1. THEORY OF LAW AND THE TRANSFORMATION OF THE LEGAL SYSTEM IN THE DIGITAL SOCIETY

UDC: 004.738.5: 316.63-053.6
DOI: 10.5937/PDSC26001P

Milan Počuča, PhD, Full Professor
Faculty of Law for Commerce and Judiciary in Novi Sad,
University Business Academy in Novi Sad,
Rector of the University Business Academy in Novi Sad
email: pocuca@pravni-fakultet.info

Dalibor Krstinić, PhD, Associate Professor
Faculty of Law for Commerce and Judiciary in Novi Sad,
University Business Academy in Novi Sad,
email: dkrstinic@pravni-fakultet.info

DIGITAL VIOLENCE AGAINST CHILDREN AND ADOLESCENTS: CIVIL-LAW AND FAMILY-LAW PROTECTION IN THE DIGITAL SOCIETY

Abstract: The development of digital technologies and the increasingly intensive presence of children in the digital space have led to the emergence of new forms of endangerment of their rights, safety and dignity. Digital violence against children includes various forms of unlawful conduct, such as insults, harassment, threats, unauthorized publication of photographs and video recordings, misuse of personal data, exclusion from digital communities, dissemination of false content, as well as other forms of violation of a child's privacy, honour and reputation. A particular problem lies in the fact that the consequences of digital violence often go beyond the boundaries of the virtual space, leaving long-term psychological, social and legal consequences for the child. The subject of this paper is the analysis of digital violence against children from the perspective of civil law and family law protection, with special reference to the protection of the right to privacy, dignity, honour, reputation, personal identity and the best interests of the child. The aim of the paper is to point out the need to adapt traditional legal institutes to new forms of violations arising in the digital environment. The paper will consider possible mechanisms for the protection of the child, including the prohibition of further harmful actions, removal of disputed content, compensation for pecuniary and non-pecuniary damage, as well as

the responsibility of parents, schools, digital platforms and other entities that may play a significant role in prevention and protection. The paper proceeds from the assumption that digital violence against children is not merely a technical or security-related issue, but a serious legal challenge requiring coordinated action within family, civil, educational and digital law. Contemporary law must ensure effective protection of the child in the digital space, while preserving the balance between freedom of expression, the right to privacy, parental responsibility and the principle of the best interests of the child.

Keywords: *digital violence, children, digital space, civil-law protection, family-law protection, right to privacy, best interests of the child, compensation for damage*

1. INTRODUCTION

The rapid development of digital technologies has fundamentally changed the social environment in which children and adolescents grow up. Communication, education, entertainment and social participation increasingly take place through digital platforms, social networks, messaging applications and other forms of electronic communication. Digital space has therefore become a real social space in which children create relationships, express identity and exercise many aspects of their personality. At the same time, it has become an environment in which new forms of risk, harm and violence may arise (UNICEF, 2017; Livingstone & Third, 2017).

Unlike traditional forms of violence, digital violence is not limited by the physical presence of the perpetrator and the victim. It may occur at any time, spread rapidly to a large number of users, remain permanently available through digital traces and affect the child even after the initial harmful act has ceased. A humiliating photograph, a threatening message, the publication of personal data or a defamatory post may be multiplied, stored and redistributed in a way that makes the consequences more intense and more difficult to control. Contemporary typologies of online risks show that risks for children appear in the domains of content, contact, conduct and commercial environment, and that these risks often overlap (OECD, 2021).

The legal relevance of this issue arises from the fact that digital violence often affects several legally protected values at the same time: privacy, honour, reputation, dignity, psychological integrity, personal identity, security and the best interests of the child. In certain cases, the same conduct may have civil-law, family-law, misdemeanour, criminal-law, educational and data-protection consequences. Constitutional guarantees of human dignity, psychological integrity and privacy therefore represent the initial national framework for interpreting this phenomenon (Ustav Republike Srbije, 2006).

The subject of this paper is the analysis of digital violence against children and adolescents from the perspective of civil-law and family-law protection. The paper starts from the assumption that existing legal institutes, such as the protection of personality rights, prohibition of harmful conduct, removal of harmful content, compensation for pecuniary and non-pecuniary damage and parental responsibility, remain relevant in the digital environment. However, their application must be interpreted in the light of the specific characteristics of online communication, platform governance and the best interests of the child.

The aim of the paper is to indicate the need for a coordinated legal approach that connects traditional civil and family-law mechanisms with contemporary standards of child protection in the digital society. The paper also points to the importance of the responsibility of parents, schools, digital platforms and public authorities. In methodological terms, the paper relies on normative analysis, comparative insights from European and international standards and an assessment of the practical challenges that arise when legal protection is sought in digital space.

2. CONCEPT AND FORMS OF DIGITAL VIOLENCE AGAINST CHILDREN AND ADOLESCENTS

Digital violence against children may be broadly understood as any unlawful or harmful conduct carried out through digital technologies that violates or endangers the rights, safety, dignity, privacy or development of a child. Such an approach is consistent with the contemporary international understanding that children's rights must be effectively respected, protected and fulfilled also in the digital environment (UN Committee on the Rights of the Child, 2021; Council of Europe, 2018).

The most frequent forms include insults, ridicule, harassment, threats, humiliation, exclusion from digital groups, spreading rumours, publication of private photographs or videos, misuse of personal data, impersonation,

creation of fake profiles, digital stalking and pressure, as well as different forms of sexualised or discriminatory harassment. Research on children's data and online privacy shows that children often do not have full awareness of the scope, permanence and later use of the data they leave in the digital environment (Livingstone, Stoilova & Nandagiri, 2019).

A specific feature of digital violence is the potential permanence of harmful content. In the physical world, a harmful act may be limited by time and space; in the digital world, content can be copied, archived, reposted and algorithmically amplified. This creates a particular problem for legal protection because the removal of the original content does not necessarily eliminate the harm. The same content may reappear on another platform, in another group or under another profile, which requires a flexible and continuous response.

Another important characteristic is the visibility and audience of the harmful act. Humiliation in front of a small peer group has a different psychological and social effect than humiliation before hundreds or thousands of users. Digital violence is often intensified by comments, sharing and reactions of third persons who may not have initiated the harm but contribute to its spread. This raises the question of secondary responsibility and the duty of platforms, schools and parents to react when they become aware of the harmful conduct.

Digital violence also affects the child's personal identity. Children and adolescents increasingly construct their social identity through online profiles, photographs, posts and interactions. Harmful conduct in this sphere may therefore affect not only reputation but also self-perception, belonging and social development. In this sense, the protection of a child in digital space must include not only protection from physical danger but also protection of dignity, privacy, emotional development and personal autonomy.

Legal classification of digital violence is complicated by the fact that the same act may simultaneously represent a violation of personality rights, an unlawful processing of personal data, discrimination, harassment, peer violence, domestic violence, a criminal offence or a breach of platform rules. The legal response must therefore be interdisciplinary. Civil-law protection is necessary because it provides remedies for the violation of subjective rights and compensation for harm. Family-law protection is necessary because it places the child's best interests, parental responsibility and institutional duties at the centre of the response.

The legal qualification of digital violence is complex because the same conduct may simultaneously represent a violation of personality rights, an

unlawful processing of personal data, discrimination, harassment, peer violence, domestic violence, a criminal offence or a breach of platform rules. In this sense, the protection of the child requires a combined interpretation of general rules on the prohibition of discrimination and special rules on the protection of personal data (Zakon o zabrani diskriminacije, 2009; Zakon o zaštiti podataka o ličnosti, 2018).

3. INTERNATIONAL, EUROPEAN AND NATIONAL LEGAL FRAMEWORK

The protection of children in the digital environment must be interpreted within the wider framework of international, European and national legal standards. The Convention on the Rights of the Child represents the central international instrument for the protection of children. Its principles, especially the best interests of the child, the right to development, the right to protection from violence, the right to privacy and the right of the child to be heard, are equally applicable in digital space (UN General Assembly, 1989; UN Committee on the Rights of the Child, 2021).

The right to respect for private and family life, protected by Article 8 of the European Convention on Human Rights, is also highly relevant. The digital publication of photographs, personal information, intimate content or defamatory statements may interfere with privacy, dignity and reputation. At the same time, the protection must be viewed through the European standard of private life (Convention for the Protection of Human Rights and Fundamental Freedoms, 1950).

At the level of the European Union, the General Data Protection Regulation established important standards concerning the processing of personal data, including the data of children. The GDPR recognises that children merit specific protection with regard to their personal data, especially because they may be less aware of the risks, consequences and their rights in relation to data processing (Regulation (EU) 2016/679, 2016).

The European Commission's guidelines on the protection of minors under the Digital Services Act additionally point to the need for platform measures that protect minors from risks such as cyberbullying, grooming, harmful content, manipulative design and inadequate use of data. These guidelines should be read together with the obligation of online platforms to ensure a high level of privacy, safety and security for minors (Regulation (EU) 2022/2065, 2022; European Commission, 2025).

In the Republic of Serbia, the legal framework relevant to digital violence against children is dispersed across several branches of law. The

Constitution of the Republic of Serbia guarantees human dignity, inviolability of physical and psychological integrity, protection of personal data and special protection of children. The Family Law regulates the relationship between children and parents, parental rights, protection measures and the principle of the best interests of the child, while the Law on the Foundations of the Education System provides the framework for the conduct of educational institutions in the protection of pupils (Ustav Republike Srbije, 2006; Porodični zakon, 2005; Zakon o osnovama sistema obrazovanja i vaspitanja, 2017).

The existence of several legal sources is not in itself a weakness. However, in practice it may produce uncertainty regarding jurisdiction, procedure, urgency and the most appropriate remedy. For this reason, it is important to develop a coherent interpretation of civil-law and family-law mechanisms applicable to digital violence. Such an interpretation should make it possible to protect the child quickly, to remove or limit the harmful consequences and to determine responsibility where the harmful conduct has caused

4. CIVIL-LAW PROTECTION OF THE CHILD IN DIGITAL SPACE

Civil-law protection has a central role in cases in which digital violence violates subjective rights of the child or causes pecuniary or non-pecuniary damage. The most important protected values are privacy, honour, reputation, dignity, psychological integrity, personal identity and the right to personal development. General rules on liability for damage enable compensation even where the damage is manifested in the non-pecuniary sphere (Zakon o obligacionim odnosima, 1978).

The first group of civil-law remedies concerns the cessation and prevention of harmful conduct. A child, through parents or legal representatives, should be able to request the prohibition of further publication, the cessation of harassment, the removal of harmful content and measures preventing repeated violation. These remedies are especially important because the main goal in cases of digital violence is often not only compensation after the harm has occurred, but the urgent interruption of the harmful digital chain.

The second group of remedies concerns compensation for damage. Digital violence may cause pecuniary damage, for example costs of psychological treatment, legal assistance, change of school or other necessary measures. More often, however, it causes non-pecuniary damage in the form of mental suffering, fear, humiliation, violation of honour and

reputation, loss of a sense of security and consequences for psychological development. The assessment of such harm must take into account the age of the child, the intensity and duration of exposure, the size of the audience, the possibility of content removal and the psychological consequences established in the specific case (Zakon o obligacionim odnosima, 1978; UNICEF, 2021).

A special issue is causation. In digital violence cases, harm may result from the initial act and from subsequent sharing by third persons. Courts and other competent bodies may therefore face the question whether the original perpetrator is responsible for all consequences or only for those that were foreseeable. Since digital dissemination is a typical and foreseeable feature of online communication, it may be argued that a person who unlawfully publishes harmful content about a child must bear responsibility for the ordinary consequences of such publication, including the foreseeable spread of the content.

The question of consent is also significant. Children may not fully understand the long-term effects of publishing personal data, photographs or private information. Even when a child has shared certain content with a limited group, this does not mean that third persons may freely redistribute it. The child's consent must be assessed in the light of age, maturity, circumstances and the best interests of the child, as well as in the light of the rules on personal data protection (Zakon o zaštiti podataka o ličnosti, 2018; Regulation (EU) 2016/679, 2016).

Civil-law protection must also consider the role of digital platforms. Platforms may not always be the direct perpetrators of violence, but they often control the technical environment in which harm is created, amplified and maintained. Notice-and-action procedures, content removal, account suspension, preservation of evidence and transparency of moderation decisions may therefore be of direct importance for the effectiveness of civil protection. The use of alternative regulatory instruments and platform duties has long been emphasised as an important part of child protection in the digital era (Lievens, 2010; Regulation (EU) 2022/2065, 2022).

Finally, civil-law protection should not be limited to litigation. Mediation, school procedures, platform reporting mechanisms and cooperation with child protection services may have practical value. However, alternative mechanisms must not replace judicial protection when the rights of the child have been seriously violated. The effectiveness of protection depends on the possibility to combine urgent removal of harm with subsequent determination of responsibility and compensation.

5. FAMILY-LAW PROTECTION, PARENTAL RESPONSIBILITY AND THE BEST INTERESTS OF THE CHILD

Family law provides the normative framework within which the child is understood not only as a holder of rights but also as a person in need of special care, guidance and protection. In cases of digital violence, the principle of the best interests of the child must be the primary criterion for choosing legal and practical measures. The aim is not only to sanction harmful conduct but also to restore the child's sense of security, protect development and prevent repeated victimisation (Porodični zakon, 2005; Šarkić & Počuča, 2020).

Parental responsibility is of particular importance. Parents have the duty to protect the child, to care for the child's development and to guide the child in the use of digital technologies. This duty does not mean total control of the child's private communication, because children also have a right to privacy and gradual autonomy. It means reasonable guidance, conversation, prevention of risks and timely reaction when the child is exposed to harm (Porodični zakon, 2005; Council of Europe, 2018).

At the same time, parents themselves may sometimes be a source of risk. The excessive publication of photographs, videos and personal information about children by parents, often described as "sharenting", may violate the child's privacy and dignity. Although such behaviour is not always violent, it may create conditions for later misuse of data and images. Family-law analysis must therefore recognise that the best interests of the child may limit parental freedom to publish content about the child. The child is not an object of parental representation in digital space, but a holder of personality rights.

Schools also have an important role because many cases of digital violence arise from peer relations connected with the school environment. Even when the harmful act occurs outside school premises and outside school hours, its effects may be visible in the classroom, in peer groups and in the child's educational process. Therefore, school procedures should not be limited to incidents that physically occur at school. If the digital violence substantially affects the safety, dignity or position of a pupil, the school must have mechanisms for support, prevention and cooperation with parents and competent services (Zakon o osnovama sistema obrazovanja i vaspitanja, 2017).

The family-law approach must avoid two extremes. The first is to trivialise digital violence as ordinary child conflict. The second is to respond only through punitive mechanisms without supporting the child and

addressing the relational context in which the harm occurred. In many cases, especially where peer relations or family relations are involved, protection requires a combination of legal, educational, psychological and social measures. Where the violence is connected with family relations or domestic circumstances, the rules on the prevention of domestic violence may also be relevant (Porodični zakon, 2005; Zakon o sprečavanju nasilja u porodici, 2016).

The best interests of the child also require protection of the child during the legal procedure itself. Public exposure, repeated questioning, unnecessary disclosure of private details and slow procedures may deepen the harm. Therefore, proceedings concerning digital violence against children should be conducted with particular attention to confidentiality, urgency and child-sensitive communication. The legal system must protect the child from the harmful act and from secondary victimisation.

6. RESPONSIBILITY OF DIGITAL PLATFORMS AND OTHER ACTORS IN THE DIGITAL SOCIETY

Digital violence cannot be effectively addressed without considering the responsibility of digital platforms and other actors that shape the online environment. Platforms provide the infrastructure for communication, visibility, algorithmic distribution and content moderation. Their design choices influence whether harmful content remains marginal or becomes widely visible. Therefore, the protection of children in digital space requires more than the removal of individual posts after damage has occurred. It requires systematic attention to safety by design, transparency and effective reporting mechanisms (Lievens, 2010; Regulation (EU) 2022/2065, 2022).

The responsibility of platforms can be understood through several duties. First, platforms should provide clear and accessible reporting mechanisms suitable for children and parents. If the reporting procedure is complicated, slow or unavailable in the language understood by the user, protection becomes ineffective. Second, platforms should react promptly to content that violates the rights and safety of children. Third, they should preserve relevant evidence when necessary for legal protection, while respecting data-protection rules. Fourth, they should design services in a way that reduces foreseeable risks to minors, including risks of contact by unknown adults, cyberbullying and harmful algorithmic amplification.

European digital regulation increasingly recognises these duties. The Digital Services Act is based on the idea that intermediary services, and especially online platforms, must act responsibly in relation to illegal

content, systemic risks and the protection of minors (Regulation (EU) 2022/2065). This does not mean that platforms become general judges of all interpersonal disputes. It means that they must have transparent, fair and effective procedures for dealing with content and conduct that may seriously harm children.

Other actors are also relevant. Public authorities must provide legal, educational and institutional mechanisms that allow families and children to seek help. Schools must establish internal rules and prevention programmes. Parents must develop digital literacy and communicate with children about risks. Civil society organisations and professional services may provide counselling, reporting assistance and psychological support. Effective protection depends on cooperation among these actors, because digital violence usually cannot be resolved by one institution acting alone.

An important challenge is the identification of the perpetrator. Digital violence may be committed through anonymous profiles, false accounts or foreign platforms. This complicates civil-law protection and the collection of evidence. However, anonymity cannot justify impunity. Legal mechanisms should enable the preservation and disclosure of relevant data under appropriate procedural safeguards, especially when the rights and safety of children are at stake.

Another challenge is the cross-border nature of digital services. A child in Serbia may be harmed through a platform established in another jurisdiction, by a user located abroad or through servers outside the state. This requires harmonisation with European standards and cooperation with platforms and authorities beyond national borders. In this sense, the digital protection of children is part of a broader transformation of law in the digital society.

7. BALANCING FREEDOM OF EXPRESSION, PRIVACY AND CHILD PROTECTION

Legal protection from digital violence must be balanced with freedom of expression. Not every unpleasant statement, criticism or conflict in digital communication represents legally relevant violence. A democratic society must protect the exchange of opinions, including opinions that may be disturbing or offensive. However, freedom of expression does not include the right to threaten, harass, humiliate, disclose private information, misuse personal data or violate the dignity of a child. In the digital environment, the balance between expression and child protection must be interpreted through the child-rights approach and the European standard of private life

(Convention for the Protection of Human Rights and Fundamental Freedoms, 1950; Livingstone & Third, 2017).

The balancing of rights is particularly delicate when minors are involved. Children may participate in public communication, express opinions and use digital platforms. At the same time, their vulnerability requires a higher level of protection. In disputes concerning children, the principle of the best interests of the child should guide the interpretation of privacy, dignity and expression. This does not automatically eliminate freedom of expression, but it requires that the harm to the child be taken seriously.

Several criteria may be useful in this balancing process: whether the content contributes to a matter of public interest; whether the child is identifiable; whether the information belongs to the private sphere; whether the content is true or false; whether it was shared with malicious intent; the age and maturity of the child; the size of the audience; the duration of availability; and the foreseeable consequences for the child. Content that humiliates a child, exposes private details or places the child in danger will usually deserve stronger legal intervention than ordinary criticism or disagreement.

A specific issue concerns the digital traces created by children themselves. Adolescents may publish content that later becomes a source of harm or manipulation. The legal response should not blame the child for the misuse of such content by others. The fact that a child communicated online does not deprive the child of privacy, dignity and protection. The law must recognise that children experiment with identity and communication and that adults and platforms have a duty not to exploit their immaturity.

The balance between freedom of expression and child protection must also be reflected in remedies. Removal of content may be justified where the content violates the rights of the child. However, removal should be accompanied by procedural safeguards, especially when disputes involve contested facts. Compensation should be proportionate to the harm suffered. Educational measures should be preferred in minor peer cases, while stronger legal measures should be available in serious cases involving threats, exploitation, repeated harassment or public humiliation.

8. PREVENTION AND THE NEED TO ADAPT TRADITIONAL LEGAL INSTITUTES

The legal response to digital violence cannot be effective if it is limited to reaction after harm has occurred. Prevention is essential because digital harm spreads rapidly and may be difficult to repair. Preventive measures include digital literacy, education about rights and responsibilities, school protocols, parental guidance, platform design standards and clear institutional cooperation (UNICEF, 2017; OECD, 2021; Council of Europe, 2018).

Digital literacy should not be understood only as technical knowledge. Children, parents and teachers must understand privacy, consent, personal data, digital traces, online reputation, reporting mechanisms and the legal consequences of harmful digital conduct. A child who knows how to recognise and report violence is in a better position to seek help. A parent who understands digital risks can react without panic and without excessive control. A teacher who understands online peer dynamics can identify digital violence even when it occurs outside the classroom.

Traditional civil-law institutes remain important, but they require adaptation. The protection of honour and reputation must take into account the speed and scale of online dissemination. The protection of privacy must include the child's digital identity and control over personal data. Compensation for non-pecuniary damage must recognise psychological suffering caused by public digital humiliation. Injunctions and removal orders must be urgent and technologically realistic. Evidence rules must allow preservation of screenshots, metadata and platform records while ensuring authenticity and legality.

Family-law institutes also require adaptation. Parental responsibility must include digital upbringing and protection. The best interests of the child must be interpreted in relation to online exposure, data protection and digital autonomy. Measures of support to the family should include counselling on digital risks and cooperation with schools and professional services. The child's opinion should be heard in accordance with age and maturity, especially when decisions concern the removal of content, reporting of peers or restrictions on digital communication.

The development of legal doctrine in this field should avoid creating a completely separate "digital law of children" detached from existing legal principles. Instead, the task is to interpret existing principles in a technologically aware manner. The child remains the same legal subject, but the environment in which rights are exercised and violated has changed.

Therefore, law must preserve continuity with traditional protection while developing new practical mechanisms suitable for digital society (UN Committee on the Rights of the Child, 2021; Livingstone, Stoilova & Nandagiri, 2019).

9. CONCLUSION

Digital violence against children and adolescents is one of the significant legal challenges of contemporary digital society. It is not merely a technical, educational or security-related issue. It is a complex legal phenomenon that may affect privacy, dignity, honour, reputation, personal identity, psychological integrity and the best interests of the child. Its consequences may be long-lasting because digital content can be copied, redistributed and preserved beyond the control of the victim.

Civil-law protection has an important role in stopping harmful conduct, removing unlawful content, protecting personality rights and compensating pecuniary and non-pecuniary damage. Family-law protection is equally important because it places the child's development, parental responsibility and the best interests of the child at the centre of the response. These two areas of law must operate together, supported by educational, data-protection and digital regulation mechanisms.

The responsibility for preventing and addressing digital violence is shared. Parents must guide and protect children in digital space, but also respect the child's privacy and dignity. Schools must react when digital violence affects the educational environment and peer relations. Digital platforms must provide effective reporting, moderation and safety measures for minors. Public authorities must ensure coherent procedures, child-sensitive protection and cooperation among institutions. The establishment and statutory institutionalization of specialized Family Courts in Serbia can provide comprehensive protection for children, both in traditional family disputes and in disputes arising from digital relationships, social media, and the Internet in the broadest sense.

The main challenge for contemporary law is to adapt traditional legal institutes to new forms of harm without abandoning fundamental principles. The protection of children in digital space must be effective, urgent and proportionate, while preserving the balance between freedom of expression, privacy, parental responsibility and the principle of the best interests of the child. Only such an approach can provide meaningful protection of children and adolescents in the digital society.

REFERENCES:

1. Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe, Rome, 1950.
2. Council of Europe. (2018). Guidelines to respect, protect and fulfil the rights of the child in the digital environment. Recommendation CM/Rec(2018)7 of the Committee of Ministers.
3. European Commission. (2025). Guidelines on measures to ensure a high level of privacy, safety and security for minors online under Article 28(1) of Regulation (EU) 2022/2065.
4. Livingstone, S., Stoilova, M. & Nandagiri, R. (2019). Children's data and privacy online: Growing up in a digital age. London: London School of Economics and Political Science.
5. Livingstone, S. & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. New Media & Society, 19(5), 657-670.
6. Lievens, E. (2010). Protecting Children in the Digital Era: The Use of Alternative Regulatory Instruments. Leiden/Boston: Martinus Nijhoff Publishers.
7. OECD. (2021). Children in the digital environment: Revised typology of risks. OECD Digital Economy Papers, No. 302.
8. Porodični zakon [Family Law]. Službeni glasnik RS, br. 18/2005, 72/2011 - dr. zakon i 6/2015.
9. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, General Data Protection Regulation.
10. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC, Digital Services Act.
11. Šarkić, N. & Počuča, M. (2020). Porodično pravo i porodičnopravna zaštita [Family Law and Family-Law Protection]. Beograd: Pravni fakultet Univerziteta Union / Službeni glasnik.
12. UN Committee on the Rights of the Child. (2021). General comment No. 25 on children's rights in relation to the digital environment, CRC/C/GC/25.
13. UN General Assembly. (1989). Convention on the Rights of the Child, resolution 44/25 of 20 November 1989.
14. UNICEF. (2017). The State of the World's Children 2017: Children in a Digital World. New York: UNICEF.

15. UNICEF. (2021). The State of the World's Children 2021: On My Mind - Promoting, protecting and caring for children's mental health. New York: UNICEF.
16. Ustav Republike Srbije [Constitution of the Republic of Serbia]. Službeni glasnik RS, br. 98/2006 i 115/2021.
17. Zakon o obligacionim odnosima [Law of Contracts and Torts]. Službeni list SFRJ, br. 29/78, 39/85, 45/89 - odluka USJ i 57/89, Službeni list SRJ, br. 31/93, Službeni list SCG, br. 1/2003 - Ustavna povelja i Službeni glasnik RS, br. 18/2020.
18. Zakon o osnovama sistema obrazovanja i vaspitanja [Law on the Foundations of the Education System]. Službeni glasnik RS, br. 88/2017, 27/2018 - dr. zakon, 10/2019, 6/2020, 129/2021 i 92/2023.
19. Zakon o sprečavanju nasilja u porodici [Law on Prevention of Domestic Violence]. Službeni glasnik RS, br. 94/2016 i 10/2023 - dr. zakon.
20. Zakon o zaštiti podataka o ličnosti [Law on Personal Data Protection]. Službeni glasnik RS, br. 87/2018.
21. Zakon o zabrani diskriminacije [Law on Prohibition of Discrimination]. Službeni glasnik RS, br. 22/2009 i 52/2021.