kesatuan Eropah memutuskan bahawa tiada pelanggaran privasi di bawah artikel 8. Mahkamah juga memutuskan bahawa majikan mempunyai hak untuk melindungi kepentingan majikan, iaitu memastikan pekerja menggunakan kemudahan komputer yang diberikan selaras dengan obligasi kontrak dan peraturan yang ditetapkan.

Mahkamah agung di Amerika Syarikat dalam kes *O'Connor* lwn *Ortega*[59] memutuskan bahawa pekerja sepatutnya boleh secara munasabahnya menjangkakan mereka mempunyai hak privasi di tempat kerja bergantung pada kes masing-masing. Terdapat banyak perbezaan pada persekitaran tempat kerja yang menyebabkan hak

57 Smith, W. P., & Tabak, F. (2009). Monitoring employee e-mails: Is there any room for privacy?. *The Academy of Management Perspectives*, *23*(4), 33 – 48.

58 [2018] *ECHR* 185.

59 480 U.S. 709 (1987).

privasi pekerja juga bergantung pada persekitaran pekerjaan tersebut. Mahkamah juga memutuskan bahawa majikan yang merupakan jabatan atau agensi kerajaan atau awam juga tertakluk pada standard yang sama, iaitu "secara munasabah" berhubung dengan pelanggaran privasi pekerjanya. Standard dalam perlindungan privasi "secara munasabah" terpakai di jabatan kerajaan sama ada siasatan tersebut berkaitan dengan pekerjaan atau tidak berkaitan dengan pekerjaan. Namun, mahkamah di Amerika Syarikat dalam kes tersebut juga memutuskan bahawa keperluan untuk majikan mendapatkan waran geledah apabila ingin membuat siasatan atau geledahan di tempat kerja pekerjanya akan mengganggu rutin perniagaan dan menyebabkan kesulitan yang tidak sepatutnya. Berhubung dengan carian atau geledahan terhadap komputer yang digunakan oleh pekerja di tempat kerja, mahkamah persekutuan di Amerika Syarikat dalam kes *Leventhal* lwn *Knapek*[60] memutuskan bahawa pekerja mempunyai jangkaan privasi yang munasabah di tempat kerja berhubung dengan kandungan komputer pejabat, tetapi siasatan yang melibatkan geledahan untuk mencari bukti dan keterangan berhubung dengan salah laku pekerja selaras dengan perlembagaan dan undang-undang sekiranya siasatan itu berlandaskan bidang kuasa yang sepatutnya, iaitu siasatan dan geledahan itu bersifat objektif dan tidak bersifat mencabuli hak (*intrusive*).

Dalam sektor swasta, pekerja diputuskan mempunyai jangkaan privasi yang munasabah dalam beberapa perkara termasuk perkara peribadi. Dalam kes *K-Mart Corp.* lwn *Trotti*[61] diputuskan bahawa pekerja yang tidak disyaki melakukan perbuatan salah laku boleh menggunakan kunci almari dengan kebenaran majikan, dan mempunyai hak jangkaan privasi terhadap almari tersebut dan kandungannya. Majikan pula boleh dikenakan tanggungan sekiranya mendedahkan maklumat yang bersifat rahsia berhubung dengan pekerjanya seperti yang diputuskan dalam kes *Miller* lwn *Motorola Inc*.[62]

60 266 F.3d 64 (2d Cir. 2001).
61 677 S.W.2d 632 (Tex. Ct. App. 1984).
62 560 N.E.2d 900 (Ill. App. 1990).

PRIVASI DI TEMPAT KERJA DI MALAYSIA

Secara ringkasnya, seperti yang dinyatakan sebelum ini, Perlembagaan Persekutuan Malaysia tidak mengiktiraf secara khusus hak privasi tetapi memperuntukkan beberapa hak yang berkaitan, termasuk kebebasan diri, kebebasan berhimpun, dan kebebasan bersuara dan bergerak di bawah Perlembagaan Persekutuan. Antara undang-undang lain yang turut mengehadkan hak privasi individu termasuklah seksyen 43 Akta Suruhanjaya Pencegahan Rasuah Malaysia 2009 yang memberikan kuasa kepada Peguam Negara untuk melakukan pemintasan e-mel dan pengintipan dengar melalui telefon dalam siasatan kes rasuah. Seksyen 234 Akta Komunikasi dan Multimedia 1998 melarang pemintasan yang menyalahi undang-undang komunikasi, dan di bawah seksyen 245 hingga seksyen 247 menetapkan peraturan bagi carian komputer, mandat akses kepada kunci penyulitan, dan membenarkan polis untuk memintas komunikasi tanpa waran jika seorang pendakwa raya percaya komunikasi mungkin mengandungi maklumat yang berkaitan dengan sesuatu penyiasatan. Walau bagaimanapun, dalam amalan peruntukan Komunikasi dan Multimedia 1998, sekatan terhadap pemintasan telekomunikasi dilihat kerap diabaikan atau dibatasi oleh undang-undang lain, termasuk seksyen 30 Akta Keselamatan Dalam Negeri 1960 dan seksyen 10(2) dan (3) Akta Jenayah Komputer 1997.

Berhubung dengan privasi pekerja di tempat kerja, tiada undang-undang khusus yang mengawal isu ini. Bekas Perdana Menteri, Tun Abdullah Hj. Ahmad Badawi (ketika itu sebagai Timbalan Perdana Menteri) dalam suatu sidang akhbar menyatakan bahawa tidak ada undang-undang khusus yang membenarkan penamatan kontrak perkhidmatan mana-mana penjawat awam yang melayari laman web lucah dengan menggunakan komputer pejabat semasa waktu bekerja. Beliau menambah bahawa hanya tindakan tatatertib boleh diambil terhadap penjawat awam yang menyalahgunakan kemudahan pejabat. Walau bagaimanapun, Pengarah Eksekutif Persekutuan Majikan Malaysia, Encik Shamsuddin Bardan berkeras dan mencadangkan bahawa pekerja yang melayari laman web lucah

pada waktu pejabat perlu diberhentikan kerana menyalahgunakan kemudahan pejabat.[63] Oleh itu, tindakan masih boleh diambil terhadap mana-mana pekerja Malaysia yang menyalahgunakan mana-mana kemudahan pejabat untuk kegunaan peribadi. Dalam erti kata lain, para pekerja tertakluk pada mana-mana pengawasan dan pemantauan oleh majikan mereka.

Walau bagaimanapun, 38 peratus pekerja di Malaysia percaya bahawa data mereka selamat dan tidak disalahgunakan oleh majikan mereka. Berdasarkan kajian yang dilakukan oleh Asia MasterCard Ideal, pekerja Malaysia sangat berhati-hati menggunakan telefon untuk kegunaan peribadi kerana mereka percaya perbualan mereka terbuka pada pemintasan oleh majikan mereka.[64]

Oleh itu, suatu undang-undang khusus perlu diwujudkan untuk melindungi privasi pekerja di tempat kerja. Buat masa ini, Malaysia masih mengguna pakai dan mengaplikasikan undang-undang *common law* untuk menangani hal yang berkaitan dengan privasi pekerja di tempat kerja.

UNDANG-UNDANG PERLINDUNGAN DATA PERIBADI MALAYSIA

Parlimen Malaysia meluluskan Akta Perlindungan Data Peribadi 2010 yang bertujuan mengawal pengumpulan, pemilikan, pemprosesan dan penggunaan data peribadi oleh individu atau organisasi supaya dapat memberikan perlindungan kepada data peribadi individu dan mewujudkan suatu set peraturan dan garis panduan yang sama tentang pengendalian dan pengawalan data peribadi oleh mana-mana orang atau organisasi.

Di bawah akta tersebut, istilah "data peribadi" atau "personal data" ditakrifkan sebagai "apa-apa maklumat yang direkodkan

63 *Utusan Malaysia*. (2002, 13 Julai). Pekerja layari laman web lucah dikenakan tindakan disiplin. Retrieved from http://ww1.utusan.com.my/utusan/info.asp?y=2002&dt=0714&pub=Utusan_Malaysia&sec=Muka_Hadapan&pg=mh_07.htm .

64 Bernama. (2001, 10 Mac). Ramai rasa selamat dengan rekod pekerja. Retrieved from http://ww1.utusan.com.my/utusan/info.asp?y=2001&dt=0311&pub=Utusan_Malaysia&sec=Ekonomi&pg=ek_06.htm.

dalam dokumen yang boleh diproses secara keseluruhannya atau sebahagiannya oleh mana-mana cara automatik atau sebaliknya yang berkaitan secara langsung atau tidak langsung kepada individu yang tinggal yang dikenal pasti atau boleh dikenal pasti daripada maklumat itu atau daripada itu dan maklumat lain milik pengguna data, termasuk apa-apa ungkapan pendapat tentang individu dan apa-apa petunjuk tentang niat pengguna data yang berkenaan dengan individu itu".[65] "Subjek data" pula bermaksud "individu yang menjadi subjek data peribadi",[66] manakala "pengguna data" bermaksud "seseorang yang sama ada bersendirian atau bersama-sama orang lain mengawal pengumpulan, memegang, memproses atau menggunakan data peribadi tetapi tidak termasuk mana-mana orang yang mengumpul, memegang, memproses atau menggunakannya bagi pihak orang lain".[67] Oleh itu, orang yang mengumpul bahan untuk pihak ketiga tidak termasuk di bawah takrifan definisi ini.

Sebarang jenis pemprosesan data peribadi juga perlu mematuhi semua prinsip data. Proses jangka ditakrifkan secara meluas sebagai "menjalankan sebarang operasi atau set operasi dan data peribadi termasuk rakaman, pindaan, pemotongan, pengorganisasian, penyesuaian, perubahan, proses mendapatkan semula, perundingan, penjajaran, kombinasi, penyekatan, pemadaman, pemusnahan atau penyebaran data peribadi."[68] Hal ini bermakna jika fail hanya diambil sudah boleh dianggap sebagai sedang diproses dan tertakluk pada prinsip data. Peruntukan seksyen 5(1) menetapkan semua prinsip data dalam jadual itu hendaklah dipatuhi apabila data peribadi yang dikumpul, dipegang, diproses atau digunakan oleh pengguna data. Antara prinsip tersebut termasuklah prinsip am; prinsip notis dan pilihan; prinsip penzahiran; prinsip keselamatan; prinsip penyimpanan; prinsip integriti data; dan prinsip akses.

Dengan kata lain, prinsip ini menetapkan bahawa data yang dikumpulkan hendaklah dikutip secara adil dan sah. Data subjek juga perlu diberitahu tentang tarikh, jenis data peribadi dan tujuan

65 Seksyen 4 Akta Perlindungan Data Peribadi 2010.
66 Seksyen 4 Akta Perlindungan Data Peribadi 2010.
67 Seksyen 4 Akta Perlindungan Data Peribadi 2010.
68 Seksyen 4 Akta Perlindungan Data Peribadi 2010.

data peribadi tersebut dikumpulkan. Dalam hal ini, pengumpulan data sah jika berkaitan secara langsung dengan fungsi atau aktiviti pengguna data, atau memenuhi keperluan tersebut. Data yang dikumpulkan juga perlu mencukupi, relevan dan tidak berlebihan. Data peribadi yang dikumpulkan juga hanya boleh digunakan untuk tujuan pengumpulan data atau apa-apa tujuan lain yang berkaitan secara langsung dengannya. Sebaik sahaja tujuan pengumpulan maklumat itu terhenti, maklumat peribadi perlu dipadam, melainkan pemadaman itu dilarang di bawah mana-mana undang-undang atau bertentangan dengan kepentingan awam.

Selain itu, prinsip di bawah seksyen 5(1) juga menghendaki bahawa data peribadi tidak boleh didedahkan kecuali yang berkaitan dengan tujuan pengumpulannya. Oleh itu, seksyen 45(2) mengandungi pengecualian terhadap pemakaian prinsip perlindungan data peribadi seperti untuk pencegahan atau pengesanan jenayah atau bagi maksud penyiasatan; penangkapan atau pendakwaan pesalah; atau pentaksiran atau pemungutan apa-apa cukai atau duti atau apa-apa pengenaan lain yang serupa jenisnya. Akhir sekali, data subjek boleh menarik balik persetujuannya untuk mendedahkan data peribadinya. Dalam hal ini, pengguna data itu mempunyai tugas untuk berhenti memegang, memproses atau menggunakan data peribadi tersebut.

Berdasarkan peruntukan Akta Perlindungan Data Peribadi 2010, didapati bahawa tiada perlindungan privasi diberikan di bawah akta ini kerana perlindungan privasi di Malaysia masih mengguna pakai prinsip *common law*.[69] Oleh yang demikian, dicadangkan agar perlindungan privasi ini diperuntukkan secara jelas dalam undang-undang bertulis, sekali gus melindungi privasi pekerja di Malaysia.

KESIMPULAN

Ramai yang percaya bahawa semenjak majikan mempunyai hak milik atau kawalan terhadap premis kerja, kandungan dan kemudahannya, pekerja menyerahkan semua hak dan jangkaan

69 Yusoff, Z. M. (2011). The Malaysian Personal Data Protection Act 2010: A Legislation Note. *NZJPIL*, *9*, 119.

terhadap privasi dan kebebasan daripada pencerobohan, manakala selebihnya hanya mengelak daripada ditanya dengan cara membuatkan para pekerja bersetuju untuk diawasi, dipantau dan diuji sebagai syarat untuk mendapatkan pekerjaan. Walau bagaimanapun, terdapat pelbagai negara di dunia mengiktiraf privasi pekerja di tempat kerja mereka, meskipun tidak mutlak. Di Amerika Syarikat, ECPA merupakan suatu bahagian daripada undang-undang yang sangat penting yang mengiktiraf hak privasi secara umum, walaupun mahkamah kebiasaannya lambat mengiktiraf hak pekerja terhadap privasi. Dalam kes *Whalen* lwn *Roe*,[70] hak perlembagaan untuk mendapatkan maklumat privasi, iaitu maklumat peribadi pekerja diiktiraf dan diputuskan boleh dilindungi daripada didedahkan oleh majikan.

Di negara Eropah, pengumpulan dan pemprosesan maklumat peribadi dilindungi oleh Perlindungan Data Kesatuan Eropah dan Arahan Privasi Telekomunikasi (*Telecommunication Privacy Directives*). Sebagai contoh, Austria, Jerman, Norway dan Sweeden mempunyai kod pekerja yang kukuh dan undang-undang privasinya secara langsung atau tidak langsung melarang atau menyekat pengawasan seperti ini. Di Finland, undang-undang baharu tentang Perlindungan Data dalam Persekitaran Kerja mula berkuat kuasa pada bulan Oktober 2001. Pada bulan Oktober 2000, Pesuruhjaya Privasi United Kingdom mengeluarkan "Kod Amalan Pekerjaan Perlindungan Data", iaitu draf kod panduan bagi hubungan majikan dengan pekerja. Pada tahun 1999, Kerajaan Sweden mewujudkan jawatankuasa untuk mengkaji isu privasi di tempat kerja. Pada bulan Mac 2002, jawatankuasa tersebut mencadangkan suatu undang-undang yang melindungi maklumat peribadi para pekerja, bekas pekerja dan pemohon pekerjaan di sektor awam dan swasta.[71] Oleh sebab itu, terdapat pandangan yang mengatakan bahawa perlindungan privasi di tempat kerja

70 429 *US* 589 (1977).

71 Lasprogata, G., & King, N. J. (2004). Regulation of electronic employee monitoring: Identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada. *Stan. Tech. L. Rev.*, 4.

dikatakan lebih terjamin di negara Eropah berbanding dengan di Amerika Syarikat.[72]

Di Asia, Hong Kong mengeluarkan garis panduan berhubung dengan privasi di tempat kerja yang dikeluarkan oleh Suruhanjaya Perlindungan Privasi Data Hong Kong. Garis panduan tersebut meliputi telefon, televisyen litar tertutup, e-mel dan penggunaan komputer dan kemungkinan pemantauan lokasi.[73] Di Australia, Akta Pindaan Privasi (Sektor Swasta) 2000 menempatkan sekatan terhad terhadap komunikasi pemantauan majikan dengan menghendaki penubuhan e-mel menggunakan polisi yang perlu diperjelas kepada semua kakitangan. Majikan juga perlu membuktikan bahawa pemantauan e-mel wajar dilakukan atas alasan penggunaan e-mel yang berlebihan oleh pekerja, pengedaran bahan yang menjelikkan, kegiatan jenayah atau menyampaikan maklumat sensitif.[74]

> Oleh itu, langkah Kerajaan Malaysia yang memperkenalkan Akta Perlindungan Data Peribadi 2010 harus dipuji meskipun kesannya terhadap perlindungan data masih belum dapat dipastikan secara jelas[75] sama ada bertindak seperti Perlindungan Data Peribadi 1998 di United Kingdom atau ECPA di Amerika Syarikat yang jelas menyediakan peruntukan bagi perlindungan privasi individu. Namun, jelasnya Akta Perlidungan Data Peribadi 2010 tidak mencakupi perlindungan privasi di Malaysia.[76] Perlindungan privasi perlu dimasukkan sebagai suatu bahagian dalam bahagian undang-undang dan tidak boleh berdiri sebagai suatu peraturan:

72 Determann, L., & Sprague, R. (2011). Intrusive monitoring: Employee privacy expectations are reasonable in Europe, destroyed in the United States. *Berkeley Technology Law Journal*, *26*(2), 979 – 1036.

73 Privacy Commissioner for Personal Data, Hong Kong. (2016). *Privacy Guidelines: Monitoring and Personal Data Privacy at Work*. Retrieved from https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/Monitoring_and_Personal_Data_Privacy_At_Work_revis_Eng.pdf.

74 Eivazi, K. (2011). Computer use monitoring and privacy at work. *Computer Law & Security Review*, *27*(5), 516 – 523.

75 Ayub, Z. A. & Mohamed Yusoff, Z. (2008). *Workplace privacy in Malaysia*: *A legal comparison* (pp. 121 – 137). Kedah: Penerbit Universiti Utara Malaysia.

76 Yusoff, Z. M. (2011). The Malaysian Personal Data Protection Act 2010: A Legislation Note. *NZJPIL*, *9*, 119.

> *... in these days of 'big brother', where through technology and otherwise, the privacy interests of individuals from all walks of life are being ignored or marginalized, it is imperative that statutes explicitly protecting these rights be strictly observed.*

Oleh sebab masih belum ada undang-undang bertulis yang mengawal selia perlindungan peribadi terhadap pekerja di Malaysia, maka prinsip undang-undang *common law* terpakai. Selain itu, keputusan Mahkamah Hak Asasi Kesatuan Eropah boleh dijadikan panduan dan rujukan untuk menangani isu yang berkaitan dengan privasi di tempat kerja. Garis panduan yang khusus hendaklah dikeluarkan oleh pihak yang berwajib untuk melindungi privasi di tempat kerja seperti yang dikeluarkan di Hong Kong dan Australia agar pekerja mengetahui hak mereka berhubung dengan privasi, dan majikan mematuhi garis panduan yang dikeluarkan.

RUJUKAN

Akta Jenayah Komputer 1997.

Akta Keselamatan Dalam Negeri 1960.

Akta Komunikasi dan Multimedia 1998.

Akta Perlindungan Data Peribadi 2010.

Akta Suruhanjaya Pencegahan Rasuah Malaysia 2009.

American Management Association. (2001). Annual Survey on Workplace Monitoring and Surveillance 2001, 18 April.

Archambault, A., & Grudin, J. (2012, Mei). A longitudinal study of facebook, linkedin, & twitter use. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2741 – 2750). ACM.

Auchard, E. (2001, 29 Mei). Monitoring shrinks worker privacy sphere. Reuters.

Ayub, Z. A., & Mohamed Yusoff, Z. (2008). Workplace privacy in Malaysia: A legal comparison (pp. 121 – 137). Sintok, Kedah: Penerbit Universiti Utara Malaysia.

Bernama. (2001, 10 Mac). Ramai rasa selamat dengan rekod pekerja. Retrieved from http://ww1.utusan.com my utusan/info.asp?y=2001&dt=0311&pub=UtusanMalaysia&sec=Ekonomi&pg=ek_06.htm.

Bloustein, E. J. (1964). Privacy as an aspect of human dignity: An answer to Dean Prosser. *NYUL rev*., *39*, 962.

Bărbulescu *lwn* Romania [2016] *ECHR* 61; [2017] *ECHR* 742.

Bohach *lwn* City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996).

Chung, W., & Paynter, J. (2002, Januari). Privacy issues on the internet. In System Sciences, 2002. HICSS. *Proceedings of the 35th Annual Hawaii International Conference* (p. 9). IEEE.

Copland *lwn* United Kingdom [2007] *ECHR* 253.

D'Urso, S. C. (2006). Who's watching us at work? Toward a structural–perceptual model of electronic monitoring and surveillance in organizations. *Communication Theory*, *16*(3), 281 – 303.

Deal *lwn* Spears, 980 F.2d 1153 (8th Cir. 1992).

Determann, L., & Sprague, R. (2011). Intrusive monitoring: Employee privacy expectations are reasonable in Europe, destroyed in the United States. *Berkeley Technology Law Journal*, *26*(2), 979 – 1036.

Eivazi, K. (2011). Computer use monitoring and privacy at work. *Computer Law & Security Review*, *27*(5), 516 – 523.

Electronic Communications Privacy Act 1986.

Garrity *lwn* John Hancock Mutual Life Insurance Co, 18 *IER* Kes 981 (Mass. Dist. Ct. 2002).

Halford *lwn* the United Kingdom [1997] *ECHR* 32 (20605/92).

Hamin, Z. (2001). E-mail @ work: Its legal implication on employer's liability. *Malayan Law Journal*, *3*, xxviii.

Hartman, L. P., & Bucci, G. (1999). The economic and ethical implications of new technology on privacy in the workplace. *Business and society review*, *102*(1), 1 – 24.

Kaupins, G., & Minch, R. (2005, Januari). Legal and ethical implications of employee location monitoring. In System Sciences, 2005. HICSS'05. *Proceedings of the 38th Annual Hawaii International Conference* (p. 133a). IEEE.

K-Mart Corp. *lwn* Trotti, 677 *S.W*.2d 632 (Tex. Ct. App. 1984).

Kopke *lwn* Germany [2010] *ECHR* 1725 Application No. 420/07.

Lasprogata, G., & King, N. J. (2004). Regulation of electronic employee monitoring: Identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada. *Stan. Tech. L. Rev*., 4.

Leftheriotis, I., & Giannakos, M. N. (2014). Using social media for work: Losing your time or improving your work? *Computers in Human*

Behavior, *31*, 134 – 142.
Leventhal *lwn* Knapek, 266 F.3d 64 (2d Cir. 2001).
Libert *lwn* France [2018] *ECHR* 185.
McVeigh *lwn* Cohen, 983 F. Supp. 215, 220 (D.D.C. 1998).
Miller *lwn* Motorola, Inc., 560 N.E.2d 900 (Ill. App. 1990).
Mishra, J. M., & Crampton, S. M. (1998). Employee monitoring: Privacy in the workplace?. *SAM Advanced Management Journal*, *63*(3), 4.
Nikon *lwn* Onof, Decision No. 4164, 2 October 2001 (99 – 42, 942).
Nord, G. D., McCubbins, T. F., & Nord, J. H. (2006). E-monitoring in the workplace: Privacy, legislation, and surveillance software. *Communications of the ACM*, *49*(8), 72 – 77.
O'Connor *lwn* Ortega, 480 U.S. 709 (1987).
Peck *lwn* The United Kingdom [2003] *EHRR* 287.
Perlembagaan Persekutuan.
Privacy Commissioner for Personal Data, Hong Kong. (2016). Privacy guidelines: Monitoring and personal data privacy at work. Retrieved from https://www.pcpd.org.hk/english/data_privacy_law/code_of practices/files/Monitoring_and_Personal_Data_Privacy_At_Work_ revis_Eng.pdf.
Privacy Foundation. (2001). The extent of systematic monitoring of employee e-mail and internet use. Retrieved from http://www.sonic. net/~undoc/extent.htm.
Smith, R. E. (2000). Ben Franklin's website: Privacy and curiosity from Plymouth Rock to the internet. *In Privacy journal.*
Smith, W. P., & Tabak, F. (2009). Monitoring employee e-mails: Is there any room for privacy? *The Academy of Management Perspectives*, *23*(4), 33 – 48.
Smith-Butler, L. (2009). Workplace privacy: We'll be watching you. *Ohio NUL Rev*., *35*, 53.
Smyth *lwn*. Pillsbury Co, 914 F. SUPP. 97 (ED Pa. 1996).
Standler, R. B. (1997). Privacy law in the USA. Retrieved from http:// www.rbs2.com/privacy.htm .
Steve Jackson Games, Inc. *lwn* United States Secret Service, 36 F.3d 457 (5 Cir. 1994).
Stewart, F. (2000). Internet acceptable use policies: Navigating the management, legal, and technical issues. *Information Systems Security*, *9*(3), 1 – 7.
Thompson *lwn* Johnson County Community College, 930 F. Supp. 501 (D. Kan. 1996).

Turban, E., Bolloju, N., & Liang, T. P. (2011). Enterprise social networking: Opportunities, adoption, and risk mitigation. *Journal of Organizational Computing and Electronic Commerce*, *21*(3), 202 – 220.

United States of America *lwn* Simons, 206 F.3d 392 (4 Cir. 2000).

Universal Declaration of Human Rights.

Utusan Malaysia. (2002, 13 Julai). Pekerja layari laman web lucah dikenakan tindakan disiplin. Retrieved from http://ww1.utusan.com.my/utusan/info.asp?y=2002&dt=0714&pub=Utusan_Malaysia&sec=Muka_Hadapan&pg=mh_07.htm.

Van Meter, K. M. (2002). Terrorists/liberators: Researching and dealing with adversary social networks. *Connections*, *24*(3), 66 – 78.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 193 – 220.

Watkins *lwn* L. M. Berry & Co., 704 F.2d 577 (11th Cir. 1983).

Whalen *lwn* Roe, 429 US 589 (1977).

Young, K. S., & Case, C. J. (2004). Internet abuse in the workplace: New trends in risk management. *CyberPsychology & Behavior*, *7*(1), 105 – 111.

Yusoff, Z. M. (2011). *The Malaysian Personal Data Protection Act 2010*: A Legislation Note. *NZJPIL*, *9*, 119.

Diperoleh (*Received*): 25 Oktober 2017
Diterima (*Accepted*): 28 Februari 2018