K Cendic 'Children's rights to privacy in times of emergency: The case of Serbia in relation to internet education technologies' (2020) 4 *Global Campus Human Rights Journal* 68-90
http://doi.org/20.500.11825/1705

Children's rights to privacy in times of emergency: The case of Serbia in relation to internet education technologies

*Kristina Cendic**

Abstract: *In the digital era the privacy of children has become an issue of particular importance. With the spread of COVID-19 many schools turned to online education, causing this vulnerable group of internet users to be more and more engaged in the digital sphere. It has thus become questionable whether children are protected enough when education systems increasingly turn to online teaching. When Serbia declared a state of emergency in an attempt to contain the new virus in March 2020, the national educational system also implemented online schooling. Since there have been severe privacy breaches in Serbia even before this pandemic, a basic question arises as to whether the right to privacy of children was adequately respected and protected when the students were required to use a number of programmes, networks and applications in order to attend classes. This article investigates the right to privacy of children during the recent application of online teaching/learning technologies and platforms in Serbia, exploring key emerging issues concerning online schooling and identifying further research on problems pertaining to this right that will inevitably appear in the years to come.*

Key words: *privacy of children; digital rights; online education; state of emergency; Serbia*

1 Introduction

Due to changes brought about by new technologies, the notion of digital rights has come into the spotlight. Digital rights encompass human rights

* BA (Novi Sad, Serbia) MA (Belgrade) MA in Democracy and Human Rights (Sarajevo, Bologna) PhD in Communication Studies (Barcelona); External expert, University of Zenica, Bosnia and Herzegovina; Kristina.cendic@gmail.com. The author is grateful to Dr Chiara Altafin, Research Manager at the headquarters of the Global Campus of Human Rights, who provided substantial insight and expertise which greatly improved this article.

in terms of people's access to and use of electronic devices and networks, thus including the right to freedom of expression, the right to freedom of assembly and the right to privacy. Indeed, if there ever was a dividing line between 'digital rights and human rights, it has blurred to the point of irrelevance' (Jansen Reventlow 2017). Digital rights have acquired particular importance when societies shifted their activities into the online sphere due to the COVID-19 pandemic. Notably, even in times of public emergency human rights must be respected, and emergency powers should be exercised within the parameters provided under international human rights law: The derogation of certain rights can be allowed only in situations threatening the life of the nation; limitations on certain rights must fulfil the requirements of legality, necessity and proportionality, and be non-discriminatory, and can be introduced only for reasons of national security or public order or for the protection of the rights and freedoms of others. However, across the world many government agencies have been collecting and analysing personal information about large numbers of identifiable people, and as our society struggles with how best to minimise the spread of the coronavirus disease, we also analyse 'the way that "big data" containment tools impact our digital liberties' (Electronic Frontier Foundation 2020). As warned by the European Digital Rights association, some of the emergency-related policy initiatives risk the abuse of sensitive personal data even while attempting to safeguard public health, which has 'significant repercussions for privacy and other rights both today and tomorrow' (EDRi 2020).

In the recent emergency context, many schools around the world explored and used technological solutions to ensure continuity in students' educational experiences and also relied on video-conferencing technologies. They 'faced choices about how to rapidly move into online platforms and services that are quick to implement, can accommodate lots of students and are user-friendly' (Bailey et al 2020). In this regard, in March 2020 the United Nations Educational, Scientific and Cultural Organisation (UNESCO) shared relevant recommendations. In particular, schools were encouraged to 'protect data privacy and data security' in the online sphere (i) by assessing 'data security when uploading data or educational resources to web spaces, as well as when sharing them with other organisations or individuals', and (ii) by ensuring 'that the use of applications and platforms does not violate students' data privacy' (UNESCO 2020). Schools were also recommended to 'blend appropriate approaches and limit the number of applications and platforms' (i) by combining 'tools or media that are available for most students, both for synchronous communication and lessons, and for asynchronous learning' and (ii) by avoiding 'overloading students and parents by asking them to download and test too many applications or platforms'. Nonetheless, experts have found 'widespread lack of transparency and inconsistent privacy and security practices in the industry for educational software and other applications used in schools

and by children outside the classroom for learning' (Strauss 2020). In fact, the digital safety of children has become a matter of concern regarding online schooling because some online portals may not have been put behind strong filters, and even before this period 'security breaches with online learning were not uncommon' (Strauss 2020).

During the pandemic digital rights have faced critical limitations and infringements in South-East and Central Europe, where 'in the semi-democracies of the region, dominated by regimes with elements of authoritarianism, there is legitimate concern about disproportionate interference in citizens' personal data' (Ristić 2020). In the case of Serbia, it has become clear that problems of data protection have caused serious breaches of citizens' rights to privacy, leading to legal uncertainty that threatens democracy (Ristić 2020). According to a research on data flow in the 'COVID-19 Information System' (Krivokapić & Adamović 2020), the current systems and registries of the country find it difficult to respond to existing needs and challenges regarding data protection and hence privacy. One of these registries is the electronic teachers' book (introduced in 2017 and applied in all Serbian schools since 2019), which contains a variety of data about students, thus posing privacy challenges. Moreover, as in the case of over 160 states that closed national schools due to the pandemic, Serbia abruptly shifted the teaching activities online, with the result that its schools had to broaden the use of technology to minimise learning disruptions related to COVID-19. However, one may wonder whether children's rights to privacy were adequately respected and protected when the students were required to use several programmes, networks and applications to attend classes. As clearly stressed by one scholar, in general 'educational technology has long posed serious privacy and equality problems, and these problems are now reaching a boiling point', and 'hasty choices now could have long-term impacts' (Han 2020).

In order to examine the right to privacy of children during this unexpected application of internet education technologies in Serbia, this article first considers relevant international, regional and domestic legal frameworks. Relevant literature on online schooling by Livingstone, Boyd, Krivokapić et al is then taken into account, giving an overview of global trends and issues progressively posed on how digital technologies impact children's safety and privacy. The specific situation in Serbia is subsequently examined by referring to the most recent studies on privacy as undertaken by SHARE Foundation, Balkan Insight, Balkan Investigative Reporting Network and others. After reflecting on the main privacy matters existing in Serbia to illustrate the setting in which schools operate, the article focuses on key emerging issues concerning online teaching and learning tools as applied due to the COVID-19 outbreak. It considers how these have affected children's privacy in Serbia, exploring what improvements could protect them in future online teaching exercises and provide safe

access to platforms, as well as pointing at possible problems about this right in the years to come.

2 Legal frameworks for the protection of a child's privacy and related rights in the digital environment

In many countries digital technologies have changed legal landscapes. States are attempting to adopt new internet-oriented laws, or to amend existing ones to make them compliant to the online sphere. These attempts have been more or less successful in different parts of the world, but what many hardly take into account are the rights of children on the internet. As highlighted by some scholars (Lievens et al 2019: 489), 'while international bodies as well as governments are actively promoting ICT access and investment so that businesses can innovate and compete in the global economy and society benefits from informational, civic, educational, and other opportunities' (UN Human Rights Council 2016), some organisations are alert to the child rights issues that arise', among others also protecting children's privacy online. In this context scholars have started to reconsider many of the articles of the Convention on the Rights of the Child (CRC) in light of their possible 'digital dimension'.

It must be emphasised that the four guiding principles as embodied in articles 2, 3, 6 and 12 of CRC are extremely important for children in the digital environment and for the purposes of our inquiry. Specifically, article 3 requires that the best interests of the child are a primary consideration 'in all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies'. Accordingly, every action with a potential impact on children's rights (such as privacy and freedom of expression) in the digital environment should take into account their best interests, the balanced assessment of which should be central in policy-making and decision-making practices (Lievens et al 2019: 492). Notably, even though article 3(1) entails an individual assessment (CRC/C/GC/14 2013: para 22), the UN Committee on the Rights of the Child (CRC Committee) has also affirmed that states have to assess and take as a primary consideration the best interests of children *as a group* or *in general*, for example, in their legislative actions or policy making (CRC/C/GC/14 2013: para 23). This entails a children's rights impact assessment that considers children's views as well as protection versus empowerment aspects (CRC/C/GC/14 2013: para 35). States also have to ensure that the assessment is undertaken in the actions by private actors (CRC/C/GC/14 2013: para 13), such as technology companies and platform providers. Focusing on article 2, the right to non-discrimination certainly entails the equality of children's access to the digital environment. In this regard, 'internet access is becoming ever more taken for granted as a means of ensuring child rights, and in consequence, lack of (sufficient or reliable) access is a pressing problem for large groups

of children across the world' (Lievens et al 2019: 491). In this regard states should support and widen policies that can overcome digital exclusion in its various forms, especially pursuing policy objectives that apply to all children and thus really are non-discriminatory. Regarding article 6 and the holistic concept of development as interpreted by the CRC Committee (CRC/GC/2003/5), in the era of new technologies a child's development has gained more and more importance, and is closely connected with education. In this vein, the goal of education is 'the development of the child's personality, talents and mental and physical abilities to their fullest potential' (article 29). Finally, article 12, which enshrines children's rights to freely express their views in all matters affecting them and have these views count in accordance with their age and maturity, has significance even in the digital context and related state policies should be created through decision-making processes that effectively include children's participation.

One of the rights particularly relevant for the purposes of our analysis is a child's right to privacy and its related dimensions under article 16 of CRC. The first paragraph requires states to ensure the protection of a child's privacy, family, home, correspondence, honour and reputation against arbitrary or unlawful attacks or interference with these rights; and the second paragraph also emphasises that children have a right to protection of the law from all relevant forms of interference or attacks. This is connected to protecting the privacy of children in the online sphere as they do not have sufficient awareness of the possible consequences of posting and revealing their personal information on the internet (OECD 2011). However, it is important to achieve a balance between the child's right to privacy and other rights relevant in the online sphere (such as freedom of expression and association). In fact, 'privacy is a fundamental component of participation, and accordingly, children should be given a voice in the policymaking process, and their perceptions of privacy should be duly taken into account' (Lievens et al 2019: 497). Moreover, article 13 of CRC recognises a child's right to 'seek, receive and impart information and ideas of all kinds' as part of the right to freedom of expression. There is the abundance of means of communication today and this right has a broad scope of application. For example, children can express their views and connect with others on blogs and social networking sites, as well as seek information on topics that are significant to them (Lievens et al 2019: 494). Equally relevant is the right to freedom of association under article 15 of CRC, as children associate in the digital environment. What is very risky for them are 'the digital traces that online expression and participation leave, especially since these tend to be automatically kept by the companies that provide platforms for social networking and their records can, under certain conditions, be demanded by States' (Lievens et al 2019: 496).

It is worth considering that in its statement on COVID-19 made in April 2020, the CRC Committee explicitly referred to 'online learning' (para 3) by calling on states to ensure that such a specific modality 'does not exacerbate existing inequalities or replace student-teacher interaction'. In highlighting the fact that this is 'a creative alternative to classroom learning but poses challenges for children who have limited or no access to technology or the Internet or do not have adequate parental support', the CRC Committee has explicitly stated that 'alternative solutions should be available for such children to benefit from the guidance and support provided by teachers'. However, it has not addressed any challenges to the right to privacy in relation to online schooling.

Importantly, the CRC Committee is drafting a General Comment on the rights of children in relation to the digital environment. In this regard Serbia submitted its remarks on the proposal of the concept of such a General Comment, recalling that in 2016 its government adopted the Regulation on Children Safety and Protection in the Use of Information and Communication Technologies. This provides for 'preventive measures' for protection and safety on the internet, which are supposed to be implemented through informing and educating children, parents and teachers, as well as through establishing a place for offering advice and receiving applications related to harmful, inappropriate, illegal content and behaviour online. In this vein, a National Contact Centre for Child Safety on the Internet was established in 2017. Serbia also recalled that the Ministry of Trade, Tourism and Telecommunications has reached agreements with international and non-governmental organisations (NGOs) (The United Nations Children's Fund (UNICEF), Save the Children, UNITES, Red Cross of the Republic of Serbia, Institute of Social Sciences, Foundation Tijana Jurić) on joint cooperation in order to increase awareness about a developing information society and the safety of children on the internet, as well as the availability of information on children's safety online. Additionally, ongoing initiatives include a draft General Protocol for the Protection of Children against Violence, a draft Strategy for the Prevention and Protection of Children against Violence, and the Draft Law on the Rights of the Child and the Protector of the Rights of the Child. However, it remains unknown as to which stage these processes have actually reached and to what extent they would deal with the exposure of children's privacy in the digital space.

Critically, on several occasions Serbia has been urged to make its legislative framework regarding the rights of children compliant with the existing international standards and to take a number of actions for enhancing its capability to ensure adequate safeguards of these rights, including privacy (UNICEF Serbia 2020). In its Concluding Observations on the combined second and third periodic reports of Serbia in 2017, the CRC Committee urged Serbia to adequately harmonise its legislation regarding children's rights, stressing the absence of a comprehensive

children's Act and noting that 'the reluctance to enact such an act poses a significant challenge to advancing children's rights in the State party' (CRC/C/SRB/CO/2-3: para 6). Concerns were also expressed over the fact that the national plan of action for children expired without any further action to produce a similar policy framework (para 8). Moreover, the Council for Child Rights of the government of Serbia, which is supposed to be the coordinating body on children's rights, has had only an advisory role with inconsistent performance of its duties. Even 'the oversight function of the committee on child rights of the National Assembly has been limited in relation to mainstreaming children's rights in national legislation' (para 10). Notably, the EU Progress Report on child-related issues and Index indicators gave Serbia a zero result (not complying at all) with envisaged standards (Child Pact 2017).

Focusing on the regional level, the Council of Europe 2016-2021 strategy for children's rights and its fifth priority area on digital environment rights have been reinforced by the Recommendation CM/Rec(2018)7 of the Committee of Ministers to member states on the Guidelines to respect, protect and fulfil the rights of the child in the digital environment. They aim to ensure children's interaction by addressing, among other aspects, privacy and data protection (paras 26-39); the right to education with specific reference to 'digital literacy' and 'educational programmes and resources' (paras 40-49); and the right to protection and safety (paras 50-66). Moreover, regionally the privacy-related legal framework has changed significantly since the adoption of the General Data Protection Regulation (EU) 2016/679 (GDPR), which superseded the Data Protection Directive 95/46/EC and which entered into force on 25 May 2018, with direct effect in the European Union (EU) and the European Economic Area. The new regulation has approached the protection of personal data and called on EU member states to harmonise data privacy laws. It has placed the emphasis on such protection and the respect of individuals' rights regarding personal data, so as not to allow commercial interests to trump the human right to privacy. The GDPR explicitly refers to children's personal data and highlights the importance of transparency and accountability when collecting and processing children's data, particularly in the online sphere. It provides guidance to those who offer online services in terms of privacy notices, and especially refers to children in article 8, stating the conditions applicable to a child's consent in relation to information society services, including that 'the processing of the personal data of a child shall be lawful where the child is at least 16 years old'. EU member states may stipulate a lower age for this purpose in their national laws, but not lower than the age of 13 years. Notably, its Recital 38 refers to the 'specific protection' of children's personal data, recognising that they may be less aware of the risks, consequences and safeguards concerned and of their rights in relation to the processing of personal data. It also stipulates that such protection should particularly apply to 'the use of personal data

of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child'.

It must be highlighted that the GDPR was taken over almost ***verbatim*** when Serbia enacted a new Law on Protection of Personal Data on 9 November 2018. Although this law appears to be a translation of the GDPR, regrettably it has omitted to establish that the citizens' rights related to insight, deletion, change and other measures of control over the processing of their data 'may be restricted by law' in cases such as: protection of national security, defence, public safety, rights and freedoms of others, and so forth. This means that the institutions and organisations processing personal data of Serbian citizens may restrict their rights arbitrarily and without any explicit legal authorisation. Such an omission is contrary to the Serbian Constitution of which article 42(2) establishes that '[e]veryone shall have the right to be informed about personal data collected about them, in accordance with the law, and the right to court protection in case of their abuse'. Nonetheless, this new Law entered into force on 21 August 2019, and there was a short time for public and private entities as well as citizens to familiarise themselves with this Law and introduce new practices. Even the national Commissioner for Information of Public Importance and Personal Data Protection urged Parliament to postpone the application of this Law as society was unprepared, but such postponement was not granted. In fact, based on the Commissioner's 2019 Annual Report, statistics show more than 7 000 cases of which the majority result from unintentional abuse and display a lack of knowledge in the field and that privacy-related awareness of citizens is low. In any case, under the new Law all entities in the public, civil and private sectors that collect, process and store personal data of Serbian citizens have various new obligations in relation to data, especially information security of all citizens, including children (Krivokapić et al 2018). In particular, article 16 refers to consent regarding the usage of information society services in Serbia: a child above 15 years of age can independently give consent for personal data processing when using these services; if the child has not turned 15, data processing is connected with the consent of a parent or another legal representative; and the controller must take reasonable measures to determine whether the consent came from one of them, taking into account available technologies. Notably, article 15 provides that the controller shall take appropriate measures to deliver (in writing or by other means) any information and communication on the processing of the data subject in a transparent, concise, intelligible and easily accessible form, utilising simple and clear language, particularly any information addressed specifically to a child. In addition, Serbian data protection legislation includes a Decision of 2019 under which assessment of the ***impact*** on personal data protection shall be performed by the controller (and require the opinion from the Commissioner) in case of processing of personal

data of children for the purpose of profiling, automated deciding or for marketing purposes; the assessment shall be done before the initiation of such processing. However, much of the relevant national laws and policies are either in their draft stage or have not yet been properly implemented. Despite the fact that some pertinent instruments are in force, in Serbia there are no adequate guidelines on their application, and institutions (including schools) lack both staff and training in matters of personal data protection.

3 Global trends on how digital technologies impact children's safety and privacy

Digital technologies have required several changes in international and national legislative frameworks, but have also 'changed the social conditions in which people speak' (Balkin 2003: 2). As we increasingly turn to online communication we must not forget that it 'is covered by notions of privacy and correspondence, as are other similar forms of telecommunication, eg voice or video calls or chats over the internet' (Milovanovic 2014: 67). Numerous 'websites, blogs, applications social networks for interaction and expression encompassed our everyday lives, but perhaps no area holds more potential for such transformation than education' (McGeveran & Fisher 2005: 7). In fact, digital learning 'extends beyond formal and traditional institutions to involve everyone with Internet access' (McGeveran & Fisher 2005: 9). Many states have attempted to achieve a balance between guaranteeing the rights of children and protecting them from online risks (Dutton 2010: 53). Nonetheless, although we have increasingly focused on the issues of access to internet (Shah 2015: 11), one scholar has rightly stressed that the children also 'need support, advice, and orientation so technology can empower them to be change-makers in their own communities' (Urbina 2015: 15). In times when the schools increasingly are switching to the online sphere, one may wonder whether children, as a vulnerable group, are sufficiently protected. It has been pointed out that 'the more children use the internet they gain more knowledge and digital skills, thus turning their presence in the online sphere into an advantage', but 'it is also important to remember that not all internet use practices bring them equal benefits' (Livingstone 2015).

Related to this, most research so far has focused on cyber-bullying and the risks that children face in such a context. There have also been studies on parental involvement in online safety of children and whether children have 'a legal or moral right to control their own digital footprint' (Steinberg 2015: 840). In fact, children seem to consider technology as another part of their everyday life (Boyd 2014: 14). One research conducted by Microsoft's Online Safety explored the negative behaviours that children encounter online, and it turned out that the vast majority of children do

the right thing in the digital space, by behaving civilly and appropriately (Beauchere 2015). Although this was a rather positive finding, online safety not only entails children being safe from cyber-bullying, but also includes being safe from any intrusion into their privacy and the protection of their personal data. Freedom of information and public interest sometimes place restrictions on individuals' right to privacy, and concerns 'our reputational information – information about an actor's past performance that helps predict the actor's future ability to perform or to satisfy the decision-maker's preferences' (Goldman 2010: 294). On the other hand, children and the youth usually are unaware of the differences between 'networked publics and other publics they belong to and it is challenging to distinguish between the online and offline versions of themselves' (Palfrey & Gasser 2008). However, it is also their personal data that is endangered while children are online, because they may be free to be collected and processed by third parties, including being used for the creation of 'reputational information' (Krivokapic 2015: 35). Although there are very few situations in which public or private interests require the collection of personal data of children and their processing, the need remains to place restrictions on such data collection and processing for the purpose of child protection against risks to their well-being and rights.

As the demand to use the internet in education has increased daily, scholars have started to stress that 'data protection in schools needs to be closely examined and evaluated' (Kuzeci 2015: 40). In particular, this entails applying not only privacy and data protection principles (such as processing fairly and lawfully; being collected for legitimate, explicit and specific purposes; being relevant, adequate, and not disproportionate in relation to the purposes for which they are collected; being kept for no longer than is necessary for such purposes), but also certain specific conditions for children (Kuzeci 2015: 40). A primary reason for this is that children are still developing and have not yet reached the psychological and physical maturity of adults, which is why they require special attention and care when it comes to protecting privacy and data. Such safeguards comprise internet access limitations, authorisation to give consent and/or the amount of data that would be collected. This was already highlighted by Article 29 Data Protection Working Party in 2008. According to this body, data protection questions regarding children are closely connected to schools as they may 'require forms, containing personal data, to be completed for the purpose of creating student files, computerised or others' (para I). As schools gather such data, they are also required to inform data subjects 'that their personal data will be collected, processed, and for what purpose, who are the controllers, and how the rights of access and correction can be exercised' as well as 'to whom these data may be disclosed' (para III). It seems very clear that, even though schools turn to digital technologies to provide more opportunities to children, 'the risks to children's safety, privacy, mental health, and well-being are equally

wide-ranging' (OECD 2011). However, applications/platforms recently developed and employed for online education seem to pose even more challenges, as demonstrated in the case of Serbia.

4 Background on technology-related privacy issues in Serbia

Over the years there have been major privacy breaches in Serbia. The most common violations refer to the illegal personal data processing, technical measures of data protection and inadequate relation to citizens' data, the illegal interception of electronic communications and publishing information about private life, whereas there have not been so many cases of unauthorised access or unauthorised alterations and insertions of content, as well as computer frauds and other types of violations (Perkov et al 2020). Critically, personal information on many occasions has found its way into public sphere.

For example, one of the biggest privacy problems occurred in 2014, when the website of the Privatisation Agency publicly made available personal data, such as names and unique master citizen numbers, of more than five million people, that is, practically the whole adult population of Serbia (SHARE Foundation 2014). However, even in such a significant case of violation of the right to privacy there was no determined legal accountability due to the statute of limitations. This was the most severe privacy breach of citizens in Serbia and the biggest security oversight in terms of personal data protection. In 2018 the protection of personal data was particularly problematic, because both public and private actors caused relevant violations (Perkov et al 2020). The most important cases were the collection of sensitive personal data via the application 'Selected Doctor', as promoted by the Ministry of Health, and the illegal processing of sensitive data by several social welfare centres in some Serbian cities (SHARE Foundation 2019). Public authorities avoided accepting their responsibility for such events, and this turned out to be a practice when it comes to privacy and personal data breaches. Moreover, in Serbia there was an illegal database of political and economic profiles of 400 000 people, which contained descriptions of citizens and for whom they vote (Perkov et al 2020). Unlike data leaking from the website of the Privatisation Agency three years earlier, where the data was legally collected, this database was created in violation of citizens' constitutional rights. In early 2019 the Minister of the Interior and the Police Director of Serbia announced that Belgrade would receive more than a thousand cutting-edge surveillance cameras with facial recognition capabilities supplied by Huawei, as part of the 'Safe Society' project (SHARE Foundation 2019).

The situation worsened with the introduction of the state of emergency, which was declared on 15 March 2020 (a few days after the first COVID-19 case had been registered) because the pandemic 'highlighted the challenges

in this area in finding the right balance between health care and respect for the confidentiality of personal health data and the right to privacy of citizens' (European Western Balkans 2020). Recently, an extremely serious privacy issue occurred when state bodies published sensitive data about the conditions of citizens who died from complications caused by the coronavirus, and one municipality even published on its official website the initials, age, workplace and street address of infected persons (SHARE Foundation 2020). The most serious case was the incident when login credentials for the COVID-19 Information System, used to process sensitive health data of citizens in connection with the pandemic, were publicly available on a website of one healthcare institution for eight days, which is enough to be indexed by Google and searchable (SHARE Foundation 2020). This has showed a severe breach of protection of the most sensitive data (health data), illustrating the disrespect for privacy and the low level of personal data protection in Serbia.

When the educational system abruptly turned to the digital sphere during the pandemic, the personal data of children came online even more. The Serbian Ministry of Education stated that classes would be held via distance learning through the programme of public broadcasters, as well as through online learning platforms. Such a type of schooling organisation, therefore, has forced students to create profiles on numerous platforms and share their private information, also forcing teachers to more than usually enter information about students into the electronic teacher's book. Crucial questions thus arise in relation to the right to privacy of children and are explored below: Were relevant and appropriate online learning/teaching tools used? Was there enough awareness of the potential risks to children's data as well as their privacy in such a digital environment?

5 Emerging issues in online schooling (technology) applied in Serbia and the effects on children's privacy

In looking at the recent and unexpected practice of schools in Serbia, which had to switch to different kinds of equipment, digital learning platforms, video lessons, broadcasting through radio and television and so forth, basic questions arise as to whether or not schools properly limited the number of ways used for the learning experience and whether they chose adequate platforms for children. In this regard several considerations may be elaborated.

First, a large number of different platforms made it difficult for students to follow some lessons such as mathematics, which has proven to be the biggest challenge for the students to understand and follow (BBC News, Serbia 2020). In Serbia the students primarily relied on Facebook groups, Messenger, Skype, Google Classroom, Viber, WhatsApp,

Moodle, Edmondo, Zoom, Microsoft Teams, their gmail accounts, and many more. Notably, even Google recently was said to be 'using its services to create face templates and "voiceprints" of children ... through a program in which the search giant provides school districts [across California] ... free access to G Suite for Education apps' (Nieva 2020). Zoom and Skype were the most popular video-conferencing platforms for communicating in Serbian schools. However, the problem is that these platforms 'collect a great deal of personal information about students', which can lead to 'long-term risks to student privacy and autonomy' (Bailey et al 2020). For instance, according to Zoom's privacy and security policy, data collected includes a user's name and other similar identifiers, a student's school, the student's device, network and internet connection and the student's use of the Zoom platform, including actions taken, date and time, frequency, duration, quantity, quality, network connectivity, and performance information related to logins, clicks, messages, contacts, content viewed and shared, calls, use of video and screen sharing, meetings and cloud recording (Bailey et al 2020). On the other hand, using Skype meant accepting Microsoft's general privacy policy. In addition, some platforms such as ClassDojo 'drew criticism over collecting vast amounts of data on children, raising questions about whom it shares this data with, and where it is stored' (UNESCO 2020). DingTalk was enabling teachers to remotely monitor students without consent, and Google's G Suite for Education was recently sued for collecting information on children without parental consent (Han 2020). Furthermore, in Serbia it emerged that some teachers did not have computers or wi-fi at their homes, while their mobile connection to the internet was not strong enough to hold all the platforms and conduct all the activities in order to conduct lessons (Danas 2020). Some schools gave laptop computers to some of the teachers in need, while others tried to share an internet connection with their neighbours to conduct classes (Danas 2020). However, although Serbian schools attempted to solve the issue of access, there may have been very few considerations regarding children's privacy. In fact, students had to create profiles in different platforms in order to follow classes and often were obligated to accept new friends, such as their classmates and teachers, even though this option may influence their privacy. Specifically, even if their profiles are officially 'private' and they have a variety of posts on them, during this phase they were forced to share them with their teachers. Teachers as well as students were required to share their cellular phone numbers, because sometimes there were 15 Viber groups to join in order to get in touch (Danas 2020). In this regard, it is questionable whether the platforms used in Serbia respected children's privacy, or whether they put them in the online sphere without adequate protection.

Furthermore, teachers received a large amount of students' data to be entered into online platforms. According to the SHARE Foundation (2020), in Serbia another platform collected data more than before the

pandemic, namely, the electronic teacher's book that represents an attempt to digitise mandatory records of pupils and students, which are kept by schools in accordance with the Law on the Basics of the Education System of 2017; but there are no guarantees that the subsequent (and imperfect) Law on Data Protection has been applied on the teachers' e-book. One may even wonder whether there is a disconnection between these two laws and how it will affect the personal data protection of students. This practice is called esDnevnik, which is a part of the Unified Information System in Education (UISE) consisting of several registries that contain personal information about pupils, parents and employees. However, according to publicly available information, UISE still is not established or operational. In addition, a private company has developed software called ***eSkola***, which should function in a manner similar to ***esDnevnik***, but with additional features for parents, depending also on the service 'package' they choose for and are prepared to pay. Interestingly, it turned out that all the data contained on ***esDnevnik*** could also be found on ***eSkola***. The privacy of Serbian children, therefore, has become even more questionable as children's education data seems to be far less safeguarded than health data.

It has been highlighted that generally a large degree of a child's data is collected by schools and their vendors when a child is online. In addition to 'basic information – name, email address, grades and test scores', other pieces of data can be collected on students, such as biometrics; personally identifiable information; behavioural, disciplinary and medical information; academic progress; geolocation; Web browsing history; IP addresses utilised by students; and classroom activities (Strauss 2020). As we witnessed many breaches in relation to health data, one may wonder what could happen with children's data that can be just as sensitive – disclosing names, home addresses, behaviours, and other highly personal details 'that can harm children and families when misused' (Han 2020). It is worth noting that in March 2020 UNESCO recommended to 'provide support to teachers and parents on the use of digital tools', (i) by organising brief training or orientation sessions for them 'if monitoring and facilitation are needed', and (ii) by helping 'teachers to prepare the basic settings such as solutions to the use of internet data if they are required to provide live streaming of lessons (UNESCO 2020). Thus, as students' data has become more and more available online, it is questionable whether there has been enough awareness of the significance of privacy among both teachers and students in Serbia, as well as whether Serbian schools have factored data privacy considerations in their selection criteria to use certain learning tools.

More precisely, taking into account the data on computer literacy, which is about 30 per cent (Stojanovic et al 2017) and media literacy ranking where Serbia ranks thirtieth out of 35 European countries (Zvijerac 2020),

it is questionable to what degree Serbia was prepared for such a shift into online education. According to research conducted in 2018 by the Belgrade Institute of Psychology, and covering 60 schools in Serbia, with children and young people aged nine to 17 years, most of the children and teens (86 per cent) used the internet on a daily basis; the students mostly spent more than three hours a day online, and more than 20 per cent of them spent up to seven hours a day on weekends, while two-thirds spent between four and seven hours; at normal time 40 per cent of students used the internet for school assignments at least once a week. It was also found that in 2018 more than two-thirds of children and young people had a profile on some social network or gaming platform, although some of them have age limitations (Kuzmanović et al 2019: 24). According to these researchers, almost half of the students aged nine to 12 years did not know how to change their privacy settings on social networks, which is rather disturbing. Focusing on their behaviour on social networks, in the schools in Vojvodina reportedly fewer than half the students read or at least glanced over the terms of use when opening their profiles, whereas 35 per cent had to say that they were older than they actually were, due to the network policies and the age limits (Report on online schooling 2020). This report also indicates that slightly fewer than 35 per cent stated that their parents had a password for their related profiles, but more than 50 per cent said that their parents were either their followers or friends on social networks, which could be a positive trend.

According to the mentioned scholars, it appears that 16 per cent of students experienced cyber-bullying, while some of them engaged in some other type of risky behaviour online. Most often, the risky behaviour involved sharing personal information, adding strangers on social media, and making contact with strangers whom they may later meet offline (Kuzmanović et al 2019: 12). Furthermore, in the schools in Vojvodina, reportedly most students believe that they are familiar with their online rights, although it seems that not all of them are entirely sure what their online rights entail. Related to this, the privacy of 45 per cent of children reportedly were violated to a greater or lesser extent so far (Report on online schooling 2020). Thus, it is questionable whether this vulnerable group of internet users still require more tools and knowledge to be able to clearly point at a privacy problem when they notice it, especially in times when they are required to spend more time online than usual.

In 2018 the Serbian Ministry of Education, Science and Technological Development proposed that secondary schools introduce Media Literacy in their curricula. Some schools have introduced the subject as an elective but, according to SHARE Foundation, potential teachers did not have sufficient training to give these lessons, even though they should contain digital literacy. In this manner, the students were deprived of learning how to behave in an online sphere, to identify risks and opportunities, to know

what information security is, how to recognise cyber-bullying, and so forth (UNICEF Serbia 2019). Such digital skills would have been especially useful during the recent emergency when students had to be online more than usual, in order to attend school, but also to share their personal data with more people. It seems that Serbia follows scholars' recent findings whereby 'schools are not always aware of or attuned to the range of online privacy and security implications' and this can be seen as 'compounded by the fact that privacy notices and terms of service agreements are rife with vagueness, legalese and double-speak' (Bailey et al 2020).

6 Conclusion

The issue of the privacy of children can become an increasingly controversial topic as internet education technologies gain momentum. The COVID-19 pandemic brought the problems of balancing children's rights, such as privacy with the application of online teaching technologies and platforms, to the fore. In fact, it has become questionable whether children, as the most vulnerable group, would be adequately safeguarded in times when they are required to spend much of their time online for education purposes. In the case of Serbia, citizens' rights to privacy have encountered several major challenges even before the state of emergency was declared in March 2020 and the schooling activities fully shifted online. The extended use of technology to minimise learning disruptions related to COVID-19, therefore, has led to raise a basic question as to whether children's rights to privacy were adequately respected and protected or, instead, challenged when the students were required to use a range of programmes, applications and networks to attend classes.

We may conclude that, even though the educational system in Serbia attempted to be adaptable by the very attempt of going online, the reviews and reconsiderations are yet to come in the next academic years, hopefully starting from the forthcoming year. Between March and June 2020 the subjects were scattered all over different platforms, requiring the students to open their profiles and exposing their personal information much more than usual. The vulnerability of children seems to have increased even more because there was no preparation that would clearly indicate what information they may share and what would be dangerous in the online sphere. In this manner, children's rights to privacy have been jeopardised, with their data available on many platforms as teachers had to place them into *esDnevnik*. However, as correctly observed by some scholars, 'it is not the job of individual educators to dig through legal terms and decide what kinds of protections students will or will not have with respect to their data'. Instead of teachers, 'ministries, departments of education and school districts need to offer clear guidance to help educators navigate decisions about educational technology' (Bailey et al 2020). In the case of Serbia these observations should first lead to crucial changes in national policies

regarding the privacy of children, because the new Law on Personal Data Protection is not sufficient for safeguarding students' personal data, and in any case has not been properly implemented yet. Serbia should urgently make its legislative framework compliant with existing international standards that provide protection for the digital rights of children, and particular attention should be paid to the core implications deriving from the proper implementation of the four guiding principles of CRC. In this regard, a new National Plan of Action for Children should be adopted and serve as a basis for effective budgeting for and monitoring of (desirable) policies on their digital rights, including in specific relation to privacy. Strengthening role of the (governmental) Council for Child Rights to coordinate all activities related to the implementation of CRC at cross-sectoral, national and local levels could also be beneficial in this regard. Similarly, the Committee on Child Rights of the National Assembly should scrutinise the adoption and implementation of policies regarding legislation relevant to digital literacy and the protection of the right to privacy in relation to online education. In parallel, the key stakeholder regarding the protection of personal data in Serbia, namely, the Commissioner for Information of Public Importance and Personal Data Protection, should strengthen its own capacities to be able to focus on the prevention of privacy breaches. The improvement of the overall knowledge about privacy rights, especially in the public sector, would advance the capacity of the Office of the Commissioner to fulfil its mandate. Relevant Serbian stakeholders, starting with the government, should certainly follow the aforementioned CoE guidelines contained in Recommendation CM/Rec(2018)7, which regrettably have not been aptly discussed at the national level. Hopefully, the forthcoming General Comment by the CRC Committee will provide further guidance on the specific issue of children's rights to privacy in relation to online education.

A genuine fear in relation to the recent online practices of schools around the world is that 'today's choices will affect privacy and equality in education long after this pandemic ends' (Bailey et al 2020). While hardly any country or school system was prepared for such an unforeseen switch to online teaching without planning and in emergency mode, the various problems highlighted as a result of these changes in the Serbian case should inspire specific efforts to improve national practices and safeguard children's rights in future online teaching exercises and to provide safe access to platforms. In particular, attention should be paid to training those who collect and process. Organisations and institutions that process personal data in the country, including schools, should involve data protection officers to comply with the international standards and to guarantee such protection, thus avoiding legal risks, whereas their users could be able to ensure their own rights more easily. In parallel, it seems that Serbia's citizens generally have little knowledge of their rights as data subjects due to a weak privacy-related culture in Serbian society. It is

positive that more citizens are recognising the importance of personal data protection, but most Serbians are not aware of the protection mechanisms under the new Law on Personal Data Protection and other relevant instruments. In this vein, teachers, students and parents should also be better educated, although this new law does not sufficiently address the problems specifically discussed in this article.

The case of Serbia shows that a country with little practice of personal data protection in general can lead to very serious forms of citizens' privacy breaches. As the educational system has turned to the online sphere more than before, children's privacy has become ever more questionable as there have been neither clear guidelines on the use of the electronic teacher's book, nor on online education overall. In Serbia all schools and individual teachers used different platforms to conduct classes during the pandemic, which made children's data even more vulnerable, in addition to the teachers' e-registry issue. This case illustrates a strong need for adequate media and digital literacy classes and courses, both for teachers and students in order to become familiar with their rights and obligations on the internet. It also illustrates a strong need for more actions from public authorities which should regularly monitor the respect of privacy in relation to children's education data and, accordingly, adopt appropriate measures. For instance, there should be clear regulations on how children's personal data in e-registry is handled and how students or their parents can request the deletion of data. In this manner children's data and privacy would be protected and any type of commercialisation of personal data could be avoided. Public authorities could even require educational technology companies to make binding statements as to how they intend to legally and ethically protect current student data, future student data, and access to both under their own ownership. In addition, the Ministry of Education should share the Digital Violence Prevention and Response manual with all schools, in order to present a good practice in the prevention of digital violence and organise related trainings. Educational institutions should also be informed about the Call Centre for Reporting of Digital Violence of the Ministry of Trade, Tourism and Telecommunications and the 'SOS line' for reporting violence in schools. The Department for the fight against high-technology crime (which, among other things, deals with cases of unauthorised data processing, unauthorised access to a computer/computer network/programme) should become more active in protecting students on the internet and, although an international contact point 24/7 for high-tech crime exists within the CoE, Serbian police administration units should familiarise themselves with this.

The way in which children's privacy has been exposed in relation to internet education technologies in Serbia may even exist in other countries of the region, and further research should be undertaken to investigate this and effectively counter related problems. For example, the critical case of

Serbia indicates an urgent regional need to expand on the already-existing wider research with regard to several major issues that have recently been documented by scholars and that are possible 'by-products' of the data practices of educational technology companies, such as 'corporate tracking of student activities both inside and outside of the classroom, discrimination against young people from marginalized communities, student loss of autonomy due to ongoing monitoring of their activities and sale of student data to third parties often for purposes of advertising to them' (Bailey et al 2020). They have also found that 'large amounts of personal and transactional information some companies collect can also open students up to privacy invasions by future employers', and 'such collection vastly increases the potential for educational surveillance of students through students' datafication'.

References

Article 29 Data Protection Working Party (2009) Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the special case of schools) 11 February 2009, 398/09/EN WP 160, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf (last visited 25 June 2020)

Bailey J, Burkell J, Regan P & Steeves V 'Children's privacy is at risk with rapid shifts to online schooling under coronavirus' *The Conversation* 21 April 2020, available at https://theconversation.com/childrens-privacy-is-at-risk-with-rapid-shifts-to-online-schooling-under-coronavirus-135787 (last visited 23 June 2020)

BBC News Serbia 'Korona virus i škola na televiziji: Pohvala za nastavu, ali mogli su bolji kadar da nađu' (Corona virus and school on TV: Praise for teaching, but the staff could have been better) 17 March 2020, available at https://www.bbc.com/serbian/lat/srbija-51929499 (last visited 10 April 2020)

Beauchere J 'Safety experts call for research on true harms of "the darker web"' in *Digitally Connected: Global Perspectives on Youth and Digital Media* (2015) Berkman Centre Research Publication 2015-6, 30-31, available at https://ssrn.com/abstract=2585686 (last visited 10 April 2020)

Boyd D (2014) *It's complicated: The social lives of networked teens* Yale University Press

Child Pact 'Serbia: MODS at the 8th Meeting of Children's Rights Council', 5 November 2019, available at https://www.childpact.org/2019/11/05/serbia-mods-at-the-8th-meeting-of-childrens-rights-council/ (last visited 23 June 2020)

Child Pact 'Children's rights in Serbia: From legislation to action' (2017), available at www.childpact.org/2017/03/21/childrens-rights-in-serbia-from-legislation-to-action/ (last visited 8 April 2020)

Danas 'Internet najveći problem za onlajn nastavu' 20 March 2020, available at https://www.danas.rs/drustvo/internet-najveci-problem-za-onlajn-nastavu/ (last visited 10 April 2020)

Danas 'Onlajn nastava: Agonija i za nastavnike i za đake' 25 March 2020, available at https://www.danas.rs/drustvo/agonija-i-za-nastavnike-i-za-djake/?fbclid=IwAR2VAp8Mjq79_DQGNFRzeVFxqTN6zJIUcFO2Ball9s1cW7xzvwMIAPh7fqg (last visited 3 April 2020)

Electronic Frontier Foundation (EFF) 'Protecting civil liberties during a public health crisis' 10 March 2020, available at https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-public-health-crisis (last visited 3 April 2020)

European Digital Rights (EDRi), 'EDRi calls for fundamental rights-based responses to COVID-19' 20 March 2020, available at https://edri.org/covid19-edri-coronavirus-fundamentalrights/ (last visited 23 July 2020)

European Western Balkans 'EC non-papers note pressures on judiciary and media in Serbia and Montenegro' 15 June 2020, available at https://europeanwesternbalkans.com/2020/06/15/ec-non-papers-note-pressures-on-judiciary-and-media-in-serbia-and-montenegro/ (last visited 20 June 2020)

Goldman E 'The regulation of reputational information' in B Szoka & A Marcus (eds) *The next digital decade: Essays on the future of the internet* (2010) Washington DC: TechFreedom

Grin F (2003) *Language policy evaluation and European Charter for Regional or Minority Languages* United Kingdom: Palgrave Macmillan

Han HJ 'As schools close over coronavirus, protect kids' privacy in online learning: Education products adopted now may long outlive today's crisis' *Human Rights Watch* 27 March 2020, available at: https://www.hrw.org/news/2020/03/27/schools-close-over-coronavirus-protect-kids-privacy-online-learning (last visited 19 June 2020)

Jansen Reventlow N 'Digital rights are human rights' *Digital Freedom Fund* 10 December 2017, available at https://digitalfreedomfund.org/digital-rights-are-human-rights/3/ (last visited 1 April 2020)

Krivokapić D et al 'Guide: Centre for the Prevention of ICT Risks (CERT)' (2017) *SHARE Foundation*, available at https://resursi.sharefoundation.info/wp-content/uploads/2018/10/cert_vodic.pdf (last visited 20 June 2020)

Krivokapić D, Petrovski A & Malinović S 'Information security: Guide for ICT systems of special importance' (2017) *SHARE Foundation*, available at https://resursi.sharefoundation.info/wp-content/uploads/2018/10/vodic_za_ikt_sisteme_od_posebnog_znacaja.pdf (last visited 20 June 2020)

Krivokapić D, Adamović J, Tasić D et al 'Guide on law on personal data protection and GDPR – Interpretation of the new legislative framework' (2018) *SHARE Foundation*, available at https://www.sharefoundation.info/Documents/vodic_zzpl_gdpr_share_2019.pdf (last visited 18 June 2020)

Krivokapic D & Adamovic J 'Data flow in the information system COVID-19' (2020) *SHARE Foundation*, available at https://www.sharefoundation.info/sr/tokovi-podataka-covid-19/ (last visited 19 June 2020)

Krivokapi D 'Who should take care of identity, privacy and 35 reputation?' in *Digitally connected: Global perspectives on youth and digital media* (2015) Berkman Centre Research Publication 2015-6 35-39, available at https://ssrn.com/abstract=2585686 (last visited 3 April 2020)

Kuzeci E 'Education, children, and (lack of) privacy: The story of the Fatih project in Turkey' in *Digitally Connected: Global Perspectives on Youth and Digital Media* (2015) Berkman Centre Research Publication 2015-6 40-43, available at http://dx.doi.org/10.2139/ssrn.2585686 (last visited 3 April 2020)

Kuzmanović D, Pavlović Z, Popadić D & Milosevic T 'Internet and digital technology use among children and youth in Serbia: EU kids online survey results, 2018' (2019) Belgrade: Institute of Psychology, Faculty of Philosophy, available at http://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/participant-countries/serbia/EU-Kids-Online-ENG-2019.pdf (last visited 2 June 2020)

Lievens E, Livingstone S, McLaughlin S et al 'Children's rights and digital technologies' in U Kilkelly & T Liefaard (eds) *International human rights of children* (2019) Singapore: Springer Nature 487

Marwick AE, Murgia Diaz D & Palfrey J 'Youth, privacy and reputation' (2010) Public Law and Legal Theory Working Paper Series, Paper 10-29, Berkman Centre Research Publication 2010-5, available at http://ssrn.com/abstract=1588163 (last visited 8 April 2020)

Microsoft (2012) *Online safety research*, available at http://www. microsoft.com/security/resources/research.aspx#onlinebullying (last visited 3 April 2020)

Milovidov E 'Children's rights in the digital environment: Paper for the European Network of Ombudspersons for Children (ENOC) on the evidence supporting the drafting of a statement on Children's Rights in the Digital Environment' (2019) *ENOC*, available at http://enoc.eu/wp-content/uploads/2019/10/FINAL-ENOC-Evidence-Paper-Sept-2019.pdf (last visited 3 April 2020)

Netokracija N '"Online" nastava ima svoje bagove – prvi časovi ipak krenuli (Online teaching has its glitches – first classes begin after all) 17 March 2020, avcailable at https://www.netokracija.rs/online-nastava-srbija-166837 (last visited 10 April 2020)

Nieva R 'Two children sue Google for allegedly collecting students' biometric data' 3 April 2020, available at https://www.cnet.com/news/two-children-sue-google-for-allegedly-collecting-students-biometric-data/ (last visited 20 June 2020)

OECD 'The protection of children online: Risks faced by children online and policies to protect them' (2011) OECD Digital Economy Papers 179 OECD Publishing, Paris, available at https://dx.doi.org/10.1787/5kgcjf71pl28-en (last visited 25 June 2020)

Palfrey J & Gasser U (2008) *Born Digital: Understanding the first generation of digital natives* New York: Basic Books

Perkov B et al 'Error 404: Digital rights in Serbia 2014-2019' October 2019 *SHARE Foundation*, available at https://resursi.sharefoundation.info/wp-content/uploads/2019/11/Greska_404.pdf (last visited 18 June 2020)

Petrovski A 'Guide: Digital security fundamentals' (March 2015) *SHARE Foundation*, available at https://resursi.sharefoundation.info/wp-content/uploads/2018/10/vodic_osnove_digitalne_bezbednosti_-_preview.pdf (last visited 20 June 2020)

Petrovski A & Ercegović K 'Guide: Security of organizations in the digital environment' (October 2015) *SHARE Foundation*, available at https://resursi.sharefoundation.info/wp-content/uploads/2018/10/vodic_bezbednost_organizacija_u_digitalnom_okruzenju.pdf (last visited 20 June 2020)

Recommendation CM/Rec(2018)7 of the Committee of Ministers, 'Guidelines to respect, protect and fulfil the rights of the child in the digital environment' Council of Europe, September 2018, available at https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a (last visited 3 April 2020)

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, and repealing Directive 95/46/EC (General Data Protection Regulation)

Republic of Serbia Regulation on Children Safety and Protection in the Use of Information and Communication Technologies, Official Gazette of the Republic of Serbia, 61/16

Report on online schooling for the schools in Vojvodina (2020) Provincial Ministry of Education, Serbia

Republic of Serbia, Government Office for Human and Minority Rights, Comments of the Republic of Serbia on the proposal of the concept of General Ccomment on the Rights of children in relation to the digital environment, 2019

Republic of Serbia, Law on Protection of Personal Data, Official Gazette of the Republic of Serbia 87/2018

Republic of Serbia, Decision on the List of Types of Personal Data Processing Operations for Which an Assessment of the Impact on the Personal Data Protection Must be Performed and the Opinion of the Commissioner for Information of Public Importance and Personal Data Protection Must be Sought, Official Gazette of the Republic of Serbia 45/2019

Ristic M 'Insults, leaks and fraud: Digital violations thrive amid pandemic' (2020) *BalkanInsight*, available at https://balkaninsight.com/2020/06/03/insults-leaks-and-fraud-digital-violations-thrive-amid-pandemic/ (last visited 20 June 2020)

Ristic M, Stojanovic M, Sirotnikova MG et al 'Europe's other coronavirus victim: Information and data rights' Balkan Investigative Reporting Network (BIRN) 24 March 2020, available at https://balkaninsight.com/2020/03/24/europes-other-coronavirus-victim-information-and-data-rights/ (last visited 20 June 2020)

Shah N 'Networked margins: Revisiting inequality and intersection' in *Digitally connected: Global perspectives on youth and digital media* (2015) Berkman Centre Research Publication 2015-6, available at SSRN: https://ssrn.com/abstract=2585686 (last visited 10 April 2020)

SHARE Foundation Monitoring Database, available at http://monitoring.labs.rs/ (last visited 3 April 2020)

SHARE Foundation Digital Rights Monitoring Reports, available at: https://resursi.sharefoundation.info/sr/monitoring-digitalnih-prava-i-sloboda/ (last visited 19 June 2020)

SHARE Foundation Personal data of more than 5 million citizens of Serbia unlawfully published, 24 December 2014, available at https://resursi.sharefoundation.info/en/resource/personal-data-of-more-than-5-million-citizens-of-serbia-unlawfully-published/ (last visited 18 June 2020)

SHARE Foundation 'Unlawful video surveillance with face recognition in Belgrade' 4 December 2019, available at https://www.sharefoundation.info/en/unlawful-video-surveillance-with-face-recognition-in-belgrade/ (last visited 23 June 2020)

SHARE Foundation 'A password pandemic. How did a COVID-19 password end up online?' 23 April 2020, available at https://www.sharefoundation.info/en/a-password-pandemic/ (last visited 23 June 2020)

Steinberg S 'Sharenting: Children's privacy in the age of social media' (2017) 66 *Emory Law Journal* 839; University of Florida Levin College of Law Research Paper 16-41, available at https://ssrn.com/abstract=2711442 (last visited 8 April 2020)

Steiner HJ, Alston P & Goodman R (2008) *International human rights in context: Law, politics, morals: Text and materials* Oxford: Oxford University Press

Strauss V 'Five concerns about the mass rush to online learning that shouldn't be ignored' *Washington Post* 30 March 2020, available at https://www.washingtonpost.com/education/2020/03/30/five-concerns-about-mass-rush-online-learning-that-shouldnt-be-ignored/ (last visited 23 June 2020)

Stojanović T, Penjišević I, Lukić T & Zivkovic JV 'Computer literacy of young people in Serbia and regional differences' (2017) 21 *Geographica Pannonica* 43, available at DOI:10.5937/GeoPan1701043SCorpus ID: 56071125 (last visited 3 April 2020)

UNESCO 'COVID-19: 10 Recommendations to plan distance learning solutions' 6 March 2020, available at https://en.unesco.org/news/covid-19-10-recommendations-plan-distance-learning-solutions (last visited 18 June 2020)

Popadić D, Pavlović Z, Petrović D & Kuzmanović D 'Global kids online Serbia: Balancing between opportunities and risks. Results from the Pilot Study' (2016)

Belgrade: University of Belgrade, available at www.globalkidsonline/serbia (last visited 11 April 2020)

UNICEF Serbia 'Child protection" available at https://www.unicef.org/serbia/en/topics/child-protection (last visited 19 June 2020)

UNICEF Serbia, Šta je digitalno nasilje i kako da ga zaustavimo? Available at https://www.unicef.org/serbia/zaustavimo-digitalno-nasilje (last visited 10 April 2020)

UN Committee on the Rights of the Child (2003) General Comment 5 on the General Measures of Implementation of the Convention CRC/GC/2003/5

UN Committee on the Rights of the Child (2013) General Comment 14 on the right of the child to have his or her best interests taken as a primary consideration (art 3, para 1) CRC/C/GC/14

UN Committee on the Rights of the Child (2020) CRC COVID-19 Statement, 8 April 2020

UN Human Rights Council (2016) Resolution on the promotion, protection and enjoyment of human rights on the internet A/HRC/32/L.20

Urbina C 'Libraries driving access to information and digital literacy for children and youth: Going "beyond access" to promote ownership and agency of ICT tools for development' in *Digitally connected: Global perspectives on youth and digital media* (2015) Berkman Centre Research Publication 2015-6, 15-17, available at https://ssrn.com/abstract=2585686 (last visited 8 April 2020)

Zvijerac P 'Media illiteracy in the Western Balkans' *Free Europe* 10 February 2020, available at https://www.slobodnaevropa.org/a/zasto-medijska-pismenost-vejzovic/30427144.html (last visited 17 June 2020)