

Digital risks to the child

Where does the role of centres for social work begin and end?

Vladimir Antić, director of the Trstenik Centre for Social Work

Igor Bošnjaković, founder of the Association of Social Protection Lawyers "Argument"

Marko Milanović, director of the Centre for Research and Social Development IDEAS

The digital environment has become an integral part of a child's life, yet the way centres for social work respond when risk arises on networks, platforms and in electronic communication is still not sufficiently regulated, either procedurally or in terms of professional methodology. This commentary examines where the boundaries of competence lie, what dilemmas arise in practice and what needs to be defined so that professional workers can make safer, better reasoned and more consistent decisions.

The digital space has long ceased to be separate from children's everyday lives. On social networks, communication platforms, in online games and other digital environments, children make contact, build relationships, exchange content, learn and enjoy themselves. In that same space they may be exposed to harassment, threats, misuse of personal data, unauthorised sharing of content and other risks, but they may also harass or insult others, or engage in other forms of what is termed digital violence, without grasping the limits of what is permitted or the consequences of such content for the rights, personality and psychological integrity of others.

When such a situation reaches a centre for social work (CSW), professional workers face a series of questions that cannot easily be answered by applying a single regulation or an existing protocol. How is risk to be assessed when the most important information is contained in electronic communication? What may and should a professional worker

establish in order to protect the child, and where does the competence of the police, the public prosecutor's office, the court or another authority begin? How can the child's safety be protected while respecting the child's right to privacy and to take part in decisions that concern them? What constitutes appropriate parental supervision in the digital space, and how is a parent's need for support to be distinguished from a serious failure to protect the child?

International standards exist, but operational questions remain

The rights of the child do not cease to apply when a child uses digital technologies. The Convention on the Rights of the Child requires that its four general principles be respected in the digital environment as well: non-discrimination, the best interests of the child, the right to life, survival and development, and the right of the child to express their views freely on matters affecting them. The digital environment is at once a space for realising the rights to information, education, play, connection and freedom of expression, and a space in which a child may be exposed to violence, exploitation, discrimination, breaches of privacy and other harmful influences.

General comment No. 25 of the Committee on the Rights of the Child, on children's rights in relation to the digital environment, explains how the Convention applies to the technologically mediated life of the child. The document requires decisions to be based on an assessment of the best interests of the child, with regard for their evolving capacities and their right to be heard. It places particular emphasis on non-discriminatory access to digital services, protection of privacy and personal data, protection from all forms of violence and exploitation, availability of comprehensible information, digital literacy, and effective mechanisms for reporting, assistance and legal protection.

It follows from these standards that protection cannot be reduced to prohibition or the confiscation of devices. A restriction may be necessary where a concrete risk exists, but it must be age-appropriate, necessary, proportionate and justified in duration. At the same time, the child should be empowered to recognise risk, seek help, understand the consequences of sharing data and gradually assume greater responsibility for their own digital choices. For the professional worker this means that safety, development, privacy, participation and support to the child must be considered together, not as mutually exclusive values.

The Recommendation of the Committee of Ministers of the Council of Europe on guidelines to respect, protect and fulfil the rights of the child in the digital environment calls on States to adopt a comprehensive approach linking legislation, public policy, training of professionals, data protection, the accountability of digital service providers and accessible assistance mechanisms. The guidelines also point to the importance of child-friendly information, assessment of the impact of digital products and measures on children's rights, privacy protection built in at the design stage of services, and the involvement of children in developing policies that affect them.

The European strategy A Digital Decade for children and youth, known as the new strategy for a Better Internet for Kids (BIK+), links three further objectives. The first is a safe digital experience and protection from harmful and illegal content, conduct and contact. The second is empowering children through digital skills and access to quality content and services. The third is the active participation of children in shaping the digital environment. Although this document is not a direct instruction for the work of CSWs in Serbia, its logic matters: sustainable protection means reducing risk, strengthening the child's capacities and holding institutions and businesses accountable, all at the same time.

International instruments therefore provide clear principles and directions for action. Their purpose, however, is not to prescribe the specific sequence of steps a professional worker in Serbia should take. They do not answer directly what a CSW does upon receiving a report, what data it may collect, how it assesses risk, how it records electronic materials and at what point it involves other authorities. The problem is not a complete absence of legal standards, but rather that those standards have not yet been sufficiently translated into a single, operational framework that CSWs can apply in practice.

The domestic framework spans several regulations but gives no single answer

The Constitution of the Republic of Serbia guarantees special protection of the child and respect for the child's personality, protects the confidentiality of communications and personal data, and requires any restriction of rights to be based on law, necessary and proportionate to a legitimate purpose. For the subject of digital risks this means that the need to protect a child does not remove the requirement that the extent of access to communication and of data processing be limited to what is necessary in the particular case.

The Family Act obliges parents and the authorities deciding on a child to be guided by the child's best interests. The Act (in particular Articles 59–82 of the Family Act of the Republic of Serbia) governs the content of parental rights and duties, the child's right to receive information and express their views, and the competences of the guardianship authority, including preventive and corrective supervision of the exercise of parental rights. These provisions offer a basis for treating digital risk as part of the child's overall safety, development and family functioning, but they do not set out specific criteria for what counts as appropriate parental supervision in the digital space.

The Social Protection Act and the Rulebook on the organisation, norms and standards of work of centres for social work govern assessment, planning, case management, protection of service users and cooperation with other services. Their focus is on the needs, strengths and risks of service users, on individualised planning and on the application of measures and services within the competence of the social protection system. They do not, however, specifically regulate how digital circumstances are incorporated into assessment, nor how electronic materials are to be handled.

The Personal Data Protection Act requires a legal basis, purpose limitation, a proportionate scope of data, accuracy, security and limited retention. These requirements are directly relevant where offences are suspected to have been committed via social networks, the internet and other contemporary information and communication technologies, and equally where a CSW seeks access to messages or accounts, makes a note of content it has seen, takes a screen capture or forwards data to another authority. Article 16 of the Act specifically governs a child's consent in relation to the direct offer of information society services. Where processing is based on consent, a person who has reached the age of 15 may give consent independently, while for a person under 15 consent is given by the parent exercising parental rights or another legal representative.

Where a criminal offence or another unlawful act is suspected, the Criminal Code, the Criminal Procedure Code, the rules on juvenile offenders and the rules on the competence of State authorities for combating high-tech crime become relevant. Their significance for the CSW lies in marking the point at which information should be preserved to an appropriate extent and submitted without delay to the authority empowered to establish the act, the identity of the perpetrator and the evidentiary value of the material.

The Information Security Act and the Regulation on the safety and protection of children in the use of information and communication technologies form part of a broader preventive and institutional framework. The Regulation governs protection and information measures, cooperation between competent authorities and the work of the National Contact Centre

for the Safety of Children Online. These mechanisms can be important for counselling and referral, but they do not replace the assessment and protective measures within the competence of the CSW.

The General Protocol for the Protection of Children from Violence establishes shared principles of prevention and of a cross-sectoral response where violence is suspected or known. It covers all children whose well-being is endangered, children at risk and children suspected of being exposed to violence, regardless of the setting in which the violence occurs. It gives the centre for social work a key role in assessing, planning and applying measures and services of social and family-law protection. The Special Protocol for the Protection of Children from Violence in the Field of Social Protection, adopted in 2024, further regulates the activities and procedures of the social protection system. Neither document, however, develops in sufficient detail the questions specific to digital accounts, private communication, the authenticity of electronic content and the limits of parental and institutional access.

Taken together, domestic regulations and protocols provide a certain basis for action, but that framework needs to be brought closer to CSW professional workers through professional methodological guidance and targeted training, and interpreted in the light of present-day circumstances. What is also missing is their consolidation into standards that match the professional mandate of CSWs and the dilemmas typical of the digital environment.

Platforms' terms of use exist, but the public is insufficiently aware of them

The centre for social work, as the guardianship authority, is encountering a growing number of reports concerning acts committed in the digital environment, often in situations where a child uses social networks contrary to their general terms of use. In this way children, unwittingly and with the tacit or conscious consent of their parents, are exposed to inappropriate content and influence, and to witnessing or endorsing various harmful social phenomena and patterns of behaviour.

Most social networks, including TikTok, Instagram, Facebook and Snapchat, set a minimum age of 13 for opening a user account. TikTok, for example, allows accounts from the age of 13, while certain features (such as LIVE broadcasting, sending and receiving gifts and other monetisation features) are available only to adult users aged 18 and over. These are the rules of particular platforms, not statutory age limits. In practice children begin using social

networks even before the minimum age set by a platform's own rules, parental supervision is often absent, and the platform's terms of use are breached.

Professional workers in CSWs therefore face the demanding task of first advancing their own knowledge, and then informing and educating parents about their responsibility to ensure compliance with the general terms of use of digital platforms, the protection of the child's privacy and the lawful processing of the child's personal data, as well as safe and age-appropriate use of digital services. These obligations flow from the very core of parental duties as defined by the Family Act and by the international standards binding on the Republic of Serbia.

Specific challenges in the work of centres for social work

A platform's age limits are not the same as a statutory prohibition

One important dilemma concerns the age of the child and the use of social networks and other digital platforms. It is essential to distinguish between the rules of a particular platform, the legal basis for processing the child's personal data, and the assessment of parental conduct.

The minimum age for opening an account set by a digital platform is part of its terms of use. A breach of that rule is not in itself a sufficient basis for concluding that the parent has neglected the child, or that the child has committed an unlawful act.

Article 16 of the Personal Data Protection Act governs a child's consent in relation to the direct offer of information society services. That provision is not a general prohibition on the use of the internet or of all digital services by a child under 15. Its application depends on the type of service and on the legal basis for processing the data.

The child's age, the opening of an account and the parent's conduct may all be important circumstances in the assessment, but they must not become automatic proof of parental failure. What must be assessed is the actual risk, the child's evolving capacities, the manner in which the platform is used, the content and context of the communication, the parent's conduct after learning of the risk, and the family's readiness to accept support.

The centre for social work assesses risk; the competent authorities establish the unlawful act

It is not the role of the CSW to establish criminal or misdemeanour liability, the identity of the perpetrator, or the evidentiary value of electronic material. The centre for social work does not need to prove who sent a message, opened an account or posted particular content in order to begin an assessment and provide support to the child.

In proceedings conducted before other authorities, including proceedings concerning acts committed in the digital environment, the CSW has an important auxiliary professional role. That role does not mean that the CSW establishes the unlawful act or criminal liability.

To begin acting, it is enough that there is information or circumstances indicating a possible risk to the safety, development, rights or well-being of the child. The professional worker should assess the nature and urgency of the risk, the child's needs, the protective capacities of the family and the need to involve other authorities. The methodological framework must, however, determine what information the CSW collects for its own assessment, how it verifies the relevance of that information, and when it must without delay notify the authority competent to establish the unlawful act and the identity of the person who committed it.

This delineation matters particularly where the person to whom conduct is attributed claims that their profile was misused, or that the electronic content was altered or generated using artificial intelligence. The professional worker records and takes such a claim into account but does not take on the work of technical expert examination. Automated tools for assessing whether content was generated by artificial intelligence are not in themselves reliable or conclusive proof of authenticity. Where authenticity is decisive, establishing it should be left to the competent authorities and to experts with the appropriate powers and technical capacity.

The child's privacy and safety are not a simple choice between two rights

Protecting a child may require access to certain data about their digital activities. It does not follow, however, that a parent or a professional worker has an unlimited right of access to the child's private communication.

A child's digital communication (chat, SMS, email) falls under the protection of privacy and correspondence. Direct parental monitoring, meaning reading the correspondence itself, should be applied only as an exception, which may be justified where there is a clear risk to the child's safety, health or life. In all other situations parents should build trust through the

child's digital literacy and open conversation about the content the child encounters and the people the child communicates with.

A child has the right to privacy, but also the right to protection from violence, abuse and exploitation. These rights should not be viewed through a predetermined hierarchy in which one right always prevails. In each case it should be assessed whether the access is based on a concrete risk, whether it is necessary, what the smallest necessary scope is, and whether there is a less restrictive way of protecting the child.

The answer cannot be the same for a child of seven, of twelve and of seventeen. As a child develops the capacity to understand risks and the consequences of their decisions, their autonomy and privacy should be respected to an increasing degree. Before accessing private communication, wherever circumstances allow, the child should be spoken to, the reason, purpose and expected scope of the action explained, and the child given the opportunity to express their views. Where there is immediate danger, intervention may be urgent, but even then its nature and scope must be reasoned and documented.

Parental responsibility encompasses support and, where necessary, protective measures

The parental duty to keep, raise, bring up and protect a child extends to the digital environment as well. What appropriate supervision means changes with the child's age and evolving capacities, the type of technology, the risk identified and the family context.

A complete lack of interest in a child's digital activities may be grounds for further assessment. Insufficient familiarity with platforms, their rules or their technical settings should not be automatically equated with the improper exercise or neglect of parental duties. A distinction must be drawn between a parent who is insufficiently informed but accepts counselling and takes reasonable protective measures, and a parent who is aware of a serious risk, refuses to cooperate and persistently or repeatedly fails to protect the child.

In the great majority of cases the CSW's initial response should be support to the family, development of parenting competences, agreement on developmentally appropriate rules for using technology, and strengthening communication between parent and child. Where the risk persists or the parent does not take the necessary measures, the CSW considers exercising the powers of the guardianship authority in accordance with the Family Act, including preventive or corrective supervision of the exercise of parental rights and the initiation of appropriate proceedings, such as deprivation of parental rights, where the

statutory conditions are met. The choice of intervention must be based on an individual assessment, on the gravity and duration of the failure and on its actual effect on the child.

Electronic materials require a clear regime for handling and data protection

Screen captures, electronic messages, photographs, video recordings, account data and statements by participants may all be important for an initial risk assessment. Collecting them at the same time raises questions of legal basis, relevance, accuracy, security and privacy protection.

It is necessary to define what a professional worker may ask to see, when it is sufficient to make an official note of the content seen, and when and under what conditions content may be copied, retained or forwarded. Rules are needed on where material is kept, on access control, on retention periods and on what happens once the purpose for which the material was collected has been fulfilled.

Sensitive content must not be reproduced without control, sent through private accounts or stored on employees' private devices. CSW records should contain only data relevant to assessing and protecting the child. At the same time, a distinction must be drawn between material sufficient for the CSW to recognise risk and begin providing support, and evidence whose authenticity and evidentiary value are established by the police, the public prosecutor's office or the court.

The child's position in the incident changes priorities, but not the duty to protect their rights

It is not the same whether a child has been exposed to harassment, threats or abuse, whether the child is a witness to harmful behaviour, or whether the child is suspected of having initiated such behaviour towards another child or an adult. The methodology should therefore distinguish between the aims and priorities of assessment, rather than reducing the child to a permanent label of victim, witness or perpetrator.

Where a child is exposed to risk, the priorities are immediate safety, stopping or limiting further harm, support to the child and involvement of the competent services. Where the child is a witness or another participant, what should be assessed is their exposure, pressure from those around them, their need for support and the manner of giving information without needless repetition of interviews.

Where a child is suspected of having initiated harmful behaviour, that child remains a rights holder and a child who may require assessment, support and an appropriate intervention. A statement by another participant or a screen capture may justify starting an assessment, but not the premature labelling of the child as a perpetrator. The child's participation must be ensured, having regard to age, developmental maturity, understanding of consequences, the family and peer environment, possible pressure from others, the consequences of the behaviour and the readiness of the child and the family to take part in change.

In all of these cases the parent should take an active part. Knowledge of parental duties, an appropriate attitude and suitable supervision of the use of information and communication technologies are important for protecting the child and preventing risk, and they are also relevant to the assessment and further action of the CSW and other competent authorities.

Cross-sectoral cooperation must be part of protection

The centre for social work cannot respond to every digital risk on its own. Depending on the circumstances, it may be necessary to involve the school, the police, the public prosecutor's office, the court, a health institution, the authority competent for personal data protection, the digital platform provider, the National Contact Centre for the Safety of Children Online or a specialised organisation.

The professional worker must know precisely whom to approach, what information to submit, on what legal basis it is exchanged, who coordinates the response and what the CSW continues to do after making a referral. Notifying another authority does not automatically end the CSW's role. While other authorities establish whether an unlawful act occurred and who is responsible for it, the CSW may continue to assess the child's needs, support the family, monitor risk and apply or coordinate measures within its own competence.

What needs to be defined in Serbia?

Existing international standards and domestic regulations provide a basis for action, but they do not give a sufficiently precise answer to all the questions professional workers face. Serbia needs a professional methodological framework for the work of CSWs in situations of digital risk to a child. That framework should cover at least the following elements.

- 01** The scope of digital risks relevant to the work of CSWs needs to be determined, explaining when unpleasant, inappropriate or conflictual behaviour becomes a risk requiring professional assessment and a protective intervention.

- 02** The content of assessment in the digital context needs to be established. The assessment should cover the nature and source of the information, the immediacy and gravity of the risk, its duration and repetition, the potential for content to spread rapidly and persist, the balance of power between those involved, the consequences for the child, the child's evolving capacities and vulnerabilities, the sources of support available, the conduct of the parents and the need for urgent involvement of other authorities.

- 03** The support provided to the child during and after the incident needs to be described. Depending on needs, it may include an immediate safety plan, counselling and psychosocial work, support in the family and school environment, referral to a health or other specialised service, and help for the child in understanding the procedure and the protection mechanisms available.

- 04** The aims and priorities of action need to be differentiated according to the child's position in the particular incident. The methodology should explain what is assessed and what support is provided where the child is exposed to risk, where the child is a witness or another participant, and where the child is suspected of having initiated harmful behaviour, prohibiting premature labelling and fully respecting the rights of every child.

- 05** The CSW's assessment needs to be clearly delineated from the work of other authorities. The framework should determine which facts the CSW establishes for the purposes of assessing and protecting the child, and at what point questions of the perpetrator's identity, the existence of an unlawful act, the authenticity of content and the evidentiary value of material are taken over by the police, the public prosecutor's office, the court or another competent authority.

- 06** A standard for interviewing the child and the parent needs to be established. That standard should cover preparation and informing of the child, the way the child's participation is secured, questions appropriate to age and evolving capacities, how to proceed where accounts differ, and measures to avoid needless repetition of interviews and additional burden on the child.

- 07** Criteria need to be established for accessing a child's digital activities and private communication. The framework should explain when access to digital activities or communication is based on a concrete risk, necessary and proportionate, who takes the decision, what the smallest necessary scope of access is, how the child is involved and how the reasons for and scope of the decision are documented.

- 08** Standards of parental supervision and the range of interventions in relation to parents need to be described. Expectations should be adjusted to the child's age, evolving capacities and the type of risk, clearly distinguishing the need for information, counselling and support from circumstances requiring preventive or corrective supervision of the exercise of parental rights, or the initiation of other proceedings within the competence of the guardianship authority.

- 09** The handling of electronic materials needs to be regulated. The rules should cover viewing, official recording, copying, receipt, storage, access control, forwarding and deletion, as well as how to proceed where the authenticity of content is in doubt or where content may have been altered or generated by artificial intelligence.

- 10** Concrete mechanisms for cross-sectoral cooperation and referral need to be established. They should include clear contact points, criteria for involving other authorities, the minimum content of a notification, the legal basis for exchanging data, responsibility for coordination and the way information is fed back to the CSW.

- 11** The documenting of professional decisions needs to be standardised. The professional worker should record the relevant risk indicators, the sources and limitations of the information available, the child's views, consultations undertaken, the assessment of needs and strengths, the decision, the reasons for choosing a particular measure and the follow-up plan.

- 12** Practical tools and lasting professional support need to be developed. These may include assessment checklists, models of practice, forms for documentation and referral, anonymised case studies, interdisciplinary training, accessible professional consultation and supervision. A mandatory, continuous programme of professional development is also needed, because the digital environment and the forms of risk that may prompt a CSW intervention change almost daily. Their purpose should be to support professional judgement, not to automate decision-making.

Key legal and professional sources

Domestic legislation

- 1 Constitution of the Republic of Serbia, Official Gazette of the RS, nos. 98/2006 and 115/2021. Available at: <https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/ustav/2006/98/1/reg> (accessed 4 August 2026).
- 2 Family Act (Porodični zakon), Official Gazette of the RS, nos. 18/2005, 72/2011 – other act, 6/2015 and 109/2025 – other act. Available at: <https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2005/18/7/reg> (accessed 4 August 2026).
- 3 Social Protection Act (Zakon o socijalnoj zaštiti), Official Gazette of the RS, nos. 24/2011 and 117/2022 – Constitutional Court decision. Available at: <https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2011/24/2/reg> (accessed 4 August 2026).
- 4 Personal Data Protection Act (Zakon o zaštiti podataka o ličnosti), Official Gazette of the RS, no. 87/2018. Available at: <https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2018/87/13/reg> (accessed 4 August 2026).
- 5 Criminal Code (Krivični zakonik), Official Gazette of the RS, nos. 85/2005, 88/2005 – corr., 107/2005 – corr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019, 94/2024 and 63/2026. Available at: <https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2005/85/6/reg> (accessed 4 August 2026).
- 6 Criminal Procedure Code (Zakonik o krivičnom postupku), Official Gazette of the RS, nos. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 – Constitutional Court decision and 62/2021 – Constitutional Court decision. Available at: <https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2011/72/1/reg> (accessed 4 August 2026).
- 7 Act on Juvenile Offenders and the Criminal–Law Protection of Minors (Zakon o maloletnim učinocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica), Official Gazette of the RS, no. 85/2005. Available at: <https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2005/85/7/reg> (accessed 4 August 2026).
- 8 Act on the Organisation and Competence of State Authorities for Combating High-Tech Crime (Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala), Official Gazette of the RS, nos. 61/2005, 104/2009, 10/2023, 10/2023 – other act, 9/2026 and 56/2026. Available at: <https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2005/61/7/reg> (accessed 4 August 2026).
- 9 Information Security Act (Zakon o informacionoj bezbednosti), Official Gazette of the RS, no. 91/2025. Available at: <https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2025/91/5/reg> (accessed 4 August 2026).
- 10 Regulation on the Safety and Protection of Children in the Use of Information and Communication Technologies (Uredba o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija), Official Gazette of the RS, no. 13/2020. Available at: <https://pravno-informacioni-sistem.rs/eli/rep/sgrs/vlada/uredba/2020/13/4/reg> (accessed 4 August 2026).
- 11 Rulebook on the Organisation, Norms and Standards of Work of the Centre for Social Work (Pravilnik o organizaciji, normativima i standardima rada centra za socijalni rad), Official Gazette of the RS, nos. 59/2008, 37/2010, 39/2011 – other rulebook, 1/2012 – other rulebook, 51/2019, 12/2020, 83/2022 and 10/2025. Available at: <https://www.zavodsz.gov.rs/sr/resurs-centar/propisi-od-zna%C4%8Daja-za-socijalnu-za%C5%A1titu/pravilnici/> (accessed 4 August 2026).

Protocols

- 12 Government of the Republic of Serbia, General Protocol for the Protection of Children from Violence, adopted by Conclusion 05 no. 560-826/2022-2 of 10 February 2022. Available at: <https://www.savetzapravadeteta.gov.rs/doc/dokumenta/Opsti-protokol-za-zastitu-dece-od-nasilja.pdf> (accessed 4 August 2026).
- 13 Ministry of Labour, Employment, Veteran and Social Affairs, Special Protocol for the Protection of Children from Violence in the Field of Social Protection, 29 October 2024. Available at: <https://www.minrzs.gov.rs/srb-lat/aktuelnosti/obavestenja/posebni-protokol-za-zastitu-dece-od-nasilja-u-oblasti-socijalne-zastite> (accessed 4 August 2026).

International standards and professional sources

- 14 United Nations General Assembly, Convention on the Rights of the Child, 20 November 1989, United Nations, Treaty Series, vol. 1577, p. 3, Refworld. Available at: <https://www.refworld.org/legal/agreements/unga/1989/18815> (accessed 4 August 2026).
- 15 United Nations Committee on the Rights of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, 2 March 2021. Available at: <https://savetzapravadeteta.gov.rs/doc/dokumenta/Opsti-komentar-KomitetaUN-za-prava-deteta-br.25%282021%29-o-pravima-deteta-u-vezi-sa-digitalnim-okruzenjem.docx>; original document: <https://digitallibrary.un.org/record/3906061> (accessed 4 August 2026).
- 16 Council of Europe, Committee of Ministers, Recommendation CM/Rec(2018)7 to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, 4 July 2018. Available at: <https://savetzapravadeteta.gov.rs/doc/dokumenta/Preporuka-Saveta-Evrope-o-zastiti-dece-u-digitalnom-okruzenju.docx>; original document: <https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html> (accessed 4 August 2026).
- 17 European Commission, A Digital Decade for children and youth: the new European strategy for a Better Internet for Kids (BIK+), COM(2022) 212 final, Brussels, 11 May 2022. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN> (accessed 4 August 2026).
- 18 UNICEF Serbia, For the safety of children online: trends in the regulation of internet platforms and what we can learn from them, February 2026. Available at: <https://www.unicef.org/serbia/publikacije/za-bezbednost-dece-na-internetu> (accessed 4 August 2026).
- 19 Institute of Psychology, Faculty of Philosophy in Belgrade, and UNICEF Serbia, Internet use and digital technology among children and young people in Serbia: findings of the EU Kids Online survey, November 2019. Available at: <https://www.unicef.org/serbia/publikacije/koriscenje-interneta-kod-dece-i-mladih-u-srbiji> (accessed 4 August 2026).

This text was prepared jointly by IDEAS and the Association of Social Protection Lawyers “Argument”, as a contribution to informed public debate.

The Centre for Research and Social Development IDEAS is one of the leading civil society organisations in Serbia. Based in Belgrade, it combines research and public policy development with direct support to the most vulnerable groups. Our mission is to build lasting solutions to complex social problems and to create a fairer society for all.

The Association of Social Protection Lawyers “Argument” is a professional association based in Leskovac that brings together lawyers employed in the social protection system. It works on the exchange of knowledge and experience in interpreting regulations, on making practice more consistent and on affirming the role of lawyers in decisions taken in social protection.