

Criminal Liability for Online Child Sexual Grooming in Electronic Games: A Comparative Study between Saudi Law and U.S. Law

Dr. Dania Marwan Yousef

Assistant Professor of Criminal Law

University of Tabuk, College of Sharia and Law, Department of Law
dyousef@ut.edu.sa

Abstract

The quick growth of the electronic gaming environments has opened new doors for child sexual grooming as a cyber enabled crime that involves psychological manipulation, anonymity and cross-platform interaction. Even with rising awareness around the world, current criminal law does not adequately reflect and respond to grooming in a highly immersive online game environment. The focus of this study is on the criminal responsibility of online child sexual grooming, addressing the same issue by comparing Saudi legislation with U.S. federal legislation. An interdisciplinary approach of doctrinal and comparative legal research methodology is employed, examining the provisions in the law, judicial interpretation and international regulatory frameworks that apply to cyber-enabled child exploitation. It also analyzes criminal responsibility by the elements of actus reus and mens rea, as well as challenges to evidence in the digital environment. The evidence shows that under U.S. law, there is a more clear and forward-looking framework, criminalizing grooming-related conduct because of laws involving coercion and enticement that also cover inchoate offenses. Saudi law, on the other hand, does not differentiate between "grooming" and other cybercrime and child protection offenses, resulting in a lack of precision in legal qualification. The study addresses the doctrinal gaps in the field of grooming in gaming platforms, introduces a more coherent conceptual framework that would make the platform more responsible, improve the evidence mechanisms, and offer a basis for early intervention in the criminal process in cases of child exploitation through the use of online gaming.

Keywords: Child Grooming, Cybercrime, Criminal Law, Saudi Law, Comparative Law, Online Games

1. Introduction

Electronic games have grown in number over the years, and computer interaction has become an immersive and social experience, especially with young children and adolescents. Today's online games are not only platforms for entertainment; they are also intricate social environments featuring real-time interactions, user-created material and virtual identities. These features do create significant criminal risks as well as improve user experience – especially in terms of child safety. Empirical and technical studies have shown how online platforms such as games can be fertile soil for all kinds of forms of online exploitation because of the interactive nature of games and the fact that they are relatively unregulated (Faraz et al., 2022). Criminologically, these contexts fit into the larger picture of the changing nature of crime in today's digital era, as the physical and virtual worlds have increasingly merged and created a new category of crime that takes advantage of the affordances of technology (Davidson & Gottschalk, 2023).

In this rapidly changing environment, one new and increasingly advanced form of child sexual grooming is taking place online. Grooming is an intentional process in which the offenders gain the confidence of minors, groom them psychologically and then gradually promote sexual exploitation. Online grooming differs from other forms of abuse in that they use tools of digital communication and

can take place completely in virtual worlds. Studies on preventing and combating child sexual exploitation have identified grooming as a gradual process that typically includes targeting, engagement, trust building and exploitation (Quayle, 2020). Recent research also emphasizes the extent and sophistication of these forms of exploitation in digital settings (e.g., video games), and the lack of robust safeguards against exploitation in the technology industry (Salter et al., 2023).

Despite the increased awareness of the problem, there is still a substantial legal barrier with respect to weak criminal law provisions to meet the challenges of grooming within a gaming platform. Traditional aspects of law have largely been designed to manage 'real world' crimes, and may not adequately account for the subtleties and preparatory nature of online grooming behaviours. The concept of "lawful communication" and "criminal intent" is particularly complex in the digital world and presents a challenge in establishing criminal liability. Legal scholarship has examined the flaws of existing criminalisation frameworks, highlighting that the definition of grooming is not clear enough in many jurisdictions, and therefore a proper prosecution of grooming has not yet taken place (Gillespie, 2022), especially where no exploitation has yet occurred. Fully mapping of the legal responses to grooming suggests that existing laws are not sufficiently specific and flexible to respond to the dynamic and technologically mediated nature of grooming in online contexts (Whittle et al., 2022).

In this context, it is clear that there is a gap in the current literature on comparative criminal law analysis, as there is a lack of specific analysis of online child grooming in the context of a game. Despite some recent research examining the psychological, criminological or policy aspects of grooming, there is a dearth of specific work that considers how the various legal traditions define and treat criminal liability for grooming in interactive digital spaces. While the differences between the two legal systems in terms of legal traditions, the mechanisms of enforcement and the ways in which cybercrime is regulated are significant, this gap is pronounced when both are compared to each other.

This study, therefore, seeks to add to the existing body of literature by making a comprehensive comparative analysis of criminal liability in relation to online child sexual grooming within an electronic gaming context under both Saudi law and U.S. law. The research aims at two main points: one, to examine the legal aspects that make up criminality in the context of grooming offenses, such as *actus reus* and *mens rea*; and, two, to study the effectiveness of Saudi and U.S. legal systems in combating the grooming offense in digital gaming platforms.

To this end, the study will be guided by the following research questions: How is criminal liability established on cases of online child grooming especially in gaming setting? How effective are Saudi and U.S. laws and regulations in tackling and prosecuting the grooming behaviors in such contexts?

The importance of this study is to contribute to the various aspects of legal and policy-making. From a criminal law perspective, it aims to further develop the doctrinal understanding of how the classical law concepts could be modified with regard to the new forms of cyber-crime. From a child protection policy perspective, it offers learnings on areas of regulatory gaps and possible reforms that will improve child safety in digital spaces. Moreover, the research adds to the current discussions on the regulation of digital platforms, as it explores the interplay between criminal liability and technological governance in the digital gaming landscape.

The paper is in five major sections in structure. The second part is devoted to the research methodology, which was used to carry out the study, with particular emphasis on the doctrinal and comparative legal method used. This is followed by an introduction of the research methodology which was adopted in the course of the study with particular emphasis on the doctrinal and comparative legal method used. The third part looks at the criminal and criminological nature of online grooming in the gaming context. The fourth part compares criminal liability in Saudi law and U.S. law, emphasizing similarities, differences and gaps in the laws. Finally, the conclusion reviews the key conclusions and makes recommendations for legal and policy changes.

2. Method

2.1 Research Design

The doctrinal legal research approach is used in this study, which is based on systematic analysis and interpretation of the provisions of criminal law related to child sexual grooming online. The doctrinal method centers on the analysis of the legal texts of the laws, legal principles, and judicial interpretations to identify the ways in which criminal liability is built and applied in the Saudi and U.S. legal systems. Within this context the study focuses on the key elements of the criminal responsibility: *actus reus* (the prohibited conduct) and *mens rea* (the necessary criminal intent) as the two main elements in the legal treatment of grooming offenses in digital environments. This method is in line with existing methods of cybercrime scholarship that focus on the doctrine to elucidate the manner in which traditional legal concepts are transformed to new, technologically-mediated ways of committing offences (Brenner, 2022). A doctrinal analysis is also part of the research as it critically discusses and evaluates similarities and differences between Saudi legal system and U.S. legal system in a comparative legal method. Comparative legal analysis enables a systematic investigation of the distinct conceptions and regulation of online grooming as a criminal offence within two legal systems: one based on a hybrid system, where the Islamic legal system influences the definition of online grooming as a criminal offence and the statutory regulation of online grooming; and the other based on common law principles. The cross-jurisdictional nature of cybercrime is especially important, as it requires a cross-jurisdictional understanding and evaluation of this type of crime. The criminological perspective of a comparative investigation is a reflection of the more general acceptance that cyber crime is an issue with multidimensional and socio-technical characteristics, which is not limited to national boundaries, and thus cannot be analysed according to a single paradigm (Yar & Steinmetz, 2023). In addition, the research design puts emphasis on analysis of the criminal law as opposed to a descriptive or policy analysis. The work focuses on the doctrinal aspects of the liability, and is designed to go beyond the general discussion of online safety and offer a precise legal analysis of the criminalisation, prosecution and adjudication of grooming behaviours. This includes an evaluation of the current legal framework to capture preparatory acts, digital interactions and intent formation in the context of gaming, and identify potential gaps in legal definitions and enforcement. The study seeks to both produce a robust doctrinal and comparative analysis of online child grooming as a modern-day cybercrime and to foster a deeper understanding of online child grooming that is both rigorous and legally sound.

2.2 Comparative Scope

The aim of this study is to use a structured framework comparing two different legal systems: the Kingdom of Saudi Arabia (KSA) and the United States. The Saudi legal framework is analysed based on the main powers and principles of legislation, including the Anti-Cybercrime Law and the Child Protection Law, which both cover offenses related to digital exploitation and digital harm to children. The United States approach is examined primarily from the perspective of federal criminal law provisions pertaining to child exploitation, such as laws that make it illegal to entice, coerce, or produce or distribute child pornography. This dual approach allows for a holistic approach to the assessment of both the system of criminal liability construction and enforcement of criminal liability for online child sexual grooming in electronic gaming environments.

Saudi legal system and U.S. legal system are selected as an example of two different legal traditions and regulatory approaches, methodologically supported by their distinct approaches. Saudi law is based on a mixture of statutory law and rulings based on Islamic law, while the U.S. law is based on common law, which emphasizes judicial interpretation and precedent. This difference offers an analytical foundation to differentiate the meaning of fundamental aspects of criminal liability, such as intent, preparatory acts and digital activity, from the legal perspective of the target legal culture. Furthermore, cybercrime is a cross-border phenomenon and international regulation may have gaps

and inconsistencies, highlighting the need to compare the regulations in place to identify the strengths of the norms and gaps at the regulatory level (Wall, 2024). Moreover, the comparative scope is enriched by the contemporary scholarship and practice that has placed an emphasis on the importance of cross-jurisdictional legal solutions to digital harms impacting children. Comparative analysis has demonstrated that it is possible to learn about best practices and better legislation from a study of several legal systems, particularly in cases where there are technological developments that are more advanced than legislative action (Okeal et al., 2026). This study is therefore not just about the two systems but critically analyses their effectiveness in tackling grooming behaviour in gaming contexts, particularly in terms of the extent to which the systems are criminalized, enforced and defined in law.

2.3 Data Sources

The study uses a wide range of legal and academic resources that are authoritative and comprehensive to support the study. Primary sources are statutes that outline the legal definition and elements of grooming-related offenses in Saudi law and the United States Code. Judicial decisions and case law are also considered crucial sources of information in a U.S. context as it relates to interpretation and application of statutory provisions – especially evidentiary standards and establishing criminal intent in an online setting.

The research includes reports of policy and conventions on OCE at the international level, as well as regulatory frameworks and documents from domestic sources. These sources offer the broader normative context and enable an assessment of the national laws in light of international laws and best practices. Moreover, the research relies on a significant amount of academic legal research and insights from interdisciplinary research on cybercrime, child protection and the regulation of digital platforms, allowing for a theoretically informed analysis of the problem.

With the technological nature of online grooming in gaming, specific focus is given to sources related to the regulation of digital platforms and AI. New studies highlight the increasing significance of platform governance and automated moderation in the context of harm in online spaces and regulation of that harm. Recent studies highlight the salience of platform governance and automatic moderation tools in terms of risks and regulatory measures concerning online harms. With this regard, the literature on topics such as AI regulation and platform accountability is in line with the ongoing intertwining of criminal law and technological regulation, as underlined in recent European teaching on digital governance (Kloza et al., 2023).

2.4 Analytical Approach

The research approach adopted in this study is structured analytical research which combines normatively legal analysis with comparative criminal law method to evaluate the existing legal responses to online child sexual grooming in electronic games. The normative aspect of the analysis looks at the adequacy and consistency of provisions of criminal law in Saudi and U.S. legal frameworks, including the definition of grooming as a cyber-enabled offence. This involves a doctrinal analysis of the concept and construction of criminal liability in law, focusing on the traditional elements of the criminal law (*actus reus* and *mens rea*) and the extent to which they are able to adequately describe digitally mediated preparatory conduct.

The comparative analytical part of the work systematically explores the similarities, differences and gaps of the two jurisdictions, in parallel. The analysis is not just descriptive, it also critically discusses how each one of these systems addresses the problem of grooming behaviors in the interactive and immersive games. This involves evaluating how successful the laws are in defining offences, whether there is a clear intention to commit an offence and the processes involved in establishing digital criminal acts in different jurisdictions.

Theory behind this analytical framework comes from recent research that has focused on online contemporary scholarship that highlights the fluid and distributed character of online interactions and

the need for an expansion of traditional legal categories in order to explain digital harms. It highlights the shifts of privacy, responsibility, and harm in the online sphere – and thus calls into question the traditional notions of criminal liability in the online realm (Citron, 2022). Literature on platforms governance also emphasizes the need for an understanding of the structures of platforms as potential sources of harm, such as algorithmic governance and private governance structures (Suzor, 2023). This means that this paper's analytical perspective is not the legal system itself, but the socio-technical environment of digital services, as a part of which criminal law is situated. This enables a more detailed analysis of the relationship between law and technology infrastructures, and the ways in which these intertwine to influence the nature and frequency of grooming activities, and the ability of legal procedures to respond effectively.

3. Criminal and criminological aspects of online grooming in game environments

Child sexual grooming in electronic games is a hybrid between criminal law and digital criminology that combines some, or all, of the features of interpersonal offences with technologically mediated interactions. To understand this phenomenon, a holistic perspective on both aspects of the legal categorization and behavioural aspects is needed, especially when considering the change in character of online platforms and immersive gaming environments.

3.1 Legal Definition and Elements of the Crime

In the criminal justice context, online child grooming is normally understood to be a calculated and deliberate act that involves developing an emotional bond and trust between the child and an offender, with the intent to sexually exploit the child. However, digital grooming differs from offences which occur in the real world in that the behaviour is incremental and can involve a series of actions that don't necessarily lead to contact, but are steps towards committing an offence.

Grooming is conceptually different from other related offences, such as sexual exploitation and sexual solicitation because it is mainly used to refer to the preparatory stage of a sexual offence and not the actual offence itself. In the criminal law context this distinction is of paramount importance as it has a significant bearing on the extent of liability as well as when criminalization starts. In some countries, such as the ones studied in this research, it is now known as an offence in itself and hence, it has been increasingly recognised as a serious crime, even if it is not completed (Abu Harbeed & Barahmeh, 2022).

There are usually two elements to the criminality of a grooming offence *actus reus* and *mens rea*. Online *actus reus* refers to online activity that constitutes the *reus*; communication via games, manipulation via in-game interaction, and extended communication with minors in virtual space. The *mens rea*, however, is revealed in the mindset of the perpetrator, his/her deceptive and manipulative nature, and his/her sexual agenda behind seemingly innocent encounters. A special focus of legal scholarship is the special evidentiary challenges of proving intent in cyberspace, where anonymity and lack of physical contact can create problems with intent (Kristich, 2025).

Moreover, criminal liability analysis should also consider the dynamics of electronic games, which allow the players to interact continuously through communication means like chat functions, voice communication, and identities based on avatars. The features make it difficult to make a traditional legal evaluation of identity and intent because the perpetrators can conceal their age, identity and purpose while using continuous grooming (Fachri & Harefa, 2025). Previous comparative legal studies also emphasize that traditional concepts of criminality and criminality of the Internet need to be adapted to the new field of grooming online, as it is digitally mediated (Abu Issa, 2019).

3.2 Modus Operandi in Gaming Environment

This *modus operandi* is closely related to the structural features of contemporary electronic games which allow for real-time communication, immersive interaction and formation of persistent identity. The in-game communication systems and voice communication channels are often used to start and

maintain contact with minors by offenders. The tools enable ongoing engagement, at times within the context of game play, which may be more difficult to suspect and increase the level of access to vulnerable users by offenders.

One of the central elements to the grooming process in online games is the way it involves using avatars and anonymity, allowing perpetrators to create fake profiles and alter the age, gender, and purpose of users. This anonymity is conducive to the development of trust-building processes, that are carried out by the offender, who after a number of interactions develops an emotional dependency by psychological manipulation techniques. These processes are particularly useful in interactive games where social interaction is an integral part of the game (Choi & Lee, 2024). Empirical evidence also demonstrates that it is not uncommon for grooming to happen across platforms – from one gaming platform to another communication platform (such as social media or private messaging apps). This shift to this cross-platform is a step forward in the process of grooming and increases the risk of offline grooming. The risks are worsened by the introduction of a metaverse based game environment, in which the player is immersed in the game, and is present in the game with other game participants and not with real people (Chawki et al., 2024). Technological assessments also show that this is particularly true of young players, because games are interactive, and they are activities that require a high level of involvement and trust. Structural design elements that promote interaction and connection between users and others, and between users and the environment also increase user exposure to potential offenders further reinforcing these dynamics (Faraz et al., 2024; Khanta, 2024).

3.3 Victim Vulnerability and Offender Profiling

The psychological and developmental factors of minors are key factors in online grooming cases, with victim vulnerability being correlated with the level of trust that minors have in those who they meet online and their inability to recognize manipulative behaviour. In most cases, grooming is a gradual process, which includes targeting, rapport building, isolating the victim and eventually exploiting the child. Each step is intended to decrease the resistance and build dependency, usually through emotional manipulation and "friendship. It has been identified from the literature that there are some types of behaviour that can be differentiated between offenders who groom online; they can be opportunistic offenders and organised offenders who grooming vulnerable minors systematically in different platforms. These types of offenders could well be very technologically adept and understand how online communication works, and exploit the online environment's structural vulnerabilities (Hamilton-Giachritsis et al., 2021). Research in both law and crime also shows that the nature of abuse and grooming is increasingly becoming interlinked, particularly in digital environments where sharing and communication of images and content are closely linked, as is content creation. This intersection makes it challenging to classify and enforce the law because damaging behavior could progress from non-criminal behavior to extreme exploitation (McGlynn & Rackley, 2023). It is known that there are large efforts to sensitise parents and to encourage digital literacy; there is also a strong emphasis on protecting institutions on an institutional level, within the framework of international child protection campaigns. Need for prevention measures to be more than law enforcement measures, as this should include platforms accountability measures, education and awareness campaigns to de-risk minors (UNICEF, 2023). Furthermore, the analysis of online interactions shows that children don't necessarily have to be passive victims, and can also demonstrate resistance behaviours in the process of being groomed. Nevertheless, this resistance is frequently counterbalanced by the determination of the perpetrator and his psychological methods of resistance, so that the whole legal and preventive mechanisms need to be addressed both from a behavioural and a technological point of view, which also involves the mitigation of the crime's consequences (Journal of Pragmatics, 2025).

4. Comparative Criminal Liability: Saudi Law vs U.S. Law

4.1 Legal Framework and Criminalization

The criminalisation of online child sexual grooming in electronic games illustrates a clear difference in the approach to the definition and regulation of child exploitation in the context of electronic games. Saudi Arabia and the United States (U.S.) have two different doctrinal positions: one is more general and criminal, while the other is more specific and statutory regarding preparatory conduct and attempted conduct in digital environments. The comparative Legal Framework for Online Child Grooming is found in Table 1.

Table 1: Comparative Legal Framework for Online Child Grooming

Dimension	Saudi Arabia	United States
Primary Legal Sources	Cybercrime Law; Child Protection Law	18 U.S.C. §2422; 18 U.S.C. §2251
Legal Classification of Grooming	Not recognized as an autonomous offense; subsumed under exploitation, enticement, and misuse of digital platforms	Not always labeled as “grooming,” but criminalized through coercion, enticement, and sexual exploitation statutes
Scope of Criminalization	Focus on completed exploitation-related acts rather than preparatory grooming conduct	Covers both completed offenses and inchoate conduct (attempt, enticement, preparation)
Treatment of Online Conduct	Broad interpretation of electronic communication as supporting evidence of exploitation	Direct criminalization of online communication used for sexual enticement of minors
Role of Intent (Mens Rea)	Inferred indirectly through general criminal provisions	Explicitly required and often established through communication and digital interaction patterns
Legal Gap Identified in Literature	Lack of specific statutory definition of grooming limits qualification of preparatory acts (Al Hamdan, 2023)	More comprehensive framework allowing early-stage intervention through attempt liability
Regional/International Influence	General child protection orientation; limited specificity for gaming environments (Al-Khawaldeh et al., 2024)	Aligns with broader international emphasis on early criminalization of grooming conduct

Saudi criminal law has a generalized protection model in which the behaviours related to grooming are seen in the context of the general provisions of the law regarding the use of digital platforms and their exploitation and misuse. This is because Al Hamdan (2023) points out that there is no clear statutory definition, which results in interpretative challenges in relation to preparatory grooming behaviours in electronic gaming contexts.

The legal systems of different jurisdictions apply their own unique evidentiary standards to determine both the acceptability and evaluation process of this evidence material. The protection-focused regional frameworks demonstrate insufficient understanding about how grooming processes develop through interactive and progressive stages according to Al-Khawaldeh et al. (2024). The Council of Europe (2021) explains that grooming needs official recognition as an individual crime because it involves mental manipulation and work that happens before any actual grooming activities begin at the international level. The European Commission (2022) supports this position through its recommendation to merge the current law with specific definitions which explain solicitation and grooming activities through both physical and digital communication channels. The United States

follows a different approach which uses criminalization before offenses occur to establish criminal responsibility for both attempted online sexual exploitation of minors and for the acts of enticement and coercion directed at minors. The framework enables legal proceedings to start before people make physical contact which helps the system handle grooming offenses that exist in their early stages. Overall, the comparative analysis reveals that U.S. federal law offers more specificity or operationality in its ability to prosecute grooming behaviour at the initial stages and in digital and gaming contexts, while Saudi law relies more on the general interpretative provisions, which may hamper applicability.

4.2 Elements of Criminal Liability and Evidentiary Standards

The liability for online child sexual grooming depends on the interpretation of the actus reus, mens rea and admissibility and reliability of electronic evidence in the context of online games. With cyber enabled crimes, actus reus now includes cyber-based acts that involve initiating contact with minors, sexually explicit communication, and attempts to manipulate or persuade victims in the context of in game chat, voice communications or avatar based interaction. Such virtual behaviours are the material aspect of the offence where a clear trajectory towards sexual exploitation is shown. The mens rea element, including the intent to exploit or engage in unlawful sexual activity with a minor, is frequently presumed from the context of a computer user's activities, rather than just his or her admitted intent. Patterns of communication, persistent contact and explicit content sent via gaming platforms are good indicators of intent that courts often use. As such, the case of *United States v. Gagliardi* (2007) shows that in online grooming cases, the intent of the defendant may be gleaned from his or her communications and his or her conduct, even if there have been no physical contacts, as long as the evidence indicates a clear and deliberate intent to exploit a minor. In terms of evidence, digital evidence is a key element to the prosecution of grooming offenses. That includes chat logs, voice recordings, information from gaming platforms and information gleaned from law enforcement agents who impersonate minors and engage in undercover operations. The Department of Justice (2020) study suggests that law enforcement officers should use undercover sting operations to monitor digital activities which produce live evidence that proves grooming behaviors and their underlying motives. The legal acceptance and assessment methods for this evidence material vary between different court systems because each system follows its own set of rules for evidence admission. International legal guidance points to inconsistencies with U.S. criminal procedure where electronic evidence can be admitted on a wide basis as long as it is authenticated and has a chain of custody. The worldwide fight against cybercrime has achieved major advancements yet countries continue to face challenges when they need to prove crimes and maintain digital evidence and share these records between borders. The worldwide operation of gaming platforms creates major obstacles because different states maintain distinct standards for digital evidence authentication and data retention protocols and inter-state digital record access. The UNODC report from 2023 points out that international gaming platforms maintain a significant obstacle because nations differ in their digital evidence authentication methods and their ability to maintain digital evidence and share these records between borders. Overall, the comparative assessment shows that U.S. law has created powerful doctrinal and procedural rules for proving intent and conduct in online grooming cases, but more international law needs to be worked out to create a harmonized evidentiary standard for such cases.

4.3 Enforcement Challenges and Legal Gaps

Although criminal measures to tackle online child sexual exploitation have been broadened, there remain important structural and operational issues in relation to the criminal liability of those who groom in electronic gaming venues. A major challenge is jurisdictional complexity, with the grooming occurring online using servers or platforms in different jurisdictions, and the groomer and the victim in others. The cross-border dimension of cybercrime poses significant challenges for investigation, prosecution, and international cooperation in extraditing the criminals. The cross border aspect of cybercrime poses significant difficulties in investigation, prosecution and international cooperation for extradition of the criminals, especially when there are variations in the definition of cybercrime and

evidentiary requirements between states. A significant challenge is also the detection of grooming within gaming platforms where communication is frequently encrypted, real-time, and integrated into the interactive platforms and functions, like chat dialogue, voice channel, or avatar interaction. The grooming process moves through its stages with an undetectable progression which Johns and Zeyzus et al. (2024) point out in their research. The early stages of grooming remain invisible to most people while the process moves through its initial phases. The current legal system lacks proper technological and regulatory support which fails to handle the ongoing evolution of digital environments. The current legal framework shows legislators fall behind when they create rules for online gaming platforms which Crepax and Mühlberg (2022) demonstrated through their research on game moderation systems and automated detection tools and data sharing mechanisms. Moha and Rahaditya (2024) observed that gaming communities receive insufficient monitoring which enables players to exploit others without facing detection for extended periods. The issue of platform accountability remains unresolved because gaming companies operate as limited liability entities which restrict their legal exposure for user-generated damage to a specific threshold.

The absence of platform requirements for monitoring and reporting proactive grooming activities according to Zahirah et al. (2025) allows law enforcement agencies to handle most of the responsibility for grooming prevention and enforcement actions while platforms continue their inactive stance. Aside from the legal dimension, the analysis shows that the enforcement gaps in cyber grooming cases are also technically related, stemming from jurisdictional fragmentation, technical issues and the lack of regulation of platforms, and call for a more holistic and flexible approach to platform regulation.

4.4 Toward an Integrated Criminal Law Framework

Online child sexual grooming in electronic gaming spaces is becoming increasingly sophisticated, and a more comprehensive and flexible criminal law system is needed that transcends the traditional 'reactive' approaches to criminalisation. One of the key reform goals is ensuring that grooming is clearly defined to include digital and games-based interactions, including through in-game communication systems, avatars and immersive virtual environments. This would enable the criminal law to encompass the complete range of preparatory and manipulative acts of those who might be directly exploiting another. At the same time, the need for the explicit criminalization of preparatory acts, such as persistent communication, psychological manipulation and gradual steps of building trust is growing, which are typical of grooming processes. As legal scholarship points out, preventing progression towards the completion of sexual crimes is best achieved through intervention at the early stages of a process, which is often a long-term one, especially in the online context where harm occurs in a gradual rather than immediate fashion. Another aspect of reform involves enhancing the liability of the platform, and assurance of proactive measures to protect players as opposed to just reactive reporting. This encompasses robust duty of care, statutory duties in relation to monitoring and a more explicit accountability for not preventing foreseeable exploitation issues in their digital environment. The technological aspect of AI detection and prevention holds great potential, but also significant legal implications. AI-driven moderation can greatly aid in the detection of suspicious user behaviour on children's platforms but should be placed under robust legal protection to ensure proportionality, privacy safeguards and that users are not over-surveilled. According to Handayani and Mangar (2025) technology needs to follow child protection rules because digital safety systems should not harm the fundamental rights of children. The successful execution of an integrated system needs countries to work together more effectively because gaming platforms and cyber crimes operate across national borders. The enforcement process faces rising difficulties because AI-driven abuse creates new obstacles which require different authorities to work together through shared tools and unified laws for their investigations. The proposed framework highlights the importance of broadening the scope of the substantive criminal law, enhancing platform governance, improve system capability for the detection of child online sexual grooming and international legal cooperation in order to effectively tackle the changing nature of CSEG in gaming platforms.

5. Conclusion

This study analysed the criminal liability for online child sexual grooming in electronic gaming environments, by comparing the criminal liability framework of Saudi and U.S. criminal law. The results show that the practice of grooming has been identified as a new type of cyberbased crime involving a slow, psychological process, anonymity and platform mediated interaction. In every instance, traditional criminal law structures come under increasing strain to come to grips with this kind of activity and to provide adequate concepts and rules for regulation in an immersed digital environment. To the first research question, the study concludes that criminal liability is being ascribed most often in the context of the interpretation of actus reus and mens rea in digital communication spaces, where intent is being assumed based on behavioural patterns, persistence in contact and the nature of the contacts in the context of gaming platforms. Digital content such as chat logs and platform information are crucial in proving conduct and intent. In response to the second research question, the comparative analysis reveals that U.S. law offers a more sophisticated and explicit approach to dealing with grooming, setting forth criminal laws that punish coercion, enticement and attempted exploitation of children at an early stage of the behavior. By contrast, the Saudi legislation is based on more general laws on cybercrime and protection of children, although in theory these are protective, it does not have a clear doctrinal classification of grooming as a standalone offence which reduces the precision in legal qualification and enforcement in the context of gaming. Both systems are evaluated here and it is concluded that the U.S. system is more effective in combating inchoate and preparatory behaviours because of its broad emphasis on the concepts of attempt and intent, while the Saudi system is more general, but less specific. However, both are challenged by the need to adjust to the swift change of gaming technologies and cross-border electronic communications. The study also sheds light on the need for the law to be modernised, particularly in criminal law, to include explicit references to digital and gaming-based environments in definitions of 'grooming'. The need to better define preparatory grooming activity as criminal, to make platforms more accountable for their activities and to improve the use of technological solutions like AI-based detection systems within legal frameworks is also urgent. The findings at the policy level suggest three main directions: (i) legislative reform to clarify and narrow down the definition of grooming-related offences, (ii) strengthening of the enforcement aspect by creating new special capabilities for investigation and improving the collection of digital evidence, and (iii) regulation of the platforms, introducing proactive duties for safeguarding against grooming. In conclusion, the study recommends additional research efforts that deepen understanding of the relationship between cybercrime, artificial intelligence and child protection law, and highlight the changing nature and function of platform governance in the prevention of online child sexual exploitation, especially in the context of metaverse environments, cross-jurisdictional enforcement approaches, and the importance of platforms in the prevention of child grooming.

References:

1. Abu Harbeed, A., & Barahmeh, N. (2022). Online child sexual exploitation: A comparative jurisprudential study with positive law. *Islamic University Journal of Sharia and Law Studies*, 30(1).
2. Abu Issa, H. (2019). *Cybercrime: A comparative study in Arab legislations* (2nd ed.). Dar Wael Publishing.
3. Al Hamdan, B. (2023). Legal protection of children from online sexual exploitation in Saudi law (Comparative study). *Legal Journal*, (2).
4. Al-Khawaldeh, M., Ali, W., & Khawaldeh, R. (2024). Criminal protection of children from sexual exploitation through online games: A comparative study between Jordanian and UAE law. *Journal of Sharia and Law*, (4).

5. Audina, W., & Muhammad, Z. A. K. Y. (2025). Controlling child grooming in the digital world: Public policy strategies based on media criminology studies. *International Journal of Environmental, Sustainability, and Social Science*, 6(4), 789–799.
6. Brenner, S. W. (2022). *Cybercrime and the law: Challenges and issues*. West Academic Publishing.
7. Chawki, M. (2025). AI moderation and legal frameworks in child-centric social media: A case study of Roblox. *Laws*, 14(3), 29.
8. Chawki, M., Basu, S., & Choi, K. S. (2024). Redefining boundaries in the metaverse: Navigating the challenges of virtual harm and user safety. *Laws*, 13(3), 33.
9. Choi, K. S., & Lee, H. (2024). The trend of online child sexual abuse and exploitation: A profile of offenders and criminal justice response. *Journal of Child Sexual Abuse*, 33(6), 804–823.
10. Citron, D. K. (2022). *The fight for privacy: Protecting dignity, identity, and love in the digital age*. W. W. Norton & Company.
11. Council of Europe. (2021). *Implementation guidelines of the Lanzarote Convention on online grooming*.
12. Davidson, J., & Gottschalk, P. (2023). *Internet child abuse: Current research and policy*. Routledge.
13. European Commission. (2022). Proposal for a regulation laying down rules to prevent and combat child sexual abuse online.
14. Faraz, A., Mounsef, J., Raza, A., & Willis, S. (2022). Child safety and protection in the online gaming ecosystem. *IEEE Access*, 10, 115895–115913.
15. Fachri, A. M., & Harefa, B. (2025). Criminal liability for child grooming operational patterns in online gaming. *Rechtsidee*, 13(2).
16. Gillespie, A. (2022). *Child grooming and the law: A critical analysis of criminalization*.
17. Hamilton-Giachritsis, C., Hanson, E., Whittle, H., & Beech, A. (2021). Online grooming and child sexual abuse: Policy and legal implications. *Journal of Sexual Aggression*, 27(2), 201–217.
18. Khanta, K. (2024). *Protecting the innocent: Safeguarding children in immersive online gaming environments* (Master's thesis, Marymount University).
19. Kloza, D., Quintais, J. P., & Gellert, R. (2023). Artificial intelligence and platform regulation in the European Union. *Computer Law & Security Review*, 49, 105786.
20. Kristich, T. A. (2025). *Online child sexual grooming: Understanding the origins and problems within the criminal justice system* (Doctoral dissertation, Liberty University).
21. McGlynn, C., & Rackley, E. (2023). *Image-based sexual abuse: Legal frameworks and reform*. Oxford University Press.
22. Okeal, T. E. S. M. A., Alkasasbeh, H., Abdullah, H. I., & Fathelbab, S. R. (2026). Preventive legislative approaches to child protection in the digital environment: A comparative study. *Nusantara: Journal of Law Studies*, 5(1), 205–228.
23. Quayle, E. (2020). Prevention, disruption and deterrence of online child sexual exploitation and abuse. *ERA Forum*, 21(3), 429–447.
24. Salter, M., Woodlock, D., & Wong, T. (2023). The sexual politics of technology industry responses to online child sexual exploitation. *Child Abuse & Neglect*.
25. Suzor, N. (2023). *Lawless: The secret rules that govern our digital lives*. Cambridge University Press.
26. UNICEF. (2023). *Global status report on preventing violence against children*.
27. UNODC. (2023). *Online child sexual exploitation and abuse: Legal responses*.

Criminal Liability for Online Child Sexual Grooming in
Electronic Games: A Comparative Study between Saudi
Law and U.S. Law

28. Wall, D. S. (2024). *Cybercrime: The transformation of crime in the information age* (2nd ed.). Polity Press.
29. Whittle, H., Hamilton-Giachritsis, C., & Beech, A. (2022). A review of online grooming: Characteristics and legal responses. *Aggression and Violent Behavior*, 62, 101706.
30. Yar, M., & Steinmetz, K. F. (2023). *Cybercrime and society* (3rd ed.). SAGE Publications.
31. Zeyzus Johns, B. A., Casola, A. R., Rea, O., Skolnik, N., & Fidler, S. K. (2024). *Safeguarding youth from online sexual exploitation in the digital era*. American Journal of Lifestyle Medicine DOI: 10.1177/15598276241268236
32. Crepax, T., & Mühlberg, J. T. (2022). *Legal and technical solutions for protecting children in online games*. <https://doi.org/10.48550/arXiv.2207.09928>
33. Journal of Pragmatics. (2025). *Children's resistance during online grooming interactions* DOI:10.1016/j.pragma.2025.08.013
34. Faraz, A., Ahsan, F., Mounsef, J., Karamitsos, I., & Kanavos, A. (2024). *Enhancing child safety in online gaming: Protectbot AI framework*. Information, 15(4), 233 <https://doi.org/10.3390/info15040233>
35. Moha, A. P., & Rahaditya, R. (2024). *Legal protection of children as victims of online pornography crimes in gaming communities*. Ranah Research Journal.
36. Zahirah, A. A., Sinaulan, R. L., & Hasibuan, E. S. (2025). *Legal protection of children from grooming in online games under child protection law*. Journal of Law and Security Studies.
37. Handayani, T. A., & Mangar, I. (2025). *Legal protection for children from the impact of violence in online games*. **Journal of Development Research**, 9(2). <https://doi.org/10.28926/jdr.v9i2.497>
38. Ó Ciardha, C., Buckley, J., & Portnoff, R. S. (2025). *AI-generated child sexual abuse material: What's the harm?* arXiv <https://arxiv.org/abs/2510.02978>
39. United States Code. (2018). 18 U.S.C. § 2422 – Coercion and enticement. <https://www.law.cornell.edu/uscode/text/18/2422>
40. United States Code. (2018). 18 U.S.C. § 2251 – Sexual exploitation of children. <https://www.law.cornell.edu/uscode/text/18/2251>
41. United States v. Gagliardi, 506 F.3d 140 (2d Cir. 2007).
42. Department of Justice. (2020). *Child exploitation and obscenity section: Prosecuting online child exploitation*. <https://www.justice.gov/criminal-ceos>