TRANSPARENT KIDS: HOW ALGORITHMIC SURVEILLANCE CHALLENGES THE PROTECTION OF CHILDREN'S RIGHTS ONLINE

Ivana STEPANOVIĆ, PhD¹ Olivera PAVIĆEVIĆ, PhD² Ljeposava ILIJIĆ, PhD³

Algorithmic surveillance embedded in social media is not simply an organising principle that regulates visibility, sorts the content, and polices the online spaces. It is a business method of commodifying personal data that stimulates the production of various forms of digital violence due to its virality potential. Ethical guidelines that are set to prevent or penalise cybercrimes are always external to the logic of the market and the algorithms themselves because they prioritise engagement and reproduction of data at any cost. Children are especially vulnerable because they are under constant surveillance while the price of opting out is too high. This paper analyses the processes of data commodification and stresses the importance of developing the legal framework for the protection of the digital rights of children while emphasising the need to reassess the impacts of surveillance practices and find comprehensive solutions against the systemic abuse of children's data online.

KEY WORDS: algorithmic surveillance / social media / children's rights / digital rights, digital violence

¹ Research Fellow, Institute of Criminological and Sociological Research in Belgrade and Institute of Advanced Studies Kőszeg, ivana.stepanovic@iask.hu

² Research Fellow, Institute of Criminological and Sociological Research in Belgrade, oliverapavicevic4@gmail.com

³ Research Fellow, Institute of Criminological and Sociological Research in Belgrade, lelalela_bgd@yahoo.com

1. INTRODUCTION: DIGITAL RIGHTS OF A CHILD IN THE AGE OF ALGORITHMIC SOCIAL SORTING

The COVID-19 pandemic has exacerbated the digital transformation of the social, leaving children vulnerable to surveillance and data misuse without adequate legal protection against technologies they use every day for education, communication, and entertainment. Almost overnight, their everyday lives have shifted from physical spaces of schools and kindergartens to virtual classrooms and play areas. While all the efforts were focused on protecting the population from the imperceptible virus particles, little was done to safeguard children from the invisible dangers of the underregulated sphere of the internet. Sophisticated communication technologies expose children to intrusive algorithmic surveillance. Phones, tablets, cameras, smartwatches, and other gadgets can capture the most private data such as eye and muscle movements, breathing rhythms or tone of a voice that reveal the innermost thoughts, feelings, and intentions. Notorious for knowing people better than they know themselves, these technologies are the magnifying glass that makes children transparent, hackable, and manipulable. The digital transformation opened possibilities for distant learning and socialising along with remote surveillance and even algorithmically reproduced digital violence.

While there are many benefits of communication technologies, including the accessibility of information, availability of education and endless possibilities to connect with peers or play games online, there are also significant dangers that come with them. Misuse of data, cyberbullying and social media addiction are only some of the issues that are jeopardising children's rights and their wellbeing, while the impact of permanent algorithmic surveillance and social sorting remains to be a neglected issue. Many parents are not aware that everyday gadgets and devices with internet connectivity double as surveillance technologies or that the social media and gaming industry utilise the algorithms for the purposes of digital marketing and sales regardless of whether they are violating children's rights. These commercial practices of digital production can be interpreted as practices of exploitation of children through the extraction of their behavioural data. Given that normalised practices of data surveillance governed by platforms' algorithms routinely violate children's privacy and other rights and freedoms, it is questionable whether they truly operate in the best interest of the child.

Children are exposed and vulnerable online despite the efforts to create legislation to regulate their digital rights or build complex protective mechanisms such as parental controls and specialised platforms designed especially for children. The main challenge to protecting their rights in online spaces is the systemic data collection that is incorporated in both hardware and software and that draws the economic processes on digital platforms from Google to TikTok. Just like grownups, children are involved in digital production and consumption. By participating in these processes, they become precarious producers, manipulated consumers and the products of their own labour. While the legislative framework for the protection of digital human rights in the age of algorithmic surveillance is still in its infancy worldwide, the basic principles of protecting children online are contained in international regulations such as the Convention on the Rights of the Child. Nevertheless, it is crucial to assess how fast-developing technologies collide with these principles and systemically violate children's rights.

2. ALGORITHMIC SURVEILLANCE AND SYSTEMIC EXPLOITATION OF CHILDREN ON DIGITAL PLATFORMS

One of the key issues with contemporary communication technologies is their capability to extract, store, analyse, interpret, and reproduce personal data. Monitoring users' behaviour while they are utilising the apps, platforms, mobile phones, and other technologies has been fully normalised even though these practices are in principle violating privacy rights. Algorithms built into these technologies are surveillance-based and created to serve the commercial needs of companies who create these technologies. Surveillance is therefore the method of digital production, while privacy is reduced from the right to protect personal data to the right to express consent for personal data collection and processing while retaining only partial control over the use of these data.

On the surface, digital technologies appear as useful tools for education, socialising, and entertainment. They were proven especially valuable during the COV-ID-19 pandemic when the whole world submerged in lockdowns and the internet offered a means to continue with normal life without leaving home. However, these technologies develop faster than it is possible to properly regulate them and prevent misuse and manipulation. It takes time for ethical conventions to adapt to new technologies, and it is especially difficult to regulate the imperceptible violations of human rights such as algorithmic surveillance that chronically lacks transparency and oversight. In the absence of legislation that would put algorithmic practices under scrutiny, privacy rights are systematically violated purely because the entire digital production relies on harvesting personal data. In other words, children's digital doubles are exposed to algorithmic surveillance in everything they do online, and this essentially means that they are being exploited. Their 'play labour' that consists of prosumtion (Fuchs, 2014) of games, social media and other content is not considered illegal unpaid child labour, but the question is whether it should be.

Algorithmic surveillance and digital exploitation of children are potentially violating several articles of the Convention on the Rights of the Child. Namely, Article 14 stipulates that a child's freedom of thought and conscience should be respected, and it can be argued that social media algorithms could be violating this right. It is now commonly accepted that social media and other platforms use certain tools to manipulate opinions and impact the decision-making of consumers (Darmody & Zwick, 2020: 1). More broadly, the algorithms have become "the fundamental arbiters of human experience" even though they are "designed, programmed, and implemented by imperfect people who exist in a profit-first kind of world" (Johnson, 2021: 34-37). They determine what is going to be visible to whom according to their calculations and analyses of behavioural data. This means that they are infiltrating the social fabric by mediating our online searches as well as our digital production and consumption which allows the big tech companies to reproduce a parallel virtual world or a kind of a 'metaverse' that escapes the logic of ethics and law. The newly proposed Digital Services Act⁴ could be an attempt to regulate the online platforms and impose new rules to better protect users against the algorithms.

Children are not spared from the digital marketing machinery and algorithmic reproduction based on data surveillance. In fact, it can even be said that "the world in which the contemporary child is conceived and raised is one that is increasingly monitored, analysed and manipulated through technological processes" and that there is a substantial "power of algorithms within the everyday of the child" (Willson, 2018: 620). Even though the Article 17 stipulates that a child should have access to "information and material from a diversity of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and physical and mental health", it is questionable to what extent this diversity of information can be achieved given that the architecture of information on the internet is organised by the pre-set algorithms. But while there are various "types of algorithmic approaches in raising and imagining the 'ideal child" (Willson, 2018: 620), there are also undercurrent tendencies to impose a certain market logic to the digital production and consumption or prosumption (Gerbaudo 2015: 81; Dyer-Witheford 2015: 92; Duffy et al 2021: 1).

These economic processes rely on big data surveillance that becomes overly intrusive and even "intimate" to such an extent that is capable of scanning thoughts and emotions to predict or even guide behaviour (Ruckenstein & Granroth, 2018: 1), which is why it routinely violates child's right to privacy defined in the Article 16 of the Convention. This article says that "no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence,

⁴ Digital Services Act eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218& uri=COM%3A2020%3A825%3AFIN Accessed on 25.04.2022.

nor to unlawful attacks on his or her honour and reputation". With normalised surveillance of communications technologies that have become a significant part of a child's everyday life, it can be claimed that children's digital privacy is consistently and systematically breached. Given that General Data Protection Regulation⁵ outlines the conditions under which it is legitimate to process personal data, online platforms are not engaging in unlawful practices, strictly speaking. Their business models involve the collection and analysis of data for profile targeting, and they offer the option for users to give their consent which is in line with the GDPR (Kardefelt-Winther, 2019: 22), but it is questionable whether such a mechanism satisfies the best interests of the child principle, especially if we consider the fact that very young children tend to use these platforms and consent to the processing of their personal data without knowing what it entails. Furthermore, it is possible to question the ethical justification of the intrusions into the privacy sphere even though they are not violating the existing laws, especially practices such as facial recognition and psychological profiling (Sharon, Koops, 2021: 331).

Algorithmic surveillance that is guided by the market needs of platforms inadvertently leads to exploitative practices of prosumption. Children are continuously engaged in unpaid digital labour of production and consumption on social media, gaming apps and other platforms. They are never simply passive users of technology, but rather active producers as their clicks, views, likes or gaming activities are the key production activities. At the same time, they are systematically monitored, analysed, and manipulated by the algorithms which consequently transform them into products of their own digital labour. As a result, children are involved in the circle of digital exploitation in which their personal data are the primary resource. These processes are rarely considered illegal even though in principle they violate article 19 of the Convention on the Rights of the Child⁶ which says that children should be protected from any form of exploitation and Article 32 that children should be protected from economic exploitation and from performing any work that is likely to be hazardous or to interfere with the child's education, or to be harmful to the child's health or physical, mental, spiritual, moral, or social development.

Algorithmic surveillance is already normalised and widely used even though its impacts on a child's health, wellbeing, safety and security or freedom of thinking have not been thoroughly assessed. Due to the lack of high-quality research on these issues, there is a significant gap in knowledge on the effects of algorithms on children in general. On the one hand, the use of contemporary communication technologies significantly contributes to children's well-being and development as

⁵ General Data Protection Regulation, (EU) 2016/679, gdpr.eu, accessed on 22.04.2022.

⁶ Convention on the Rights of the Child www.ohchr.org/en/instruments-mechanisms/ instruments/convention-rights-child, Article 19, accessed on 22.04.2022.

they use them for education and entertainment. However, there are also many adverse effects as children are exposed to cyber-hate, discrimination, and various types of cyber violence, including online sexual harassment, bullying, stalking and many others. These threats are palpable because they are associated with traditional crimes while algorithmic practices that are potentially manipulative and exploitative in elusive ways are rarely considered criminal offences. Current debates around "platform biometrics" (Crampton: 2019) and "behaviour profiling" (Eder, 2020: 23) are pointing towards a new understanding of digital criminology that includes normalised algorithmic practices that are not properly regulated by international or national laws. Imperceptible monitoring and profiling of children's personal data is a potential threat to the collective rights and freedoms of children, and it requires further research, public scrutiny, and a more articulated legal framework that would ensure better protection of digital privacy, dignity, freedom of thinking and other rights of a child in the online world.

3. DIGITAL RIGHTS OF CHILDREN IN SERBIA

Serbia ratified the Convention on the Rights of a Child in 1990 and therefore accepted all obligations stipulated in this document⁷. It also has its own Personal Data Protection Law⁸ in line with GDPR⁹ aimed at safeguarding online privacy and Family Law that includes eight chapters dedicated to the rights of the child¹⁰. Additionally, the Serbian Government has a specialised department for cybercrime that defines types of offences that fall in this category, namely, child pornography, the spread of hate online and many others that directly or indirectly concern children¹¹.

Digital rights of a child in Serbia are mainly discussed in relation to classic cybercrimes and the security of children online and not in a broader context of digital criminology that is also concerned with algorithmic surveillance or manipulation and exploitation of children in less apparent ways. The main issue is children's online security, and their protection against cyberbullying and various practices re-

⁷ Law on ratification of the United Nations Convention on the Rights of a Child, Official Gazette SFRJ – International contracts, No. 15/90 and Official Gazette SRJ – International contracts, No. 4/96 and 2/97

⁸ Data Protection Law, Official Gazette RS, No. 87/2018

⁹ General Data Protection Regulation (EU) 2016/679

¹⁰ Family Law, Official Gazette RS, No. 18/2005, 72/2011, 6/2015

¹¹ Government of Serbia, mup.gov.rs/wps/portal/sr/gradjani/saveti/Visokotehnoloski+kriminal (Accessed: 21.04.2022.)

lated to sexual abuse such as the so-called grooming, exposure to pornographic text and images, sexting and others (Pavlović, 2017: 124). The Information Security Law adopted in 2016 has been created with the aim to protect users against misuse of information and communication technologies, and Article 19a outlines the measures for the protection of children's safety and security on the internet¹².

However, existing research projects on the effects of information technologies on children in Serbia are scarce, and algorithmic practices are neglected. One of the valuable research projects is Global Kids Online conducted by the UNICEF Office of Research-Innocenti, The London School of Economics, and EU Kids Online in 2016¹³. One of the main conclusions of the research team is that Serbia does not yet carry out systematic research in the field despite the fact that information technologies play a central role in children's lives (Popadić et al. 2016: 5). According to this research, most of the children who participated in surveys use the internet every day, and every third child reported being exposed to aggression (ibid. 6). Moreover, the research shows evidence that children are regularly facing various risks while using the internet, and they include online bullying, exposure to upsetting or unwanted sexual content, meeting potentially dangerous online acquaintances in real life, password thefts, computer viruses and unauthorised use of personal data (ibid. 32). Additionally, the research findings show that the kids in Serbia are inclined to use pirate software more often than their peers in other European countries, which means that they are more vulnerable to computer viruses and malware and that they are at a greater risk of adopting a laid-back attitude towards piracy and perhaps breaking social norms in general (ibid. 41). While this research gives some insightful views of the dangers of using the internet, it also shows how children utilise electronic devices for educational purposes. Namely, it shows that use the internet to write, make presentations, source information, practice their skills and perform other activities, even though most of these practices are performed outside school (ibid. 25). These results are supporting the argument that children rely on information technologies to source information and empower themselves, which is why they have many digital skills (ibid. 29).

Among many benefits, information technologies offer better protection for children in court proceedings. It is especially important to emphasise the advantages of using video link in the court because this protects children and minors from secondary victimisation (Stevanović, Kolaković-Bojović, 2021: 61). It mirrors the principle of acting in the best interest of the child in the context of criminal proceedings, and Serbian institutions are currently working on developing a functional system of protecting children through adequate use of information technologies (ibid. 74).

¹² Information Security Law, Official Gazette RS No. 6/2016, 94/2017, 77/2019

¹³ Global Kids Online http://globalkidsonline.net/ (Accessed: 22.04.2022.)

The main issue discussed Wider implications of information technologies and their impact on children's health, safety and wellbeing in Serbia and worldwide are not thoroughly researched. Effects of algorithmic surveillance and behavioural profiling are typically not discussed in the context of digital criminology even though they can be harmful and lead to breaches of fundamental rights guaranteed by the international treaties and Serbian laws.

4. CONCLUSION: TOWARDS SYSTEMIC SOLUTIONS FOR SAFER ONLINE LIVES OF CHILDREN

Understanding the intricate processes linked to the new digital economy is essential for investigating how information technologies work for and against children. Algorithmic social sorting should be the central concept in this analysis because it is the organising principle of online platforms and the basis of digital production. This new type of economy is sometimes referred to as "surveillance capitalism" (Zuboff, 2019) because it depends on the collection and processing of personal data. While children are playing with mobile phones, tablets, and personal computers, they are inadvertently and often without the knowledge of their parents being involved in production processes through which their behaviour online is being monitored, classified, interpreted and commodified. Algorithms extract their personal data to analyse their activities, decode their desires and predict their actions to monetise their play labour.

Even though these practices are normalised, they should be re-evaluated because of their potential to strip children of privacy and even freedom of thinking. Limiting the right to privacy to the triviality of consent and the partial control over the collection, sharing and processing of personal data results in weakening the concept of the private sphere and leaving children exposed and vulnerable. Platforms' algorithms are extracting children's data to create psychological profiles and target them with advertisements, offer them personalised content, decide what they will be able to see online and motivate them for certain actions. Since they are turning children's clicks, likes, comments and other activities into behavioural data that are further repurposed for their business objectives, the platforms are exploiting all their users for free labour and children are not an exception. In this sense, it is important to consider criminal aspects of business models that are based on algorithmic surveillance. The two new proposed EU laws, namely Artificial Intelligence Act¹⁴ and Digital Services Act¹⁵ have been introduced to address

¹⁴ Artificial Intelligence Act, artificialintelligenceact.eu/the-act/, accessed on 22.04.2022.

¹⁵ Digital Services Act, eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218& uri=COM%3A2020%3A825%3AFIN, accessed on 22.04.2022.

some of these issues, broaden the scope of digital crimes and prevent or sanction some of the already established practices of algorithmic surveillance. However, it is also necessary to rethink the concept of child's privacy, especially in light of the intimate surveillance of children, their involvement in play labour of prosumption and the possible impacts of algorithms on their health and wellbeing, access to information, freedom of thinking and exposure to violence.

REFERENCES

- 1. Artificial Intelligence Act, artificialintelligenceact.eu/the-act/, accessed on 22.04.2022
- 2. Convention on the Rights of the Child www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child, Article 19, accessed on 22.04.2022
- 3. Crampton, J. W. (2019) Platform Biometrics, Surveillance & Society, 17(1/2)
- 4. Data Protection Law, Official Gazette RS, No. 87/2018
- 5. Darmody, A., Zwick, D. (2020) Manipulate to Empower: Hyper-relevance and the contradictions of marketing in the age of surveillance capitalism, *Big Data & Society*, doi: 10.1177/2053951720904112
- 6. Digital Services Act, eur-lex.europa.eu/legal-content/en/TXT/?qid=160811 7147218&uri=COM%3A2020%3A825%3AFIN, accessed on 22.04.2022.
- Duffy, E. B., Pinch, A., Sannon, S., Sawey, M. (2021). The Nested Precarities of Creative Labour on Social Media, *Social Media + Society* 7(2) doi: 10.1177/20563051211021368.
- 8. Dyer-Witheford, N. (2015). *Cyber Proletariat: Global Labour in the Digital Wortex*. London: Pluto Press.
- Eder, N. (2020) Privacy, Non-Discrimination and Equal Treatment: Developing a Fundamental Rights Response to Behavioural Profiling in Ebers, M., Cantero Gamito, M. (eds) *Algorithmic Governance and Governance of Algorithms*, Data Science, Machine Intelligence, and Law, vol. 1, Cham: Springer, pp. 23-48, doi: 10.1007/987-3-030-50559-2_2
- 10. Family Law, Official Gazette RS, No. 18/2005, 72/2011, 6/2015
- 11. Fuchs, C. (2014). *Digital Labour and Karl Marx*. New York and Oxon: Routledge.
- 12. General Data Protection Regulation (EU) 2016/679, gdpr.eu, accessed on 22.04.2022.
- 13. Gerbaudo, P. (2012). *Tweets and the Streets: Social Media and Contemporary Activism*. London and New York: Pluto Press.

- 14. Global Kids Online http://globalkidsonline.net/, accessed on 22.04.2022.
- 15. Government of Serbia, mup.gov.rs/wps/portal/sr/gradjani/saveti/Visokotehnoloski+kriminal, accessed on 22.04.2022.
- 16. Information Security Law, Official Gazette RS, No. 6/2016, 94/2017, 77/2019
- Johnson, J. D. (2021) Algorithm in Kennerly, M., Samuel Frederick, and Jonathan E. Abel (eds.) *Information*. New York: Columbia University Press, pp. 31-44
- 18. Kardefelt-Winther, D. (2019) *Child Rights and Online Gaming: Opportunities and Challenges for Children and the Industry.* Florence: UNICEF Office of Research - Innocenti
- Law on ratification of the United Nations Convention on the Rights of a Child, Official Gazette SFRJ – International contracts, No. 15/90 and Official Gazette SRJ – International contracts, No. 4/96 and 2/97
- 20. Pavlović, Z. (2017) ICT (Information and communication technologies) based children's protection in Serbia, *Journal of Eastern European Criminal Law* 1, pp. 124-136,
- 21. Popadić, D., Pavlović, Z., Petrović, D., Kuzmanović, D. (2016) *Global Kids Online Serbia; Balancing Between Opportunities and Risks: Results from the Pilot Study.* Belgrade: University of Belgrade
- 22. Ruckenstein, M., Granroth, J. (2018) Algorithms, advertising and the intimacy of surveillance, *Journal of Cultural Economy*, doi: 10.1080/17530350.2019.1574866
- 23. Sharon, T., Koops, BJ. (2021) The ethics of inattention: revitalising civil inattention as a privacy-protecting mechanism in public spaces. *Ethics and Information Technology* 23, pp. 331–343 doi:10.1007/s10676-020-09575-7
- 24. Stevanović, I., Kolaković-Bojović, M. (2021) Informacione tehnologije u službi zaštite deteta u krivičnom postupku, in Beatović, S. (ed) *Videolink i druga tehnička sredstva kao načini preduzimanja procesnih radnji u kaznenom postupku (norma, praksa i poželjni slučajevi širenja mogućnosti primene.* Beograd: Misija OEBS-a u Srbiji
- 25. Willson M. (2019) Raising the ideal child? Algorithms, quantification and prediction. *Media, Culture & Society*, 41(5), pp. 620-636. doi:10.1177/0163443718798901
- 26. Zuboff, S. (2019) The Age of Surveillance Capitalism. London: Profile Books.

Dr Ivana Stepanović Naučni saradnik, Institut za kriminološka i sociološka istraživanja u Beogradu

Dr Olivera Pavićević Naučni saradnik, Institut za kriminološka i sociološka istraživanja u Beogradu

Dr Ljeposava Ilijić Naučni saradnik, Institut za kriminološka i sociološka istraživanja u Beogradu

TRANSPARENTNA DECA: KAKO ALGORITAMSKI NADZOR UGROŽAVA ZAŠTITU PRAVA DETETA¹⁶

Algoritamski nadzor utkan u društvene mreže nije prosto sistem organizacije koji reguliše vidljivost, sortira sadržaj i reguliše prostore interneta već predstavlja mašineriju za trgovinu privatnim podacima. Ovaj ekonomski system motiviše proizvodnju različitih formi digitalnog nasilja i visokotehnološkog kriminala zahvaljujući njihovom viralnom potencijalu. Etičke smernice uspostavljene kako bi sprečavale ili kažnjavale krivična dela uvek su spoljašnja u odnosu na logiku tržišta pa i u odnosu na same algoritme jer prioritizuju angažovanje korisnika i reproduckciju podataka po svaku cenu. Deca su naročito ranjiva zato što su pod stalnim nadzorom dok koriste komunikacione tehnologije a cena odricanja od njih je previse visoka. Imajući u vidu kompleksne procese komodifikacije privatnih podataka, ovaj rad ukazuje na kršenja postojećih zakonskih regulativa i naglašava značaj daljeg razvoja zakonskog okvira za zaštitu digitalnih prava dece. Takođe, rad ističe važnost procene uticaja već normalizovanih praksi nadzora i pronalaženja sveobuhvatnih rešenja za zaštitu dece od sistemske zloupotrebe ličnih podataka i ugrožavanja njihovog blagostanja.

KLJUČNE REČI: algoritamski nadzor / društvene mreže / prava deteta / digitalna prava / digitalno nasilje

¹⁶ Ovaj rad nastao je kao rezultat istraživačkog angažovanja prema Planu i programu rada Instituta za kriminološka i sociološka istraživanja za 2022. godinu (na osnovu Ugovora broj 451-03-68/2022-14 od 17. 01. 2022 god.)