ENTERTAINMENT AND SPORTS LAW JOURNAL

Shinohara, T. 2025. Precautionary Principle for the Use of Facial Recognition Technology within the Esports Ecosystem? *Entertainment and Sports Law Journal*, 23(1): 4, pp. 1–7. DOI: https://doi.org/10.16997/eslj.1873

ARTICLE

Precautionary Principle for the Use of Facial Recognition Technology within the Esports Ecosystem?

Tsubasa Shinohara

Assistant Professor, University of Tsukuba, Institute of Humanities and Social Sciences, Ibaraki, JP / Head of Legal Department & Human Rights Officer, Swiss Esports Federation, Bern, CH

shinohara.tsubasa.gb@u.tsukuba.ac.jp

Esports ('electronic sports') are gradually emerging as a significant economic market. Esports participants – including professional and amateur players, workers, and fans who are part of the esports ecosystem – have been subjected to various forms of toxic behaviours, particularly online sexual harassment. To ensure a safe environment for all individuals involved in esports, video game publishers and third-party organisers are expected to implement appropriate measures to mitigate such behaviours because it can improve the negative image of video game communities and can further increase the number of gamers. Against this background, this article explores whether video game publishers and third-party organisers may lawfully employ facial recognition technology as a protective measure to prevent harmful conducts in online environments. Therefore, the deployment of facial recognition technology could prove to be a valuable tool for both video game publishers and third-party organisers in fostering safer online and offline environments within the esports ecosystem. To that end, it will consider how the precautionary principle can be applied to the use of facial recognition technology within the esports ecosystem, as a means of preventing toxic behaviour by players and fans. This research seeks to lay the foundation for the responsible use of emerging technologies to safeguard esports participants within the esports ecosystem.

Keywords: Precautionary principle; esports players; facial recognition technology; human rights; toxic behaviours; esports ecosystem; video game publishers

1. Introduction

Esports ('electronic sports') are gradually becoming a significant economic market (Newzoo 2022: 34). There are various definitions of 'esports' within academic circles; however, this article adopts the definition proposed by Nothelfer, Jenny, and Besombes, which describes esports as 'an organised and codified competition between human players using video games' (Nothelfer, Jenny, & Besombes 2024: 11). In other words, the term 'esports' should be necessarily understood as including the following elements: (1) video games; (2) human players; and (3) the organisation of competitions utilising those video games.

Esports participants – including professional and amateur players, workers, and fans who are part of the esports ecosystem – have been subjected to various forms of toxic behaviours, particularly online sexual harassment (Aguerri, Santisteban & Miró-Llinares 2023: 2; Ratan et al. 2020). For professional esports players, competitions are not held anonymously, and tournament organisers may lawfully collect their personal information prior to the event. In contrast to this, professional and amateur players who use esports titles for personal training or informal online playing with anonymous participants would suffer the toxic behaviours. To ensure a safe environment for all individuals involved in esports, video game publishers and third-party organisers (including esports leagues organisers, tournament organisers, and esports federations) are expected to implement appropriate measures to mitigate such behaviours (for instance, see Riot Games, 2022) because it can improve the negative image of video game communities and can further increase the number of gamers.

Against this background, this article explores whether video game publishers and third-party organisers may lawfully employ facial recognition technology as a protective measure to prevent harmful conducts in online environments. Therefore, the deployment of facial recognition technology could prove to be a valuable tool for both video game publishers and third-party organisers in fostering safer online and offline environments within the esports ecosystem. However, the deployment of such technology raises significant human rights concerns, particularly regarding potential infringements on the right to privacy and data protection. In this context, the precautionary principle – originally developed within the field of environmental law (Stevens, 2002) – may play a critical role. This principle 'enables

decision-makers to adopt precautionary measures when scientific evidence about an environmental or human health hazard is uncertain and the stakes are high' (Bourguignon 2015: 1). The reason why this article relies on this principle is that it is extremely difficult to objectively prove harmful behaviours, especially sexual harassment, and even if these issues are recognised, introducing facial recognition to prevent them could potentially violate human rights such as the right to privacy and data protection, which could delay the introduction of this technology.

In light of the foregoing, the central question of this article is how the precautionary principle can be applied to the use of facial recognition technology within the esports ecosystem, as a means of preventing toxic behaviour by players and fans. This research seeks to lay the foundation for the responsible use of emerging technologies to safeguard esports participants within the esports ecosystem. To achieve the purpose, this article is structured as follows: After this introduction, Section 1 will provide a brief overview of toxic behaviours in esports. Section 2 will then examine the potential benefits and drawbacks of employing facial recognition technology within the esports context. Building on this, Section 3 will explore how the precautionary principle may serve to pave the way for the use of facial recognition technology within the esports ecosystem. The article will conclude by addressing the central research question.

2. Toxic Behaviours in Esports

The term 'toxic behaviours' serves as an umbrella term encompassing various forms of negative behaviours, which is ambiguous and unclear but is shared understanding referring to negative and disruptive behaviours within the esports ecosystem (Adinolf & Türkay 2018; see also Aguerri, Santisteban & Miró-Llinares 2023: 4–7; Formmel & Mandryk 2024: 531; Shinohara 2024). Therefore, Formmel and Mandryk argue that the term 'toxicity' in esports and video gaming contexts 'broadly refers to various types of negative behaviors involving abusive communications directed towards other players and disruptive behaviours that violate the rules and social norms of the game' (Formmel & Mandryk 2024: 529).

More concretely, Adinolf and Türkay argue that toxic behaviours may include harassment, griefing (e.g., deriving enjoyment from intentionally provoking or irritating other players), trolling, cyberbullying, and deliberately assisting opposing players to the detriment of one's own team (Adinolf & Türkay 2018: 366). Furthermore, a recent study conducted by Formmel and Mandryk shows that toxic communications can include harassment, verbal abuse, hate speech, flaming, raging, spamming communications, trolling, and griefing, cheating, threatening the safety of players through doxxing, and swatting (Formmel & Mandryk 2024: 529–530).

Due to these toxic behaviours, esports players have suffered negative effects on their psychological and emotional conditions. For instance, online sexual harassment and cyberbullying can have severe psychological and emotional effects on esports players (Adinolf & Türkay 2018: 365–367), posing a significant challenge to fostering a positive image and culture within the esports industry. Hate crime and hate speech (ADL 2024; Casarosa & Moraru 2021: 25) can discourage the participation of vulnerable groups – including women, LGBT persons, and persons with disabilities – from engaging in esports (Marczyk 2017; Ratan et al. 2020; Tseng 2020: 224–236).

In light of these examples, toxic behaviours are recognised as a major issue within the esports ecosystem. Consequently, video game publishers and third-party organisers have a responsibility to address such behaviours in order to remove barriers to equitable and inclusive participation (McWhertor 2012; Zigelman 2020). To solve this issue, Formmel and Mandryk identify several methods for detecting and mitigating toxic behaviours, including reporting systems, automated filtering using artificial intelligence, and options to mute or avoid toxic players (Formmel & Mandryk 2024: 532–533). Based on this understanding, this article explores how video game publishers and third-party organisers might implement facial recognition technology in practice, while considering the potential impact on the fundamental human rights of esports participants due to such a technology.

3. Facial Recognition Technology in Esports: Advantages and Disadvantages

The deployment of facial recognition technology offers numerous advantages, contributing to greater convenience and efficiency in various aspects of modern life. However, it is essential for the esports ecosystem to recognise and address the potential negative consequences that may arise from its use. This section aims to examine both the potential benefits and the associated risks of using the facial recognition technology inside and outside the esports competitions.

Primarily, the use of facial recognition technology enables video game publishers and third-party organisers to verify players' ages by cross-referencing facial images with the personal information provided during registration. For example, China has implemented facial recognition technology to combat gaming addiction and enforce legislation prohibiting minors from playing electronic games between 10 p.m. and 8 a.m. (Narayan 2021). According to this law, Chinese video game publisher, Tencent Games, has adopted facial recognition technology 'through [its] Balanced Online Entertainment System, from "pre-game" (Parental Guardian Platform), "in-game" (Healthy Gameplay System) to "post-game" (Payment Notification and Online Consultation System)' (Tencent n.d.). Tencent asserts that this comprehensive approach is effective in preventing underage players from participating in their video games outside permitted hours.

However, the use of facial recognition technology may give rise to significant human rights concerns, particularly in relation to the right to privacy as protected under international human rights instruments, such as Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and Article 8 of the European Convention on Human Rights (ECHR) (Marsch 2020: 46). In addition, it raises the question of whether such practices might violate the right to the protection of personal data, as guaranteed by Article 8(1) of the Charter of Fundamental Rights of the European Union (EU Charter).

The Human Rights Committee (HRC) and the European Court of Human Rights (ECtHR) have interpreted these provisions to encompass the right to data protection (ECtHR 2025, para. 234; Joseph & Castan 2013: 559–561; HRC 1988, para. 10; see also ECtHR 2020). The automatic collection of individuals' facial data may be regarded as a direct intrusion into their privacy. Nevertheless, such interference might be deemed justifiable if it serves a legitimate aim – such as the prevention of toxic behaviours in esports – and is necessary and proportionate to achieving that aim.

In the recent case of *Glukhin v. Russia*, the ECtHR ruled in favour of the applicant, finding a violation of Article 8 of the ECHR. The breach arose from the use of facial recognition technology in administrative proceedings, which significantly interfered with the applicant's right to respect for private life (paras. 72–73). The Court held that the state's use of facial recognition technology – specifically, identifying the applicant via photographs and video footage published on Telegram, which subsequently led to his arrest while travelling on the Moscow underground – did not meet the threshold of a 'pressing social need' and was not considered 'necessary in a democratic society' (paras. 78–91). This case underscores the inherent tension between the use of facial recognition technology to protect esports participants from toxic behaviours and the risk of infringing upon their fundamental rights. It highlights the need to carefully assess whether such technological measures satisfy the legal criteria of necessity, proportionality, and legitimacy under human rights law (see Buzenche 2022: 2–3; European Parliament 2023).

In light of the foregoing, video game publishers and third-party organisers should seek effective solutions to prevent toxic behaviours and promote a safer and more inclusive gaming environment. One proposed measure is the adoption of facial recognition technology. This section examines both the potential benefits and drawbacks of employing such technology. On the one hand, video game publishers and third-party organisers may utilise facial recognition technology to verify players' ages by analysing facial images in conjunction with personal information provided during registration. This could support the enforcement of age-related restrictions and help protect younger players. On the other hand, serious concerns arise regarding potential human rights violations, particularly in relation to the right to privacy. The collection and processing of biometric data through facial recognition may constitute a significant intrusion, raising questions about the necessity, proportionality, and legitimacy of such practices under international human rights law.

4. Precautionary Principle and the Use of Facial Recognition Technology in Esports

4.1. What Is the Precautionary Principle?

First of all, this section will consider the following important question before considering the applicability of the precautionary principle to the esports ecosystem: What is the precautionary principle? However, it is important to note that there is no universally accepted definition (Zander 2010: 26–31, 35 and 46) and thus, this section will briefly consider a hypothetical definition of this principle (See De Sadeleer 2020: 137–153).

At the European level, the precautionary principle is enshrined in Article 191 of the Treaty on the Functioning of the European Union (TFEU) (European Union, 2012; Zander, 2010: 76–151). According to this provision, the European Union interprets the precautionary principle as 'an approach to risk management, where, if it is possible that a given policy or action might cause harm to the public or the environment and if there is still no scientific agreement on the issue, the policy or action in question should not be carried out' (European Union n.d.). In simpler terms, the precautionary principle applies to situations involving uncertain risks (Zander 2010: 14–15). This principle is most commonly invoked in the context of environmental law – for example, Principle 15 of the 1992 Rio Declaration on Environment and Development – as decision-makers often face difficulties in predicting environmental or human health hazards with a sufficient level of scientific certainty (Fischer & Ghelardi 2016: 4–7; Schröder 2014, para. 2; Von Schomberg 2006: 28).

Furthermore, Bourguignon states that '[t]he precautionary principle enables decision-makers to adopt precautionary measures when scientific evidence about an environmental or human health hazard is uncertain and the stakes are high' (Bourguignon 2015: 1). In this context, this principle serves to prompt decision-makers to consider the potential harmful effects of their activities on the environment before proceeding with them (Cameron & Abouchar 1991: 2), given the inherent difficulty in obtaining all the required scientific evidence regarding potential environmental impacts beforehand.

Put differently, decision-makers encounter scientific uncertainty when attempting to establish a causal link between their activities and the potential risks they may pose (Zander 2010: 31). Sovereign states have frequently employed this argument to justify their inaction for the prevention of potential environmental damages due to the lack of full proof (Fisher et al. 2006: 3). However, it is crucial to recognise that environmental damage is often irreversible and incurs higher costs for remediation. Therefore, adhering to the precautionary principle requires that decision-makers ought to undertake necessary measures to avoid potential environmental damage and health hazards, even in the absence of definitive scientific proof of causation (Tickner & Kriebel 2006: 47).

Based on this interpretation, the precautionary principle requires decision-makers to evaluate and mitigate the potential adverse effects of their actions before such actions are undertaken – particularly in situations where no clear scientific evidence establishes a direct causal link between the action and the potential harm. At its core, the principle seeks to prevent irreversible harm by proactively addressing risks before they materialise. Accordingly, the precautionary principle is relevant to the adoption of new digital technologies, especially where there is no conclusive scientific evidence confirming that such technologies do not infringe upon individuals' human rights under internationally recognised legal standards. Despite this, some critics argue that applying the precautionary principle to AI technologies

may stifle innovation and hinder technological advancement (Castro & McLaughlin 2019: 12–18). Nevertheless, the use of facial recognition technology within the esports ecosystem presents clear and tangible risks, particularly with respect to the potential violation of human rights.

4.2. How Can the Precautionary Principle Apply to the Use of Facial Recognition Technology in Esports?

4.2.1. Human Rights Due Diligence of Video Game Publishers and Third-Party Organisers under the United Nations General Principles on Business and Human Rights

Before exploring this subsection, it is important to note that, under the United Nations Guiding Principles on Business and Human Rights (UNGPs) – a non-legally binding instrument – business enterprises should voluntarily implement a corporate responsibility to respect human rights.

Principle 12 of the UNGPs stipulates that non-state actors should implement 'human rights due diligence' for their operations of business to prevent human rights violations (Buzenche 2022: 4–5). Furthermore, Principle 13 of the UNGPs states that business enterprises should take necessary measures to mitigate potential risks for human rights violations in their activities in order to fulfil the Principle 13's responsibility. More importantly, Principle 17 of the UNGPs provides for human rights due diligence of business enterprises to prevent and mitigate adverse human rights impacts.

According to these Principles, it can be considered that businesses endorse a risk management perspective that places the responsibility of human rights due diligence on business enterprises to mitigate potential risks of human rights infringements caused by their activities. This concept is based on a 'precautionary approach', aiming to prevent irreparable harm to individuals due to business activities, even in the absence of a direct causal link between those activities and the potential harms (Fasterling 2017: 227–230).

Based on the UNGPs' principles, there has been an attempt to apply them to the technology sector (Allison-Hope et al. 2022; BSR 2022). In 2019, the Office of the United Nations High Commissioner for Human Rights (OHCHR) initiated the B-Tech project with the aim of offering authoritative guidance and resources for implementing the UNGPs within the technology space. The purpose of this project is to 'contribute to addressing the urgent need to find principled and pragmatic ways to prevent and address human rights harms connected with the development of digital technologies and their use by corporate, government and non-governmental actors, including individual users (OHCHR 2019: 2–3).

In pursuit of this objective, the B-Tech Project is founded upon three key pillars aligned with the principles of the UNGPs: (1) 'Guide what responsible business conduct looks like in practice regarding the development, application, sale and use of digital technologies'; (2) 'Guide policy makers in applying a smart mix of regulation, incentives and public policy tools – providing human rights safeguards and accountability without hampering the potential of digital technologies to address social, ecological and other challenges'; and (3) 'Develop workable models for remedy and accountability when harm has occurred' (OHCHR 2019: 3). On these basis, the project identifies several research questions pertaining to these pillars (OHCHR 2019: 5–9).

In light of the foregoing, IT companies should also be held responsible for the respect of human rights and fulfil the human rights due diligence before they develop, invent and release their digital technologies in accordance with the UNGPs' principles. Put simply, IT companies should implement measures to conduct human rights impact assessments before deploying their digital technologies to mitigate potential human rights risks.

As indicated earlier, if it is feasible to apply the UNGPs to emerging fields, this understanding could extend to the esports ecosystem. This implies that video game publishers and third-party organisers usually operate as business enterprises and are thus subject to the same principles outlined in the UNGPs. Therefore, video game publishers and third-party organisers should respect their corporate responsibilities under Principles 12, 13, and 17 of the UNGPs to implement facial recognition technology aimed at protecting esports participants from toxic behaviours. In particular, video game publishers bear greater responsibility than other stakeholders, as they hold the authority – under their copyright ownership – to determine with whom they enter into agreements. Accordingly, they are accountable for selecting sincere and trustworthy partners who are committed to implementing corporate responsibility to respect human rights within their operations. This selection process is essential to fulfilling their broader corporate responsibilities in the organisation and governance of esports competitions.

4.2.2. How Should the Precautionary Principle Apply to the Esports Industry?

Based on the previous subsection, the precautionary principle can apply to non-state actors in the context of the deployment of the AI technology. In this regard, Castro and McLaughlin indicate that:

> The precautionary principle is the idea that if a technological innovation may carry a risk of harming the public or the environment, then those proposing the technology should bear the burden of proving it will not. If they cannot, governments should limit the use of the new technology until proven safe (Castro & McLaughlin 2019: 2).

Therefore, this principle can apply not only environmental law, but also digital technology industry to prevent potential human rights hazard caused by the use of the new digital technology.

In this context, how can the precautionary principle help mitigate the potential risk of human rights violations arising from the use of facial recognition technology within the esports ecosystem? In addressing this question, the

precautionary principle may require video game publishers and third-party organisers to assess the potential human rights risks associated with facial recognition technology prior to its implementation as a tool to prevent toxic behaviours in the esports environment.

Although there is currently insufficient scientific evidence to fully justify the use of this relatively new technology, video game publishers and third-party organisers nonetheless bear a responsibility to protect esports participants from online harassment and other forms of toxic behaviours. To this end, facial recognition technology may contribute to achieving this protective aim. The precautionary principle plays a crucial role in weighing the benefits of using such technology against the risks of human rights infringements, particularly regarding privacy and data protection.

Furthermore, applying the precautionary principle in this context reinforces the corporate responsibility to conduct human rights due diligence, in line with Principles 12, 13, and 17 of the UNGPs. This imposes video games publishers and third-party organisers on the respect of precautionary principle. In this context, adherence to the precautionary principle would justify the responsible and proportionate use of facial recognition technology as a means of safeguarding esports participants from toxic behaviours within the esports ecosystem, particularly at the initial stage of its deployment. After its deployment in practice, potential issues concerning privacy infringement and data protection arising from the use of facial recognition technology must be carefully analysed.

5. Conclusion

In using new technology within our society, potential risks can arise. However, it is essential not to prohibit such new technology but rather to find ways to enhance our lives with the use of this new technology. In this context, facial recognition technology poses potential legal issues, particularly concerning the infringement of the right to privacy and data protection. On the other hand, it could also contribute to protecting esports participants against toxic behaviours, such as verification of their age and identification of who conducts such behaviours while playing video games.

To strike a balance between preventing toxic behaviours and the potential risks of human rights violations, this article refers to the precautionary principle. This principle urges decision-makers, namely video game publishers and third-party organisers, to carefully consider the potential harmful effects of their activities before pursuing them, especially when there is no clear scientific evidence proving a direct causal link between those activities and the potential harmful effects. This principle aligns with the concept of human rights due diligence prescribed in Principles 12 and 13 of the UNGPs.

In conclusion, the precautionary principle can play a significant role in encouraging decision-makers to assess the potential risks associated with the initial deployment of facial recognition technology, thereby contributing to the prevention of toxic behaviours within the esports ecosystem. Accordingly, the responsible use of such technology may serve as an effective remedy for mitigating harmful conduct and fostering a safer esports environment.

Competing Interests

The author has no competing interests to declare.

References

Adinolf, S and **Türkay, S** 2018 Toxic behaviors in esports games: player perceptions and coping strategies. *CHI PLAY'18 Extended Abstracts*, 365: 1–6. DOI: https://doi.org/10.1145/3270316.3271545

Aguerri, J C, Santisteban, M, and **Miró-Llinaresm, F** 2023 The enemy hates best? Toxicity in League of Legends and its content moderation implication. *European Journal of Criminal Policy and Research*, 29(3): 437–456. DOI: https://doi.org/10.1007/s10610-023-09541-1

Allison-Hope, D, et al. 2022 Applying the UNGPs to technology: our point of view. *BSR Blog*, 7 March 2022 Available at https://www.bsr.org/en/blog/applying-the-ungps-to-technology-our-point-of-view [Last accessed 9 May 2025].

Anti-Defamation League (ADL) 2024 Hate is no game: hate and harassment in online games 2023, 2 June 2024. Available at https://www.adl.org/resources/report/hate-no-game-hate-and-harassment-online-games-2023 [Last accessed 9 May 2025].

Bourguignon, D 2015 The precautionary principle: definitions, applications and governance, 9 December 2015. Available at https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2015)573876 [Last accessed 8 November 2024].

BSR 2022 Input to the High Commissioner report on the practical application of the UNGPs to the activities of technology companies, February 2022. Available at https://www.bsr.org/reports/BSR_OHCHR_Submission.pdf [Last accessed 9 May 2025].

Buzenche, M 2022 Non-state actors and law-making in IBHR: the internet intermediaries' responsibility to respect human rights and the UNGPs' non-state-based grievance, August 2022. *Working Paper: EUI AEL, European Society of International Law (ESIL) Papers*. Available at https://hdl.handle.net/1814/74558 [Last accessed 9 May 2025].

Cameron, J and **Abouchar, J** 1991 The precautionary principle: a fundamental principle of law and policy for the protection of the global environment. *Boston College International and Comparative Law Review*, 14(1): 1–27. https://lira.bc.edu/work/ns/f06efb0b-19f6-4b96-b64c-276e8548c8c4

Casarosa, F and **Moraru, M** 2021 Handbook on techniques of judicial interaction in the application of the EU Charter: freedom of expression and countering hate speech, 2021. *European University Institute*. Available at https://cadmus.eui.eu/handle/1814/73441 [Last accessed 9 May 2025].

Castro, D and **McLaughlin, M** 2019 Ten ways the precautionary principle undermines progress in artificial intelligence, 4 February 2019. *ITIF Report*. Available at https://itif.org/publications/2019/02/04/ten-ways-precautionary-principle-undermines-progress-artificial-intelligence/ [Last accessed 9 May 2025].

De Sadeleer, N 2020 *Environmental principles: from political slogans to legal rules*, 2nd edition. Oxford: Oxford University Press. DOI: https://doi.org/10.1093/acprof:oso/9780199254743.001.0001

European Court of Human Rights (ECtHR) 2020 *Guide to the case-law of the European Court of Human Rights: data protection*, 1st edition, 31 December 2020. Available at https://rm.coe.int/guide-data-protection-eng-1-2789-7576-0899-v-1/1680a20af0 [Last accessed 9 May 2025].

European Court of Human Rights (ECtHR) 2025 *Guide on Article 8 of the Convention – Right to respect for private and family life, home and correspondence*, updated on 28 February 2025. Available at https://ks.echr.coe.int/web/echr-ks/article-8 [Last accessed 9 May 2025].

European Parliament 2023 *EU AI Act: first regulation on artificial intelligence*. Available at https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence [Last accessed 9 May 2025].

European Union n.d. Precautionary principle. *EU-Lex Glossary*. Available at https://eur-lex.europa.eu/EN/legal-content/glossary/precautionary-principle.html [Last accessed 9 May 2025].

European Union 2012 *Consolidated version of the Treaty on the Functioning of the European Union*. Official Journal of the European Union, C 326, 26 October 2012: 47–390. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT [Last accessed 9 May 2025].

Fasterling, B 2017 Human rights due diligence as risk management: social risk versus human rights risk. *Business and Human Rights Journal*, 2(2): 225–247. DOI: https://doi.org/10.1017/bhj.2016.26

Fischer, A J and **Ghelardi, G** 2016 The precautionary principle, evidence-based medicine, and decision theory in public health evaluation. *Frontiers in Public Health*, 4(107): 1–7. DOI: https://doi.org/10.3389/fpubh.2016.00107

Fisher, E, et al. 2006 Implementing the precautionary principle: perspectives and prospects. In: Fisher, E, et al. (eds.) *Implementing the Precautionary Principle: Perspectives and Prospects*. Cheltenham: Edward Elgar, pp. 1–16. DOI: https://doi.org/10.4337/9781847201676.00009

Formmel, J and **Mandryk, R L** 2024 Toxicity in esports. In: Jenny, S et al. (eds.) *Routledge handbook of esports*. Routledge, pp. 529–539. DOI: https://doi.org/10.4324/9781003410591-57

Human Rights Committee (HRC) 1988 *CCPR General Comment No. 16: Article 17(Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988. Available at https://www.refworld.org/legal/general/hrc/1988/en/27539 [Last accessed 9 May 2025].

Joseph, S and **Castan, M** 2013 *The international covenant on civil and political rights: cases, materials, and commentary*, 3rd edition. Oxford: Oxford University Press. DOI: https://doi.org/10.1093/law/9780199641949.001.0001

Marczyk, J 2017 Online games, harassment and sexism, 26 November 2017. *Psychology Today*. Available at https://www.psychologytoday.com/us/blog/pop-psych/201711/online-games-harassment-and-sexism [Last accessed 9 May 2025]

Marsch, N 2020 Artificial intelligence and the fundamental right to data protection: opening the door for technological innovation and innovative protection. In: Wischmeyer, T and Rademacher, T (eds.) *Regulating artificial intelligence*. Cham: Springer, pp. 33–52. DOI: https://doi.org/10.1007/978-3-030-32361-5_2

McWhertor, M 2012 The League of Legends team of scientists trying to cure 'toxic behavior' online, 14 October 2012. *Polygon*. Available at https://www.polygon.com/2012/10/17/3515178/the-league-of-legends-team-of-scientists-trying-to-cure-toxic [Last accessed 9 May 2025].

Narayan, N 2021 Tencent introduces face recognition feature to prevent children from gaming at night, 13 July 2021. *European Gaming*. Available at https://europeangaming.eu/portal/latest-news/2021/07/13/96109/tencent-introduces-face-recognition-feature-to-prevent-children-from-gaming-at-night/ [Last accessed 9 May 2025].

Newzoo 2022 *Global esports & live streaming market report 2022*. Free Version. Available at https://newzoo.com/insights/trend-reports/newzoo-global-esports-live-streaming-market-report-2022-free-version/ [Last accessed 9 May 2025].

Nothelfer, N, Jenny, S, and **Besombes, N** 2024 Defining and spelling esports. In: Jenny, S et al. (eds.) *Routledge handbook of esports*. Routledge, pp. 6–18. DOI: https://doi.org/10.4324/9781003410591-3

Office of the United Nations High Commissioner for Human Rights (OHCHR) 2019 *UN human rights business and human rights in technology project (B-Tech): applying the UN guiding principles on business and human rights to digital technologies*, November 2019. Available at https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/B_Tech_Project_revised_scoping_final.pdf [Last accessed 9 May 2025].

Ratan, R, et al. 2020 Toxicity in gaming is dangerous. Here's how to stand up to it, 9 December 2020. *WIRED*. Available at https://www.wired.com/story/toxicity-in-gaming-is-dangerous-heres-how-to-stand-up-to-it/ [Last accessed 9 May 2025].

Riot Games 2022 *Zero harm in comms: Riot and Ubisoft working together on research project to create more positive gaming communities*, 16 November 2022. Available at https://www.riotgames.com/en/news/riot-games-ubisoft-tackling-toxicity-in-games-with-new-project [Last accessed 9 May 2025].

Schröder, M 2014 Precautionary approach/principle, *Oxford Public International Law: Max Planck Encyclopaedias of International Law*, March 2014. Available at https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1603?rskey=sLKDQq&result=1&prd=EPIL [Last accessed 9 May 2025].

Shinohara, T 2024 Human rights in esports, *Esports Legal Wiki*, 5 February 2024. Available at https://esportslegal.news/esports-legal-wiki/human-rights/human-rights-in-esports/ [Last accessed 9 May 2025].

Stevens, M 2002 The precautionary principle in the international arena. *Sustainable Development Law & Policy*, 2(2): 13–15. DOI: https://digitalcommons.wcl.american.edu/sdlp/vol2/iss2/7/

Tencent n.d. *Balanced online entertainment system for underaged users*. Available at https://www.tencent.com/en-us/responsibility/balanced-online-entertainment-system-for-underaged-users.html [Last accessed 9 May 2025].

Tseng, Y 2020 The principles of esports engagement: a universal code of conduct. *Journal of Intellectual Property Law*, 27(2): 209–250. DOI: https://digitalcommons.law.uga.edu/jipl/vol27/iss2/3/

Von Schomberg, R 2006 The precautionary principle and its normative challenges. In: Fisher, E, et al. (eds.) *Implementing the precautionary principle: perspectives and prospects*. Cheltenham: Edward Elgar, pp. 19–41. DOI: https://doi.org/10.4337/9781847201676.00011

Zander, J 2010 *The application of the precautionary principle in practice: comparative dimensions*. Cambridge: Cambridge University Press. DOI: https://doi.org/10.1017/CBO9780511779862

Zigelman, K 2020 *How Riot games used science to curb toxic behavior in League of Legends*, 19 March 2020. *Spectrum Labs*. Available at https://www.spectrumlabsai.com/the-blog/how-riot-games-is-used-behavior-science-to-curb-league-of-legends-toxicity [Last accessed 9 May 2025].

How to cite this article: Shinohara, T. 2025. Precautionary Principle for the Use of Facial Recognition Technology within the Esports Ecosystem? *Entertainment and Sports Law Journal*, 23(1): 4, pp. 1–7. DOI: https://doi.org/10.16997/eslj.1873

Submitted: 09 May 2025 **Accepted:** 15 July 2025 **Published:** 04 August 2025

Entertainment and Sports Law Journal is a peer-reviewed open access journal published by University of Westminster Press.

OPEN ACCESS