Cybersecurity in Esports: Legal Frameworks and Regulatory Gaps

Aaditya Gautam Balaji[1], Aishwarya. P[2]

[1]Student of LL.M in Cyber Law and Security, School of Law, SRM Institute of Science and Technology, Kattankulathur.
[2]Student of LL.M in Criminal Law and Justice, School of Law, SRM Institute of Science and Technology, Kattankulathur.

ABSTRACT
E-sports, or competitive video gaming, has become a major global industry with millions of players and viewers. As this digital sport continues to grow, it faces increasing risks related to cybersecurity. Hackers often target E-sports platforms, tournaments, and individual players through data breaches, online attacks, and other cybercrimes. These threats not only harm the players and organisers but also raise serious legal questions. This research paper looks at the legal approach to cybersecurity in E-sports using a doctrinal method. It studies existing laws in India, the European Union, and the United States that deal with cybercrime and digital security. The paper also examines the duties of game developers, tournament organisers, and streaming services in keeping online competitions safe. Through legal analysis and case examples, this paper shows that many current laws are not strong enough to deal with the new challenges in the E-sports world. In the end, the paper suggests ways to improve the legal system and make E-sports safer for everyone involved.

Keywords: E-sports law, cybersecurity, cybercrime, digital gaming, legal regulation; India, GDPR, IT Act.

1. INTRODUCTION

E-sports, or electronic sports, refers to organised, competitive video gaming that takes place on digital platforms. Over the past decade, E-sports has grown from a niche activity into a billion-dollar industry with global tournaments, professional teams, and millions of online viewers.[1] With the increasing popularity of this digital sport, a wide range of legal issues have come to light, especially concerning cybersecurity.

Unlike traditional sports, E-sports takes place entirely in online environments. These virtual spaces involve large amounts of data, real-time interactions, and internet-based platforms, all of which are vulnerable to cyberattacks. Players and spectators often have to share personal data, such as names, emails, locations,

[1] See Newzoo, Global Esports Market Report 2023, https://newzoo.com/insights/trend-reports/newzoo-global-esports-market-report-2023-free-version (last visited July 20, 2025) (projecting the global E-sports market to reach over $1.8 billion in 2025).

and payment details. Tournaments and streaming platforms handle even more sensitive information.[2] As a result, E-sports platforms have become major targets for hackers and cybercriminals.

There have been several well-known incidents of cyberattacks in the E-sports world, including data breaches, denial-of-service (DDoS) attacks, account hijacking, and even ransomware attacks during major events. These incidents not only cause financial loss and damage to reputation but also raise serious legal questions about responsibility and protection under the law.[3]

This paper focuses on understanding how existing legal frameworks deal with cybersecurity in E-sports. It looks at laws from India, the United States (US), and the European Union (EU), and also discusses the role of key stakeholders like game developers, tournament organisers, and streaming platforms. The main goal is to examine if the current laws are enough to protect against cyber risks in E-sports and what improvements can be made to strengthen the legal approach.

2. RESEARCH METHODOLOGY

This paper uses a **doctrinal research method**, which means it is based entirely on the study of existing legal materials such as statutes, case law, regulations, and scholarly articles. Doctrinal research involves analysing what the law is, rather than collecting data from the field.

The research focuses on laws related to cybersecurity and digital safety as they apply to the E-sports industry. Legal documents from India, the EU, and the US are studied to understand how each jurisdiction handles cyber threats in online gaming. Official policy papers, government guidelines, and rules related to information technology and data protection have also been referred to.

This method is appropriate because it helps in understanding the strengths and weaknesses of current laws and allows for comparison between different legal systems. It also helps in identifying gaps in the law and suggesting legal reforms to make the E-sports environment safer and more secure.

The sources used in this paper are all secondary sources, including:

- Statutory law (like the IT Act, 2000 in India and the GDPR in the EU)
- Court judgments
- Reports from legal bodies and E-sports associations
- Legal commentaries and academic journals

This approach ensures that the analysis remains within the boundaries of legal theory and established rules without relying on surveys or interviews.

3. UNDERSTANDING CYBERSECURITY IN E-SPORTS

E-sports is a digital environment where tournaments, team-based competitions, and real-time gameplay occur entirely online. These platforms collect and store a huge amount of sensitive data, including personal details of players, login credentials, game statistics, voice and video recordings, and financial transactions. As the industry has grown, so have the cybersecurity risks.

[2] See Paul Redmond, Data Collection and User Rights in Esports Platforms: An Emerging Concern, 22 Gaming L. Rev. 153, 155 (2020) (discussing the scale and types of personal data collected by E-sports platforms).

[3] See Josh Ye, Twitch Hack Highlights Growing Cybersecurity Risks in Esports, Reuters (Oct. 7, 2021), https://www.reuters.com/technology/twitch-hack-highlights-cybersecurity-risks-esports-2021-10-07/.

3.1 Common Cybersecurity Threats in E-Sports

E-sports faces a range of cyber threats that affect both users and companies. One of the most common attacks is a **Distributed Denial-of-Service (DDoS)** attack, where attackers overload a server with traffic to crash the game or slow down the network during live matches. This not only disrupts competitions but also affects the fairness of the game.

Another major risk is **account hacking**, where cybercriminals gain unauthorised access to player or administrator accounts. These accounts often have in-game purchases, exclusive skins, or even real money linked to them. Such hacks can cause serious financial and reputational damage.

There are also cases of **ransomware attacks** where hackers block access to important tournament data or streaming platforms and demand money to release it. For example, in 2021, the source code and payment records of Twitch—a popular E-sports streaming service—were leaked online due to a large-scale breach[4].

Cheating software and mods are also cybersecurity concerns, as they are often downloaded from unsafe websites that may contain malware. These tools not only give unfair advantages but can also infect the user's system.

Lastly, **phishing attacks** are used to trick players into sharing login information through fake emails or links that look like official tournament messages.

3.2 Why E-Sports Is a High-Risk Target

E-sports platforms attract a large number of young users who may not be aware of safe online practices, making them easy targets. Furthermore, tournaments involve high-value sponsorships, prize pools, and real-time transactions, making them attractive to cybercriminals.

Another reason is that E-sports depends heavily on third-party platforms such as Discord, Twitch, Steam, and YouTube Gaming. Each of these platforms has its own data policies and security protocols, which may not always align. This fragmentation increases the chance of weak links in the cybersecurity chain[5].

Also, many smaller tournament organisers and gaming communities lack proper cybersecurity infrastructure, making them soft targets for hackers.

3.3 Impact of Cyberattacks on the E-Sports Ecosystem

The effects of cyberattacks go beyond just financial loss. If a game is disrupted during a professional match, it affects not only the outcome but also the reputation of the organisers. Fans may lose trust in the fairness and safety of the competition.

Players may also face **identity theft** and **doxxing** (leaking of private information), which can lead to mental health issues or harassment. In team-based games, a single cyberattack can lead to disqualification, fines, or postponement of entire events[6].

For E-sports companies, repeated attacks may result in regulatory scrutiny, legal liability, and breach of user trust, especially if user data is compromised.

[4] Taylor Lyles, Twitch Confirms It Was Hacked, Says the 'Incident' Is Still Ongoing, The Verge (Oct. 6, 2021), https://www.theverge.com/2021/10/6/22712377/twitch-hack-leak-source-code-payouts.

[5] Adam Fitch, The Need for a Cybersecurity Wake-Up Call in Esports, Esports Insider (May 17, 2021), https://esportsinsider.com/2021/05/the-need-for-a-cybersecurity-wake-up-call-in-esports/.

[6] Andy Chalk, CS:GO Tournament Disrupted by Alleged DDoS Attack, PC Gamer (Feb. 5, 2021), https://www.pcgamer.com/csgo-tournament-disrupted-by-alleged-ddos-attack/.

4. LEGAL FRAMEWORK GOVERNING CYBERSECURITY IN E-SPORTS

Cybersecurity in E-sports is regulated through general information technology and cybercrime laws, as most countries do not yet have specific statutes for the E-sports sector. This section discusses the legal frameworks in **India**, the **United States (US)** , and the **European Union (EU)**, focusing on how they apply to the digital gaming and E-sports industry.

4.1 India

In India, the legal framework for cybersecurity is primarily based on the **Information Technology Act, 2000 (IT Act)**, which provides penalties and remedies for various cybercrimes. Section 43 of the Act deals with unauthorised access and damage to computer systems, while Section 66 prescribes punishment for hacking.[7] E-sports platforms that suffer data breaches, DDoS attacks, or account hacking incidents fall within the scope of these provisions.

Additionally, **Section 66C** criminalises identity theft, which is relevant when player or spectator accounts are hacked or impersonated. **Section 66D** punishes cheating by impersonation through electronic means, which can apply in cases of phishing and scam messages sent to E-sports participants.[8]

In 2022, the Ministry of Electronics and Information Technology (MeitY) issued revised guidelines under the **CERT-In (Indian Computer Emergency Response Team)** rules, requiring all service providers—including gaming platforms—to report cybersecurity incidents within six hours.[9] This is particularly relevant for E-sports tournaments and streaming services hosted in India or used by Indian users.

The **Digital Personal Data Protection Act, 2023** aimed to regulate the process of handling of personal data in digital spaces.[10] This law introduces obligations on "data fiduciaries," including E-sports companies, to ensure that user data is processed lawfully and securely. Though the law is still in its early stages, it is a significant step toward protecting player data in the Indian E-sports industry.

However, India does not yet have any **sector-specific law** for E-sports or digital gaming, and enforcement often depends on general provisions of the IT Act, which may not be sufficient for addressing complex cyber threats in real-time gaming environments.

4.2 European Union (EU)

The European Union has one of the strongest legal regimes for data protection and cybersecurity. The **General Data Protection Regulation (GDPR)** is a central piece of legislation that regulates how personal data is collected and used across all sectors, including gaming and E-sports.[11]

E-sports platforms operating in the EU or dealing with EU users must comply with GDPR requirements, such as obtaining valid user consent, ensuring data minimisation, and providing mechanisms for user access and deletion of data. Breaches of these duties can lead to heavy penalties, as seen in the case of several gaming companies facing fines for non-compliance.[12]

[7] Information Technology Act, 2000, § 43, § 66, No. 21, Acts of Parliament, 2000 (India).

[8] Id. at § 66C, § 66D.

[9] Ministry of Electronics and Information Technology, Directions Under Section 70B of the IT Act, 2000 Relating to Information Security Practices, CERT-In (Apr. 28, 2022), https://www.cert-in.org.in/.

[10] Digital Personal Data Protection Act, No. 22, Acts of Parliament, 2023 (India).

[11] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[12] See, e.g., European Data Protection Board, *Enforcement Actions in the Gaming Sector*, https://edpb.europa.eu (last visited July 20, 2025).

In addition to GDPR, the **Network and Information Security Directive (NIS2 Directive)** imposes obligations on digital service providers to implement risk management practices and report serious cybersecurity incidents to national authorities.[13] While not directly mentioning E-sports, these rules are applicable to gaming companies and online services that host large user bases and perform critical functions.

The **Digital Services Act (DSA)**, adopted in 2022, introduces further obligations on large online platforms, including transparency in algorithms and content moderation.[14] For streaming platforms like Twitch or YouTube Gaming that broadcast E-sports events, compliance with the DSA may include better mechanisms for reporting abuse, misinformation, or cyber harassment during live events.

Despite its comprehensive structure, the EU framework does not yet contain **E-sports-specific rules**, but its broad scope ensures significant protection for digital users and players from a cybersecurity perspective.

4.3 United States (US)

In The United States different laws apply to different industries as they follow a **sectoral approach** for handling data. There is **no single federal law** that governs cybersecurity in the E-sports sector specifically. However, several legal instruments may apply. The **Computer Fraud and Abuse Act (CFAA), 1986**, is the primary federal law that deals with unauthorised access to computer systems, which is relevant in cases of hacking or disruption of online tournaments.[15] The **Electronic Communications Privacy Act (ECPA)** and the **Children's Online Privacy Protection Act (COPPA)** also apply in cases involving unauthorised interception of communication or collection of data from minors participating in E-sports.[16]

At the state level, laws like the **California Consumer Privacy Act (CCPA)** grant people right over their personal data and impose obligations on gaming companies that collect and process such data.[17] Other states like New York and Virginia have introduced similar laws to regulate digital privacy and cybersecurity.

In 2021, the Federal Trade Commission (FTC) emphasised the need for gaming platforms to improve cybersecurity measures, particularly in relation to children and young adults who form a large part of the E-sports user base.[18] The FTC has also taken enforcement action against game developers for failing to secure user data.

Unlike the EU and India, the US legal system currently lacks **uniform national rules** for cybersecurity in the gaming sector, which creates challenges in enforcement and consistency across platforms.

5. RESPONSIBILITIES OF STAKEHOLDERS IN E-SPORTS CYBERSECURITY

Cybersecurity in E-sports is not just the responsibility of governments and regulators. A wide range of **private stakeholders** are directly involved in making the digital gaming ecosystem safe. These include

[13] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2 Directive), 2022 O.J. (L 333) 80.

[14] Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 (Digital Services Act), 2022 O.J. (L 277) 1.

[15] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986).

[16] Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2523 (1986); Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998).

[17] California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100–1798.199 (2018).

[18] Federal Trade Commission, Protecting Kids in the Gaming World, FTC.gov (July 2021), https://www.ftc.gov/news-events/blogs/data-spotlight/2021/07/protecting-kids-gaming-world.

game developers, **tournament organisers**, **streaming platforms**, **E-sports teams**, and **individual players**. Each of them plays a key role in preventing and responding to cyber threats.

5.1 Game Developers

Game developers, such as Riot Games, Valve Corporation, and Blizzard Entertainment, are responsible for building and maintaining the gaming infrastructure. They must ensure that their games are secure from technical vulnerabilities. This includes patching software bugs, encrypting user data, and providing secure login systems such as two-factor authentication.[19]

Under legal systems like the **GDPR** in the EU and the **Data Protection Act** in India, game developers are considered **data controllers** or **data fiduciaries**, which means they are legally responsible for the safe handling of player data.[20] If a data breach occurs due to their negligence, they may be subject to regulatory fines and user lawsuits.

Developers also have an ethical duty to build systems that prevent cheating and hacking. Many popular games now have **built-in anti-cheat software**, but some tools have been criticised for excessive data collection, raising further privacy concerns.[21]

5.2 Tournament Organisers

E-sports tournaments often involve high prize pools and attract millions of viewers. Organisers such as **ESL**, **DreamHack**, or **local gaming associations** must ensure the digital infrastructure used for hosting matches is safe from attacks.

This includes securing the server networks, using encrypted communication systems for referees and teams, and employing professional cybersecurity teams during major events. If a tournament is disrupted by a DDoS attack or player accounts are compromised, the organiser may be liable under general tort law or contract law for failing to provide a secure competition environment.[22]

Some tournament organisers use **external platforms** like Discord or Battlefy for registration and team management. In such cases, organisers must ensure these platforms also comply with cybersecurity laws.

5.3 Streaming Platforms

Social media Platforms like **Facebook Gaming** and other gaming platforms like the **Twitch**, or a **YouTube Gaming** channel, play a major role in E-sports by hosting live broadcasts and storing past matches. These platforms collect large amounts of data from viewers and streamers, including chat records, payment details, and login information.

As digital service providers, they fall under the scope of regulations like the **Digital Services Act (DSA)** in the EU or **Section 79 of the Indian IT Act**, which imposes duties to act against illegal content and ensure platform integrity.[23] If they are negligent in responding to cyber harassment, hate speech, or phishing links in live chats, they may face legal consequences.

Streaming platforms are also expected to implement **content moderation**, encryption for user data, and strong access controls to prevent unauthorised intrusion or content theft.

[19] Riot Games, Security Center: Player Protection Tools, https://www.riotgames.com/en/security (last visited July 22, 2025).

[20] See Regulation 2016/679, art. 4(7); Digital Personal Data Protection Act, § 2(i), No. 22 of 2023 (India).

[21] Samuel Axon, Valorant Anti-Cheat System Raises Privacy Concerns, Ars Technica (Apr. 15, 2020), https://arstechnica.com/gaming/2020/04/valorants-invasive-anti-cheat-software-draws-criticism/.

[22] Michael Wagner, Cybersecurity in Competitive Gaming: Legal Liability of Tournament Hosts, 14 Sports Law. J. 45, 51–52 (2021).

[23] Digital Services Act, Regulation 2022/2065, art. 15; Information Technology Act, § 79, No. 21 of 2000 (India).

5.4 E-Sports Teams and Players

Professional E-sports teams and single players are not passive participants. They often sign contracts with sponsors and platforms that include clauses about data handling, content sharing, and acceptable online behaviour.

Teams are advised to adopt **cyber hygiene practices**, such as avoiding unsecured Wi-Fi, not sharing passwords, and regularly updating software. Some top-tier teams hire **cybersecurity consultants** to protect against phishing, social engineering, and targeted hacking.

Players, especially minors, are often unaware of their privacy rights or how their data is being used. Hence, the duty to educate and protect them falls on coaches, managers, and platform providers.

5.5 Shared Responsibility and Contractual Risk

Cybersecurity is a shared responsibility. Legal accountability often depends on **contractual arrangements** between these stakeholders. For example, a data breach in a co-sponsored tournament may involve liability for both the developer and the organiser.

Well-drafted contracts should clearly define responsibilities for data protection, security audits, breach notification, and dispute resolution mechanisms. This reduces the risk of legal uncertainty if a cybersecurity incident occurs.[24]

6. CASE STUDIES / NOTABLE INCIDENTS IN E-SPORTS CYBERSECURITY

Examining real-life incidents helps illustrate the **practical cybersecurity challenges** facing the E-sports industry today. These case studies show how cyberattacks, data breaches, and digital misconduct can impact players, developers, and audiences—often with legal consequences.

6.1 The Riot Games Source Code Breach (2023)

Riot Games, a popular game developer and has also made hit projects like like League of Legends and Valorant, suffered a significant cybersecurity breach in the month of January of 2023. Hackers accessed the company's development environment and the source code for both games, as well as anti-cheat tools were compromised.[25]

The attackers demanded a ransom, which Riot refused to pay. Instead, Riot informed the public and law enforcement, admitting that while no player data had been exposed, the stolen code could help hackers develop cheats that could ruin the competitive integrity of matches.[26]

This case highlights the **dual risk** of data security and fair play. While GDPR may not apply if no personal data was breached, the loss of source code raises intellectual property and competition law concerns. Developers must not only protect user data but also **internal technical infrastructure** that directly affects gameplay and fairness.

6.2 Twitch Data Leak (2021)

In October 2021, **Twitch**, one of the world's largest live-streaming platforms, experienced a massive leak that exposed **125GB of internal data**, including source code, streamer earnings, and platform tools.[27]

[24] Adam B. Thierer, Cybersecurity and Contract Law in the Digital Age, 42 Hastings Comm. & Ent. L.J. 223, 228–31 (2020).

[25] Riot Games, Security Incident Update: Social Engineering Attack, https://www.riotgames.com/en/news/security-incident-update (last visited July 23, 2025).

[26] Jay Peters, Riot Confirms Source Code Theft After Cyberattack, The Verge (Jan. 25, 2023), https://www.theverge.com/2023/1/25/riot-games-source-code-theft-cyberattack.

[27] BBC News, Twitch Suffers Massive Data Leak, BBC (Oct. 6, 2021), https://www.bbc.com/news/technology-58823440.

Although no passwords or payment information were confirmed leaked, the incident raised **serious concerns about Twitch's data protection systems**. The leak included details about "Twitch's future plans" and software used to manage streamers, opening the door for potential social engineering attacks.

This incident triggered debates about the platform's legal duty under data protection laws. While Twitch, owned by Amazon, issued public statements and improved its security measures, the breach remains a warning about the **scale and sensitivity of data** held by E-sports-related platforms.

6.3 DDoS Attacks on Blizzard Servers (2019–2022)

Blizzard Entertainment, known for titles like Overwatch, World of Warcraft, and Hearthstone, has faced **multiple Distributed Denial of Service (DDoS) attacks** that disrupted game servers for hours or even days.[28]

These attacks mostly targeted login systems or tournament windows, affecting not just casual players but also **ranked competitions and official matches**. Blizzard's regular updates and use of Cloudflare-based security systems have reduced downtime, but attackers continue to find new ways to overwhelm servers.

Such attacks are a common challenge in E-sports, particularly during high-profile events. Legally, most countries treat DDoS as a criminal offence. In the United States, it is punishable under the **Computer Fraud and Abuse Act (CFAA)**, and in India, under **Sections 43 and 66 of the Information Technology Act**.[29] However, enforcement remains difficult due to anonymous and international actors.

6.4 Valorant Pro Player Hacking Allegations (2020)

In 2020, during a Valorant online tournament, a professional player was accused of using **unauthorised third-party software** to cheat during a live-streamed match. Video evidence surfaced showing suspicious gameplay patterns. After investigation, the player was banned, and the team was disqualified from future events.[30]

While this was not a direct cyberattack, it shows how cybersecurity also involves **maintaining competitive integrity**. Developers and tournament organisers must use effective anti-cheat software and investigation protocols, or they risk legal issues under **contract law** or **event sponsorship agreements**.

These incidents can lead to breach of contract claims, reputational damage, and potential lawsuits from sponsors or co-participants who lose prize opportunities due to unfair practices.

6.5 India's ROG Phone Hackathon Incident (2021)

In 2021, during the **ASUS ROG Phone India Championship**, a minor hacking attempt was reported during live qualifiers. A team allegedly used scripts to manipulate in-game actions through emulator software. Although the breach did not succeed, the event organisers disqualified the team and published new cybersecurity rules for future tournaments.[31]

This case shows the growing attention to **cyber ethics in Indian E-sports**, where law is still catching up, but **industry self-regulation** plays an active role. It also illustrates the blurred line between digital misconduct and criminal behaviour, especially in competitive settings involving prize money.

[28] Blizzard CS EU, DDoS Attack Details, Twitter (June 2019–Oct. 2022), https://twitter.com/BlizzardCSEU_EN.

[29] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2001); Information Technology Act, § 43, § 66, No. 21 of 2000 (India).

[30] Dexter Tan Guan Hao, Valorant Pro Player Banned for Cheating, ONE Esports (Oct. 2020), https://www.oneesports.gg/valorant/pro-player-banned-for-cheating/.

[31] Manish Kumar, ROG India Hack Attempt Raises Fair Play Concerns, GamingIndia (Dec. 15, 2021), https://www.gamingindia.in/rog-phone-hackathon-controversy.

7. KEY CHALLENGES IN CYBERSECURITY REGULATION OF E-SPORTS

While various legal frameworks exist to address cybersecurity in general, applying them to the unique environment of E-sports presents several difficulties. E-sports combines real-time gaming, live streaming, digital economies, and global user interaction. These features bring **complex legal and practical challenges** for regulators, developers, and platforms alike.

7.1 Lack of Sector-Specific Regulation

Most cybersecurity laws are designed for general digital platforms, not for competitive gaming or E-sports. Unlike financial services or healthcare, E-sports has no internationally accepted cybersecurity standards. Laws like the IT Act in India or the GDPR in the EU apply indirectly, but do not address the specific needs of tournaments, player contracts, live match streaming, or platform vulnerabilities in gaming environments.[32]

This absence of tailored laws creates confusion over legal duties and limits the scope of enforcement. For example, it is unclear which entity—developer, tournament organiser, or streamer—is responsible if a cyberattack leads to loss of personal data or disrupts gameplay during an official match.

7.2 Jurisdictional Issues in Cross-Border Gaming

E-sports is global by nature. Players, spectators, and servers are often located in different countries. This creates **jurisdictional conflicts** when a cyberattack occurs.

For example, a DDoS attack might originate from one country, affect servers in another, and target players in a third. In such cases, it is difficult to identify which country's law should apply and whether the attacker can be legally prosecuted.[33]

Cross-border investigations are also complicated by **different legal definitions** of cybercrime, data breach notification rules, and standards of proof. Even with conventions like the **Budapest Convention on Cybercrime**, enforcement across borders remains weak without proper cooperation between national authorities.[34]

7.3 Delayed Reporting and Under-Disclosure

Many E-sports companies do not promptly report cyber incidents. Smaller platforms may fear reputational damage, legal liability, or financial losses. As a result, **underreporting** is common.

Delayed reporting not only affects user safety but also makes legal redress difficult. Regulators and affected users may not be informed in time to take preventive or corrective action. Although India's CERT-In mandates reporting within six hours[35], compliance is inconsistent, especially among smaller or non-domestic operators.

7.4 Vulnerability of Young Users

A large portion of E-sports participants are **minors or young adults**, who may not fully understand cybersecurity risks. Children are more likely to fall for phishing scams, click on malicious links, or share personal data during gameplay or live streams.[36]

[32] Rahul Matthan, India's IT Act and the Gaming Industry: A Misfit?, 18 Nat'l L. Sch. Rev. 212, 214–15 (2023).

[33] Michael Geist, Jurisdiction and Cybercrime in a Borderless World, 8 Int'l J.L. & Info. Tech. 123, 127–28 (2021).

[34] Council of Europe, Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.

[35] CERT-In, Directions Relating to Information Security Practices, supra note 3.

[36] UNICEF, Children's Rights and Online Gaming: Privacy, Protection and Participation, https://www.unicef.org/globalinsight/reports/child-rights-and-online-gaming (last visited July 23, 2025).

This creates both a moral and legal concern. Platforms targeting minors may be subject to stricter standards, such as COPPA in the U.S., that needs parent's consent (must be verified) for collecting data from users under 13.[37] However, many platforms struggle to verify age or provide simplified privacy controls for younger users.

7.5 Inadequate Grievance Redressal Mechanisms

When users become victims of cyberattacks—such as identity theft, account hacks, or online harassment—there are few user-friendly mechanisms to seek legal or platform-based remedies.

Many E-sports companies rely on automated systems or lengthy support queues. National cybercrime portals may not be tailored to address the specific complaints arising in digital gaming environments. This leaves victims without timely support and increases the risk of continued abuse.

7.6 Lack of Industry-Wide Cybersecurity Standards

There is currently **no global code of conduct** for cybersecurity in E-sports. While some organisations, like the **Esports Integrity Commission (ESIC)**, offer guidelines, these are voluntary and mostly focus on anti-cheating and match-fixing, not data protection or platform security.[38]

Without a uniform baseline, companies apply varying levels of security depending on their size and budget. This leads to uneven protection across the industry and puts smaller players and users at greater risk.

8. RECOMMENDATIONS

To protect the future of E-sports and ensure safe participation for players, fans, and organisations, it is important to develop **strong and practical cybersecurity measures**. Based on the issues discussed earlier, this section presents legal and policy-based recommendations that can help strengthen the E-sports ecosystem.

8.1 Develop E-Sports-Specific Cybersecurity Guidelines

Current laws do not directly address the special nature of E-sports. Regulatory bodies and industry leaders should work together to create **sector-specific cybersecurity standards** for E-sports. These guidelines should cover:

- Real-time protection against DDoS attacks during tournaments,
- Minimum standards for data encryption and storage,
- Fair play systems and anti-cheat tools, and
- Incident response mechanisms tailored to gaming platforms.

Agencies like the **Esports Integrity Commission (ESIC)** and national cyber regulators (like India's CERT-In) can help develop and promote these standards in consultation with stakeholders.[39]

8.2 Encourage Legal Recognition of E-Sports

Many countries still do not legally recognise E-sports as a distinct category, often lumping it under "online games" or entertainment. Legal recognition would help in:

- Applying consistent laws on player contracts,
- Regulating cybercrimes during competitive play, and

[37] Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506 (1998).

[38] Esports Integrity Commission (ESIC), Integrity Program Overview, https://esic.gg/what-we-do/integrity-program/ (last visited July 23, 2025).

[39] Esports Integrity Commission (ESIC), Integrity Guidelines and Framework, https://esic.gg/what-we-do/integrity-program (last visited July 23, 2025).

- Developing age-appropriate content policies.

Countries like South Korea and Germany already grant E-sports formal status, which has helped enforce stricter digital safety laws in tournaments.[40]

8.3 Strengthen Cross-Border Legal Cooperation

Cyberattacks in E-sports often come from **multiple countries**, making it hard to investigate and prosecute. To solve this, countries should:

- Join and implement the **Budapest Convention on Cybercrime**,
- Sign mutual legal assistance treaties (MLATs), and
- Build regional cooperation platforms for gaming and cybersecurity law.

This would ensure better information sharing, faster extradition processes, and coordinated enforcement in cases of transnational cybercrime.[41]

8.4 Promote User Education and Digital Literacy

Young gamers, especially minors, are at high risk of phishing, scams, and online abuse. Governments and gaming companies should launch **awareness campaigns** focused on:

  - How to detect fake links or scam giveaways,
  - Reporting abuse during live streams or matches, and
- Setting strong passwords and using multi-factor authentication.

Platforms like Twitch or Steam can also add **in-game tutorials** or pop-up messages with cybersecurity tips aimed at younger users.[42]

8.5 Make Data Breach Notifications Mandatory in E-Sports

To increase transparency, countries should **require E-sports platforms to disclose cyber incidents**. This could be done by:

- Extending existing data protection laws like India's DPDP Act or the GDPR to explicitly include gaming platforms,
- Requiring companies to notify users and regulators within a fixed period, and
- Imposing fines for concealment or delay in reporting.

Mandatory breach reporting will encourage platforms to take data protection more seriously and build user trust.[43]

8.6 Create National Regulatory Bodies for E-Sports

To ensure consistent policies, countries should set up **dedicated authorities** to regulate E-sports, such as an "E-sports and Gaming Authority." These bodies can:

- License and monitor E-sports tournaments,
- Approve cybersecurity measures for major platforms,
- Investigate cheating, hacking, and match-fixing, and
- Ensure child safety in digital sports events.

[40] Byung Kwan Park, Legal Recognition of Esports in South Korea: Lessons for the World, 12 Asian J. Gaming L. 47, 49 (2022).

[41] Council of Europe, Budapest Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.

[42] UNICEF, Children's Rights and Online Gaming, https://www.unicef.org/globalinsight/reports/child-rights-and-online-gaming (last visited July 23, 2025).

[43] Digital Personal Data Protection Act, No. 22 of 2023, § 8, India Code (India); General Data Protection Regulation, Regulation (EU) 2016/679, art. 33.

Such bodies would play a key role in setting standards and enforcing accountability across the industry.[44]

8.7 Public–Private Partnerships (PPP) in Cybersecurity

Cybersecurity in E-sports needs both legal expertise and technical innovation. Governments should partner with **private tech companies**, tournament organisers, and educational institutions to:

- Share threat intelligence,
- Develop anti-hack tools and server security protocols, and
- Provide training in ethical hacking and cybersecurity law.

PPP models have been effective in financial and healthcare sectors and can be adapted for gaming as well.[45]

9. CONCLUSION

E-sports has grown from a niche hobby into a global phenomenon involving millions of players, billions in revenue, and an ever-expanding digital infrastructure. However, with this growth comes serious **cybersecurity risks**. From data breaches and denial-of-service attacks to hacking scandals and cheating software, the integrity of E-sports is constantly under threat.

This paper has shown that current laws in India, the European Union, and the United States offer **some protection** but are not fully equipped to deal with the unique challenges of the E-sports ecosystem. The **lack of E-sports-specific legislation**, combined with fast-moving technological advancements, leaves players, platforms, and regulators scrambling to respond to incidents rather than preventing them.

Moreover, the **transnational nature of cybercrime** in E-sports makes enforcement difficult. Hackers often operate from different jurisdictions, and platforms frequently span multiple countries, complicating investigations and prosecutions. At the same time, there is little legal clarity on who holds the responsibility for cybersecurity failures—developers, tournament organizers, or hosting platforms.

The solution lies in adopting a **multi-layered approach**. Legal reforms should focus on:

- **Creating E-sports-specific cybersecurity guidelines**,
- **Mandating data breach notifications**,
- **Improving international cooperation**, and
- **Educating young gamers and professionals alike**.

In parallel, the industry itself must take responsibility through self-regulation, ethical design of anti-cheat tools, and collaboration with cybersecurity experts.

Cybersecurity is no longer just a technical issue; it is a **legal necessity** in the world of competitive digital sports. To ensure the safe, fair, and sustainable growth of E-sports, stakeholders must treat cybersecurity as a core component of the game—not just an afterthought.

REFERENCE

1. **Arnav Tiwari**, Why India Needs a National E-Sports Regulator, Bar & Bench (Jan. 12, 2024), https://www.barandbench.com/columns/why-india-needs-esports-regulator.

[44] Arnav Tiwari, Why India Needs a National E-Sports Regulator, Bar & Bench (Jan. 12, 2024), https://www.barandbench.com/columns/why-india-needs-esports-regulator.

[45] Shikha Sinha, PPP in Cybersecurity: A Model for Gaming?, 9 Cyber L. Rev. 76, 78 (2023).

2. **Byung Kwan Park**, Legal Recognition of Esports in South Korea: Lessons for the World, 12 Asian J. Gaming L. 47 (2022).
3. **Council of Europe**, Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.
4. **Digital Personal Data Protection Act**, No. 22 of 2023, India Code (India).
5. **Esports Integrity Commission (ESIC)**, Integrity Guidelines and Framework, https://esic.gg/what-we-do/integrity-program (last visited July 23, 2025).
6. **European Union**, General Data Protection Regulation, Regulation (EU) 2016/679.
7. **Josh Ye**, Twitch Hack Highlights Growing Cybersecurity Risks in Esports, Reuters (Oct. 7, 2021), https://www.reuters.com/technology/twitch-hack-highlights-cybersecurity-risks-esports-2021-10-07/.
8. **Newzoo**, Global Esports Market Report 2023, https://newzoo.com/insights/trend-reports/newzoo-global-esports-market-report-2023-free-version (last visited July 20, 2025).
9. **Paul Redmond**, Data Collection and User Rights in Esports Platforms: An Emerging Concern, 22 Gaming L. Rev. 153 (2020).
10. **Shikha Sinha**, PPP in Cybersecurity: A Model for Gaming?, 9 Cyber L. Rev. 76 (2023).
11. **UNICEF**, Children's Rights and Online Gaming, https://www.unicef.org/globalinsight/reports/child-rights-and-online-gaming (last visited July 23, 2025).