Facial Recognition Technology in Esports? Youth Protection vs. Human Rights Risks

Tsubasa Shinohara *
Institute of Humanities and Social Sciences, University of Tsukuba
ORCID 0000-0002-2972-7460

DOI: 10.54103/milanoup.215.c457

Abstract

Esports ('competitive video games' or 'electronic sports') have rapidly developed. Currently, the esports industry is composed of many esports stakeholders and becomes one of the worldwide economic markets. Due to such rapid growth, however, the esports society has faced many problems, such as doping, match-fixing, physical and mental health issues, and sexual harassment against vulnerable esports players etc. In this situation, some states enact national legislation on video games to protect children against negative consequences, such as violent scenes, images of sexual expression, gaming addiction and disorders. National legislation has created an age limitation for children to play competitive video games. Despite this, children still have access to esports activities because their parents or other adult give them prohibited video games. Therefore, it is difficult for states to restrict children's access to competitive video games. In this situation, this chapter considers whether esports society should use facial recognition technology to protect youth esports players. To answer this main question, this chapter will examine the following research questions: (1) How has facial recognition technology been used in esports society?; (2) What human rights risks can be identified due to the use of facial recognition technology?; and (3) How should the esports society strike a balance between youth protection in esports and human rights risks caused by the use of facial recognition technology? Through this research, it may clarify how esports publishers and esports event/league organisers may evaluate the impact on fundamental human rights by using facial recognition technology in the esports society.

* Assistant Professor, University of Tsukuba (Institute of Humanities and Social Sciences), Ibaraki, Japan, shinohara.tsubasa.gb@u.tsukuba.ac.jp; Human Rights Officer, Swiss Esports Federation, Bern, Switzerland, tsubasa.shinohara@sesf.ch.

Keywords
Facial Recognition Technology, Esports, Youth Protection, Human Rights Risks

1. Introduction

Esports ('competitive video games' or 'electronic sports') have rapidly developed. According to the Newzoo's free report in 2022, the global revenue of the esports industry in 2021 reached 1,136.5 million dollars and the expected global revenue by 2025 will be 1,866.2 million dollars.[1] At the present time, the esports industry is composed of many esports stakeholders, such as esports publishers (eg Electronic Sports League (ESL), Valve and Riot Games), electronic equipment companies (eg Logitech and Dell), television and media companies (eg CBS, ESPN and Swisscom), streaming platform providers (eg Twitch and YouTube), video game distributors (eg Google Play Store and Apple Store) etc.[2] Thus, it can be said that the esports industry becomes one of the worldwide economic markets.

Due to such rapid growth, the esports society has faced many problems, such as doping,[3] match-fixing,[4] physical and mental health issues,[5] sexual harassment against vulnerable esports players[6] etc. In this situation, some states enact national legislation on video games to protect children against negative consequences, such as violent scenes, sexual expression images and gaming addiction

1 Newzoo, *Global Esports & Live Streaming Market Report 2022* (Free Version, 2022) at 34, <https://newzoo.com/insights/trend-reports/newzoo-global-esports-live-streaming-market-report-2022-free-version/> accessed 30 May 2024.

2 See Tsubasa Shinohara, 'Global Governance in International Esports Society?' (2023) 27(4) Gaming Law Review 1.

3 Tsubasa Shinohara, 'The Protection of Esports Players against the Use of Doping Substances and Methods under the European Convention on Human Rights: The Swiss Example' (2021) 1(1) International Journal of Esports 1<https://www.ijesports.org/article/69/html> accessed 30 May 2024.

4 'The continued rise of eSport – Efforts to combat match fixing and improve integrity' (*LawInSport*, 2 September 2016) <www.lawinsport.com/topics/features/item/the-continued-rise-of-esport-efforts-to-combat-match-fixing-and-improve-integrity> accessed 30 May 2024; Ryan P Toomey, 'Upholding the Integrity of Esports To Successfully and Safely Legitimize Esports Wagering' (2019) 23(1) Gaming Law Review 14-16; Peter K Czegledy, 'Esports Integrity Policies' (2021) 25(4) Gaming Law Review, 167; Atish Ghoshal, 'Ethics in Esports' (2019) 23(5) Gaming Law Review 340 .

5 Tsubasa Shinohara, 'The Protection of Professional Esports Players Against Physical and Mental Health Problems under the International Covenant on Economic, Social and Cultural Rights' (2022) 13(1) UNLV Gaming Law Journal 1.

6 Jay Castello, 'Foul play: tackling toxicity and abuse in online video games' *The Guardian* (17 August 2018); John T Holden and others, 'The #E-Too Movement: Fighting Back Against Sexual Harassment in Electronic Sports' (2020) 52(1) Arizona State Law Journal, 11–14.

and disorders.[7] The national legislation creates an age limitation for children to play competitive video games. Nevertheless, children can still have access to esports because their parents or other adults may give them prohibited video games.[8] Therefore, it is difficult for states to restrict children's access to competitive video games.

In this connection, facial recognition technology has gradually become a part of our daily lives. For instance, Apple Inc. uses 'Face ID' to unlock iPhones, authorise purchases, and download apps without the need for passwords.[9] At airports, facial scanning machines simplify the boarding process for passengers.[10] In the context of esports, the technology has been used to restrict children's access to esports activities in order to protect them against gaming addiction.[11] For instance, the Chinese government has implemented a national

7 On 26 March 2021, the German Federal Council approved the reform of the Youth Protection Act submitted by the Federal Ministry of Family Affairs that restricts access of children to the internet in order to protect them against harmful contents, sexual exploitation and cyberbullying. This new law entered into force from 1 May 2021. *Zweites Gesetz zur Änderung des Jugendschutzgesetzes*, 9 April 2021, BGBl I 2021, N 16, 15 April 2021, S 742. See also 'Bundesrat billigt Reform des Jugendschutzgesetzesthe' (*BMFSFJ*, 26 March 2021) <www.bmfsfj.de/bmfsfj/aktuelles/alle-meldungen/bundesrat-billigt-reform-des-jugendschutzgesetzes-161184> accessed 30 May 2024; 'Zweites Gesetz zur Änderung des Jugendschutzgesetzes', (*BMFSFJ*, 26 March 2021) <www.bmfsfj.de/bmfsfj/service/gesetze/zweites-gesetz-zur-aenderung-des-jugendschutzgesetzes-147956> accessed 30 May 2024.

8 Joyce Cheng and Iris Zhao, 'Chinese internet giant introduces facial recognition technology in a bid to control underage gaming' *ABC News* (21 July 2021) <www.abc.net.au/news/2021-07-22/chinese-gaming-company-midnight-patrol-using-facial-recognition-/100306444> accessed 30 May 2024.

9 'About Face ID advanced technology' (*Apple,* 10 January 2024) <https://support.apple.com/en-us/HT208108> accessed 30 May 2024. See also Lindsey Jacques, 'Facial Recognition Technology and Privacy: Race and Gender – How to Ensure the Right to Privacy is Protected' (2021) 23(1) San Diego International Law Journal 111, 116-117.

10 Narita Airport in Japan started 'Face Express' to use facial recognition technology to facilitate boarding process <www.narita-airport.jp/html/faceexpress/en/index.html> accessed 30 May 2024; see also World Economic Forum, UNICRI, INTERPOL and Netherlands Police, 'A Policy Framework for Responsible Limits on Facial Recognition: Use Case: Law Enforcement Investigations' (October 2021) 10 <www.weforum.org/whitepapers/a-policy-framework-for-responsible-limits-on-facial-recognition-use-case-law-enforcement-investigations/> accessed 30 May 2024.

11 Tiffany May and Amy Chang Chien, 'Game Over: Chinese Company Deploys Facial Recognition to Limit Youth's Play' (*The New York Times*, 8 July 2021), <www.nytimes.com/2021/07/08/business/video-game-facial-recognition-tencent.html> accessed 30 May 2024; Sean Hollister, 'How Tencent's sweeping new facial scans will catch Chinese kids playing past curfew' (*The Verge*, 9 July 2021), <www.theverge.com/2021/7/9/22567029/tencent-china-facial-recognition-honor-of-kings-game-for-peace> accessed 30 May 2024; Hospes Coetu, 'Risks of Facial Recognition in Gaming' (*xsreviews,* 24 November 2020) <https://xsreviews.co.uk/editorial/risks-of-facial-recognition-in-gaming/> accessed 30 May 2024.

law prohibiting minors from playing video games between 10pm and 8am.[12] To enforce this law, it started 'online patrol' by using facial recognition technology to pick up young gamers.[13] Therefore, if esports society may use this technology to protect young esports players, it might play an important role in the protection of young esports players against negative consequences due to esports activities. However, the use of facial recognition technology may cause human rights risks, particularly concerning the right to privacy, due to the collection and retention of sensitive personal data (ie biometric data).[14]

In this situation, this chapter will consider whether the esports society should use facial recognition technology to protect young esports players. To answer this main question, it will examine the following research questions: (1) How has facial recognition technology been used in esports society?; (2) What human rights risks can be identified due to the use of facial recognition technology?; and (3) How can the use of facial recognition technology be justified in esports activities? This research will serve to clarify how esports publishers and esports event/league organisers may assess an impact on fundamental human rights by using the facial recognition technology in the esports society.

In the light of the foregoing, this chapter will be divided into the following sections: After this introduction, it will provide an overview of how facial recognition technology is currently being used in the esports society to protect young esports players against negative consequences. Furthermore, it will examine the right to privacy guaranteed by international human rights law and identify human rights risks associated with the use of facial recognition technology. On this basis, this chapter will consider how the esports society should strike a balance between the protection of young esports players and the protection of their rights to privacy when it uses the facial recognition technology in esports. Finally, it will answer the main question of whether the esports society should use facial recognition technology to protect young esports players.

12 Javier C Hernández and Albee Zhang, '90 Minutes a Day, Until 10 P.M.: China Sets Rules for Young Gamers' (*The New York Times*, 6 November 2019) <www.nytimes.com/2019/11/06/business/china-video-game-ban-young.html> accessed 30 May 2024.

13 Chandan Khanna, 'China to impose curfew on young gamers in bid to cut gaming addiction rates' (*ABC News*, 7 November 2019) <www.abc.net.au/news/2019-11-07/china-imposes-online-gaming-curfew-tackles-video-game-addiction/11680522> accessed 30 May 2024.

14 See Manon Laganà, 'Facial Recognition And Human Rights In Europe' (*Human Rights Pulse*, 1 April 2022) <www.humanrightspulse.com/mastercontentblog/facial-recognition-and-human-rights-in-europe> accessed 30 May 2024; Council of Europe, 'Facial recognition: strict regulation is needed to prevent human rights violations' (*Council of Europe*, 28 January 2021) <https://www.coe.int/en/> accessed 30 May 2024; Elizabeth Fernandez, 'Facial Recognition Violates Human Rights, Court Rules' (*Forbes*, 13 August 2020) <www.forbes.com/sites/fernandezelizabeth/2020/08/13/facial-recognition-violates-human-rights-court-rules/?sh=4823b4ca5d44> accessed 30 May 2024.

2. Facial recognition technology in esports?

As previously mentioned, China has implemented facial recognition technology to enforce its national law prohibiting young gamers from playing between 10pm and 8am, with the aim of protecting minors from gaming addiction. However, how should facial recognition technology be used in esports activities? To answer this question, this section will firstly provide an overview of what facial recognition technology is, and then describe how it is currently being used in the esports society.

2.1. What is facial recognition technology?

First of all, what is facial recognition technology? According to the Cambridge Online English Dictionary, the term 'facial recognition' means 'technology that makes it possible for a computer to recognize a digital image of someone's face'.[15] More precisely, Elizabeth McClellan indicated that '[f]acial recognition technology is an algorithm used to recognize a human face through the use of biometrics, which track facial features from a photo or video'.[16] Furthermore, the Danish Institute for Human Rights explained that:

> Facial recognition is based on technology that captures biometric data to identify natural persons. The technology has many uses, ranging from comparing one image with one individual (so-called 'one-to-one' comparison) to more general surveillance of citizens and comparison of facial images against large databases ('one-to-many' comparison).[17]

Furthermore, it can be trained to improve the ability for the identification and verification of human faces via machine learning technology through the analysis of the large quantities of facial images.[18] In other words, this technology is combined with machine learning technology to enhance their capacity and quality to recognise human faces and to identify a specific person through the analysis of large quantities of facial images. On this basis, this art defines the term 'facial recognition technology' as an algorithm used to recognise human

15 'Meaning of facial recognition in English' (*Dictionary Cambridge*) <https://dictionary.cambridge.org/dictionary/english/facial-recognition> accessed 30 May 2024.

16 Elizabeth McClellan, 'Facial Recognition Technology: Balancing the Benefits and Concerns' (2020) 15(2) Journal of Business & Technology Law 363.

17 The Danish Institute for Human Rights, 'Memo: Facial Recognition to Combat Crime' (*The Danish Institute for Human Rights,* 20 February 2020) 3 <www.humanrights.dk/publications/facial-recognition-combat-crime> accessed 30 May 2024.

18 Sarah Chun, 'Facial Recognition Technology: A Call for the Creation of A Framework Combining Government Regulation and A Commitment to Corporate Responsibility' (2020) 21(4) North Carolina Journal of Law & Technology 99, 104–105.

faces and to identify and verify a specific person via machine learning through the analysis of a huge amount of facial images.

Based on this definition, what benefits can facial recognition technology provide us? This technology is used for the following three purposes[19]: (1) identification (identifying one person from among others in a database (one-to-many comparison)); (2) authentication/verification (verifying a person's identity, such passport photos (one-to-one comparison)); and (3) classification/categorisation (classifying a facial image into sex, colour and age etc. (matching general characteristics)).[20] It would be beneficial for the esports society to utilise this technology to ensure a safe environment for young esports players. In doing so, esports publishers and esports event/league organisers need to verify the age of players using their facial images and personal information provided during registration. This method would prevent underage players from accessing esports activities.

2.2. Different reactions to the use of facial recognition technology in Asia and Europe

Based on this definition, this subsection will provide an overview of the different reactions to the use of facial recognition technology in Asian and European countries. This is because each country has taken a different approach to the use of facial recognition technology.[21]

---

19 See Vera Lúcia Raposo, '(Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation' (2022) Information & Communications Technology Law 45.

20 Christopher S Milligan, 'Facial Recognition Technology, Video Surveillance, and Privacy' (1999) 9(1) Southern California Interdisciplinary Law Journal 295, 306; Desara Dushi, 'The use of facial recognition technology in EU law enforcement: Fundamental rights implications' (*Global Campus Policy Briefs: South East Europe*, 2020) 3 <http://dx.doi.org/10.25330/528> accessed 30 May 2024; Laganà (n 14); FRA, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (*FRA*, 21 November 2019) 7-8. <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law>; Tambiama Madiega and Hendrik Mildebrath, *Regulating facial recognition in the EU* (European Parliament September 2021) 1–2.

21 Russian Federation has already used the facial recognition technology for surveillance of the Russian citizens. In this situation, victims submitted a complaint about a violation of their rights to respect for private life under art 8 of the European Convention on Human Rights (ECHR) against the Russian government before the European Court of Human Rights (ECtHR). See Anastasiia Kruope, 'Moscow's Use of Facial Recognition Technology Challenged Activists File an Application to European Court of Human Rights' (*Human Rights Watch*, 8 July 2020), <www.hrw.org/news/2020/07/08/moscows-use-facial-recognition-technology-challenged> accessed 30 May 2024; Jacques (n 9) 137–138; regarding the United States, ibid 139-141; Elizabeth A Rowe, 'Regulating Facial Recognition Technology in the Private Sector' (2020) 24(1) Stanford Technology Law Review <https://law.stanford.edu/publications/regulating-facial-recognition-technology-in-the-private-sector/> accessed 30 May 2024.

In Asian countries, there is often less opposition to the deployment of machines with facial recognition technology. For instance, Japan decided to use facial recognition technology to check physical temperature and vaccination status.[22] In South Korea, the government launched a pilot project to use facial recognition technology of CCTV cameras to track the movement of infected people with the COVID-19 in 2021.[23] Furthermore, China uses this technology to monitor every actions of Chinese citizens[24] and invented other facial recognition technology which is capable of identifying human faces wearing a mask.[25] In addition to this, the Chinese government enforces Chinese population to scan their faces before using mobile internet services.[26] India started to use the facial recognition technology in various locations to monitor the population during COVID-19, even though there was no national legislation in place to govern its use.[27] In light of these examples, Asian countries tend to face less opposition when deploying facial recognition technology.[28]

---

22 Kyodo News, 'Japan firm NEC to introduce facial recognition vaccination check system' (*Kyodo News*, 3 December 2021) <https://english.kyodonews.net/news/2021/12/45d-18baf8341-nec-to-introduce-facial-recognition-vaccination-check-system.html> accessed 30 May 2024; Nick Statt, 'ACLU sues facial recognition firm Clearview AI, calling it a "nightmare scenario" for privacy' (*The Verge* 28 May 2020) <www.theverge.com/2020/5/28/21273388/aclu-clearview-ai-lawsuit-facial-recognition-database-illinois-biometric-laws> accessed 30 May 2024.

23 Jin Yu Young, 'A South Korean city will test facial recognition as a way to track the virus' *The New York Times* (13 December 2021) <www.nytimes.com/2021/12/13/world/asia/south-korea-facial-recognition-coronavirus.html> accessed 30 May 2024.

24 Chun (n 18) 109–111; Simon Denyer, 'Beijing bets on facial recognition in a big drive for total surveillance' *The Washington Post* (7 January 2018) <www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/?itid=lk_interstitial_manual_13> accessed 30 May 2024.

25 Seungha Lee, 'Coming into Focus: China's Facial Recognition Regulations' (*CSIS*, 4 May 2020), <www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations> accessed 30 May 2024.

26 Rosie Perper, 'Chinese government forces people to scan their face before they can use internet as surveillance efforts mount' (*Business Insider*, 2 December 2019) <www.businessinsider.com/china-to-require-facial-id-for-internet-and-mobile-services-2019-10?r=US&IR=T> accessed 30 May 2024; Jane Li, 'Getting a new mobile number in China will involve a facial-recognition test' (*Quartz*, 3 October 2019) <https://qz.com/1720832/china-introduces-facial-recognition-step-to-get-new-mobile-number> accessed 30 May 2024.

27 Konina Mandal, 'Facial Recognition Technology and its Impact on Privacy Rights of Children' (2021) 4(4) International Journal of Law Management & Humanities 1142, 1142-1144 ; Murali Krishnan, 'Facial recognition software spreads across India but regulation is slow' (*rfi*, 6 August 2022) <www.rfi.fr/en/international/20220806-facial-recognition-software-spreads-across-india-but-regulation-is-slow> accessed 30 May 2024.

28 However, Chinese District Court decided that the use of facial recognition technology to enter into the zoo was an excessive interference with the right to privacy. See Eva Dou, 'China built the world's largest facial recognition system. Now, it's getting camera-shy' *The Washington Post* (30 July 2022) <www.washingtonpost.com/world/

In contrast to the situations of Asian countries, the use of facial recognition technology has been recognised as a sensitive issue in Europe. In France and the United Kingdom, the law enforcement authorities, especially police, started to experiment the facial recognition technology to prevent terrorism.[29] However, the European Parliament recently called for a ban on the use of facial recognition technology in public space.[30] Although Germany strongly supports this position,[31] France is not in favour of total ban on the use of facial recognition technology.[32] The UK courts have already examined the use of facial recognition technology with CCTV camera by police in *R (on the application of Bridges) v Chief Constable of South Wales Police*.[33] In this case, the Court of Appeal considered that the use of facial recognition technology infringed the right to respect for private life under art 8(1) of the ECHR, but the interference by the South Wales Police Force (SWP) with the art 8(1)'s right could be justified

---

facial-recognition-china-tech-data/2021/07/30/404c2e96-f049-11eb-81b2-9b7061a582d8_story.html> accessed 30 May 2024.

29 Monika Zalnieriute, 'Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State' (2021) 22(2) Science and Technology Law Review 284, 286-287.

30 Melissa Heikkilä, 'European Parliament calls for a ban on facial recognition' (*Politico*, 6 October 2021) <www.politico.eu/article/european-parliament-ban-facial-recognition-brussels/> accessed 30 May 2024; Clothilde Goujard, 'Europe edges closer to a ban on facial recognition' (*Politico*, 20 September 2022) <www.politico.eu/article/europe-edges-closer-to-a-ban-on-facial-recognition/> accessed 30 May 2024.

31 Melissa Heikkilä, 'German coalition backs ban on facial recognition in public places '(*Politico*, 24 November 2021) <www.politico.eu//german-coalition-backs-ban-on-facial-recognition-in-public-places/> accessed 30 May 2024.

32 For instance, the Conseil d'État authorised the creation of Alicem ('Authentification en ligne certifiée sur mobile'). This service permits smartphone users with a passport or residence permit to identify themselves for access to online services. However, this service requires the users to register their facial images by means of facial recognition technology. See Décret n°2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé «Authentification en ligne certifiée sur mobile». Gérard Haas, 'Reconnaissance faciale: Alicem validée par le Conseil d'État' (*haas avocats*, 17 November 2020), <https://info.haas-avocats.com/droit-digital/reconnaissance-faciale-alicem-validée-par-le-conseil-détat> accessed 30 May 2024. Furthermore, French airports started to use facial recognition technology for identity checks, see Pierre Jova, 'La reconnaissance faciale débarque à l'aéroport' *La Croix* (9 July 2018) <www.la-croix.com/France/Securite/reconnaissance-faciale-debarque-laeroport-2018-07-09-1200953660> accessed 30 May 2024.

33 *R (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, paras 1-3; Rafe Jennings, 'Facial Recognition Technology not "In Accordance with Law"' (*UK Human Rights Blog*, 13 August 2020) <https://ukhumanrightsblog.com/2020/08/13/facial-recognition-technology-not-in-accordance-with-law/> accessed 30 May 2024. Regarding the case summary, see Simons+Simons, 'UK Court of Appeal finds facial recognition technology unlawful' (*Simons+Simons*, 2 September 2020) <www.simmons-simmons.com/en/publications/ckelg1z7p8kjt09008l0bet7c/uk-court-of-appeal-finds-facial-recognition-technology-unlawful> accessed 30 May 2024. Regarding this case summary, see Monika Zalnieriute (n 29) 292-296.

under art 8(2) of the ECHR. However, it stated that the SWP's interference was not in accordance with the law[34] and the SWP did not conduct adequate 'data protection impact assessment' (DPIA).[35] Therefore, it decided that there was an infringement of art 8 of the ECHR because the SWP's interference did not satisfy the art 8(2)'s conditions.[36] Therefore, European countries are reluctant to accept the use of facial recognition technology in order to protect the right to respect for private life under art 8 of the ECHR.

In short, Asian countries generally did not face significant opposition to the use of facial recognition technology, while European countries (excluding France) have been strongly opposed to it. This is largely due to concerns that collecting facial images could infringe on the right to privacy, which will be discussed in the following subsection. Accordingly, different reactions of Asian and European countries to the use of facial recognition technology can be discerned.

2.3. Facial recognition technology in esports

In light of the different reactions of Asian and European countries to the use of facial recognition technology, this subsection will provide an overview of how the esports society uses facial recognition technology. In doing so, it will refer to some examples, in particular China and European countries.[37]

As previously mentioned, China has implemented facial recognition technology to prevent gaming addiction and enforce its national law that prohibits minors from playing electronic games during 10 pm to 8 am. To enforce this law, the Chinese gaming company, Tencent Games, has introduced facial recognition technology to prevent minors from playing at night.[38] However, the majority of young esports players may still have access to competitive video games because their parents provide them with smartphones or gaming IDs for competitive video games.[39]

---

34 *R (on the application of Bridges)* paras 54–130.

35 ibid paras 145–154.

36 ibid paras 209–210.

37 In South Korea, the government enacted the Youth Protection Act (or the Shutdown Law), Youth Protection Act, Act No 15987, 18 December 2018, prohibiting children under the age of 16 from playing online video games between 0:00 am to 6:00 am under art 26(1) of the Shutdown Law to protect young esports players against negative consequences in 2011. However, it was abolished by the National Assembly of the South Korea in 2021 to revise the Youth Protection Act. See Korea Herald, 'Shutdown law shuttered' (*The Korea Herald*, 16 November 2021) <www.koreaherald.com/view.php?ud=20211115000803> accessed 30 May 2024.

38 Niji Narayan, 'Tencent Introduces Face Recognition Feature to Prevent Children from Gaming at Night' (*European Gaming*, 13 July 2021) <https://europeangaming.eu/portal/latest-news/2021/07/13/96109/tencent-introduces-face-recognition-feature-to-prevent-children-from-gaming-at-night/> accessed 30 May 2024.

39 Cheng and Zhao (n 8).

European countries have not yet used facial recognition technology in the context of esports. In this connection, the European Parliament called for a ban on the use of facial recognition technology in public space.[40] In this sense, European countries are reluctant to use this technology to defend individuals' privacy in Europe. Therefore, esports publishers and event/league organisers in Europe are hesitant to use this technology and are subject to strict requirements under European data protection law.

To sum up, China is a leading country for the use of facial recognition technology in esports. European countries have faced huge obstacles to implement this technology in European esports activities because the use of this technology may cause a potential human right violation. In other words, it arbitrarily interferes with the right to privacy guaranteed by international human rights treaties. This issue has been recognised as one of the most concerning aspects for the use of the facial recognition technology.[41] Therefore, the next section will consider if there is a violation of the right to privacy guaranteed by international human rights law.

3. Youth protection in esports vs. human rights risks caused by the use of facial recognition technology

Based on the previous section, it is clear that the esports society has gradually used the facial recognition technology. However, the following question may be raised: What human rights risks does the use of facial recognition technology cause? To answer this question, this section will examine the risk of a violation of the right to privacy (or the right to respect for private life) guaranteed by international human rights law, especially the Universal Declaration of Human Rights (UDHR),[42] the International Covenant on Civil and Political Rights (ICCPR)[43] and the European Convention on Human Rights (ECHR).[44]

40 Heikkilä (n 30); Goujard (n 30). Regarding this discussion, see Madiega and Mildebrath (n 20).

41 McClellan (n 16) 378–380.

42 Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR).

43 International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR). It is important to note that China does not ratify but signs the ICCPR so it has an obligation not to defeat the object and purpose of the ICCPR under Art 18(a) of the Vienna Convention on the Law of Treaties (adopted 23 May 1969, entered into force 27 January 1980) 1155 UNTS 331 (VCLT). China acceded the VCLT on 3 September 1997.

44 Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).

Children under 18 years old may also enjoy this protection under art 16 of the Convention on the Rights of the Child (CRC).[45]

Under these human rights treaties, it is important to note that international human rights treaties impose on state parties the following two categories of legal obligations[46]: (1) negative obligations to refrain from interfering with the enjoyment of rights; and (2) positive obligations to take necessary measures to prevent and protect human rights violations caused by states and non-state actors.[47] In the context of esports, esports publishers and esports event/league organisers are non-state actors and, thus, they are not held responsible for the implementation of both obligations under international human rights law. However, the state parties must implement positive obligations to prevent human rights violations caused by non-state actors.[48] Therefore, if esports publishers and esports event/league organisers infringe the right to privacy due to the use of the facial recognition technology, states must take necessary measures to avoid such human rights violations within the territories.[49]

In light of the foregoing, this section will be divided into the following subsections: Firstly, it will consider if there is a violation of the right to privacy due to the use of facial recognition technology in light of the provisions of the ICCPR and ECHR.[50] If so, it will then take into consideration how the state interference can be justified to use this technology under these treaties.

3.1. Is there a violation of the right to privacy due to the use of facial recognition technology?

At the beginning of this section, this subsection will refer to art 12 of the UDHR, which reads as follow:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

45 Convention on the Rights of the Child, (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 (CRC). China signed and ratified the CRC.

46 See art 2(1) of the ICCPR; art 1 of the ECHR. See also OHCHR, 'The right to privacy in the digital age: report of the Office of the United Nations High Commissioner for Human Rights' (30 June 2014) A/HRC/48/31 para 10.

47 Walter Kälin and Jörg Künzli, *The Law of International Human Rights Protection* (2nd edn, Oxford University Press, 2019) 87–90.

48 See *K.H. and Others v Slovakia*, App no 32881/04 (ECtHR, 28 April 2009) paras 44–48.

49 The use of facial recognition technology causes a violation of the right to human dignity, but this art will not consider this issue. See FRA (n 20) 20–21.

50 This article will not consider the provisions of the CRC.

In other words, this provision firstly guarantees the right to privacy for everyone at the international level. However, it is important to note that the UDHR has no legally-binding effect on states, but this non-legally binding norm was converted into a legal obligation after the adoption of the ICCPR in 1966.[51] Therefore, this subsection will provide an overview of the right to privacy in the context of the use of facial recognition technology in light of art 17(1) of the ICCPR and art 8(1) of the ECHR.[52] Furthermore, it will consider how the General Data Protection Regulation (GDPR)[53] may apply to the use of facial recognition technology in the context of esports because the GDPR is an important instrument for the protection of the right to privacy in Europe.

3.1.1 The right to privacy under art 17 of the ICCPR

First of all, art 17(1) of the ICCPR stipulates that 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation'. This provision guarantees the right to privacy which 'is an expression of human dignity and is linked to the protection of human autonomy and personal identity'.[54] Under this provision, state parties to the ICCPR shall enact the national legislation prohibiting arbitrary or unlawful interference with individual's privacy by state and non-state actors (positive obligations).[55]

Regarding the protection of personal data, the Human Rights Committee (HRC)'s General Comment No 16[56] explains that 'The gathering and holding of personal information on computers, data banks and other devices whether by public authorities or private individuals or bodies, must be regulated by law. (…)'.[57] In particular, it uses the term 'other devices' in this paragraph and this term should be interpreted to include the facial recognition technology on the basis of a *living document* doctrine which reflects the social and technological

51 Kälin and Künzli (n 50) 36.

52 The use of facial recognition technology also causes discrimination based on race, skin colour and gender. In this regard, see Jacques (n 9) 119–122; Joy Liddicoat, *Human Rights and the Internet* (Intersentia, 2021)148.

53 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR) [2016] OJ L119/1. In practice, this website is much easier to see the legal text of the GDPR: <https://gdpr-info.eu> accessed 30 May 2024.

54 OHCHR (n 46) para 7.

55 UN Human Rights Committee, 'CCPR General Comment No. 16: Art 17 (The right to respect of privacy, family, home and correspondence and protection of honour and reputation)' (8 April 1988) <www.refworld.org/legal/general/hrc/1988/en/27539> accessed 30 May 2024; Sarah Joseph and Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary* (3*rd* edn, OUP, 2013) 541.

56 Art 28 ICCPR.

57 UN Human Rights Committee (n 55).

development for the interpretation of human rights treaties.[58] As had been mentioned in the previous section, the facial recognition technology has been grown up in our society and it cannot be ignored. In this situation, the OHCHR's Report on the Right to Privacy in the Digital Age (hereinafter: the OHCHR report) indicates:

> Aspects of privacy that are of particular importance in the context of the use of AI include informational privacy covering information that exists or can be derived about a person and her or his life and the decisions based on that information, and the freedom to make decisions about one's identity.[59]

Therefore, the right to privacy should be taken into account when the facial recognition technology with machine learning is used.

In conclusion, it can be considered that the use of facial recognition technology falls within the scope of art 17(1) of the ICCPR and the state parties are held responsible for taking necessary measures to protect personal information collected by the facial recognition technology. However, each state has no specific national legislation on the use of facial recognition technology. In this situation, how can the state parties implement the positive obligations to prevent a violation of the right to privacy against the use of facial recognition technology under art 17(1) of the ICCPR? In doing so, this art should refer to each national data protection law regulating the treatment of personal information by electronic device, but it cannot all be dealt with. Therefore, it will refer to the GDPR as an example to know how the personal data collected by the facial recognition technology should be treated and protected.

3.1.2. The right to respect for private life under art 8 of the ECHR

Furthermore, art 8(1) of the ECHR prescribes that 'Everyone has the right to respect for his private and family life, his home and his correspondence'. The ECtHR explains that the concept of 'private life' is a broad term covering the physical and psychological integrity of a person, an individual's physical and social identity, a right to personal development, and the right to establish and develop relationships with other human beings and the outside world.[60] On this basis, this provision imposes on state parties negative obligations to refrain from interference with private and family life and positive obligations to protect individuals from violations of their rights to private life.[61] In particular, state

58 See David Harris and others, *Harris, O'Boyle & Warbrick: Law of The European Convention on Human Rights* (4*th* edn, OUP, 2018) 501.

59 OHCHR (n 46) para 7.

60 *Pretty v The United Kingdom*, App no 2346/02 (ECtHR, 29 April 2002) para 61; William A Schabas, *The European Convention on Human Rights: A Commentary* (Oxford University Press, 2015) 370.

61 ibid 367–369; Harris (n_58) 510–513.

parties must take legislative or administrative measures to implement negative obligations, but they may enjoy a certain margin of appreciation allowing them to decide how to strike a balance between the competing public and private interests or Convention rights.[62]

Regarding the protection of personal data, David Harris and others point out that '[t]he collection , storage, and disclosure of information by the state about an individual will interference with his right to respect for private life'.[63] Thus, the use of new technologies to collect biometric data may interfere with art 8(1)'s rights.[64] In this context, it can be interpreted that the use of facial recognition technology falls within the scope of art 8(1) of the ECHR on the basis of a living instrument doctrine.[65]

In conclusion, the use of facial recognition technology is considered the interference with the right to respect for private life under art 8(1) of the ECHR because this technology can collect biometric data, especially facial images, by means of automated processing.[66]

3.1.3 Data protection under the General Data Protection Regulation

Finally, this part will refer to the provisions of the GDPR in the context of the use of facial recognition technology as one of the examples of data protection law. As has been mentioned in the previous section, the facial recognition technology can collect sensitive personal data, especially biometric data,[67] without any explicit consent by data subjects.[68] In this regard, art 4(14) of the GDPR provides that:

> 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person,

62 Schabas (n 60) 368; ECtHR, Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence (Council of Europe/European Court of Human Rights, Updated on 9 April 2024) para 8 <https://ks.echr.coe.int/web/echr-ks/all-case-law-guides> accessed 30 May 2024.

63 Harris (n 58) 538.

64 The retention of fingerprints, cellular samples and DNA profiles, which fall within the scope of the biometric data, by public authorities constitutes an interference with the right to respect for private life. *S and Marper v The United Kingdom*, App no 30562/04 and 30566/04 (ECtHR, 4 December 2008) para 77 and para 86. See also *Peck v The United Kingdom*, App no 44647/98 (ECtHR, 28 January 2003) para 59; *Gaughran v The United Kingdom*, App no 45245/15 (ECtHR, 13 February 2020) para 63; ECtHR, Guide to the Case-Law of the of the European Court of Human Rights: Data Protection (Council of Europe/European Court of Human Rights, Updated on 29 February 2024) paras 24–30, <https://ks.echr.coe.int/web/echr-ks/all-case-law-guides> accessed 30 May 2024.

65 ibid paras 62 and 378.

66 Laganà (n 14).

67 Jacques (n 9) 114.

68 See *R (on the application of Bridges)* paras 21-23.

such as facial images or dactyloscopic data.[69]

Furthermore, the Court of Justice of the European Union and the ECtHR has also recognised facial images as sensitive personal data (or biometric data).[70] Therefore, facial images collected by facial recognition technology can be categorised as 'biometric data'.[71]

On this basis, art 5 of the GDPR stipulates that the processing of biometric data collected by facial recognition technology must be lawful, fair and transparent with an explicit consent and purpose.[72] Regarding the explicit consent, arts 6(1)(a) and 7 of the GDPR stipulate that data subjects must give an explicit consent to data controllers and data processors to conduct a treatment of their personal data. If there is no explicit consent, the processing of special categories of personal data is prohibited under art 9(1) of the GDPR. However, the processing of biometric data can be justified if the data subjects give data controllers an explicit consent to process their personal data under art 9(2)(a) of the GDPR or this processing is necessary for the protection of other interests set forth in art 9(2)(b) to (j) of the GDPR. However, it is important to note that the GDPR has no legally-binding effect on non-member states to the Council of Europe.

In light of these provisions of the GDPR, when esports publishers and esports event/organisers use the facial recognition technology, data subjects (ie young esports players) have no opportunity to give an explicit consent to data controllers and processors (ie esports publishers and esports event/organisers) in order to process their biometric data because this technology automatically collect and process their personal data. Thus, the use of facial recognition technology can be recognised as the interference with the rights to privacy or the right to respect for private life.[73]

3.2. Justification of interference with the right to privacy

Despite the fact that there is a violation of the right to privacy or the right to respect for private life due to the use of facial recognition technology,

69 See also art 3(13) of the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89.

70 Case C–291/12 *Michael Schwarz v Stadt Bochum* [2013] ECLI:EU:C:2013:670 paras 48-50; *Szabó and Vissy v Hungary*, App no 37138/14 (ECtHR, 12 January 2016) paras 52-89.

71 See also Madiega and Mildebrath (n 20).

72 ibid 11–14; FRA (n 20) 23–25.

73 The Danish Institute for Human Rights (n 17).

international human rights treaties make an exception for this protection.[74] In this regard, art 8(2) of the ECHR stipulates that:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing 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.

In other words, the state interference with the right to respect for private life can be justified[75] only if it is in accordance with the law,[76] purses a legitimate aim,[77] and is necessary in a democratic society.[78] To consider the necessity in a democratic society, the ECtHR considers the reason of state intervention is relevant and sufficient and the measures are proportionate to achieve the legitimate aim.[79] In doing so, the ECtHR examines that "a margin of appreciation should be left to the competent national authorities in striking a fair balance between the relevant conflicting public and private interests".[80] If these conditions are satisfied, the state interference can be justified and, thus, there is no violation of art 8(1) of the ECHR.

In contrast to this, does the ICCPR prescribe the conditions for justifying the state interference with the right to privacy? For this question, the ICCPR does not specify the conditions for the restriction on the right to privacy, but art 17(1) of the ICCPR provides that any interference with the right to privacy must not be arbitrary or unlawful. In this regard, the OHCHR's report explains the term 'unlawful' in the following meaning:

> States may interfere with the right to privacy only on the basis of law and in accordance with that law. The law itself must comply with the provisions, aims and objectives of the International Covenant on Civil and Political Rights and must specify in detail the precise circumstances in which such interference is permissible.[81]

Furthermore, it also indicates the purpose of the term 'arbitrary' to "guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant, and should, in any event, be

74 Dushi (n 20) 5–8; see also OHCHR (n 46) paras 12–14.
75 Schabas (n 60) 401–406.
76 ECtHR (n 62) paras 15–21.
77 ibid paras 22–28.
78 ibid paras 29–31.
79 *Peck v The United Kingdom* para 76.
80 ibid para 77.
81 OHCHR (n 46) para 8.

reasonable in the particular circumstances".[82] In other words, any interference with the right to privacy under art 17(1) of the ICCPR must be restricted under the conditions that such interference is provided by law, is necessary to achieve a legitimate purpose, and be proportionate to that purpose.[83] Accordingly, the right to privacy under art 17(1) of the ICCPR can be limited only when states parties to the ICCPR may prove that such interference is arbitrary or unlawful because it has no legitimate purpose, is not necessary for achieving such purpose and does not meet the proportionality requirement. Exceptionally, state parties may also derogate from art 17(1)'s obligations under the state emergency in accordance with art 4(1) of the ICCPR,[84] but this provision should not be examined in the context of esports.

In conclusion, restriction on the right to privacy (art 17(1) of the ICCPR) and the right to respect for private life (art 8(1) of the ECHR) can be justified only when such interference is provided by law, is necessary in a democratic society, and be proportionate to achieve that purpose.[85]

4. How can the use of facial recognition technology be justified in esports activities?

Based on this understanding, how can the use of facial recognition technology be justified in esports activities? In doing so, it is necessary to strike a balance between youth protection in esports and human rights risks, that is an infringement of the right to privacy, caused by the use of facial recognition technology. However, international human rights law allows state parties to enjoy the margin of appreciation to choose the means for achieving the legitimate aim of state interference with human rights. Therefore, each state may decide if they should establish national legislation on the use of facial recognition technology. Furthermore, it is important to note that esports publishers and esports event/league organisers are not states but business enterprises and, thus, international human rights law cannot impose on them any legal obligations to protect the right to privacy guaranteed by art 17(1) of the ICCPR and art 8(1) of the ECHR. However, international human rights law imposes on state parties a positive obligation to ensure that even business enterprises should respect the provisions of international human rights treaties within their jurisdiction. In this context, the esports publishers and esports event/league organisers are also held responsible for the respect of human rights and should pay attention

82 ibid paras 8 and 39.

83 ibid para 8.

84 See UN Human Rights Committee, 'General Comment no. 29, States of emergency (article 4) : International Covenant on Civil and Political Rights' (31 August 2001) CCPR/C/21/Rev.1/Add.11.

85 See also art 29(2) of the UDHR.

to use the facial recognition technology while preventing a potential violation of the right to privacy.

In light of the foregoing, this section will firstly overview a corporate responsibility to respect human rights under the United Nations Guiding Principles on Business and Human Rights (UNGPs)[86] because esports publishers and esports event/league organisers are not states actors, but business enterprises and, thus, they have no legal obligations under international human rights law. On this basis, it will then consider how the use of this technology can be justified in the context of esports in accordance with the human rights law and data protection law. More importantly, it will examine how the esports society should strike a balance between community's interests (ie youth protection against negative consequences (ie, gaming addiction and disorder)) and individual's interests (ie violation of the right to privacy) due to the use of facial recognition technology in esports.

4.1. The Responsibility of Business Enterprises to Respect Human Rights Under the UNGPs

As had been mentioned above, esports publishers and esports event/league organisers are business enterprises and, thus, international human rights law cannot impose legal obligations on them. However, the UNGPs, which is not legally-binding instrument, clarify a corporate responsibility for business enterprises to respect internationally recognised human rights. Principle 11 of the UNGPs stipulates that 'Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved'.[87]

In this regard, the OHCHR reports states that this responsibility is considered 'human rights due diligence' "to identify, assess, prevent and mitigate adverse impacts on human rights that an entity may cause or to which it may contribute or be directly linked".[88] More precisely, Principle 13 of the UNGPs provides that:

> The responsibility to respect human rights requires that business enterprises:
>
> Avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur;
>
> Seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if

86 OHCHR, *The UN Guiding Principles on Business and Human Rights implementing the United Nations 'Protect, Respect and Remedy' Framework* (United Nations, 2011).

87 See also OHCHR (n 46) para 11.

88 ibid paras 48–49.

they have not contributed to those impacts.

In the context of esports, esports publishers and esports event/league organisers have a negative responsibility to avoid infringing human rights law and a positive responsibility to address adverse human rights impacts through their esports activities in light of international human rights treaties (see Principle 12 of the UNGPs) when they deploy and operate the facial recognition technology in esports activities.[89]

4.2. Justification of the Use of Facial Recognition Technology in Esports: Youth Protection Against Negative Consequences or Protection of the Right to Privacy?

The use of facial recognition technology constitutes an interference with the right to privacy or the right to respect for private life under international human rights treaties. So, the question is how it can be justified in the context of esports in order to protect young esports players against negative consequences, such as gaming addiction and disorders, caused by esports activities. In doing so, this subsection will consider how the esports publishers and esports event/league organisers should strike a balance between public and private interests in esports activities.

In this situation, public interests mean the protection of young esports players against negative consequences caused by esports activities. In particular, China has already been faced with gaming addiction and gaming disorder and, thus, it adopted national legislation prohibiting young esports players from playing from 10pm to 8pm. During this period, the public authority has conducted a night policing to enforce the implementation of this national legislation. In contrast to this, private interests can be considered the protection of the right to privacy due to the use of facial recognition technology. Based on this understanding, this chapter will consider how states or esports publishers and esports event/league organisers can justify the use of facial recognition technology to prevent negative consequences due to esports activities.

In light of the foregoing, states should enact a specific legislation on the use of facial recognition technology to achieve the prevention of negative consequences of young esports players. As had been mentioned in the previous subsection, however, they enjoy the margin of appreciation to decide if the use of this technology is permitted or not in light of the domestic situation. In contrast to this, esports publishers and esports event/league organisers should establish certain conditions for the use of the facial recognition technology to avoid an infringement of the right to privacy in accordance with international

89 ibid para 48.

human rights law and data protection law.[90] Therefore, this subsection suggests the following minimum conditions for the use of the facial recognition technology in esports activities:

1. Esports publishers and esports event/organisers should determine and specify the purposes and methods of collecting sensitive personal data of young esports players by the facial recognition technology;
2. Esports publishers and esports event/organisers should clarify how and why the sensitive personal data of young esports players should be processed by the facial recognition technology;
3. Esports publishers and esports event/organisers should ensure that young esports players and their parent freely give them explicit consents to process their sensitive personal data by the facial recognition technology; and
4. Esports publishers and esports event/organisers should conduct a Data Protection Impact Assessment (DPIA)[91] to identify potential risks arising out of the processing of sensitive personal data with the facial recognition technology and to minimise these risks as far as possible.[92]

If all the conditions are satisfied, the use of facial recognition technology can be justified. In this situation, the esports society may use the facial recognition technology to protect young esports players against negative consequences in esports when it takes measures to mitigate human rights risks for a violation of the right to privacy under international human rights law.

5. Conclusion

This final section will answer the main question of whether esports society should use facial recognition technology to protect youth esports players? To answer this main question, this chapter examined the following research questions: (1) How has facial recognition technology been used in the esports society?; (2) What human rights risks can be identified due to the use of facial recognition technology?; and (3) How can the use of facial recognition technology be justified in esports activities? So, this chapter will address these research questions and then answer the main question posed in this chapter.

90 Raposo (n 19) 19.

91 Regarding the DPIA, see Ben Wolford, 'Data Protection Impact Assessment (DPIA)' (*GDPR.EU*) <https://gdpr.eu/> accessed 30 May 2024.

92 See Council of Europe, Commissioner for Human Rights, 'Unboxing artificial intelligence: 10 steps to protect human rights' (*Council of Europe*, May 2019) 7–8 <www.coe.int/en/web/commissioner/-/unboxing-artificial-intelligence-10-steps-to-protect-human-rights> accessed 30 May 2024; Michael O'Flaherty, 'Opinion: Facial Recognition Technology and Fundamental Rights' (2020) 6(2) European Data Protection Law Review 173.

Firstly, how has facial recognition technology been used in the esports society? For this question, this chapter defined the term 'facial recognition technology' as an algorithm used to recognise human faces and to identify and verify a specific person via machine learning through the analysis of a huge amount of facial images. Based on this definition, this technology has been used for the prevention of crime by police in Asian countries. In the context of esports, China only uses it for the effective enforcement of Chinese law prohibiting minors from playing electronic games during 10pm to 8am. The purpose of this legislation is to protect young esports players against gaming addiction and disorder. Therefore, the esports society has already used the facial recognition technology to achieve youth protection in esports.

Based on this understanding, the second question in this chapter was what human rights risks can be identified due to the use of facial recognition technology. In this regard, it has been considered that the use of facial recognition technology causes a clear interference with the right to privacy guaranteed by art 12 of the UDHR, art 17(1) of the ICCPR, art 8(1) of the ECHR. However, state parties to these international human rights treaties may justify the use of facial recognition technology if it is prescribed by law and necessary for democratic society to achieve a legitimate aim. If these conditions are satisfied, the right to privacy can be restricted for the purpose of the use of facial recognition technology.

Finally, this chapter considered how the use of facial recognition technology can be justified in esports activities? Each state must take legislative measure to ensure the enjoyment of the right to privacy under art 17(1) of the ICCPR and art 8(2) of the ECHR. However, they may exercise the margin of appreciation to decide how they enact national legislation on the use of facial recognition technology. In this situation, the Pillar II of the UNGPs stipulates that business enterprises have a corporate responsibility to respect human rights. In doing so, it should take action to avoid a violation of the right to privacy caused by the use of the facial recognition technology and conduct a human rights impact assessment to mitigate the human rights risks.

In light of the foregoing, this chapter considered how the esports publishers and esports event/league organisers should strike a balance between public and private interests in esports activities. While public interests mean the protection of young esports players against negative consequences caused by esports activities, private interests can be considered the protection of the right to privacy due to the use of facial recognition technology. Based on this understanding, this chapter examined how states or esports publishers and esports event/league organisers can justify the use of facial recognition technology to prevent negative consequences due to esports activities. To achieve the prevention of negative consequences of young esports players, states should enact a specific legislation on the use of facial recognition technology, but they may exercise

the margin of appreciation under international human rights law. However, esports publishers and esports event/league organisers should establish certain conditions for the use of the facial recognition technology to avoid an infringement of the right to privacy in accordance with international human rights law and data protection law. Therefore, this chapter proposed several minimum conditions for the use of the facial recognition technology in esports activities in the previous section. If all the conditions are satisfied, it can be considered that the use of facial recognition technology may be justified. In this situation, the esports society can use the facial recognition technology for the purpose of protecting young esports players against negative consequences in esports when it takes measures to mitigate human rights risks for a violation of the right to privacy under international human rights law.

In conclusion, the esports society should use facial recognition technology to protect young esports players against negative consequences because this technology is helpful and useful for esports publishers and esports events/leagues organisers to verify if esports players meet the required age to have access to the esports activities. However, it is important to note that the esports society should strike a balance between the interests of youth protection and human rights concerns about the right to privacy guaranteed by art 12 of the UDHR, art 17(1) of the ICCPR and art 8(1) of the ECHR. If the esports society would like to use this technology, it must carefully pay attention to comply with data protection law because of the margin of appreciation of state parties to the international human rights treaties. If so, it can be considered that the use of facial recognition is permitted to be used by the esports publishers and esports event/league organisers to ensure a safe esports environment for young esports players.