

Digital Child Abuse in Saudi Arabia: Legal Protection and Enforcement Mechanisms

Tareq S. Alshammari

Department of Law, College of Shariah and Law, University of Ha'il, Kingdom of Saudi Arabia

doi: <https://doi.org/10.37745/gjplr.2013/vol14n5116>

Published September 14, 2026

Citation: Alshammari T.S. (2026) Digital Child Abuse in Saudi Arabia: Legal Protection and Enforcement Mechanisms, *Global Journal of Politics and Law Research*, 14(5),1-16

Abstract: *Digital abuse can adversely affect the well-being and safety of children in this information age. In response, Saudi Arabia has developed legal protection and enforcement mechanisms to safeguard children. Utilizing a doctrinal legal approach, this study examines these mechanisms vis-à-vis three forms of digital abuse: psychological, sexual, and privacy. The study shows that Saudi Arabia has a multi-layered legal and institutional framework consisting of laws, regulations, and helplines (rather than a single law) to protect children and enforce legal and criminal accountability (via fines and/ or imprisonment). This framework includes the Child Protection Law (2014) and its Executive Regulations (2023), the Anti-Cyber Crime Law (2007), the Anti-Harassment Law (2018), the Personal Data Protection Law (2021), the MHRSD helpline 1919, and the NFSP child helpline 116111. The study reveals how the Saudi legal and institutional mechanisms collectively operate to protect children against abuse in the evolving digital environment. The findings can help Saudi policymakers, authorities, and stakeholders better understand and apply the mechanisms for addressing digital child abuse in Saudi Arabia.*

Keywords: child protection, digital child abuse, enforcement mechanism, legal framework, legal protection, Saudi Arabia

INTRODUCTION

In this information age, digital systems have become vital for communication, education, entertainment, and social interactions. Children increasingly use these systems (such as social media apps, gaming platforms, messaging services, AI technologies, etc.) for entertainment, social communication, and academic activities (Al Ghamdi, 2025). These systems provide certain advantages but also expose the impressionable minds of children to new forms of abuse (especially digital abuse), which previous generations had not experienced to the same extent (Odgers & Jensen, 2020). The growing use of social media has also exposed children to security risks and digital abuse (Singh, 2017). Digital abuse can affect the psychological well-being of children (Hamm et al., 2015) and threaten their personal and sexual safety (Fry et al., 2025). Therefore, nations need to develop legal protection and enforcement mechanisms to safeguard their children

(Al Faryan et al., 2019; Pandey et al., 2017; Singh, 2016). This is especially important in countries with a young population, such as Saudi Arabia (Salam, 2023). Therefore, this research examines the phenomenon of digital child abuse in the context of Saudi Arabia. It also examines the legal protection and enforcement mechanisms available in Saudi Arabia to protect children from digital abuse.

Digital abuse can take different forms and can affect children's well-being and safety differently. Digital psychological abuse is one form, which means threatening, insulting, humiliating, or bullying a child online (Gohal et al., 2023). Digital sexual abuse and exploitation is another form, which includes online sexual messaging, grooming, blackmailing, requesting and/ or sending explicit content involving children (Fry et al., 2025). Finally, digital privacy abuse is another prominent form, which entails using, morphing, or sharing children's photos, videos, and/ or sensitive personal or identity information in a harmful manner (Alashwali & Alashwali, 2022; Singh, 2018; Stoilova et al., 2021). These three prominent forms of digital abuse can have a detrimental effect on the children's psychology, identity, and self-image. Therefore, there should be appropriate legal protection and enforcement mechanisms in countries like Saudi Arabia to adequately protect the nation's future.

In Saudi Arabia, there are several connected laws (rather than a single law) to protect children from digital abuse (Alshammari & Singh, 2018). This Saudi legal framework also provides enforcement mechanisms and criminal accountability provisions to protect children (Singh & Alshammari, 2020). The Child Protection Law (2014) and its Executive Regulations (2023) provide general child protection provisions (Kingdom of Saudi Arabia, 2014; Ministry of Human Resources and Social Development, 2023). The Anti-Cyber Crime Law (2007) contains provisions against online offenses and provides penalties (Kingdom of Saudi Arabia, 2007). The Anti-Harassment Law (2018) contains provisions to protect against online sexual harassment and provides penalties for harassing children (Naji, 2025; Saudipedia, 2023). The Personal Data Protection Law (2021) contains provisions related to the collection, processing, use, and disclosure of personal data to protect privacy, including children's personal data (Kingdom of Saudi Arabia, 2021). These Saudi laws and regulations include provisions to protect children, report incidents, conduct investigations, prosecute offenders, and rehabilitate victims, reflecting the broader importance of institutional reporting mechanisms (Alhamad & Singh, 2022). There are also reporting and support channels under the Saudi legal framework, such as the Ministry of Human Resources and Social Development (MHRSD) Domestic Violence Reporting Center (Ministry of Human Resources and Social Development, 2026) and the National Family Safety Program Child Helpline (Saudi Press Agency, 2022). These channels help enforce the Saudi legal and institutional framework for protecting children effectively in practice.

Prior research in Saudi Arabia has either focused on individual digital harms, specific online offenses, or specific cyber laws (Alshammari & Singh, 2018; Singh & Alshammari, 2020). Previous research conducted in Saudi Arabia related to children has examined cyberbullying, online harassment, online abuse, and online protection laws (Alashwali & Alashwali, 2022; Al

Ghamdi, 2025; Gohal et al., 2023; Naji, 2025). There is a dearth of comprehensive research in Saudi Arabia that has examined various forms of digital abuse against children along with legal protection and enforcement mechanisms. This study aims to fill this research gap by examining the three types of digital abuse (psychological, sexual, and privacy) along with Saudi legal protection and enforcement mechanisms to protect children. The current research focuses on children below 18 years, as this aligns with the definition of a child in the Child Protection Law (2014) (Kingdom of Saudi Arabia, 2014). The study utilizes a doctrinal examination of Saudi laws, regulations, and related enforcement mechanisms. Consequently, this study intends to answer the following research questions:

RQ1: What legal protections does the Saudi legal framework provide to protect children against three forms of digital abuse (psychological, sexual, and privacy)?

RQ2: What enforcement mechanisms support the implementation of the legal framework for child protection against digital abuse in Saudi Arabia?

The rest of the research is organized as follows. Section 2 presents a thorough review of the literature for this study. Section 3 deals with the research methodology. Section 4 is dedicated to the legal analysis and discussion. Section 5 presents the conclusions and recommendations of this study.

LITERATURE REVIEW

This section presents a literature review of the phenomenon of digital abuse of children with particular reference to Saudi Arabia. This study examines three broad forms of digital abuse: psychological, sexual, and privacy. Section 2.1 presents digital psychological abuse. Digital sexual abuse is presented in Section 2.2. Section 2.3 is dedicated to digital privacy abuse. Furthermore, Section 2.4 presents the legal protection and enforcement mechanisms to protect children from digital abuse in Saudi Arabia.

Digital Psychological Abuse

Digital psychological abuse for children uses online tools, devices, and platforms to threaten, insult, humiliate, or bully a child online (Gohal et al., 2023). Cyberbullying is the most researched form of psychological abuse (Lee et al., 2026; Zhu et al., 2021). However, this study employs the broader term because psychological abuse can go beyond cyberbullying to include isolated threats, intimidation, humiliation, or harassment. Digital psychological abuse can intensify harm as the victim can be reached at any time or place. Further, the offender may remain anonymous and hard to trace. The abusive content can also spread rapidly to a large audience in a short time, which has a detrimental effect on the psychology of children (Li & Hesketh, 2021; Zhu et al., 2021).

Children may suffer several negative effects due to digital psychological abuse. There are immediate emotional effects that negatively affect their self-esteem and lead to embarrassment (Hamm et al., 2015). Al Ghamdi's (2025) Saudi study identified social and emotional risks (such as fear, isolation, harassment, and embarrassment) caused by digital psychological abuse (such as

cyberbullying). According to Hu et al.'s (2021) meta-analysis, digital psychological abuse (like cyberbullying) is associated with depression among adolescents, which suggests negative mental health effects. There are also functional and behavioral effects that lead to poor school attendance and academic performance. Gohal et al. (2023) conducted research in the Jazan region of Saudi Arabia and reported that cyberbullying was linked to considering school leaving, study disruptions, and possible self-harm. As per Alfakeh et al.'s (2021) study, Saudi parents perceived digital abuse (like cyberbullying) as harmful to their children. Considering the seriousness of digital psychological abuse, it cannot be treated as merely inappropriate online behavior, and it is important to have legal protection and enforcement mechanisms to safeguard the children.

Digital Sexual Abuse

Digital sexual abuse for children includes online sexual messaging, grooming, blackmailing, requesting and/ or sending explicit content (Fry et al., 2025). Digital sexual abuse could involve content-based abuse, image-based abuse, and include sexual extortion. Content-based abuse may include deception and flattery to gain trust and develop intimacy, sexual solicitation, grooming, and coercive sexual communications (Whittle et al., 2013). Image-based abuse may include requesting, producing, recording, manipulating, and/ or sharing sexual images of children (Finkelhor et al., 2023). Sexual extortion is a form of blackmail in which money, sexual acts, or further images could be demanded by threatening to disclose sexual images (Fry et al., 2025). Digital technology intensifies sexual abuse as sensitive content involving children could be distributed online rapidly and spread to a wide audience. The content can be easily copied, stored, and redistributed, which could lead to repeated victimization of children (Finkelhor et al., 2023; Whittle et al., 2013).

Digital sexual abuse could lead to adverse effects on children. According to a systematic review by Page et al. (2025), children could experience anxiety, depression, social isolation, and lack of trust in others due to digital sexual abuse. The repeated circulation of sensitive images online could have a chilling effect on the children's psychology and could lead to fear, humiliation, and victimization (Finkelhor et al., 2023; Page et al., 2025). Further, the blackmail and grooming of children discourage disclosure because they could fear social stigma related to disclosure (Whittle et al., 2013). According to a study conducted by Al Ghamdi (2025) in Saudi Arabia, digital sexual abuse was associated with feelings of deception and exploitation among children and their parents. Naji's (2025) study in Saudi Arabia examined Saudi legislative treatment of digital harassment of children. However, the extant Saudi literature on digital sexual abuse has not fully explored the various aspects of digital sexual abuse, such as grooming, sextortion, and repeated online circulation. Therefore, there is a need to examine the Saudi legal framework vis-à-vis the various facets of digital sexual abuse.

Digital Privacy Abuse

Digital privacy abuse includes using, morphing, or sharing children's photos, videos, and/ or sensitive personal or identity information in a harmful manner (Alashwali & Alashwali, 2022; Stoilova et al., 2021). Digital privacy abuse could involve unauthorized image/content use,

personal data misuse, and unauthorized data collection and tracking. Unauthorized image/content use could involve copying, morphing, or distributing children's images and videos illegally (Bunn, 2021). Personal data misuse could involve misusing names, addresses, mobile numbers, identity documents, or social media information to cause harm to children (Stoilova et al., 2021). Unauthorized data collection and tracking involve access and use of children's location, camera, microphone, and contacts by apps, which can be abused by anti-social elements (Alashwali & Alashwali, 2022; Stoilova et al., 2021). Digital technology intensifies the abuse of children's privacy, as sensitive personal information and documents could be hacked by anti-social elements and misused for personal benefit.

Digital privacy abuse could have a detrimental effect on children, including loss of dignity, embarrassment, and a lack of trust in systems (Bunn, 2021; Stoilova et al., 2021). Alqahtani et al. (2017) conducted an investigative study in Saudi Arabia that found parent's concern about the protection of their children's privacy in the digital world, but frequently lacked a clear strategy about how to reduce those risks. Al-Naim and Hasan's (2018) study reported that some Saudi parents employ technical mediation tools to monitor their children online out of privacy concerns. According to Alashwali and Alashwali's (2022) study, Saudi parents have privacy concerns about the use of smart device apps, as they fear these apps could compromise their children's sensitive information. Al Ghamdi's (2025) study in Saudi Arabia also supported parents' concerns about their children's privacy in the online world. These Saudi studies show significant parental concern about children's privacy in the digital world, but the risks extend beyond privacy and include misuse of images/videos, personal data misuse, and tracking. Therefore, the Saudi legal framework should be examined vis-à-vis the various facets of digital privacy abuse.

Legal Protection and Enforcement Mechanisms

Digital technologies bring psychological, sexual, and privacy risks for children. Thus, it is important for the legal framework of a country like Saudi Arabia to identify potential digital risks, establish criminal accountability, and impose penalties to protect children. The Saudi legal framework to protect children encompasses several interconnected laws and regulations. The Child Protection Law (2014) provides general protection against psychological and sexual abuse of children and addresses threats to their safety (Kingdom of Saudi Arabia, 2014). According to Almuneef et al.'s (2026) study, the implementation of the Child Protection Law (2014) led to a 7-fold increase in the reporting of child maltreatment incidents as compared to the pre-law period. The Executive Regulations (2023) under the Child Protection Law provide operational procedures for handling digital abuse cases, reporting, coordination, and victim support (Ministry of Human Resources and Social Development, 2023). Owaidah et al. (2022) reported some implementation issues in these Saudi regulations, as a lack of knowledge and experience hampered their effective use. The Anti-Cyber Crime Law (2007) covers issues like blackmail, invasion of privacy, defamation, and exploitation of children. Nusairat (2023) examined criminal accountability under the Anti-Cyber Crime Law (2007) regarding the exploitation of children using electronic means. The Anti-Harassment Law (2018) encompasses harassment through electronic means and provides enhanced penalties if the victim is a minor (Naji, 2025; Saudipedia, 2023). Naji's (2025) study

examined the Anti-Harassment Law (2018) regarding the online harassment of minors and highlighted challenges related to evidence and reporting. The Saudi Personal Data Protection Law (2021) aims to protect individual privacy and includes provisions related to the unauthorized collection, processing, and distribution of personal data, including children's data (Kingdom of Saudi Arabia, 2021). Bamashmoos (2024) examined the consent requirements in the Saudi Personal Data Protection Law (2021) for the collection and processing of data, along with limits on unnecessary or coercive data collection.

Along with the legislative framework, it is important for Saudi Arabia to have an enforcement mechanism (via case reporting, assessment, referral, investigation, prosecution, and victim support). In Saudi Arabia, there are also reporting and support channels that enable the enforcement of legal protections for children. The MHRSD operates the Domestic Violence Reporting Center, which can be called at 1919 (Ministry of Human Resources and Social Development, 2026). 1919 receives the case reports, assesses their seriousness, and refers them to protection units or security agencies. The National Family Safety Program (NFSP) child helpline is available by calling 116111 (Saudi Press Agency, 2022). 116111 provides children with advice and support, and also refers them to relevant authorities. Al-Eissa (2019) reported in a Saudi study that nearly half of surveyed adolescents indicated willingness to use a child helpline. It is also important to have coordination among various enforcement units (such as MHRSD, police, prosecution, advice and support units, and judicial authorities) to close the loop from reporting to victim support. Al-Eissa et al.'s (2018) study on youth views in Saudi Arabia about child protection enforcement mechanisms cautioned against delayed support responses and ineffective reporting channels.

METHODOLOGY

This study adopts a doctrinal legal approach to examine Saudi laws, regulations, and related enforcement mechanisms for the protection of children. This approach is used because it supports systematic analysis of legislation, regulations, principles, and other legal materials (Hutchinson & Duncan, 2012; McConville & Chui, 2017). The legal framework and enforcement mechanisms examined in this study include the Child Protection Law (2014), Executive Regulations (2023) under the Child Protection Law, Anti-Cyber Crime Law (2007), Anti-Harassment Law (2018), Personal Data Protection Law (2021), MHRSD helpline 1919, and NFSP child helpline 116111. These instruments and mechanisms were selected as they address children's digital abuse (psychological, sexual, and privacy). The analysis was done in two stages. In the first stage, we examined the legal and regulatory provisions that deal with digital abuse (psychological, sexual, and privacy) of children in Saudi Arabia. Subsequently, we examined the enforcement mechanisms related to reporting, investigation, prosecution, penalties, institutional coordination, and support for children in digital abuse cases.

LEGAL ANALYSIS AND DISCUSSION

Section 4.1 presents the doctrinal legal analysis of the legal framework in Saudi Arabia, which helps to prevent three forms of digital abuse (psychological, sexual, and privacy) (RQ1). Further, the section also discusses these legal protections vis-à-vis the extant literature. Section 4.2 presents the enforcement mechanisms that support the implementation of the legal framework for child protection against digital abuse in Saudi Arabia (RQ2). This section also discusses these enforcement mechanisms with reference to the extant literature.

Legal Protections against Digital Child Abuse

This section addresses the RQ1 related to the Saudi legal protections against three forms of digital abuse (psychological, sexual, and privacy). Table 1 presents the relevant laws and regulations.

Psychological Child Abuse

The Child Protection Law (2014), its Executive Regulations (2023), and the Anti-Cyber Crime Law (2007) collectively endeavor to prevent digital psychological abuse of children (Table 1). Article 1(2) of the Child Protection Law (2014) defines psychological abuse as maltreatment causing psychological or health harm (Kingdom of Saudi Arabia, 2014). Article 3(9) of the Child Protection Law (2014) treats humiliating or degrading language as abuse; Article 3(14) treats threats to psychological well-being as abuse; and Article 6 seeks to provide general protection against abuse (Kingdom of Saudi Arabia, 2014). Executive Regulations (2023) of the Child Protection Law define a threat of harm as an act or statement that causes fear of intended harm (Ministry of Human Resources and Social Development, 2023). Article 3(15) of Executive Regulations (2023) seeks to protect against repeated psychological abuse, whereas Article 3(16) seeks to protect against harmful or age-inappropriate material (Ministry of Human Resources and Social Development, 2023). Article 3(2) of the Anti-Cyber Crime Law (2007) aims to protect against threats or blackmail due to unauthorized access, whereas Article 3(5) deals with defamation or harm due to misuse of information technology devices. Both articles impose up to 1 year imprisonment and/or a SAR 500,000 fine (Kingdom of Saudi Arabia, 2007).

Saudi legal framework regarding digital psychological abuse of children broadly covers the issues identified in the literature, such as threats, humiliation, harassment, and harm of children (while cyberbullying may fall within these protections) (Gohal et al., 2023; Zhu et al., 2021). The literature focuses on cyberbullying as a prominent form of psychological abuse (Lee et al., 2026; Zhu et al., 2021), whereas the Saudi legal framework covers various forms of psychological abuse. The protections in the Saudi legal framework align with the forms of digital psychological abuse identified in the literature related to Saudi Arabia (Alfakeh et al., 2021; Al Ghamdi, 2025; Gohal et al., 2023).

Sexual Child Abuse

The Child Protection Law (2014), its Executive Regulations (2023), the Anti-Cyber Crime Law (2007), and the Anti-Harassment Law (2018) collectively aim to prevent digital sexual abuse of children (Table 1). Article 1(2) of the Child Protection Law (2014) defines sexual abuse as any sexual assault, harm, or exploitation (Kingdom of Saudi Arabia, 2014). Article 3(7) of the Child Protection Law (2014) treats sexual harassment or exploitation as abuse; Article 3(10) treats obscene or age-inappropriate behavior as abuse; and Article 9 prohibits sexual exploitation of children (Kingdom of Saudi Arabia, 2014). Article 1(9) of Executive Regulations (2023) defines sexual exploitation as prostitution or unlawful sexual acts involving a child (with or without consent) (Ministry of Human Resources and Social Development, 2023). Article 1(30) of Executive Regulations (2023) defines sexual harassment as sexual activities and exposure/production/ distribution of pornographic materials (Ministry of Human Resources and Social Development, 2023). Article 3(7) of Executive Regulations (2023) classifies sexual exploitation or harassment as child abuse or neglect, whereas Article 3(13) requires authorities to make arrangements to protect children from sexual exploitation (Ministry of Human Resources and Social Development, 2023). Article 3(2) of the Anti-Cyber Crime Law (2007) contains provisions to protect against threats or blackmail (including sextortion) via unlawful computer access and imposes up to 1 year imprisonment and/or a SAR 500,000 fine (Kingdom of Saudi Arabia, 2007). Article 6(3) of the Anti-Cyber Crime Law (2007) prohibits preparing, publishing or promoting pornographic materials and imposes up to 5 years imprisonment and/or a SAR 3 million fine (Kingdom of Saudi Arabia, 2007). Article 8(3) of the Anti-Cyber Crime Law (2007) requires at least half the maximum punishment when minors are lured or exploited (e.g., sexually) using cybercrimes (Kingdom of Saudi Arabia, 2007). Article 1 of the Anti-Harassment Law (2018) defines sexual harassment through any means, including modern technology, whereas Article 6(2)(a) provides imprisonment of up to 5 years and/or a fine of 300,000 when the victim is a child (SaudiPedia, 2023).

Saudi legal framework regarding digital sexual abuse of children covers several issues identified in the literature, such as sexual exploitation, harassment, sextortion, luring minors, pornographic materials, etc. (Fry et al., 2025; Whittle et al., 2013). Literature also identifies image-based sexual abuse, which is covered by the Saudi legal framework through protection against pornographic materials abuse (Finkelhor et al., 2023). The literature identifies issues such as online grooming and image manipulation (Finkelhor et al., 2023; Whittle et al., 2013) that may not be specifically covered in the Saudi legal framework, although broader protections in the legal framework apply in such cases. Broadly, the protections available in the Saudi legal framework correspond with the forms of digital sexual abuse identified in the literature related to Saudi Arabia (Al Ghamdi, 2025; Naji, 2025).

Privacy Child Abuse

The Anti-Cyber Crime Law (2007) and the Personal Data Protection Law (2021) collectively aim to prevent the digital abuse of children's privacy (Table 1). Article 3(1) of the Anti-Cyber Crime Law (2007) imposes up to 1 year imprisonment and/or a SAR 500,000 fine for unauthorized data

interception of people (including children); Article 5(1) imposes up to 4 years imprisonment and/or a SAR 3 million fine for unauthorized access related to leakage or redistribution of private data; whereas Article 6(1) imposes up to 5 years imprisonment and/or a SAR 3 million fine for producing, transmitting, or storing digital materials that infringes privacy of people (including children) (Kingdom of Saudi Arabia, 2007). Article 5 of the Personal Data Protection Law (2021) requires consent (including legal guardians) for processing personal data; Article 10 requires the personal data to be used only for the stated purpose; Article 11 prevents unnecessary, unauthorized, and excessive data collection (especially private); whereas Article 15 prevents unauthorized disclosure or sharing of personal data (Kingdom of Saudi Arabia, 2021).

Saudi legal framework regarding digital privacy abuse of children covers several issues identified in the literature, such as unauthorized access, collection, use, disclosure, and distribution of personal data (Alashwali & Alashwali, 2022; Stoilova et al., 2021). The literature also identifies issues such as misuse of children's photos/videos and unauthorized tracking by digital means (Alashwali & Alashwali, 2022; Bunn, 2021), which may not always be expressly identified as privacy abuses in the Saudi legal framework; however, broader privacy and data protection protections apply in such cases. Broadly, the protections available in the Saudi legal framework align with the forms of digital privacy abuse identified in the literature related to Saudi Arabia (Alashwali & Alashwali, 2022; Alqahtani et al., 2017).

Table 1: Legal Protections against Digital Abuse of Children in Saudi Arabia

Form of Digital Abuse	Law / Regulation	Specific Provision and Legal Effect
Psychological	Child Protection Law (2014)	Art. 1(2): Defines psychological abuse.
		Art. 3(9): Humiliating or degrading language.
		Art. 3(14): Threats to psychological well-being.
		Art. 6: Protection from all forms of abuse.
	Executive Regulations (2023)	Art. 1(6): Defines threats of harm.
		Art. 3.15: Repeated verbal or psychological abuse.
		Art. 3.16: Harmful or age-inappropriate material.
Sexual	Anti-Cyber Crime Law (2007)	Art. 3(2): Threats or blackmail after unauthorized access (up to 1 year/SAR 500,000).
		Art. 3(5): Online defamation or harm (up to 1 year/SAR 500,000).
		Art. 1(2): Defines sexual abuse.
Sexual	Child Protection Law (2014)	Art. 3(7): Sexual harassment or exploitation.

Form of Digital Abuse	Law / Regulation	Specific Provision and Legal Effect
		Art. 3(10): Obscene or age-inappropriate scenes.
		Art. 9: Prohibits sexual exploitation.
	Executive Regulations (2023)	Art. 1(9): Defines sexual exploitation.
		Art. 1(30): Defines sexual harassment and pornographic use of children.
		Art. 3(7): Sexual exploitation/harassment as abuse/neglect.
		Art. 3(13): Requires authorities to protect children from sexual exploitation.
	Anti-Cyber Crime Law (2007)	Art. 3(2): Threats or blackmail (up to 1 year/SAR 500,000).
		Art. 6(3): Pornographic material (up to 5 years/SAR 3 million).
		Art. 8(3): Luring or exploiting minors (at least half the maximum prison term and fine).
	Anti-Harassment Law (2018)	Art. 1: Defines harassment through modern technology.
		Art. 6(2)(a): Child victim (up to 5 years/SAR 300,000).
Privacy	Anti-Cyber Crime Law (2007)	Art. 3(1): Unauthorized data interception (up to 1 year/SAR 500,000).
		Art. 3(4): Camera-based privacy invasion (up to 1 year/SAR 500,000).
		Art. 5(1): Leakage or redistribution of private data (up to 4 years/SAR 3 million).
		Art. 6(1): Digital material infringing privacy (up to 5 years/SAR 3 million).
	Personal Data Protection Law (2021)	Art. 5: Consent for processing.
		Art. 10: Collection and purpose limitations.
		Art. 11: Lawful and minimum-necessary collection.
		Art. 15: Restrictions on data disclosure.

Enforcement Mechanisms for Digital Child Protection

This section addresses RQ2 by examining the enforcement mechanisms that support the implementation of the legal framework for child protection against digital abuse in Saudi Arabia. Table 2 presents the enforcement mechanisms, legal/ institutional basis, and the purpose served.

Article 22 of the Child Protection Law (2014) requires anyone aware of child abuse/ neglect to report it. It also requires the authorities to facilitate the reporting of child abuse, especially by children (Kingdom of Saudi Arabia, 2014). Article 23 of the Child Protection Law (2014) contains provisions for investigating child abuse cases, prosecution by the competent authorities, and criminal penalties through court action (Kingdom of Saudi Arabia, 2014). MHRSD helpline number 1919 serves as a formal reporting channel for receiving child abuse cases and their referral to competent authorities (Ministry of Human Resources and Social Development, 2026). Article 22 of the Executive Regulations (2023) contains provisions for receiving, assessing, referring, and handling child abuse reports (Ministry of Human Resources and Social Development, 2023). The subsections under Article 22 depict provisions as: 22(7) deals with receiving and assessing reports; 22(8) deals with referring reports to the social protection units; 22(16) deals with assessment of the seriousness of child abuse cases and handling them; and 22(17) to 22(19) deal with protection, counselling, treatment, and rehabilitation of child abuse cases. NFSP child helpline number 116111 provides advice, support, and referral to relevant authorities for children who are victims of abuse (such as digital abuse) (Saudi Press Agency, 2022).

Table 2. Enforcement Mechanisms for Digital Child Protection in Saudi Arabia

Enforcement Mechanism	Basis	Purpose
Abuse Reporting Duty	Child Protection Law (2014), Art. 22	Requires reporting of child abuse by anyone aware; facilitates reporting by children
Investigation and Prosecution	Child Protection Law (2014), Art. 23	Requires investigation of violations, prosecution, and criminal penalties.
MHRSD Reporting Channel	Helpline 1919	Receives abuse reports, assesses cases, and refers them to relevant authorities.
Handling of Reports	Executive Regulations (2023)	Provides procedures for receiving, assessing, referring, and handling child abuse reports.
NFSP Child Helpline	Helpline 116111	Provides children with advice, support, and referral to relevant authorities.

CONCLUSIONS AND RECOMMENDATIONS

This research investigated the extant legal protection framework in Saudi Arabia to protect children from digital abuse (psychological, sexual, and privacy) (RQ1). The research also examined the enforcement mechanisms in Saudi Arabia that support the implementation of the legal framework for child protection against digital abuse (RQ2). To systematically address the research questions, the study employed a doctrinal legal approach (Hutchinson & Duncan, 2012; McConville & Chui, 2017) and examined Saudi laws, regulations, and related enforcement mechanisms for the protection of children.

To answer RQ1, the legal framework examined in the study includes the Child Protection Law (2014), Executive Regulations (2023) under the Child Protection Law, the Anti-Cyber Crime Law (2007), the Anti-Harassment Law (2018), and the Personal Data Protection Law (2021). These laws and regulations collectively endeavor to protect children from digital abuse (psychological, sexual, and privacy). Specifically, the Child Protection Law (2014), its Executive Regulations (2023), and the Anti-Cyber Crime Law (2007) contain provisions to protect children from digital psychological abuse. The Child Protection Law (2014), its Executive Regulations (2023), the Anti-Cyber Crime Law (2007), and the Anti-Harassment Law (2018) contain provisions to protect children from digital sexual abuse. The Anti-Cyber Crime Law (2007) and the Personal Data Protection Law (2021) collectively endeavor to protect children from digital privacy abuse. These laws and regulations contain both protective and penal provisions (including fines and imprisonment) to prevent the digital abuse of children in Saudi Arabia.

To answer RQ2, the enforcement mechanisms examined in the study include the Child Protection Law (2014), Executive Regulations (2023) under the Child Protection Law, MHRSD helpline 1919, and NFSP child helpline 116111. Collectively, these legal and institutional enforcement mechanisms help in the reporting, investigation, prosecution, case handling, and supporting victims of digital child abuse.

The study shows that Saudi Arabia has a comprehensive legal framework (rather than a single law) that endeavors to protect children against digital abuse. This legal and institutional framework consists of laws, regulations, and helplines to protect children. The framework also seeks to punish violators through fines and/or imprisonment to enforce criminal accountability. Thus, the framework contains provisions that address two important dimensions: prevention/protection and legal/criminal accountability. Furthermore, the framework covers various forms of digital child abuse in Saudi Arabia, such as psychological, sexual, and privacy abuse. The laws, regulations, and enforcement mechanisms under the Saudi legal framework complement each other in addressing digital child abuse. Together, they provide a multi-layered legal and institutional response in Saudi Arabia for protecting children from abuse in the digital world. This study offers practical implications by consolidating various legal and institutional mechanisms, which can help policymakers, child-protection authorities, and relevant stakeholders better understand and apply the mechanisms for preventing, reporting, and addressing digital child abuse in Saudi Arabia.

This research is limited to a doctrinal legal examination of relevant Saudi laws, regulations, and institutional mechanisms dealing with digital child abuse (psychological, sexual, and privacy). Future research can empirically examine the effectiveness of these Saudi legal and institutional mechanisms in real-world settings. Future research can also assess the efficacy of the legal and institutional mechanisms by examining real-world cases and experiences of victims of digital child abuse in Saudi Arabia. In addition, future research can assess how the Saudi legal protection and enforcement framework for digital child abuse compares with those of other nations.

REFERENCES

- Al Faryan, N., Frederico, M., & Young, J. (2019). Listening to child protection workers in Saudi Arabia: Child protection workers speak of how they experienced the policies and programs introduced to protect children between 2010 and 2013. *International Social Work*, 62(2), 768–783. <https://doi.org/10.1177/0020872817742695>
- Al Ghamdi, A. (2025). Online safety challenges: Saudi children and parents' perspectives on risks and harms. *Social Sciences*, 14(9), 551. <https://doi.org/10.3390/socsci14090551>
- Alashwali, E., & Alashwali, F. (2022). Saudi parents' privacy concerns about their children's smart device applications. *International Journal of Child-Computer Interaction*, 33, 100486. <https://doi.org/10.1016/j.ijcci.2022.100486>
- Al-Eissa, M. A. (2019). Utilization of child helpline (CHL) among adolescents in Saudi Arabia: Results from a national survey. *Child & Family Social Work*, 24(1), 84–89. <https://doi.org/10.1111/cfs.12584>
- Al-Eissa, M. A., ElChoueiry, N., AlBuhairan, F., Saleheen, H. N., & Almuneef, M. A. (2018). Child maltreatment prevention strategies: Saudi youth perspectives. *International Journal of Pediatrics and Adolescent Medicine*, 5(3), 92–98. <https://doi.org/10.1016/j.ijpam.2018.06.002>
- Alfakeh, S. A., Alghamdi, A. A., Kouzaba, K. A., Altaifi, M. I., Abu-Alamah, S. D., & Salamah, M. M. (2021). Parents' perception of cyberbullying of their children in Saudi Arabia. *Journal of Family and Community Medicine*, 28(2), 117–124. https://doi.org/10.4103/jfcm.JFCM_516_20
- Alhamad, I. A., & Singh, H. P. (2022). Digital technologies and information translucence in healthcare management: An institutional theory perspective for adopting electronic incidence reporting systems. *Amazonia Investiga*, 11(57), 30–38. <https://doi.org/10.34069/AI/2022.57.09.3>
- Almuneef, M. A., Aljaber, A., Althunayan, F., Abalkhail, A., Alanazi, A., Alqahtani, B., Abed, S., Alharbi, D., Ureeg, A., Alqanatish, J., & Almutairi, A. (2026). Impact of child-protection law on child maltreatment reporting: A comparison of pre- and postlaw data from a hospital registry. *Journal of Family & Community Medicine*, 33(3). https://doi.org/10.4103/jfcm.jfcm_32_26
- Al-Naim, A. B., & Hasan, M. M. (2018). Investigating Saudi parents' intention to adopt technical mediation tools to regulate children's internet usage. *International Journal of Advanced Computer Science and Applications*, 9(5), 456–464. <https://doi.org/10.14569/IJACSA.2018.090560>
- Alqahtani, N., Furnell, S., Atkinson, S., & Stengel, I. (2017). Internet risks for children: Parents' perceptions and attitudes: An investigative study of the Saudi context. 2017 *Internet Technologies and Applications*. <https://doi.org/10.1109/ITECHA.2017.8101918>
- Alshammari, T. S., & Singh, H. P. (2018). Preparedness of Saudi Arabia to defend against cyber crimes: An assessment with reference to Anti-Cyber Crime Law and GCI Index. *Archives of Business Research*, 6(12), 131–146. <https://doi.org/10.14738/abr.612.5771>

- Bamashmoos, A. M. (2024). Consent requirements and limitations in Saudi Arabia's Personal Data Protection Law: An in-depth analysis. *Taibah University Journal of Law*, 3(5), 16–43. <https://www.taibahu.edu.sa/sites/default/files/2025-07/Protection%20Law%2C%20An%20In-depth%20Analysis%2C%20Dr.%20Ahmed%20M.%20Bamashmoos.pdf>
- Bunn, A. (2021). Unwanted distribution of children's images and the right to development. *The Modern Law Review*, 84(2), 334–370. <https://doi.org/10.1111/1468-2230.12590>
- Finkelhor, D., Turner, H., Colburn, D., Mitchell, K., & Mathews, B. (2023). Child sexual abuse images and youth produced images: The varieties of image-based sexual exploitation and abuse of children. *Child Abuse & Neglect*, 143, 106269. <https://doi.org/10.1016/j.chiabu.2023.106269>
- Fry, D., Krzeczowska, A., Ren, J., Lu, M., Fang, X., & Into the Light Index Study Group. (2025). Prevalence estimates and nature of online child sexual exploitation and abuse: A systematic review and meta-analysis. *The Lancet Child & Adolescent Health*, 9(3), 184–193. [https://doi.org/10.1016/S2352-4642\(24\)00329-8](https://doi.org/10.1016/S2352-4642(24)00329-8)
- Gohal, G., Alqassim, A., Eltyeb, E., Rayyani, A., Hakami, B., Al Faqih, A., Hakami, A., Qadri, A., & Mahfouz, M. (2023). Prevalence and related risks of cyberbullying and its effects on adolescent. *BMC Psychiatry*, 23(1), 39. <https://doi.org/10.1186/s12888-023-04542-0>
- Hamm, M. P., Newton, A. S., Chisholm, A., Shulhan, J., Milne, A., Sundar, P., Ennis, H., Scott, S. D., & Hartling, L. (2015). Prevalence and effect of cyberbullying on children and young people: A scoping review of social media studies. *JAMA Pediatrics*, 169(8), 770–777. <https://doi.org/10.1001/jamapediatrics.2015.0944>
- Hu, Y., Bai, Y., Pan, Y., & Li, S. (2021). Cyberbullying victimization and depression among adolescents: A meta-analysis. *Psychiatry Research*, 305, 114198. <https://doi.org/10.1016/j.psychres.2021.114198>
- Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. *Deakin Law Review*, 17(1), 83–119. <https://doi.org/10.21153/dlr2012vol17no1art70>
- Kingdom of Saudi Arabia. (2007). Anti-Cyber Crime Law (Royal Decree No. M/17). Bureau of Experts at the Council of Ministers. <https://www.wipo.int/wipolex/en/legislation/details/14570>
- Kingdom of Saudi Arabia. (2014). Child Protection Law (Royal Decree No. M/14). Ministry of Human Resources and Social Development. <https://www.hrsd.gov.sa/sites/default/files/2024-10/Child%20Protection%20Law.pdf>
- Kingdom of Saudi Arabia. (2021). Personal Data Protection Law (Royal Decree No. M/19; amended by Royal Decree No. M/148 in 2023). Saudi Data & AI Authority. <https://sdaia.gov.sa/en/SDAIA/about/Pages/RegulationsAndPolicies.aspx>
- Lee, J., Choo, H., Zhang, Y., Cheung, H. S., Zhang, Q., & Ang, R. P. (2026). Cyberbullying victimization and mental health symptoms among children and adolescents: A meta-analysis of longitudinal studies. *Trauma, Violence, & Abuse*, 27(2), 391–406. <https://doi.org/10.1177/15248380241313051>

- Li, J., & Hesketh, T. (2021). Experiences and perspectives of traditional bullying and cyberbullying among adolescents in mainland China: Implications for policy. *Frontiers in Psychology*, 12, 672223. <https://doi.org/10.3389/fpsyg.2021.672223>
- McConville, M., & Chui, W. H. (Eds.). (2017). *Research methods for law* (2nd ed.). Edinburgh University Press. <https://doi.org/10.1515/9781474404259>
- Ministry of Human Resources and Social Development. (2023). Executive Regulations of the Child Protection Law [Arabic]. <https://www.hrsd.gov.sa/en/knowledge-centre/decisions-and-regulations/regulation-and-procedures/720527>
- Ministry of Human Resources and Social Development. (2026). General Department for Protection from Domestic Violence and Child Protection [Arabic]. <https://www.hrsd.gov.sa/ministry/about-ministry/about-us/ministry-sectors/767581>
- Naji, I. M. A. (2025). The Legislative Confrontation of the Minors' Harassment Crime Through Electronic Means. *Arab Journal for Security Studies*, 41(1), 66–77. <https://doi.org/10.26735/tuka9433>
- Nusairat, W. M. (2023). Criminal responsibility for sexual exploitation of children via electronic means of communication considering Saudi Arabia's Anti-Cyber Crime Law. *Russian Law Journal*, 11(2). <https://doi.org/10.52783/rj.v11i2.523>
- Odgers, C. L., & Jensen, M. R. (2020). Annual Research Review: Adolescent mental health in the digital age: facts, fears, and future directions. *Journal of Child Psychology and Psychiatry*, 61(3), 336–348. <https://doi.org/10.1111/jcpp.13190>
- Owaidah, S. F., Alharaz, R. I., Aljubran, S. H., Almuhan, Z. Y., & Menezes, R. G. (2022). Factors affecting reporting of suspected child maltreatment in Saudi Arabia. *Journal of Forensic and Legal Medicine*, 89, 102371. <https://doi.org/10.1016/j.jflm.2022.102371>
- Page, S., McFeeters, A., Mat Rani, S., Slater, C., Fry, D., Stevenson, J., & Quayle, E. (2025). Psychological and emotional harms of online child sexual exploitation and abuse in children under the age of 18: A systematic review of the evidence. *Child Abuse Review*, 34(4), e70048. <https://doi.org/10.1002/car.70048>
- Pandey, U. S., Kumar, V., & Singh, H. P. (2017). *Cyber crimes and laws*. Himalaya Publishing House.
- Salam, A. A. (2023). Ageing in Saudi Arabia: new dimensions and intervention strategies. *Scientific Reports*, 13(1), 4035. <https://doi.org/10.1038/s41598-022-25639-8>
- Saudi Press Agency. (2022). National Family Safety Program launches the annual campaign to introduce the Child Helpline [Arabic]. <https://www.spa.gov.sa/2328960>
- Saudipedia. (2023). Anti-Harassment Law in Saudi Arabia. <https://saudipedia.com/en/anti-harassment-law-in-saudi-arabia>
- Singh, H. P. (2016). E-commerce security: Legal and policy aspects of technology solutions in India. *Mumukshu Journal of Humanities*, 8(1), 1–7.
- Singh, H. P. (2017). Strategic Analysis and Security Issues of Social Media Services: A Study of Facebook. *International Journal of Information Movement*, 2(5), 134–139.
- Singh, H. P. (2018). Data protection and privacy legal-policy framework in India: A comparative study vis-à-vis China and Australia. *Amity Journal of Computational Sciences*, 2(2), 24–29. <https://www.amity.edu/ajcs/current-issue.aspx>

- Singh, H. P., & Alshammari, T. S. (2020). An institutional theory perspective on developing a cyber security legal framework: A case of Saudi Arabia. *Beijing Law Review*, 11(3), 637–650. <https://doi.org/10.4236/blr.2020.113039>
- Stoilova, M., Nandagiri, R., & Livingstone, S. (2021). Children’s understanding of personal data and privacy online – a systematic evidence mapping. *Information Communication & Society*, 24(4), 557–575. <https://doi.org/10.1080/1369118x.2019.1657164>
- Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of online grooming: Characteristics and concerns. *Aggression and Violent Behavior*, 18(1), 62–70. <https://doi.org/10.1016/j.avb.2012.09.003>
- Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying among adolescents and children: A comprehensive review of the global situation, risk factors, and preventive measures. *Frontiers in Public Health*, 9, 634909. <https://doi.org/10.3389/fpubh.2021.634909>