RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES
Social Science Journal

A Critique on Cybercrimes Concerning Online Games and Content: Need for Comprehensive Legal Framework in India

By

Areena Parveen Ansari
Assistant Professor, Dharmashastra National Law University, Jabalpur, M.P, India
Email: apa2702@gmail.com

Abstract

Cyberspace is nothing but a web that captures and unnavigated the entrants. The germane notion is that widespread usage of technology predominantly results in abuse. The virtual world is considered to be in continual conflict with the utilization and manipulation of technology. Cybercrime is one example of the technical defect of the virtual world, where concomitantly several activities transpire in cyberspace that imposes a risk on the privacy, safety, and security of the people and the nation. Cybercrimes currently form an integral part of cyberspace although unsolicited. Numerous activities take place in cyberspace. Online Gaming is one imperative aspect of the same. The contemporary age developers diurnally introduce novel and enhanced games, aiming at different strata of society. In addition, online gaming is estimated to be flourishing further with the advancement of technology. Enhanced products and services (licensed or non-licensed) are luring people to a greater extent, compelling them to avail themselves of so-called pristine technologies, resultantly posing a worldwide threat to the privacy and security of the user's personal information and the relevant confidential data. Furthermore, the application of Artificial Intelligence in online gaming entails additional challenges by providing actual/second life experience in the virtual world. The menace is not limited to privacy infringement but is sometimes used as a tool to induce crimes such as Gambling, Cyberstalking, and Circulation of illicit content, to name a few. Cybercrime in online games encompasses a whole new challenge to the existing inadequacies primarily in terms of security and privacy issue in cyberspace. In such a scenario and the prospects require a stringent approach to be adopted by the legislatures to eliminate and control malpractices and crimes prevailing in the virtual world. On this note, the existing Indian legislative framework is considered to be non-comprehensive and incompetent for the digital age. Therefore, there is a need to have a more comprehensive approach to regulate online platforms. The present work is an attempt to discuss the overall phenomenon of cybercrime regarding online games with the help of suitable facts and figures. Additionally, the paper will explore the cogency of the regulatory framework in India based on existing and proposed laws.

Keywords- Online Gaming, Cyberspace, Artificial Intelligence and Online Games, Cybercrime, Censorship of Games, and Gaming Laws in India.

Introduction

With the advancement of technology and the economy, the internet has played a significant role in our lives. Although, it has brought substantial convenience in the history of humankind yet it has generated some perennial issues in the virtual world. There is hardly any disagreement that cybercrime cases are increasing by leaps and bounds in the world. Technology has transformed the entire world into a global hamlet by generating what you called Cyberspace. It is the generic heritage of humankind, however, regrettably, the mass has

tainted the same. Consequentially, cyberspace has emerged as a new-fangled frontier of diverse forms of crimes.

Cyberspace facilitates farfetched experiences for the game operator, it possesses the tendency of turning the imaginary experience into reality and vice-versa, thus, online platforms are flourishing more than ever. There was a time when online games were the only source of entertainment, now, it encompasses other facets as well, namely, education, circulation of information, money, data transmission, storage, and so on. Needless to say, that virtual world has brought way more complications to the existing problem of the real world. With the amplifying digitalization, numerous products and services are being introduced diurnally to prosperous the business and strengthen the financial position in the global market. The gaming industry emerged as a boon owing to the Covid-19 pandemic, amidst the disruption and cessation, it had widened the scope of producing and providing education, and financial sources globally to all kinds of users.

Statement of the Problem

Owing to the connectivity with all age groups and global networking, the gaming business since its inception has been constantly popular, it is thriving with time by giving interactive and intellectually rich experiences.[1] Employing the law in the technology and administering the same overseas is laborious for any country. Pointedly, the laws and norms of the countries immensely depend on Social, Political, and Economic construction. Striding law with technology and innovation is a challenge that the country cannot master. To enact the laws are one thing and their enforcement is another thing. Fundamentally, the online platform intermediaries, creators, developers, designers, and gamers all are bound by the laws of the country in which the game was created and accessed. Quite a few platforms exist that comply with standard regulations of the countries and the rest dodge the legal obligations. The creators of the game are required to mandatorily acquire the authorised license and are subjected to the terms of use and conditions, for which the license has been issued. Likewise, the users ought to follow the conditions prescribed as the "term of use" and heedfully read the "privacy clause". It is the duty of the creator and gamer both to cautiously protect and handle the security details from the third-party intruder.

The growth of the gaming industry is entirely dependent on technologies and innovations. One such example of the same is a widely prevalent application of Artificial Intelligence (hereinafter AI). The problem exists in the unconventional and interactive instinct of Artificial Intelligence that has heightened the gaming experience and is quite supportive in generating gross revenue. The excessive usage of AI and its role in the metaverse is intensifying leading to uncontrollable and unregulated online activities. "The online gaming industry is booming. This ever-growing ecosystem consists of numerous entities, including gamers, streamers, tournament platform hosts, developers, and, of course, cheats who try to obtain an unfair advantage and illegal profits."[2]

In India, cybercrimes in online games are destructively and significantly increasing. As per the Research conducted by Akamai Technologies Inc. in the year 2019, India is

[1] BOAVENTURA DACOSTA, & SOONHWA SEOK, "CYBERCRIME IN ONLINE GAMING" (2020) HTTPS://WWW.IGI-GLOBAL.COM/VIEWTITLESAMPLE.ASPX?ID=248090&PTID=223181&T=CYBERCRIME+IN+ONLINE+GAMING ACCESSED JANUARY 05, 2023.
[2] Kaspersky, "Game Security" (2019) https://go.kaspersky.com/rs/802-IJN-240/images/Kaspersky_Game_Security_brochure_web.pdf accessed January 12. 2023.

meticulously active in cybercrimes being targeted as and being the source country, refer to the figure below[3].

Top 10 Target Countries
November 2017 - March 2019

COUNTRY	TOTAL ATTACKS	GLOBAL RANK
United States	2,666,156,401	01
United Kingdom	210,109,563	02
Germany	135,061,575	03
Brazil	118,418,554	04
India	113,280,600	05
Japan	95,550,352	06
Canada	84,443,615	07
Australia	54,187,181	08
Italy	47,784,870	09
Netherlands	47,390,611	10

Top 10 Source Countries - All Verticals
November 2017 - March 2019

COUNTRY	TOTAL ATTACKS	GLOBAL RANK
United States	967,577,579	01
Russia	608,655,963	02
Netherlands	280,775,553	03
China	218,015,784	04
Brazil	155,603,585	05
Ukraine	154,887,375	06
India	142,621,086	07
France	121,691,941	08
Germany	113,233,187	09
United Kindom	102,531,816	10

Additionally, due to the COVID-19 and government initiative of Digital India, India has witnessed an upsurge in digital platforms especially dealing with Cryptocurrencies, Non-Fungible tokens, and online games, all of these subsidized cyber security and threats. In the past two years, several new agencies reported cases of cyberbullying, privacy breaches, fraud, and other threats that are increasing quite often in India.[4]

Rational of the Study and Approach Adopted/ Research Direction

The ubiquity of cybercrime in cyberspace has become an expected phenomenon that poses a worldwide challenge to the security, and privacy of individuals and the country. In some cases, online audio/video games are being designed, developed, and distributed in a fashion that endorses, gambling, obscenity, money laundering, violence, suicide, etc. directly

[3] Akamai Research, "*State of the Internet/Security Web Attacks and Gaming Abuse Report*" (2019), Volume 5, Issue 3 https://www.akamai.com/site/en/documents/state-of-the-internet/soti-security-web-attacks-and-gaming-abuse-report-2019.pdf accessed February 26, 2023.

[4] See, for reference,
"RISING CASES OF CYBERBULLYING, DATA PRIVACY AND OTHER THREATS IN ONLINE GAMING: REPORT" BUSINESS INSIDER, (2022), HTTPS://WWW.BUSINESSINSIDER.IN/ADVERTISING/AD-TECH/ARTICLE/RISING-CASES-OF-CYBERBULLYING-DATA-PRIVACY-AND-OTHER-THREATS-IN-ONLINE-GAMING-REPORT/ARTICLESHOW/89611643.CMS#:~:TEXT=ACCORDING%20TO%20THE%20NORTON%20CYBER,A%20CYBERATTACK%20AT%20SOME%20POINT ACCESSED JANUARY 14, 2023.
"ED RAID: KOLKATA BUSINESSMAN IN MOBILE GAMING APP FRAUD CASE GOES UNTRACEABLE" LIVE MINT (2022). HTTPS://WWW.LIVEMINT.COM/NEWS/ED-RAID-KOLKATA-BUSINESSMAN-IN-MOBILE-GAMING-APP-FRAUD-CASE-GOES-UNTRACEABLE-11662884717869.HTML ACCESSED JANUARY 14, 2023.
"WOMAN FILES CYBER FRAUD CASE AFTER SON BUYS 'WEAPONS' WORTH LAKHS FOR ONLINE GAME" INDIA TV, CHHATTISGARH (2021), HTTPS://WWW.INDIATVNEWS.COM/CRIME/12-YEAR-OLD-BUYS-WEAPONS-WORTH-LAKHS-ONLINE-BATTLE-GAME-CHHATTISGARH-KANKER-715468 ACCESSED JANUARY 14, 2023.
"75% OF INDIAN GAMERS HAVE EXPERIENCED CYBERATTACK: SURVEY" BUSINESS LINES, (2021) HTTPS://WWW.THEHINDUBUSINESSLINE.COM/NEWS/VARIETY/75-OF-INDIAN-GAMERS-HAVE-EXPERIENCED-CYBERATTACK-SURVEY/ARTICLE37516843.ECE ACCESSED JANUARY 14, 2023.
"GAMERS IN INDIA ARE LOSING THOUSANDS OF RUPEES DUE TO CYBER ATTACKS" INDIA TODAY, (2021) HTTPS://WWW.INDIATODAY.IN/TECHNOLOGY/FEATURES/STORY/GAMERS-IN-INDIA-ARE-LOSING-THOUSANDS-OF-RUPEES-DUE-TO-CYBER-ATTACKS-1877183-2021-11-16 ACCESSED JANUARY 14, 2023.

or in disguise. At times, the companies themselves commit the crime and at times it becomes the victim of cybercrime.[5] The byzantine cyber trajectory is a challenge in itself, whereas regulating the cybercrime associated with online games and their content exacerbates the prevailing problems. Thus, for administration and to further combat cybercrime, laws play a pivotal role. The regulation of the platforms, sources, and content censorship is a requirement of the present digital arena.

The motivation behind the research is to examine the problems of the digital age whilst evaluating the existing laws, hypothesising, that the non-comprehensive and facile laws are the root cause of cybercrime in online games. The study also reproaches and identifies the core issues involved in the content of online gaming. Consequently, appraising the present and the proposed legal framework is appropriate for Digital India or not?

Review of the existing studies

Cybercrimes concerning Online Games

The term Cybercrime is indeterminate. The scholars and academicians attempted to describe the term as per their respective studies and research, however, the definitions lack a universal application.[6] Further, the term has not been postulated by the legislatures in any of the statutes. Nevertheless, the term commonly understood as unlawful activity occurs in Cyberspace.[7] These unlawful activities are not limited to cyber security threats, information or data infringement, or licensing issues but the laws are violated through the delivery of the content, data theft, fraud, and so on. Needless to mention, Audio/Video Games are easily accessible and downloadable either freely or with subscription fees or pirated versions are also prevalent around the globe. Quotidian, technology giants are introducing novel gadgets/devices, enhanced features, added capacity, etc, all these factors, directly and indirectly, influence the online gaming industry. To provide a rich experience, to beat the competitors, and most importantly to boost their position in the market, the developers and designers are compromising the quality of the content, security of the data, norms of the society, and primarily the laws of the state. For example, though Some states in India prohibit games involving money and some allow the same subject to the condition precedent and subsequent under the state laws[8] but due to duped applications and pirated online games these proscribed digital games are accessible. Substantially, due to the intricacies involved in cyberspace, identification of all kinds of illegal software, platform, or owner is nearly impossible. Ironically, the abundant digital database lacks in providing information concerning imposters, pirated software developers, and distributors in the digital market are restricted, insufficient, and lack transparency. Thus, it is challenging for the regulators to detect, recognize and monitor the pirated channels and persons involved.[9] Wipro in its paper Game on the need for Cybersecurity in gaming has detected the Cyber threats in Gaming as follows-[10]

---

[5] Ibid.

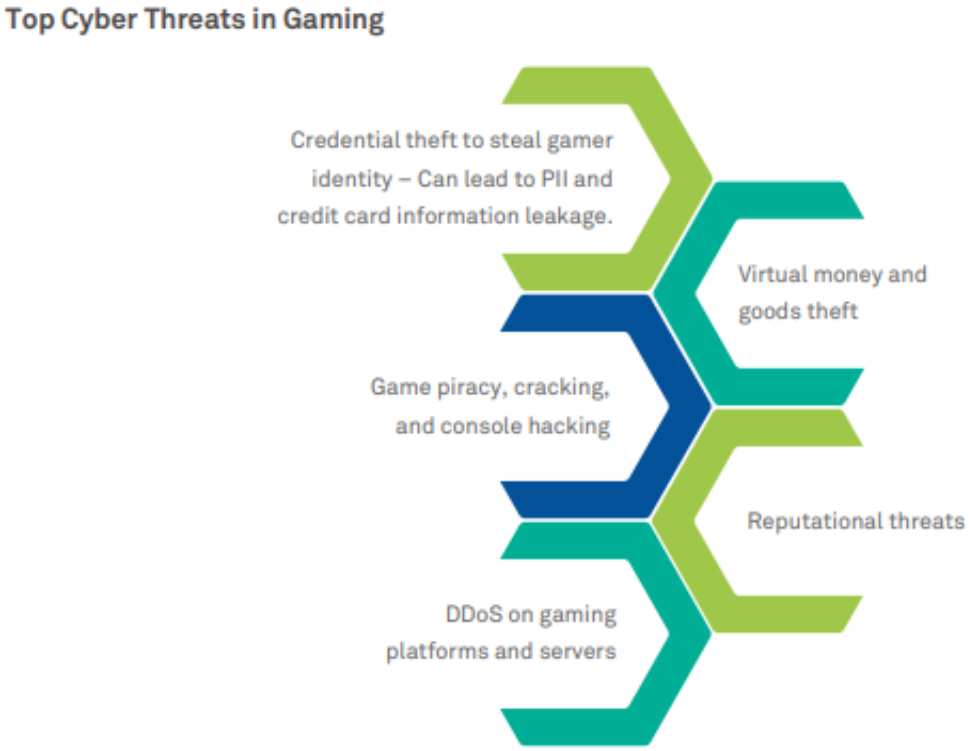
[6] Robert, Ebi, "Attempting a Definition of Cyber Crime" (SSRN, 2021) https://ssrn.com/abstract=3830589 or http://dx.doi.org/10.2139/ssrn.3830589 accessed January 08, 2023.

[7] Prof. R.K.Chaubey, "An Introduction to Cyber Crime and Cyber law", (Kamal Law House, 2012) https://www.bbau.ac.in/dept/Law/TM/1.pdf accessed January 08, 2023.

[8] POOJA TIDKE AND MALLIKA NOORANI, "STATE OF PLAY: ONLINE GAMING AND ANTI-GAMBLING LAWS IN INDIA" (MONDAQ, 2022). HTTPS://WWW.MONDAQ.COM/INDIA/GAMING/1198906/STATE-OF-PLAY-ONLINE-GAMING-AND-ANTI-GAMBLING-LAWS-IN-INDIA ACCESSED JANUARY 08, 2023.

[9] Shri Krishnan, Naren Natarajan, Vaddadi Karthik, "A Study on Purchase/Download Intentions towards Pirated Games" (2019), Vol. 8, Issue 8 International Journal of Innovative Research in Science, Engineering and Technology http://www.ijirset.com/upload/2019/august/8_1_A_Study.PDF accessed January 10, 2023.

[10] Harshwardhan Kamdi, "Game on: the need for Cybersecurity in gaming" (Wipro Limited 2020) https://www.wipro.com/content/dam/nexus/en/industries/platforms-and-software-products/latest-thinking/game-on-the-need-for-cybersecurity-in-gaming.pdf accessed February 28, 2023.



Artificial Intelligence (AI) and Cybercrime

The gaming industry is revolutionizing with technological advancement, the application of Artificial Intelligence into online gaming is giving experiences like never before, the personalized interaction, real-time involvement, and novel content all these are luring people, especially Gen Z. The AI is delivering services in all spheres, be it gameplay, pathfinding, design, realism or the interactivity of Avatar.[11] AI understands no boundaries, it is now prevalent almost everywhere and prospectively it seems to grow more. However, it appears that the more AI fostering, the more technical issues are rising resulting in heightened technical, ethical, and regulatory problems.[12]

Online Platforms and Cybercrime

Digital Media platforms facilitate numerous kinds of online games for all age groups specifically targeting children and adolescents. At times, the game developers and designers are found to be tangled in creating and endorsing several illegitimate games linked with Gambling, Pornography, Data Theft, Libel, Cyberbullying, etc.

A United Nations study on Cybercrime deliberated upon-

"In 2008, 26 individuals – including reputed mafia organized crime family members – were indicted on charges of operating a sophisticated illegal gambling enterprise, including four gambling websites in a country in Central America. The District Attorney commented that 'law enforcement crackdowns over the years on traditional mob-run wire rooms have led to an increased use by illegal gambling rings of offshore gambling websites where action is available

[11] **Ranga Jagannath, "**Revolutionizing the Gaming Industry with Artificial Intelligence", (Express Computer 2022) https://www.expresscomputer.in/guest-blogs/revolutionizing-the-gaming-industry-with-artificial-intelligence/91886/ accessed January 11, 2023.

[12] Qing Huang, Driving Artificial Intelligence Use in Responsible Gambling Practices, (2020), University of Nevada, Las Vegas. https://www.unlv.edu/sites/default/files/page_files/27/huang-report_drivingAI-responsible.pdf accessed January 11, 2023.

around the clock.' While gambling was illegal in the prosecuting jurisdiction, the websites took advantage of different legislation in other jurisdictions. Bets were placed in the country but processed offshore and the data 'bounced' through a series of server nodes to evade traditional law enforcement detection methods."[13]

A study on cybercrime and criminals conducted by Dr. Mike McGuire,

"Research into online gaming laundering in 2013 (Richet 2013) found a variety of sites offering information on how to launder money through 99 gaming currencies. Especially common was the role of MMORPGs (massively multiplayer online role-playing games) like Minecraft, which allow players to interact across differing jurisdictions and to exchange currencies with limited international controls. Data was gathered from a number of forums where advice was freely offered on how to do this."[14]

As discussed earlier in this article that the regulatory framework of the country differs in several aspects, in such a situation, cybercriminals take advantage of permissible and licensed games and publicized them in another state where it is prohibited. Resultantly, the illegitimate business of money transmission originates. In absence of a proper record or record-keeping mechanisms and the location of the cybercriminal are hard to track down and, in most cases, unidentifiable to enforce the regulations. From time to time, the game developers collaborate with other websites and applications on digital platforms to promote the games, whereas inappropriate games are casually displayed and promoted by employing advertisements skippable and non-skippable in certain cases. These unlicensed game developers, programmers, and designers are involved in the activities like capturing the user's data, selling the data in the market, or promoting their product or services outside the permissible limits, etc.[15]

Cybercrime concerning Contents of the Games and the Need for Censorship

It is a well-established notion that the commercialisation of product and services, cut-throat competition, and greed for excessive economic gain often leads to unethical and immoral practices. Consequently, the content of the game and censorship of inappropriate content plays an imperative role. Essentially, the primary concern is to review and legalize the content prior to and post-formation in the market. Vigilance is a must to check the violation and compliance of the Central and State Laws globally.

At present, there exist several online games that contain inappropriate content and information which could be used to commit cybercrime. In one instance "a 14-year-old boy from Austria downloaded bomb-making plans onto his PlayStation games console"[16]. Further, it exposes the user to Obscenity and Pornography, it has now become a common phenomenon that game developers are creating and designing games that endorses nudity, and obscenity in

[13] United Nations Office on Drugs and Crime, "Comprehensive Study on Cybercrime" (United Nations, 2013), https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf accessed January 12, 2022.
[14] Dr. Mike McGuire, "Into the Web of Profit" (Bromium, Inc., 2018) https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf accessed January 12, 2023.
[15] Marco Gercke, "Understanding Cybercrime: Phenomena, Challenges and Legal Response" (2012) Infrastructure Enabling Environment and E-Application Department, ITU Telecommunication Development Bureau. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf accessed January 10, 2023.
[16] Reuters Staff, "Teenager in Austrian 'Playstation' terrorism case gets two years" (2015) https://www.reuters.com/article/us-mideast-crisis-austria-idUSKBN0OB0LK20150526 accessed January 12, 2023.

disguise and corrupt young minds.[17] The content, at times, entails religious, racist remarks,[18] and offence relating to Libel for example, by way of slanderous/libellous messages. Through social networking sites, dishonest and defamatory information is being provided and circulated. The sources are anonymous or pseudonymous with cannot be verified or identified.[19]

Further, offences concerning Copyright, Trademark, and other computer-related cyber offences that induce violence, fraud, cyberbullying, stalking, suicide, etc.[20] are stirring because of the influence that the contents of the game created in the mind of the user. The amount of time one spent on certain activities surely is reflected in our behaviours, for example playing violent video games, the content of the game leaves an impact on the psychology, physically and sexually. The Blue Whale Challenge, Warcraft, and Neknominate, these games are classic examples of such phenomena among many.[21][22] Thus, to safeguard the interest of all the stakeholders, especially the end users censorship of the games is required.

Players and Cybercrimes

Sometimes, the players themselves are offenders. They create an account individually or in a troupe to intimidate or incite other players, especially in multiplayer games. The disruptive behaviour of the players renders the online gaming environment toxic. These include but are not limited to, offensive name-calling or comment, threats, virtual violence, bullying, etc.[23] Lately, gun violence, cyberbullying, stalking, physical threats, and harassment issues are quite fecund[24], the toxic content of the metaverse even includes virtual sexual assault.[25][26] In absence of a watchdog and impediment to the virtual world, the players are free to accomplish illegal activities without the attainment of any kind of punishment for their criminal acts. For example-

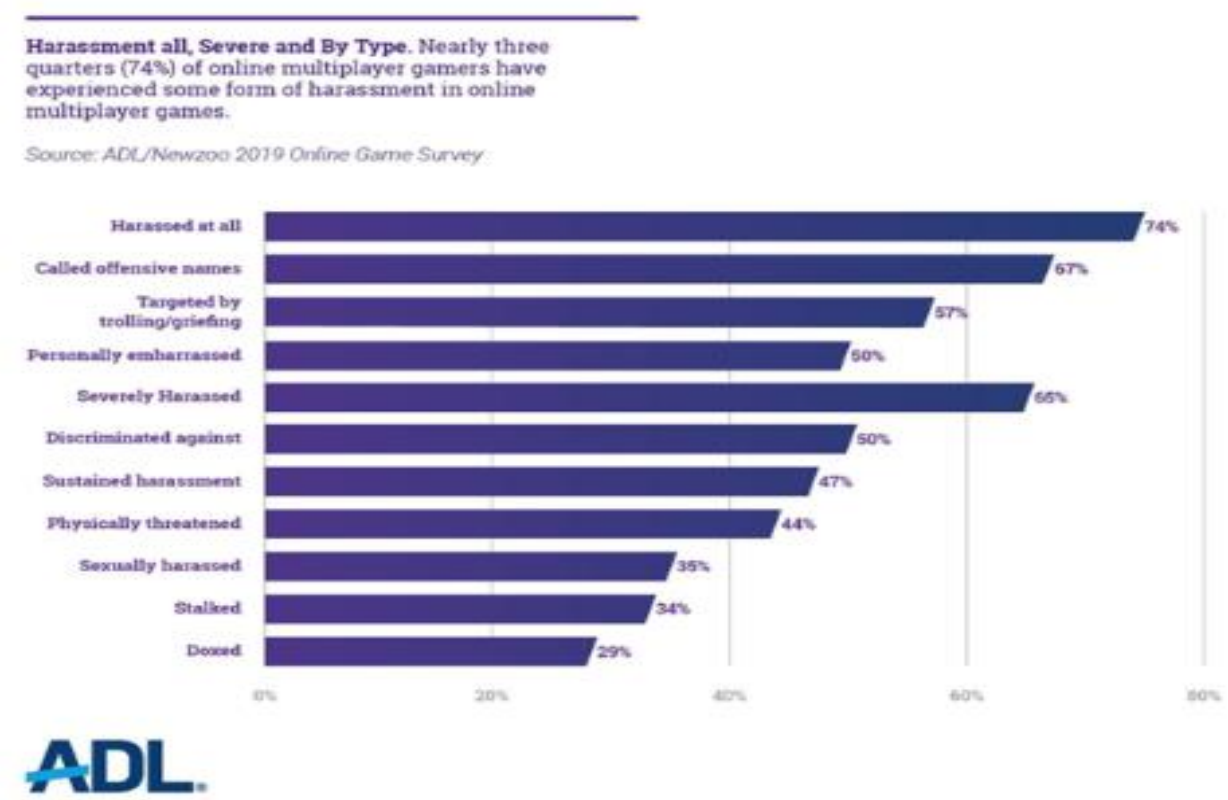
"The term "virtual mugging" was coined when some players of Lineage II used software applications that run over the web, called bots, to defeat other player's characters and take their items. Japanese police arrested a foreign exchange student in August 2005 following the reports of virtual mugging and the online sale of the stolen items. The number of game players who have experienced some manner of virtual crime is already large. South Korea, a

[17] See, for example,
"Cybercriminals Using Online Gaming To Target Kids" The Economic Times (2021) https://telecom.economictimes.indiatimes.com/news/cybercriminals-using-online-gaming-to-target-kids/81869543 accessed January 10, 2023.
"Crime Among City Youths Due To Online Gaming A Concern: Cops" The Times of India (2021) http://timesofindia.indiatimes.com/articleshow/81728208.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst accessed January 10, 2023.
[18] Kirsty Phillips 1, Julia C. Davidson, and Ors, "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies" (Forensic Science, 2022) https://www.mdpi.com/2673-6756/2/2/28 accessed February 26, 2023.
[19] Supra n 7.
[20] Ibid.
[21] Harikumar Pallathadka, "Censorship on Video Games: Timepass or Mania?" (2020) European Journal of Molecular & Clinical Medicine, Volume 07, Issue 06, https://ejmcm.com/article_15312_2ae5083cf38e4e6554cc6a32d01af40f.pdf accessed January 10, 2023.
[22] Ce Dr Sumanta Bhattacharya, "With Advancement in Technology and Increasing Cyber Space Industry, What Has Been the Impact on the Young Mind" (2021), International Journal of Innovative Research in Science, Engineering and Technology Volume 10, Issue 11 http://www.ijirset.com/upload/2021/november/75_With_NC.pdf accessed January 09, 2023.
[23] ADL Report, "Hate Is No Game Hate and Harassment in Online Games" (ADL, 2022) Center for Technology & Society, https://www.adl.org/sites/default/files/documents/2022-12/Hate-and-Harassment-in-Online-Games-120622-v2.pdf accessed January 12, 2023.
[24] Supra at 16, 17.
[25] SumOfUs: "Metaverse: Another Cesspool of Toxic Content" (SumOfU Research, May 2022), https://www.sumofus.org/images/Metaverse_report_May_2022.pdf accessed January 11, 2023.
[26] See for reference:
C KRISHNASAI, "21-YEAR-OLD WOMAN VIRTUALLY RAPED, HARASSED IN METAVERSE: REPORT" WION NEWS (2022) HTTPS://WWW.WIONEWS.COM/WORLD/21-YEAR-OLD-WOMAN-VIRTUALLY-RAPED-HARASSED-IN-METAVERSE-REPORT-483043 ACCESSED JANUARY 11, 2023.

country with many active gamers, had over 22,000 reported cases of various types of virtual crime involving games in 2003."[27]

"In the game "The Sims Online," an MMO, a "cyber-brothel" was developed by a 17-year-old boy using the game alias "Evangeline."4 Customers paid sim-money ("Simoleans") for cybersex by the minute. His account was canceled, but no legal action was taken."[28]

The research conducted by Anti-Defamation League in the year 2019 conducted a survey that discusses the Hate Harassment issue and its impact. The figure below reflects the diverse means of harassment[29]



National Cyber Crime Research & Innovation Centre on Cyber Harassment Cases discusses the techniques Cyber harassment amongst quite prevalent is the Swatting-

"Swatting refers to a harassment technique most often perpetrated by members of the online gaming community. Online gamers make a hoax call, wherein they dial authorities and give them some false information diverting the police and emergency service response team to another person's address."[30]

Cybercrime by Third-Party Intruder

Cybercrime in online games by a third party is where the breach of cyber security is pitched by the third party either on the creator or on the user or in some cases both.

[27] Supra n 13.
[28] Ibid.
[29] ADL Report, Free to Play? Hate, Harassment, and Positive Social Experiences in Online Games, (ADL, 2019) Center for Technology & Society, ADL https://www.adl.org/sites/default/files/pdfs/2022-12/Free%20to%20Play%2007242019.pdf accessed January 12, 2023.
[30] National Cyber Crime Research & Innovation Centre, "Investigative workflow Manual On Cyber Harassment Cases" (Bureau of Police Research & Development 2021) https://bprd.nic.in/WriteReadData/Orders/BPRD%20Cyber%20harassment%20cases%206-3-21.pdf accessed February 28 2023.

Fundamentally, virtual data tampering is the root cause of the problems by way of creating falsified virtual goods or data[31]. Third-party intruders expose the operators to numerous risks, in the form of viruses and worms or compromise to the server, through insecure Game Coding, Hacking, Privacy infringement, and other various means that poses a Cyber threat to the computer and network[32] Cyber criminals take advantage of the poor protection of the data by the creator and the end user. Furthermore, cybercriminals often look out for the vulnerability of the computer system and through several means and measures, they conclude criminal activities[33] like fraud, money laundering, data or identity theft, credential stuffing, etc. affect all the stakeholders[34]

Eric J. Hayes, Playing it Safe: Avoiding Online Gaming Risks, US-CERT

"In South Korea, more than a thousand gamers had their identities compromised through a fantasy game called "Lineage." Game accounts were created in their name without their knowledge."[35]

Trend Micro Forward-Looking Threat Research (FTR) Team,

"Competitive aspect between gamers is what fuels cybercriminals to sell online gaming currency. Though competition is considered one of the many factors in the proliferation of online gaming currency markets, a game's popularity is also something cybercriminals consider when it comes to picking what gaming currencies to sell in their websites. For instance, the game World of Warcraft has around 5.5 million paying players in 2015, thus becoming a huge target of cybercriminals."[36]

Indian Cyber Institute,

"It was reported that fake versions of online games (including Temple Run, Free Flow and Hill Climb Race) that are popular and have huge number of downloads were uploaded on play stores as free downloads. Innocent people not able to distinguish between the real and the fake versions, downloaded the fake version and ended up in giving entire personal data that resided on their devices and a hacker can also infect the devices with malwares and thereby causing financial losses and also commit identity theft."[37]

Akamai Research, State of the Internet/Security Web Attacks and Gaming Abuse Report

"Criminals target popular games like Fortnite and Counter-Strike: Global Offensive (CS: GO), looking for valid accounts and unique skins. Once a player's account is successfully compromised, it can then be traded or sold."[38]

---

[31] Chen Zhao, "Cyber Security Issues in Online Games" (AIP Publishing, 2018) https://aip.scitation.org/doi/pdf/10.1063/1.5033679 accessed January 08, 2023.
[32] Eric J. Hayes, "Playing it Safe: Avoiding Online Gaming Risks," (US-CERT, 2006) https://www.cisa.gov/uscert/sites/default/files/publications/gaming.pdf accessed January 10, 2023.
[33] Supra n 1.
[34] Akamai Research, "*State of the Internet/Security Web Attacks and Gaming Abuse Report*" (2019), Volume 5, Issue 3 https://www.akamai.com/site/en/documents/state-of-the-internet/soti-security-web-attacks-and-gaming-abuse-report-2019.pdf accessed January 11, 2023.
[35] Supra n 13, 19 and 20.
[36] A Trend Labs Research Paper, "The Cybercriminal Roots of Selling Online Gaming Currency, Trend Micro Forward-Looking Threat Research" (2016). https://documents.trendmicro.com/assets/wp/wp-cybercrime-online-gaming-currency.pdf accessed January 12, 2023.
[37] Dr Ananth Prabhu G, "Cyber Safe Girl" (Indian Cyber Institute, 2018), https://police.py.gov.in/Cyber%20Awareness%20-%20Cyber%20Safe%20Girl%20v2.0.pdf accessed January 12, 2022.
[38] Supra n 25.

Challenges: Overall

Virtual game economics encircle the development and expansion of digital assets. Consequently, digital media indulges in cut-throat competition to gain a highly lucrative economic position in the national and international markets. A substantial transformation has occurred in the gaming industry since 2010 and there onwards novel innovative equipment, products, and services deepened the market rendering it to be prone to cybercrime. Direct or indirect criminal threats in cyberspace by game developers, designers, publishers, and gamers pose a serious challenge to the government. All operators and users are subjected to abide by international law and domestic laws, policies, and practices. The jurisdictional issues[39] are grim in a scenario where the originated sources are unknown to apply the crucial laws of the country and the national approaches towards cybercrimes. However, there exist few international forums that endeavour to facilitate the dais to ensure technology-oriented, market-friendly legal practices.

Speaking of International discourses, there exist guidelines for online games to serve human rights, it was developed by the Council of Europe for the member states[40] these guidelines deliberate upon the virtual world, its activities, and the associated factors to draw attention toward the dissemination of information, the guidelines did not make applicable to the online casino or bookmaking websites. Other than this, International Masters of Gaming Law, founded in 2000 is a not-for-profit association of "gaming attorneys, regulators, educators, executives and consultants from around the world who are dedicated to education and the exchange of professional information and advice"[41] and the International Association of Gaming Regulation was established in the year 2011, which "provides a forum for gaming regulators from around the world to meet, learn best practice techniques and strategies, network, and exchange views, share information and discuss legislation, policies, and procedures".[42]

Nonetheless, international bodies and organisations are yet to formalise the consensus and encapsulate the cybercrimes and related offences worldwide, to control and regulate.

Legal Analyses of Indian Laws

The foremost legislation in India concerning Gaming is the Public Gambling Act, which was enacted in the year 1867, the act provides for the punishment of public gambling and probability except for the lotteries. It is Central legislation.[43] Subsequently, post-independence states have enacted their laws.[44] The Constitution of India empowers the State Government (as subjected under the State list), to enact laws on the regulation of gambling, betting, and Lottery.[45] Thus, each state possesses the legislative competence exclusively to ratify laws within the state.[46] Additionally, through the judicial interpretations, the terms "Game of Skill"

[39] Andrew Montgomery, "Online Gaming: Prohibition vs. Regulation" (University of Nevada, Las Vegas 2010), https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=1656&context=thesesdissertations accessed February 2023.
[40] Council of Europe, "Human Rights Guidelines for Online Games Providers*" (*Developed by the Council of Europe in co-operation with the Interactive Software Federation of Europe 2008). https://rm.coe.int/16805a39d3 accessed February 26, 2023.
[41] International Masters of Gaming Law, https://www.imgl.org/ accessed February 26, 2023.
[42] The International Association of Gaming Regulators, https://iagr.org/about-iagr/partners/ accessed February 26, 2023.
[43] The Public Gambling Act, 1867.
[44] Some of the State laws that are enacted pertaining to gambling and betting activities are West Bengal Gambling and Prize Competition Act, 1957, Bombay Prevention of Gambling Act, 1887, Punjab Public Gambling Act, 1961, Kerala Gambling Act, 1960, Goa, Daman and Diu Public Gambling Act, 1976, Sikkim Regulation of Gambling (Amendment) Act, 2005 etc.
[45] See, Lotteries (Regulation) Act, 1998, Lotteries (Regulation) Rules, 2010 and Section 294 A of the Indian Penal Code, 1860 (IPC), Lotteries ban except non-profit lotteries by the States of Andhra Pradesh, Gujarat, Karnataka, Maharashtra, etc) and complete ban by the State of Bihar, through the Bihar Ban on Lottery Act, 1993.
[46] The Constitution of India, 1949.

and "Game of Chance" was established, which even today is not settled.[47] The notion elucidates that betting/gambling reflecting a game of chance is verboten and the "Game of Skill" is an exception.

The legal framework for online games started with the State of Sikkim. The state introduced the Sikkim Online Gaming (Regulation) Act, of 2008, and the Sikkim Online Gaming (Regulation) Amendments Act, of 2009. To take administrative control over the online games and to generate government revenue, the state regulates the online games by providing licenses to the games.[48] Another regulation was enacted by the state of Nagaland as the Nagaland Prohibition of Gambling and Promotion and Regulation of Online Games of Skill Act, 2016, the act provides license to be obtained under the act for the purpose of wagering and betting on online games. The act explicitly emphasized the term "Games of Skill" (Section 2 (3)) to be promoted in online games in any territory in India in which the "Games of Skill" is permitted (Section 2 (2)).[49] The State of Meghalaya shares the same regulatory model of governance.[50]

In addition to this, the Telangana government has passed the Telangana Gaming (Amendment) Act, 2017 to further amend the Telangana Gaming Act, 1974, the act has incorporated provisions for prohibiting online gaming the objective was to eradicate the menace of gambling, its addiction, and threat.[51] However, the amendment was challenged and the matter is sub judice.[52] Similarly, the challenged Andhra Pradesh Gaming (Amendment) Ordinance 2020 is pending with the High Court.[53] Subsequently, in the year 2021, the state of Tamil Nadu intended to amend the law[54] to prohibit all forms of online gaming, and the same was struck down by the High Court of Tamil Nadu.[55] Recently, the government has promulgated the Tamil Nadu Prohibition of Online Gambling and Regulation of Online Games Ordinance, 2022. Though it is not yet notified.[56] Furthermore, the State of Karnataka, through the Karnataka Police (Amendment) Act, 2021 has banned online games and the High Court of Karnataka struck down contentious provisions and allowed online gaming activities.[57]

Similarly, there also exists other regulation that directly or indirectly deals with diverse aspects of online gaming like content, crimes concerning fraud, obscenity, copyright infringement, and advertisement, etc.[58] Amongst all, the most prominent for the purpose of

---

[47] For example, see, *The State of Bombay v. R. M. D. Chamarbaugwala* 1957 AIR 699, *State of Andhra Pradesh v K Satyanarayana* 1968 AIR 825, *Mahalakshmi Cultural Association v. The Director, Inspector General of Police and Ors* Special Leave to Appeal (C) No(s).15371/2012 (Arising out of impugned final judgment and order dated 22/03/2012 in WA No. 2287/2011 passed by the High Court of Madras). *Dr. K.R. Lakshmanan v State Of Tamil Nadu And Anr*. 1996 AIR 1153, *Dominance Games Private Limited v. the State of Gujarat and Others* (2018)1GLR801 etc.

[48] *Sikkim Government, Directorate of State Lotteries. https://sikkim.gov.in/department/departmentmenudetails?url=Menu%3Dfinance-revenue-expenditure-department%2Fdirectorate-of-state-lotteries accessed January 12, 2023.*

[49] Nagaland Prohibition of Gambling and Promotion and Regulation of Online Games of Skill Act, 2015.

[50] Meghalaya Regulation of Gaming Act, 2021.

[51] The Telangana Gaming (Amendment) Act, 2017.

[52] W.P.(MD)No.15231 of 2020 https://www.livelaw.in/pdf_upload/pdf_upload-384181.pdf accessed January 12, 2023.

[53] The Tamil Nadu Prohibition of Online Gambling and Regulation of Online Games Ordinance, 2022. https://prsindia.org/bills/states/the-tamil-nadu-prohibition-of-online-gambling-and-regulation-of-online-games-ordinance-2022#:~:text=when%20played%20online.-,The%20Tamil%20Nadu%20Prohibition%20of%20Online%20Gambling%20and%20Regulation%20of,of%20chance%20played%20for%20stakes accessed January 13, 2023.

[54] *Tamil Nadu Prohibition of Online Gambling and Regulation of Online Games Act, 2022.*

[55] See for reference, *Junglee Games India Pvt. Ltd. & Anr. v. The State of Tamil Nadu & Ors* W.P.Nos.18022, 18029 available at: https://www.livelaw.in/.

[45] Supra n 44.

[57] *All India Gaming Federation v. State of Karnataka*, WP 18703/2021: 2022. https://www.livelaw.in/pdf_upload/all-india-gaming-federation-v-state-of-karnataka-409739.pdf accessed January 13, 2023.

[58] The Lotteries (Regulation) Act, 1998, Indian Penal Code, 1860, Prize Competitions Act, 1955, Foreign Exchange Management Act, 1999, Payment and Settlement Systems Act, 2007, The Prevention of Money Laundering Act, The Young Person's (Harmful Publications) Act, 1956, The Indecent Representation of Women (Prohibition) Act, 1986, Cigarettes & Other Tobacco Products (Prohibition of Advertisement Regulation of Trade & Commerce, Production, Supply & Distribution) Act, 2003, Copyright Act 1957, the Trade Marks Act 1999, Telecom Commercial Communications Customer Preference Regulations, 2010, The Cable Television Network Rules, 1994, Income Tax Act, 1961,

regulations are the provisions for standard forms of contracts, Click, Shrink, and Web Wrap Contracts under the Indian Contract Act, 1872, the Information Technology Act, 2000 (IT Act) which provides provisions concerning civil liability and criminal penalty for specific proscribe activities under the act, related to computer and computer network. Recently, The Information Technology (Intermediaries Guidelines) Rules, 2021 has unified the liability of the intermediaries and mandated the Digital media to ensure due diligence[59] The Digital Personal Data Protection Bill, 2022 has been notified freshly to protect the personal data and process the personal data for the lawful purposes.

In addition to this, the government attempting to ensure safe and accountable internet in the country, they are conducting their invigilation and investigation to protect the country from cybercrimes for example, the Indian government discovered that there are applications and games which are security threats, and prejudicial to the Sovereignty and Integrity of India, Defence of India, also, they are a threat to the security of the state and public order, thus, several games like PUBG, BGMI, Chess Rush, etc. have been blocked by the government.[60] Along with this, the government has come up with scheme 14C,[61] the scheme aims to protect the information in cyberspace including the entire information infrastructure.[62] The government continues to impart awareness on the National Cyber Crime Reporting Portal.[63] Central Government sending text messages, providing a handbook for adolescents/students on cyber safety[64] , and soon, to educate the general public the government is going to initiate awareness campaigns.[65] Recently, in the year 2022, the government constituted an inter-ministerial panel to regulate the gaming industry and to identify the nodal ministry for surveillance, resultantly, Ministry of Electronics and Information Technology released a Draft amendment to the IT (Intermediary Guidelines & Digital Media Ethics Code) Rules, 2021[6667] affecting online gaming.

Solutions

The abundance of data and the record renders pervasiveness of the cybercrime, it is nearly impossible for the regulator to keep a check on the game's developers, games circulation, and content. In absence of laws that fit the contemporary scenario, it is quite problematic for the national and international regulatory authorities to invigilate online

The Consumer Protection Act, 1986, Central Goods and Services Tax Act, 2017 Prevention of Money Laundering Act, 2002, and the Advertising Content in India ("ASCI Code") etc.

[59] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. PART II Due Diligence by Intermediaries and Grievance Redressal Mechanism, Section 3. Due diligence by an intermediary.

[60] Ministry of Electronics & IT, "Government Blocks 118 Mobile Apps" Which are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order, (2020) https://pib.gov.in/PressReleasePage.aspx?PRID=1650669 accessed January 08, 2022.

[61] MINISTRY OF HOME AFFAIRS, "**DETAILS ABOUT INDIAN CYBERCRIME COORDINATION CENTRE (I4C) SCHEME."** HTTPS://WWW.MHA.GOV.IN/DIVISION_OF_MHA/CYBER-AND-INFORMATION-SECURITY-CIS-DIVISION/DETAILS-ABOUT-INDIAN-CYBERCRIME-COORDINATION-CENTRE-I4C-SCHEME **ACCESSED JANUARY 14, 2023.**

[62] Indian Cyber Crime Coordination Centre (I4C) – A 7-Pronged Scheme to Fight Cyber Crime Ministry of Home Affairs (Press Information Bureau, 2019).https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579184 accessed January 14, 2023.

[63] Ministry of Home Affairs, National Cyber Crime Reporting Portal https://cybercrime.gov.in/webform/crime_onlinesafetytips.aspx accessed January 14, 2023.

[64] Ministry of Home Affairs, Handbook for Adolescents/Students on Cyber Safety https://www.mha.gov.in/sites/default/files/CyberSafety_English_Web_03122018_0.pdf accessed January 14, 2023.

[65] JASMINE ANAND, "CRYPTO & ONLINE GAMING AWARENESS CAMPAIGN SOON TO BE ROLLED OUT BY GOVT" INDIA TODAY (2023) HTTPS://WWW.INDIATODAY.IN/CRYPTOCURRENCY/STORY/CRYPTO-ONLINE-GAMING-AWARENESS-CAMPAIGN-SOON-TO-BE-ROLLED-OUT-BY-GOVT-2316276-2023-01-02 ACCESSED JANUARY 14, 2023.

[66] Government of India, Ministry of Electronics and Information Technology Draft Notification, 2023 https://www.meity.gov.in/writereaddata/files/Draft%20notification%20for%20amendment%20to%20IT%20Rules%202021%20for%20Online%20Gaming.pdf accessed January 14, 2023.

[67] Ministry of Electronics & IT, MeitY releases Draft amendments to the IT (Intermediary Guidelines & Digital Media Ethics Code) Rules, 2021 in relation to online gaming, (2023) https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1888143 accessed January 14, 2023.

activities and control the same by facilitating surveillance. The formation of international norms with the help of organisations working with innovative technology and a group consisting of legislators and judicial bodies would be the plausible solution. Along with this, the institutionalisation of a trusted nodal agency or association (worldwide networking with the state agency) could be entrusted to provide a forum for the addressal of grievances all over the world, according to the established legislative framework agreed upon amongst the countries. Global regulation, agencies and the collaboration of the governments to introduce and implement the cyber practices standard is ought to be planned out considering the constant boom in the technology now and the way forward. To keep a check on the market of online gaming and compliance of the same with established rules and regulations, a cooperative model can be adopted by the government to involve and get the expertise of the Self-regulatory bodies[68] who can collaborate with the government to achieve the common goal.

Focusing on India's position of laws, the Central legislation is essential for the advanced age. As the gaming platform is rising and gambling and batting activities are increasing nationally and globally. Technology will be more rigorous in the future as compared to the existing one as per the notion of Digital India. Thus, the quintessential law dealing with all the relative aspects of online gaming on the central level would be the solution to deal with all the problems associated with online gaming.

In absence of uniformity and consensus to prohibit online games in their entirety or not, the parliament can settle the position by enacting Central legislation to regulate the game industry and relative activities. Quoting the recommendation of the Law Commission, it has observed-

"However, incapability to enforce a complete ban has resulted in rampant increase in illegal gambling, resulting in a boom in black-money generation and circulation. Since it is not possible to prevent these activities completely, effectively regulating them remains the only viable option. Thus, if Parliament or the State Legislatures wish to proceed in this direction, the Commission feels that regulated gambling would ensure detection of fraud and money laundering, etc. Such regulation of gambling would require a three-pronged strategy, reforming the existing gambling (lottery, horse racing) market, regulating illegal gambling and introducing stringent and overarching regulations."[69]

Resultantly, a bill on Online Gaming (Regulations) 2022, has been filed in the Lok Sabha, to create an operative regulatory mechanism and to prevent the deception and misappropriation of online games.[70] However, the proposed bill fails to serve a wide-ranging resolution to the existing problems inclusive of money laundering but not limited to advertising restrictions, grievance procedures, restrictions of the digital market, etc.[71]

Nevertheless, a model law and standards are required to be framed in a manner that is not restricted to online batting, money laundering, or gambling only but it should contain aspects related to the content, advertisement, cybersecurity, privacy, and piracy of the games, etc. events causing cybercrime. Apparently, the proposed bill does not ensure justice to the

[68] See, for example, (In the same line as) Advertising Standards Council of India (ASCI), All India Gaming Federation (AIGF), Internet and Mobile Association of India (IMAI)) etc.
[69] Law Commission of India Report No. 276, *Legal Framework: Gambling and Sports Betting Including in Cricket in India*, (2018) https://cdnbbsr.s3waas.gov.in/s3ca0daec69b5adc880fb464895726dbdf/uploads/2022/08/2022081655-1.pdf accessed January 13, 2023.
[70] The online regulation bill 2022 https://www.medianama.com/wp-content/uploads/2022/05/78-of-2022-as-introduced.pdf accessed February 26, 2023.
[71] TANUSHREE SAXENA, "ONLINE GAMING REGULATIONS 2022: UNLOCKING A NEW LEVEL" (CYBERPEACE FOUNDATION 2023).

current phenomenon as expected. Stringent regulation with the growth of technology is a dire need of society to prevent cybercrime.

The future regulation of online gaming ought to be paced with the expansion of Artificial Intelligence and its relative impact on Indian society. The laws are required to be essentially technologically sound to handle content and jurisdictional issues, online investigation, inquiries, the contradiction of the legal provisions (if arise between the states), the conviction of cyber criminals, and associated aspects.

Conclusion

Cyberspace has numerous dimensions including positive and negative. Precisely, the gaming industry has become a major source of entertainment, it had developed as an innovative industry, infuses Foreign Direct Investment, and creates ample opportunities for gaming companies, developers, designers, and even users. It is a source of generating enormous revenue for the country. However, to know and guard against the risks associated with internet gaming and to create and enjoy a secure internet environment, it is mandated for each stakeholder to comply with the law of the land to control and eliminate cybercrimes. Additionally, we have reached a stage where rather than debating on the issues concerning games of skill and chance, we focus on the real problem of the forthcoming high-tech world and its socio-economic and legal impact.

In India, the gaming industry is thriving more than ever, thus, restricting fiscal need and banning online games would not be feasible for the Indian economy. Moreover, during and post-COVID-19 pandemic, the majority of the population has shifted to the internet for entertainment, to earn money, to generate funds or to get educated, and for relative activities, plus, the current use of AI applications and advancements in the future seems to cultivate more. Therefore, the standards of online games ought to be improved considering the volume and their impact on society. Online gaming per se requires an operative, comprehensive, advanced central legislation and a nodal agency to serve as a watchdog. Consequently, it is high time that cyber activities are to be regulated and controlled thoroughly to combat cybercrimes in general and the crimes concerning online games and gaming in particular.