Facial Recognition Technology in Malaysia: Concerns and Legal Issues

Shao Zheng Chong and Chee Ying Kuek(✉)

Faculty of Law, Multimedia University, Melaka, Malaysia
cykuek@mmu.edu.my

Abstract. In this era where technology is advancing at an unprecedented rate, facial recognition technology (FRT) has been increasingly deployed for policing, surveillance systems, security access control and other purposes. However, corresponding concerns have been raised particularly on the threat to the individual's right to privacy and the risk of data being misused. Although the right to privacy is recognised as a fundamental liberty protected by the Federal Constitution, the law relating to the right of privacy in Malaysia is limited and unable to address the privacy concerns of the FRT comprehensively. This article adopts the doctrinal research method by examining the laws governing FRT in the United States and the United Kingdom. As the Personal Data Protection Act 2010 of Malaysia does not sufficiently cater for the FRT, it is imperative to amend it to govern this technology and address the related concerns. There is a need to strike a balance between the individual's rights to privacy and the application of the FRT for the purposes of private use, commercial transactions and public security.

Keywords: Facial recognition technology · Fundamental liberty · Right to privacy · Surveillance

1 Introduction

Facial recognition is a biometric technology which involves the automatic processing of digital images comprising individuals' faces to identify, authenticate, verify, or categorise them. The processes include image acquisition, face detection, normalisation, feature extraction, enrolment, and comparison [1]. In this era where technology is advancing at an unprecedented rate, facial recognition technology (hereinafter "FRT") has been increasingly deployed by the government bodies, corporate and commercial organisations, and sometimes private entities in the auxiliary of criminal justice, policing, surveillance system, security access control and other purposes. During the Covid-19 outbreak, the application of FRT was expanded to include tracking individuals who are Covid-19 patients [2].

In the context of Malaysia, since 2018, the government has entered into agreements with Chinese companies, including Yitu Technology and Huawei Technologies, to implement the FRT for the purpose of public security [3]. In addition, since 2019, the Penang government has incorporated the FRT into close circuit televisions (CCTVs) installed

Y. C. Adam and A. W. Abdull Manaf (Eds.): ICLD 2022, ASSEHR 707, pp. 101–109, 2022.
https://doi.org/10.2991/978-2-494069-59-6_10

by the Penang Island City Council to trace and arrest wanted criminals [4]. In 2020, KK Super Mart became the first convenience store to introduce FRT in which the faces captured by their CCTVs can be detected and recognised. Technology such as this can allow businesses to produce a blacklist and trigger an alert if a face blacklisted is detected [5]. During the pandemic, hotels, commercial organisations and even universities correspondingly utilise the FRT and body temperature measurement system as surveillance solutions. A person without a mask on or a person with high fever can be detected and the management will be alerted [6].

Although the FRT has been gradually used by the government and the private entities in Malaysia, there is no specific law governing the application of the FRT, which may potentially violate an individual's right to privacy, and the fact that the FRT itself may also be misused. This article seeks to examine the concerns raised pertaining to the use of the FRT and recommend the regulatory measures in the context of Malaysia. Doctrinal research was adopted in this study, in which statutory provisions and court cases are analysed.

This article is structured in the following manner: Sect. 1 introduces the research background and problem, the research objective as well as the method of study. Section 2 discusses the concerns raised pertaining to the application of FRT. Sections 3 and 4 examine the privacy rights in the international legal documents and the privacy laws of FRT in the United States, United Kingdom and Malaysia. Section 5 recommends amendments to the Personal Data Protection Act 2010 of Malaysia. Section 6 concludes the study.

2 Concerns Arising from Facial Recognition Technology

Two primary concerns raised against the use of FRT are concerns on the individual's privacy and concerns on the risk of the FRT being misused.

2.1 Privacy Concerns

In *Toh See Wei v Teddric Jon Mohr & Anor* [7], the right to privacy was defined as "the right to be let alone, the right… to be free from unwarranted publicity and the right to live without undue interference by the government or any private individuals" in matters that are irrelevant to the public. Individuals have the right to control the collection, use, and disclosure of their personal information. According to a survey of 123 participants in the USA who were exposed to FRT in their daily lives, it was perceived that the significant privacy risks of FRT are that the FRT deprives the right to be let alone, FRT disables people from staying anonymous, and the concern of secondary use of data collected without the consent of the data subject [8].

2.2 Misuse of Facial Recognition Data

There are substantial risks that the data or face print generated from the FRT could be abused for identity theft, leading to fraud or other unlawful activities. The offence

of identity theft can be effortlessly committed by simply utilising deep fake technology. According to the bill of the United States, section 2(n)(3) of the DEEP FAKES Accountability Act defines "deep fake" as a forged video recording, electronic image or photograph generated by artificial intelligence technology using the face of a person to impersonate him. For example, deep fake videos were produced to impersonate the Russian President, Putin, as well as the former United States President, Barack Obama [9]. These indicate that numerous people would be severely harmed if the face data generated by the FRT is abused, leaked, or hacked.

3 Privacy Rights in International Legal Documents

This section canvasses the privacy rights embodied in selected salient international legal documents, namely the Universal Declaration of Human Rights (UDHR), International Covenant on Civil and Political Rights (ICCPR) and General Data Protection Regulation (GDPR).

Despite not addressing the FRT, both the UDHR and the ICCPR outline privacy rights, which are worth referencing. The foundation of the right to privacy is enshrined in both Article 12 of the UDHR and Article 17 of the ICCPR. The declarations made in both articles bear a resemblance, wherein both articles guarantee every person's privacy rights to be free from arbitrary interference and shall be protected under the law against such interference. Further on this point, courts have ruled that the right to privacy is linked to the right to dignity in cases involving privacy issues. This connection is aptly described in *EG and others v Attorney General and consolidated petitions (DKM and others, interested parties)* [10], where the court asserted that privacy enhances human dignity to the extent that it safeguards an individual's right to a 'sphere of private intimacy and autonomy.'

On the other hand, the GDPR provides a clearer formulation of privacy rights. On a true construction of Article 6(1) of the GDPR, the processing of data is legitimate only if, *inter alia*, the data subject consented to the processing, and/or the processing is required to fulfil a contractual obligation. It follows from Article 7(3) of the GDPR that data subjects have the legal right to revoke their consent at any time where processing is based on their consent. Apart from that, the data subject shall be informed prior to giving consent. It is pertinent to note that Recital 32 states that consent must be given in a clear affirmative action; in other words, it cannot be given by silence, pre-ticked checkboxes, or inaction.

4 Privacy Laws of FRT in the United States, United Kingdom and Malaysia

4.1 United States

The Biometric Information Privacy Act (hereinafter "BIPA") was enacted in 2008 by the State of Illinois. Similar provisions are made in the National Biometric Information Privacy Act of 2020, a bill introduced in the senate.

Section 10 of the BIPA includes face geometry within the definition of "biometric identifier", and any information acquired based on the biometric identifier to identify an individual is "biometric information". In *Vance v. Microsoft Corp.* [11], Microsoft argued that the facial scans generated from the photographs are not biometric identifiers and biometric information. Nevertheless, the court held that the facial scans fall within the purview of biometric identifiers under the BIPA.

Notably, under the same section, "private entity" encompasses any individual, corporation, association, or other groups, excluding the State and local government agencies. Furthermore, section 15(a) of the BIPA mandates a private entity that possesses biometric identifiers or biometric information to have a written policy accessible by the public. The written policy has to entail the retention schedule and destruction guidelines when the initial purpose is achieved or within three years since the individual's last engagement with the private entity, whichever takes place first.

Moreover, section 15(b) of the BIPA prohibits private entities from obtaining or purchasing a person's biometric identifier or biometric information unless the subject is notified in writing that a biometric identifier or biometric information is being collected, along with the particular objective and duration of the collection. Apart from that, a written release from the subject is also required to allow such collection. Further on this point, section 15(e) imposes the reasonable standard of care to secure all biometric identifiers and biometric information from disclosure, and the form of protection must be the same as or more protective than the form in which the private entity secures other confidential information.

At this juncture, it is essential to note that section 20 of the BIPA confers the right of action on the person aggrieved by a violation of the BIPA against the offending party. The remedies include damages, reasonable attorneys' fees, other litigation expenses, and other reliefs such as an injunction. The damages are statutorily enunciated as shown in Table 1.

Table 1. Degree of culpability and the respective recoverable damages

Degree of culpability	Recoverable damages
Negligence	$1,000 or actual damages, whichever is greater
Intentional or reckless violation	$5,000 or actual damages, whichever is greater

It is pertinent to note that an aggrieved person under the BIPA does not necessarily have to suffer or prove actual damages. It is sufficient as long as his legal right is invaded by the offending party, as decided by the Supreme Court in *Rosenbach v. Six Flags Entm't Corp.* [12].

4.2 United Kingdom

The main privacy legislation in the United Kingdom is the Data Protection Act 2018. At this point, it is worth exploring section 64 of the Data Protection Act 2018. This section requires the controller to conduct a data protection impact assessment if the data processing would lead to a high risk to the individuals' rights and freedom. Subsection

(3) further laid out the elements of the assessment, *inter alia*, a general description of the operations, an evaluation of the risks to the rights and freedoms of the data subjects, methods to mitigate the risks, and safeguards to protect personal data. In addition, Subsection (4) requires assessment of the data processing's nature, scope, context, and objectives.

In *R (on the application of Bridges) v Chief Constable of South Wales Police (Information Commissioner and others intervening)* [13], the South Wales Police Force utilised the live automated facial recognition technology overtly to act as surveillance by capturing the digital images of persons. The Court of Appeal held that it was unlawful as it contravened Article 8 of the European Convention on Human Rights, which guarantees the right to respect for private and family life. Additionally, it was held that the police force failed to comply with the data protection impact assessment, which is statutorily enunciated in section 64 of the Data Protection Act 2018 and the public sector equality duty, as stipulated in section 149 of the Equality Act 2010.

4.3 Malaysia

It is noteworthy that, in the context of Malaysia, businesses that hire workers or assign workers to work or conduct business in the European Union are subject to the requirements of the GDPR [14]. Additionally, section 4(4) of the Human Rights Commission of Malaysia Act 1999 attached significance to the UDHR, while the Federal Court in *Leow Fook Keong (L) v Pendaftar Besar Bagi Kelahiran dan Kematian, Jabatan Pendaftaran Negara, Malaysia & Anor* [15] attached weight to the ICCPR, even though Malaysia has not ratified the ICCPR. Nonetheless, it is pertinent to note that the *sine qua non* of giving effect to the privacy rights enshrined in the UDHR, ICCPR, and GDPR is the passage of relevant legislation in Parliament; otherwise, they remain unenforceable in Malaysia until incorporated into Malaysian domestic law [16].

Despite the fact that the right to privacy has been recognised as a fundamental liberty under Article 5(1) of the Federal Constitution, as affirmed by the Federal Court in *Sivarasa Rasiah v Badan Peguam Malaysia & Anor* [17], the laws governing the right to privacy, particularly in respect of FRT, are limited. This indicates that the aggrieved parties would have limited right of action against the offending party. This is affirmed by the Federal Court in *Beatrice a/p AT Fernandez v Sistem Penerbangan Malaysia & Ors* [18], where one could not sue another individual or private entity for the infringement of one's constitutional right.

The only legislation in Malaysia which governs data privacy is the Personal Data Protection Act 2010 (hereinafter "PDPA"). Arguably, the data generated from FRT may fall within the definition of "personal data" in section 4 of the PDPA since it allows the data subject to be identified or identifiable from that information possessed by the data user. However, the PDPA is merely applicable to the personal data concerning commercial transactions, as stated in section 2(1) of the PDPA. Section 3(1) of the PDPA also expressly excludes its application to the Federal and State Governments. Moreover, section 3(2) of the PDPA expressly excludes any personal data processed outside Malaysia from the scope of the Act, unless the data will be further processed in Malaysia. Apart from that, the definition of "personal data" under section 4 of the PDPA does not include any data processed for credit reporting business. It thus follows that, as

the FRT is mainly used for security and surveillance reasons in this country, the PDPA does not seem to provide sufficient legal protection to an individual whose privacy rights may be infringed by the use of FRT by a certain private entity or the government.

Notwithstanding that, the personal data protection principles are embodied in section 6 to section 12 of the PDPA, which include the general principle, notice and choice principle, disclosure principle, security principle, retention principle, data integrity principle, and the access principle. No commercial entities may breach the principles aforementioned, if in so doing, it leads to the consequences spelt out in section 5(2) of the PDPA. Furthermore, a data subject has the right to prevent the processing of any personal data that may cause damage or distress, as enunciated in section 42 of the PDPA. At this point, it is worth noting that an aggrieved person, at most, could lodge a written complaint to the Personal Data Protection Commissioner [19] as the PDPA does not provide any right of private action, as noted in *Navaneeth Perpakaran v. Sumita Manian & Ano*r [20].

As for cases where privacy rights are infringed by the public bodies, one may claim remedies under breach of constitutional right. There are three elements laid out in *Koperal Zainal Mohd Ali & Ors v. Selvi Narayan & Anor* [21], *inter alia*, the plea of the plaintiff's constitutional right is infringed, and it is preferable for the specific constitutional right to be identified, the person depriving the plaintiff's constitutional right has acted under or for the State, and the plaintiff suffered or lost his constitutional right due to the acts or omissions of the person. In the light of the elements set out above, the plaintiff may rely on Article 5(1) of the Federal Constitution to claim remedies if his privacy rights are infringed by the public bodies.

As for cases where privacy rights are infringed by individuals who have no commercial relationship with the plaintiff, the plaintiff may rely on the cause of action of breach of privacy. In *Lew Cher Phow @ Lew Cha Paw & Ors v Pua Yong Yong & Anor* [22], it was held that the defendant was liable for breach of privacy due to the CCTV pointing right at the plaintiffs' house, which amounted to video surveillance on them. Furthermore, in *Lee Ewe Poh v Dr Lim Teik Man & Anor* [23], the defendants were liable for invasion of female privacy rights relating to modesty, decency and dignity for photographing the female patient's intimate parts without her prior knowledge. Notwithstanding, it is pertinent to note that both cases are merely limited to cases in relation to surveillance and violation of the modesty of a woman. Therefore, Malaysian privacy law has to move forward in order to address the concerns arising from the implementation of FRT.

5 A Way Forward: Recommendations and Suggestions

Despite the fact that the courts in *Lew Cher Phow* and *Lee Ewe Poh* have recognised the right to privacy, there is no enacted law available to be referred to. This means that the tort of invasion of privacy in these cases could only be limited to the extent of surveillance and invasion of a female's private morality and modesty. They are unable to comprehensively cover the application of FRT.

Since FRT is an axiomatic trend, it is vital to take prophylactic measures to ensure that the FRT is not abused and the face data of individuals is not compromised. At this

point, the current PDPA is not sufficient as it does not reflect the novel nature of FRT. The current PDPA also does not sufficiently protect the rights of privacy of the data subject since its application is limited to information relating to commercial transactions and it is not applicable to the Federal and State Governments.

Therefore, it is humbly submitted that the PDPA should be amended so that it also regulates the application of FRT. The definition of "biometric data" which includes facial images resulting from technical processing should be inserted. At this point, it is recommended to model the BIPA of Illinois to impose a reasonable duty of care upon the data user and affirm an individual's right of action upon data users to file a lawsuit against the private entities for any violations of privacy rights.

Furthermore, the amended PDPA shall strike a balance between privacy rights and the application of FRT for the purposes of private use, commercial transactions, and public security. The amended PDPA shall incorporate fundamental principles such as necessity, proportionality, accuracy, fairness, transparency [24] and accountability.

It is highly suggested that, in the application of FRT in private use or commercial transactions, FRT should only be used against individuals who have given their prior informed consent. There should be transparency in the sense that the purpose of data collection, data retention period and measures for protecting the data should be made available to the public so that they can make informed decision. The data subject should have the right to withdraw his or her consent.

As for the purpose of public security, a proportionate risk-based approach should be adopted. The application of FRT in surveillance should be limited to prevent imminent and substantial risks to public security, where the threats to public safety are documented, credible and serious [25]. In other words, to justify invasion of privacy, the use of FRT must be proportionate to the threat to the public security and the benefits that can be derived. Further, the deployment of FRT, if possible, should be in a covert manner, rather than an overt manner.

The data collected should not be used for different or secondary purposes, and should not be shared with other parties unless with legitimate reason such as public security in enforcing the law. The data should not be retained beyond the fulfilment of the purpose. Once the data is no longer required, it should be deleted permanently. The party which uses the FRT or the data user has the duty to take reasonable steps to ensure that the data recorded is accurate and not misleading. Any decision to be made against an individual should not solely rely on the FRT without human intervention [26]. In addition, there should be security safeguards to protect the data against unauthorised access or modification.

6 Conclusion

It is undeniable that the PDPA at this stage is insufficient to address the privacy concerns that are arising tremendously in this era of technological advancement. Therefore, it is proposed to amend the PDPA, modelling the BIPA of Illinois to address the privacy concerns of FRT by taking prophylactic measures to prevent the privacy rights of individuals from being compromised.

It is imperative to strike a balance between the privacy rights and application of FRT for private use, commercial transactions, and public security. As for the purposes of

private use and commercial transactions, the application of FRT against an individual should only be allowed if the individual has given his prior informed consent. As for the purpose of public security, although consent may not be required, the threat to the public must be serious and credible, justifying its usage. Moreover, guidelines governing the data processing and the fundamental principles have to be expressly enunciated in the amended PDPA.

In that connection, it is believed that the amended PDPA is able to ameliorate the privacy rights concerning FRT and give effect to Article 5(1) of the Federal Constitution in Malaysia.

Acknowledgments. The authors would like to extend their gratitude to the Multimedia University's Siti Hasmah Digital Library for the accessibility of the extensive online databases.

Authors' Contributions. Both authors contributed in the study design, data collection, data analysis, writing and editing.

References

1. Article 29 Data Protection Working Party. (2012). Opinion 02/2012 on facial recognition in online and mobile services. 00727/12/EN WP 192
2. Cha, S. (2021, December 13). S. Korea to test AI-powered facial recognition to track Covid-19 cases. Reuters. Retrieved May 7, 2022. https://www.reuters.com/world/asia-pacific/skorea-test-ai-powered-facial-recognition-track-covid-19-cases-2021-12-13/.
3. Tan, CK. (2018, April 18). *Malaysian police adopt Chinese AI surveillance technology*. Nikkei Asia. Retrieved May 7, 2022. https://asia.nikkei.com/Business/Companies/Chinas-startup-supplies-AI-backed-wearable-cameras-to-Malaysian-police.
4. Mok, O. (2019, January 2). *Penang launches country's first facial recognition CCTV surveillance*. Malay Mail. Retrieved May 7, 2022, https://www.malaymail.com/news/malaysia/2019/01/02/penang-launches-countrys-first-facial-recognition-cctv-surveillance/1708422.
5. MSMEAdmin. (2020, August 12). *Official launching of facial recognition system in KK Super Mart*. Malaysia SME. Retrieved June 6, 2022, https://www.malaysiasme.com.my/official-launching-of-facial-recognition-system-in-kk-super-mart/
6. *Covid-19: How Malaysian businesses can benefit from an AI-revolutionised surveillance system.* (2021, February 25). Malay Mail. Retrieved May 7, 2022 https://www.malaymail.com/news/malaysia/2021/02/25/covid-19-how-malaysian-businesses-can-benefit-from-an-ai-revolutionised-sur/1952699.
7. Toh See Wei v Teddric Jon Mohr & Anor [2017] 11 MLJ 67 [47]-[48]
8. Zhang, S., Feng, Y., & Sadeh, N. (2021, August 9–10). Facial recognition: Understanding privacy concerns and attitudes across increasingly diverse deployment scenarios. In *Seventeenth Symposium on Usable Privacy and Security* (pp. 243–262). Retrieved May 7, 2022 https://www.usenix.org/conference/soups2021/presentation/zhang-shikun.
9. Wakefield, J. (2022, March 18). *Deepfake presidents used in Russia-Ukraine war*. BBC News. Retrieved May 7, 2022 https://www.bbc.com/news/technology-60780142.
10. EG and others v Attorney General and consolidated petitions (DKM and others, interested parties) [2019] 4 LRC 422 [341]
11. Vance v. Microsoft Corp., 525 F. Supp. 3d 1287
12. Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186

13. R (on the application of Bridges) v Chief Constable of South Wales Police (Information Commissioner and others intervening) [2020] EWCA Civ 1058
14. Protection of Employee's Personal Data in Malaysia - General Data Protection Regulation ("GDPR") and |Skrine - Advocates & Solicitors. Skrine - Advocates & Solicitors. (2020). Retrieved 3 June 2022, from https://www.skrine.com/insights/alerts/november-2020/protection-of-employee%E2%80%99s-personal-data-in-malaysia#_ftnref2.
15. Leow Fook Keong (L) v Pendaftar Besar Bagi Kelahiran dan Kematian, Jabatan Pendaftaran Negara, Malaysia & Anor [2022] 1 MLJ 398 [36]
16. Letitia Bosman v Public Prosecutor and other appeals (No 1) [2020] 5 MLJ 277
17. Sivarasa Rasiah v Badan Peguam Malaysia & Anor [2010] 2 MLJ 333
18. Beatrice a/p AT Fernandez v Sistem Penerbangan Malaysia & Ors [2005] 3 MLJ 681
19. Personal Data Protection Act 2010, section 104.
20. Navaneeth Perpakaran v. Sumita Manian & Anor [2021] 1 LNS 2389
21. Koperal Zainal Mohd Ali & Ors v. Selvi Narayan & Anor [2021] 6 CLJ 157
22. Lew Cher Phow @ Lew Cha Paw & Ors v Pua Yong Yong & Anor [2011] MLJU 1195
23. Lee Ewe Poh v Dr Lim Teik Man & Anor [2011] 1 MLJ 835
24. Kouroupis, K. (2021). Facial recognition and privacy: finding the right balance: Part 1. *Privacy & Data Protection*, *21(5)*, 12–14. Retrieved 6 May 2022, from https://launch.westlawasia.com/document/I47858D00A49111EB9F1DC1B3BC2E42F3.
25. Purshouse, J., & Campbell, L. (2019). Privacy, crime control and police use of automated facial recognition technology. *Criminal Law Review*, *3*, 188–204.
26. Sarabdeen, J. (2022). Protection of the rights of the individual when using facial recognition technology. *Heliyon*, 8(3), e09086