Право. Журнал Высшей школы экономики. 2022. Т. 15. № 5.
Law. Journal of the Higher School of Economics. 2022. Vol. 15, no 5.

Research article
УДК
DOI: 10.17323/2072-8166.2022.5.162.176

Privacy of a Child in the Digital Environment: New Risks Unaddressed

Natalya Vyatcheslavovna Kravchuk

Institute of Scientific Information for Social Sciences, Russian Academy of Sciences, 15 Krzhizhanovskogo Str., Moscow 117218, Russian Federation, natkravchuk@mail.ru

Abstract

Digital technologies have brought with them new possibilities for exercising and protecting human rights; however, their potential for violations of human rights has also grown exponentially. Use of ICT influences the daily lives of adults, but their impact on children is even greater, as the risks of harm they face are now mediated and exacerbated online. The importance of children's right to privacy has manifested itself anew in the context of digital technologies. In addition to concerns about safety, there are other considerations such as data processing and the "digital footprints" created by children themselves. Parents have traditionally been considered the primary agents for guidance and support of children's rights online as well as for the protection of their children, but they are now seen as their children's main publicity agents. Nevertheless, the problem of "sharenting" remains unaddressed at both the national and international levels. Measures developed to protect the privacy of the child follow a paradigm of rendering support to parents without stressing their obligation not to disclose information about their child. The General Comment on children's rights in relation to the digital environment adopted by the UN Committee on the Rights of the Child in 2021 reflects this approach. Its stance demonstrates the power of traditional perceptions that reinforce seeing the child as an object incontestably cared for and ruled by their parents This precludes consideration of parents' online activities as potentially harmful to their children and also impedes the development of norms and remedies for protecting the right of the child to privacy against infringements by their parents.

Keywords

human rights; rights of the child; right to privacy; digital environment; parents; sharenting; UN Committee on the Rights of the Child.

For citation: Kravchuk N.V. (2022) Privacy of a Child in the Digital Environment: New Risks Unaddressed. *Pravo. Zhurnal Vysshey shkoly ekonomiki,* vol. 15, no. 5, pp. 162–176 (in English). DOI: 10.17323/2072-8166.2022.5.162.176

Introduction

The relationships between the digital environment[1] and human rights are complex ones. These relationships have attracted the attention of scholars and policymakers as well as international organizations. A body of norms for protecting human rights, including the right for privacy, from ICT-specific risks or risks elevated by digital technologies is being formulated at the international level.

The importance of the right of a child for privacy has manifested itself anew in the digital environment. The risk factors faced by children and that are being addressed include safety, data processing and "digital footprints" created by children themselves. Parents play a key role in guiding and supporting the exercise of children's rights online, as well as ensuring their safety. Accordingly, the measures developed to protect the privacy of the child are being framed within the paradigm of rendering support to parents.

The issue of "sharenting" — use of social media to share news, images, etc. of one's children remains unaddressed at both the national and international levels even though this phenomenon and the risks it poses to children's privacy have been the object of numerous academic studies. In this article it is argued that, as the United Nations General Comment on children's rights in relation to the digital environment demonstrates, the international community is not yet ready to move away from the basic premise that parents should be supported in their role as a child's representative and defender but should not otherwise be controlled. This precludes consideration of parents' online activities as potentially harmful to their children and also hampers development of norms and remedies aimed at defense of the right of the child to privacy against infringements by their parents both on international fora and within national jurisdictions.

The remainder of the paper is divided into five sections. Section 1 outlines the developments in the international legislative accommodation of interactions between the digital environment and human rights. Section 2 explores global and regional responses to the risks to children's rights mediated and exacerbated on the Internet. Section 3 analyses various contexts in which the privacy of the child is addressed. Section 4 characterizes the recently recognized phenomenon of sharenting. Section 5 explores national and international efforts to regulate sharenting.

[1] "Digital environment" is understood as encompassing information and communication technologies (ICT), including the internet, mobile and associated technologies and devices, as well as digital networks, databases, content and services. See: Recommendation CM/Rec (2018)/7 of the Committee of Ministers of the Council of Europe to Member States on guidelines to respect, protect and fulfill the rights of a child in the digital environment.

1. Human Rights and the Digital Environment

An analysis of the interactions between the digital environment and human rights requires an understanding of the specific nature of this environment. Researcher M.L.Trajkovska, among many, notes new technologies are characterized by their global character, the swift dissemination of information, and the endless possibilities of the replication of that information. These technologies have brought with them new possibilities for exercising and protecting human rights. However, the possibilities for violating human rights have also grown exponentially [Trajkovska M.L., 2015: 335].

Adaptation of both national and international rules to advances in science and technology is frequently perceived as being too slow and consequently inadequate for regulating new legal situations created by developments in ICT and its influence on social culture. Making those rules more responsive to ICT requires a reconceptualization of traditional human rights in light of the latest technological developments [Coccoli J., 2017: 224]. This process is being conducted at the global and regional levels simultaneously.

The Resolution "The Right for Privacy in the Digital Age", adopted by the UN General Assembly in 2013, has stressed that the rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy as set out in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights; and that right is therefore an issue of increasing concern.[2] The right to privacy was consequently considered not only as one of the rights most affected by digitalization, but also as a gateway to the realization of human rights.

After a number of preliminary studies, consultations, and the introduction of the mandate for the Special Rapporteur on the right to privacy a report under the title "The Right to Privacy in the Digital Age" was issued by the United Nations High Commissioner for Human Rights.[3] Although a variety of measures had been introduced at the regional level to protect human rights, including the European Union's General Data Protection Regulation; the Council of Europe's Protocol to update and modernize the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the African Union Commission's Personal Data Protection Guidelines for Africa, the UN High Commissioners report emphasized that many laws or items of proposed legislation in this

[2] A/RES/68/167 of 18 December 2013.

[3] A/HRC/39/29 of 3 August 2018.

regard fall short of applicable international human rights standards and raise serious concerns (para 2 of the Report). The High Commissioner has recommended that national governments recognize the full range of implications that new technologies have for the right to privacy but also for all other human rights; that they adopt strong, robust and comprehensive privacy legislation that complies with international human rights law in terms of safeguards, oversight and remedies to effectively protect the right to privacy; that they establish independent authorities with powers to monitor state and private sector data privacy practices, investigate abuses, receive complaints from individuals and organizations, and issue fines and other effective penalties for the unlawful processing of personal data by private and public bodies; and that they ensure that all victims of violations and abuses of the right to privacy have access to effective remedies (para 61 of the Report).

At the regional level the "living instrument" doctrine developed by the European Court of Human Rights (hereinafter ECtHR) provides premises are ideally suited for adjusting the obligations of the state to meet today's challenges to human rights. The idea that the European Convention on Human Rights (hereinafter ECHR) must arrive at positions that are aligned with present-day conditions and that evolve through the interpretation of the Court has been a central feature of ECtHR case law from its early days. The ECHR has shown it is capable of evolving in parallel with society. In this respect its formulations have proved their worth over several decades [Wildhaber L., 2004: 84]. During the last several years the ECtHR lived up to this doctrine when it considered a number of cases covering issues such as the use and protection of electronic data, use of email, GPS, the Internet, surveillance and radio communications.[4] In particular, the Court emphasized the importance of a prudent approach to a state's positive obligations to protect human rights in new environments and of the need to recognize the diversity of possible methods to secure these rights. In *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, the mentioned Court recognized that the risk of harm posed by communications on the internet to the exercise and enjoyment of human rights and freedoms, particularly the respect for private life, is certainly higher than that posed by the press. Therefore "the policies, governing reproduction of materials from the printed media and the Internet may differ. The latter undeniably has to be adjusted according to the technology's specific features in order to secure the protection and promotion of the rights and freedoms concerned" (para 63).

2. The Rights of a Child in the Digital Environment

Modern technologies influence the lives of adults, but their influence over children is far greater. These technologies have undoubtedly enhanced children's au-

[4] Factsheet — New Technologies. European Court of Human Rights, Press unit. March 2022.

tonomy and independence. At the same time, children face many more risks of harm, which are now mediated and exacerbated online. Livingstone note that in its earliest days public policy regarding the protection of children on the Internet focused on inappropriate content and activity involving the sexual abuse of children. Both children's increased use of new technologies and their acquisition of sophisticated digital skills have helped increased awareness of the diversity of possible risks to them. This has shifted public perception away from viewing cyberspace as a distinct sphere in need of targeted regulation and toward growing acceptance that what is illegal or inappropriate offline should be the same online. This leaves policy makers and legislators with a difficult balancing act between supporting and empowering children online while at the same time protecting them at the same time [Livingstone S., O'Neill B., 2014: 20].

In response to increased awareness of the risks that children face globally, the UN Committee on the Rights of the Child issued General Comment No. 25 on children's rights in relation to the digital environment.[5] During the drafting process the Committee received 132 submissions from 26 states, regional organizations, United Nations agencies, national human rights institutions, children's commissioners, child and adolescent groups, civil society organizations, academics, the private sector, and other entities and individuals expressing their views on the matter.[6] The document adopted explains how states should implement the UN Convention on the Rights of the Child (UNCRC) in relation to the digital environment. It refers to civil rights and freedoms, problems with violence against children, family environment and alternative care, children with disabilities, education, leisure and cultural activities and other specific issues, thus covering full range of rights provided for by the UNCRC.

The development of Council of Europe (CoE) legislation also takes into consideration the necessity to protect children from ICT-related risks. One major success was the Convention on Cybercrime (2001),[7] which became the first international treaty on crimes committed via the Internet and other computer networks. Due to its limited scope, child-related offenses covered under the treaty are limited exclusively to child pornography (Article 9). Other risks are considered in the CoE

[5] CRC/C/GC/25 of 2 March 2021.

[6] The Council of Europe was among the bodies that made a submission. Based on the CoE Strategy for the Rights of the Child for the Period 2016–2021 (2016), which identified the rights of the child in the digital environment as one of its priority areas and recognised that children are entitled to receive support and guidance in their discovery and use of the ICT (paras. 56–61), it referred to the key rights which should be addressed by the pending General Comment. These include: the right to freedom of expression and information, the right to education, the right to participation, the right to engage in play, the right to assembly and association, the right to protection of privacy, data and identity, and the right to protection and safety.

[7] The Convention is open for accession by non-member states as well.

Guidelines to respect, protect and fulfil the rights of the child in the digital environment (2018). This document is based on assessing the best interests of the child and his or her evolving capacities, and it recommends that the governments of member states review their legislation, policies and practices to ensure that they promote the full array of the rights of the child. In particular, a comprehensive legal framework should provide for preventive and protective measures in relation to the digital environment. This is to provide support measures for parents and caretakers in order to prohibit all forms of violence, exploitation and abuse; to provide effective remedies as well as recovery and reintegration services; to establish child- and gender-sensitive counselling, reporting and complaint mechanisms; to encompass child-friendly mechanisms for consultation and participation; and to set up accountability mechanisms. The Guidelines thus reflect international recognition of a broad range of challenges to the rights of the child in the digital environment.

3. The Privacy of a Child: a New Dimension for Familiar Concerns

Attention to the protection of children's privacy[8] on the Internet has recently been on the increase [Schreiber A., 2014: 13]; [Phippen A., 2017: 29]; [van der Hof S., Lievens E., 2018: 33]. Although the right to privacy had been acknowledged from the outset, the UNCRC provides for it explicitly in Article 16, as its importance has been highlighted anew in the context of digital technologies. Morgan attributes this to a sharp increase in Internet usage by ever younger children together with the complexity of a technology-mediated environment [Morgan A., 2018: 44).[9] Privacy protection in such a complex environment has become a prerequisite for guaranteeing online child safety and therefore has begun to evolve as a separate, though interrelated, pillar within many online child safety initiatives [Macenaite M., 2016: 2].

Safety is indeed the most prevalent discourse in the field of child privacy protections. This risk is addressed on all levels through national guarantees [Balajanov E., 2018]; [Williams K., 2003] and international norms, including the CoE Convention on Cybercrime[10] and soft law such as the recent UNCRC Guidelines

[8] Current conceptions of the right to privacy draw together three related aspects of privacy: informational privacy (right to control over information pertaining to a person, specifically preventing others from obtaining or using that information), constitutional, or decisional, privacy (the right to ability to make autonomous life choices without outside interference or intimidation (or without "being governed by the state" and physical privacy (the right to a private space and to bodily integrity. See: UNICEF Annual Report. London, 2017. Ch. 7).

[9] An estimated one third of Internet users across the globe are under 18 years old. These Internet users are operating in a world that was not originally designed with them in mind.

[10] The treaty is open for accession by non-member states as well. It became the first international treaty on crimes committed via the Internet and other computer networks.

regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child concerning the sale of children, child prostitution and child pornography.[11]

The ECtHR addressed online safety issues in *K.U. v. Finland*. The Court has noted that posting advertisements of a sexual nature about a twelve-year-old applicant was a criminal act that resulted in a child becoming a target for pedophiles and therefore called for a criminal law response that included an appropriate investigation and prosecution. The Court has noted too that new forms of communication required even greater prudence when the information is related to child privacy concerns. States have a positive obligation to establish a legislative framework to protect children in a timely manner from grave interference with their privacy (para 49).

A new theme addressing violations of data processing as part of protecting child privacy is quickly taking shape. The EU General Data Protection Regulation (GDPR)[12] offers a valuable addition to the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981),[13] which does not contain specific norms aimed at the protection of children but no doubt has a direct bearing on the issue. Atkinson notes that Recital 38 of the GDPR sets the overall tone for the treatment of a child's personal data when it says that children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences, safeguards, and of their rights in relation to the processing of personal data [Atkinson L., 2018: 31].

The ECtHR has not so far considered any data-processing cases where violations of a child's privacy is at issue. Apart from the safety-driven *K.U. v. Finland*, the Court has seen relatively few cases related to child privacy in general and even fewer that involve the digital environment. In *Avilkina and Others v. Russia* confidential medical information about the applicants, one of whom was a minor, was disclosed by a medical facility by request from the prosecutor's office. The Court reiterated that the protection of personal data, including medical information, is of fundamental importance to a person's enjoyment of their right to respect for their private and family life as guaranteed by Article 8 of the ECHR. The disclosure of such data may seriously affect a person's enjoyment of their private and family life, as well as their social and employment situations, by exposing them to opprobrium and the risk of ostracism (para 45).

The effect of disclosing information on a child's reputation was considered in *Aleksey Ovchinnikov v. Russia.* The ECtHR reiterated that in certain circumstances

[11] CRC/C/156 of 10 September 2019.

[12] The GDPR is not applicable to non-EU member states.

[13] A protocol amending the Convention for the Protection of Individuals with regard to the Processing of Personal Data was adopted by the Committee of Ministers at its 128th Session on 18 May 2018.

a restriction on reproducing information that has already entered the public domain may be justified. It concluded that the fact that the information about the child had already been disclosed by another newspaper and that the incident had been widely discussed in the press and on the internet was not relevant, because the child's reputation was at stake and "publication of the names of the juvenile offenders…did not make any contribution to a discussion of a matter of legitimate public concern" (para 50–52). This case is an important development of the Court's jurisprudence and confirms that a child's privacy must be protected not only in cases of a potential threat to safety, but also in order to respect their reputation. This is in line with Article 16 of the UNCRC, which states that, "no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation."

The ECtHR will no doubt see more cases relating to child privacy issues in the future. Global and regional initiatives reflect social concerns and indicate an understanding that, as Baroness Kidron stated, "a child is a child until they reach maturity — not until they reach for their smartphone" [Kidron B., 2018: 26], and therefore children require special protection and care as much online as offline.

In the context of danger that children may bring on themselves when they use ICT [Altun D., 2019: 77][14] is linked to the role of parents as bearing primary responsibility for their children's media-related development and well-being. This is widely accepted in academic circles [Naab T., 2018: 94]; [Livingstone S., Byrne J., 2018: 19] and by legislators. We can see this in para 28 of the CoE Guidelines to respect, protect and fulfil the rights of the child in the digital environment that entrusts to parents the authority to decide if their child's data can be processed.[15] Lim speaks about the emergence of "new parenting obligations" necessary to ensure that parents "are the voices of authority to guide their children towards all that is edifying and beneficial in media, and to steer them away from that which is risky and harmful". This new kind of parenting, he notes, goes beyond traditional childcare. It transcends the online sphere and extends to the offline interactions of the child. The question, however, is whether parents are ready and capable of embracing their new obligations [Lim S., 2018: 36].

Parents may not understand the nature of the risks encountered online. Much of the contemporary research on parenting in the digital environment, as well as conversations among parents themselves, focuses on keeping children safe from

[14] According to the studies only 58 out of 100 applications designed for preschool-aged children are appropriate for their level of development.

[15] The Guidelines emphasize that member states should ensure that their legal frameworks encompass the full range of unlawful acts that can be committed within the digital environment (para 73–74 of the Guidelines). The reference to "the full range of unlawful acts" is particularly important bearing in mind the constant development of technologies. It provides an obligation to states to keep their legislations updated to address current threats to the rights of children.

harm [Clark L., Brites M., 2018: 81]. Parents are also concerned about the potential harm ICT may cause to children's emotional development, as well as about the addictive and time-consuming nature of these technologies [Altun D., 2019: 88]; but threats to their child's reputation is not something most parents routinely consider.

Another reason parents may be ineffective in this regard is because unlike modern "digital children" they were not born into these new technologies and have to learn for themselves how to manage them. They do not trust the integrity of security measures and privacy settings offered by social network sites, and they lack the skills needed to cope with them [Autenrieth V., 2018: 225]. Some authors, for example [Livingstone S., Byrne J., 2018: 23, 25] note parents who are less confident of their own or their child's digital skills take a more restrictive approach to mediating their children's online activities. In trying to keep their children safe, they not only deprive them of the opportunities that ICT offers but also impede the exercise of their rights to privacy and freedom of expression, and consequently they hamper their children's ability to seek outside help or advice when problems at home arise.

4. The Privacy of a Child: New Risks

Excessive control by parents was until recently considered the main negative impact of their authority over their children's online activities [Livingstone S., O'Neill B., 2014: 28]; [Atkinson L., 2018: 32]. However, they are now viewed as the main contributors to publicizing their children.[16] Parents leave a trace of their children in a digital space when they decide to share their child's personal information online or to share information about themselves that might directly or indirectly be linked to their child.[17] The shared information may not only endanger the safety of the child; it may also undermine their dignity and reputation [Steinberg A., 2017: 848].[18] An illustrative example of this parental ignorance is the so-called "YouTube families", which make a show out of their daily routines and open up the lives of their children to the public in every possible detail.[19]

[16] A digital footprint survey across ten European countries revealed that 81% of mothers digitally upload photographs of their children aged 0–2 years.

[17] Some 92% of children by the age of two years have an online presence due to their parents' disclosures.

[18] According to recent studies, 56% of parents shared (potentially) embarrassing information about their children online, 51% provided information that could lead to identification of their child's location at a given time, and 27% of participants shared (potentially) inappropriate photos.

[19] See, for example, the "8 Passengers" vlog by a family with six children. Available at: https://www.youtube.com/channel/UCQ3FRaHOIwXLOQNeUwVpBUA (accessed: 12.07.2019); the KBS show "The Return of Superman". Available at: https://www.youtube.com/playlist?list=PLMf7VY8La5RFIeOyIZ5IOm68WVb7c2dyT (accessed: 12.07. 2019)

"Sharenting", the habitual use of social media to share news, images, etc. of one's children, frequently begins before birth with the uploading of fetal ultrasound photographs, and it has become tightly interwoven with parenting practices. Interestingly enough, the practice became widespread because it gave parents an opportunity for the (re) production of parental self-identity and social approval [Damkjaer M., 2018: 216], but now it is undergoing public criticism [Autenrieth V., 2018: 219].

Parents are not completely ignorant of the potential risks that posting information about their children online can bring. They fear "stranger danger" as well as the commercial misuse of their child's photos. They have exhibited some awareness that they need to consider the reactions of their children once they are old enough to know about the photos of them that their parents shared. The development of new photo practices that allow parents to display their children while maintaining some anonymity can be considered one strategy to mitigate these risks [Autenrieth V., 2018: 226]. Although parents understand their online actions can be a threat to their children's privacy and therefore try to manage it, most keep "sharenting" anyway.

M. Damkjaer points out that in order to grasp the growing significance of sharenting we must acknowledge that parents' approaches to communication technologies do not spring from rational, intentional decision-making. There is a broad range of reasons why parents sharent. It is true that some do this to earn income. However, most do it to receive information and guidance, build and maintain social relationships, and to develop a parental identity [Damkjaer M., 2018: 210, 211]. Becoming a parent entails major practical, emotional, social, and relational changes, not all of which can be handled on one's own. The possibility of connecting with other parents and receiving positive personal support, whether emotional or practical, from the community is particularly important for families with medically fragile children. Whatever the reasons for sharenting are, it can instigate a conflict between parental rights and the right of children to their own privacy [Steinberg A., 2017: 842, 852]; [Bessant C., 2018: 7, 8].

Of all the current threats to the privacy of the child, the one created by parents' activities online seems to be the most difficult to address. Parents are presumed to play a key role in the protection of their children's rights, since they are ideally positioned to assess and address the particular "best interests" of their children [Livingstone S., Byrne J., 2018: 27]. Measures developed to protect the privacy of the child are consequently framed within a paradigm of rendering support to parents, and not in the context of their obligation not to disclose information about their children.

5. Are we Ready to Regulate Sharenting?

The sharenting phenomenon has been the object of numerous academic studies. It was found that parents' and guardians' online activities may cause damage to their children's privacy. While many parents are aware of the safety-related

risks incurred by sharenting and try to mitigate them, threats to a child's reputation are mostly ignored. To address this problem, some national jurisdictions have made efforts to regulate sharenting.

In the US the infringement of children's privacy by parents can be considered as abuse. If the state can demonstrate that parental actions caused substantial harm to their child's well-being, it is authorized to intervene in such circumstances in order to protect children from the harm occurring in online forums. Authorities can seek a remedy through the courts or consider obtaining an injunction precluding the parents from posting additional harmful content online. Steinberg underscores that it is the state actor, not the child, who would bring forth this litigation. This remedy is not ideal as it is aimed only at parents who share the information. They can be required to delete offensive material from the internet sites they possess. However, it gives the authorities little control over the information shared on sites not possessed or controlled by the parent or where the material has been downloaded or shared by third parties [Steinberg A., 2017: 872].

A direct obligation of parents to protect the privacy of their children is stipulated by the privacy laws of contemporary France. Parents can be prosecuted for publishing intimate details about their child. The penalty is very severe, tens of thousands of euros or up to a year in jail. While children may take their parents to court only upon attaining their majority, this regulation is nevertheless a significant step forward. When paired with suitable informational campaigns, it can cause parents to reconsider their behaviour.

The introduction of new parental obligations to protect the privacy of their children is currently being debated within United Kingdom academic circles [Oswald M., 2017: 3, 12]. However, UK law at present does not recognize a child's right to privacy in cases of infringement by their parents. Analyzing remedies that a child might use to prevent sharenting and to secure the removal of sharented information, Bessant points to a range of legal avenues potentially available to anyone who objects to the online dissemination of their personal, private or confidential information, including a breach of confidence action or a tort of misuse of private information. She notes that where a child's privacy has been violated by their parents, their ability in practice to obtain a remedy is in some regards potentially more limited than that of an adult. Children rarely have the financial means to bring court proceedings. Furthermore, they must prove that their information was confidential one, that the parent was subject to a duty of confidence, and that the sharenting was unjustified. Substantive as well as procedural legal hurdles help to explain why there is no substantial jurisprudence on this issue in the UK, and it "has yet to be seen how the English courts will respond to the new phenomenon of sharenting" [Bessant C., 2018: 17–20].

The United Kingdom Data Protection Act also has provisions for adjudication of children's privacy rights. Under this act a child may apply to the UK Informa-

tion Commissioner's Office (ICO), requesting it to undertake an assessment to determine whether their personal data is being processed in breach of the Act. In cases where a parent has not sought the consent of the child to publish their private information online and the ICO concludes that there has been a serious breach of the data protection principles, it may serve an enforcement notice requiring the parents to delete the objectionable information. However, the law has placed the burden of initiating the process on the child. Children should ask their parents in writing to stop posting and/or to remove the information posted online within a specified period. The notice should state why the child believes continued online disclosure is causing or likely to cause them unwarranted and substantial damage or distress. If the parent ignores the notice, the child is entitled to seek assistance from the courts. Again, this course of action would be too complicated procedurally for the average child to carry out [Clark L., Brites M., 2018: 87].

While the United States and France have already introduced norms meant to combat harmful sharenting and the UK is anticipating the development of new practices within existing remedies, most countries are still debating certain aspects of the child's right to privacy [Ogrodnik-Kalita A., 2022: 176][20] or are completely silent about the problem. Is it a problem that there is no child-friendly reporting and complaint mechanism, as recommended by CoE Guidelines to respect, protect and fulfil the rights of the child in the digital environment? Would the privacy of the child in fact be protected in case such a mechanism existed? We daresay it would not. The establishment of a child-friendly complaint mechanism is not a remedy in itself so long as the parents are considered only in their capacity as defenders of their children.

It would be an exaggeration to suggest that this perception is never questioned. The United Nations Committee on the Rights of the Child addressed these concerns while drafting its General Comment on children's rights in relation to the digital environment.[21] However, the reactions from the academic community, the NGO sector and international organizations have confirmed that parental authority is still considered critical, "in terms of recruiting the adults in children's lives as educators and as citizen participants in a global project that focuses on delivering children's rights across all aspects of young lives".

The text of the adopted document reflects this approach. While the General Comment has several paragraphs devoted to the issue of automatic processing of a child's data (para 70–72), the danger of parents sharing online is barely acknowledged. Parents are listed among other persons whose actions may be threatening to a child's privacy (para 67) with no further elaboration on the legislative, admin-

[20] In Poland, for example, the question of when a child is granted the right to privacy is contested.

[21] UNCRC. General Comment on Children's Rights in Relation to the Digital Environment Concept Note. Mode of access. Available at: https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx, (accessed: 03.07.2019)

istrative, and other measures states should take to ensure that children's privacy is respected and protected in this context. The General Comment stipulates the necessity of obtaining consent from the parent or caregiver in certain cases prior to processing child's data (para 71). There is no mention of a possible conflict between a parent and a child on this issue or ways to resolve one. The stance taken by the UN Committee on the Rights of the Child with regard to sharenting should serve as a demonstration of the power of the traditional cultural perceptions that reinforce understanding the child as incontestably an object of care and rule by their parents [Livingstone S., O'Neill B., 2014: 30].

Conclusion

The rapid development of digital technologies has unquestionably changed human daily life. They have brought about new possibilities for exercising and protecting human rights, but at the same time the possibilities for human rights violations have also grown exponentially. In order to address the new risks, the law and policies aimed at protecting human rights need to be adjusted in response to ICT's specific features.

Of all the contemporary threats to the privacy of children, the one created by parental activity online seems to be the most difficult to address. Parents are presumed to play a key role in the protection of their children's rights. Measures developed to protect children's privacy reflect the strong tradition of respecting parental rights to control and shape the lives of their children. Though some national jurisdictions have made some effort to provide legal remedies for children in case of a conflict between their rights and the rights of their parents, the international community seems to be unprepared to move away from the basic premise that the only role of parents is to guide and support children in the exercise of their rights. This is demonstrated by the position taken by the UN Committee on the Rights of the Child with regard to sharenting in its recent General Comment on children's rights in relation to the digital environment.

In the absence of a strongly articulated position from the main international body charged with setting child protection standards that apply to defending the right of the child to privacy against their parents, it would be unreasonable to expect a unified response to this new risk to child's privacy at the national level. It can be confidently stated that we are not yet ready (at both the national and international level) to regulate sharenting.

References

1. Altun D. (2019) An investigation of preschool children's digital footprints and screen times, and of parents' sharenting and digital parenting roles. *The International Journal of Eurasia Social Sciences*, vol. 10, pp. 76–97.

2. Atkinson L. (2018) Interpreting the child-related provisions of the GDPR. *The Communications Law*, vol. 23, no. 1, pp. 31–32.

3. Autenrieth U. (2018) Family photography in a networked age. Anti-sharenting as a reaction to risk assessment and behaviour adaption. In: G. Mascheroni, C. Ponte and A. Jorge (eds.) Digital Parenting: The Challenges for Families in the Digital Age. Göteborg: Nordicom Press, pp. 219–231.

4. Balajanov E. (2018) Setting the minimum age of criminal responsibility for cybercrime. *The International Review of Law, Computers and Technology*, vol. 32, no. 1, pp. 2–20.

5. Bessant C. (2018) Sharenting: balancing the conflicting rights of parents and children. *The Communications Law*, vol. 23, no 1, pp. 7–24.

6. Coccoli J. (2017) The challenges of new technologies in the implementation of human rights: an analysis of some critical issues in the digital era. *Peace Human Rights Governance*, vol. 1, no. 2, pp. 223–250.

7. Damkjaer M. (2018) Sharenting = good parenting? Four parental approaches to sharenting on Facebook. In: G. Mascheroni, C. Ponte, A. Jorge (eds.) Digital Parenting: The Challenges for Families in the Digital Age. Göteborg: Nordicom Press, pp. 209–218.

8. Kidron B. (2018) Are children more than "clickbait" in the 21st century? *The Communications Law*, vol. 23, no. 1, pp. 25–30.

Lim S. (2018) Transcendent parenting in digitally connected families. When the techno9. logical meets the social. In: G. Mascheroni, C. Ponte, A. Jorge (eds.) Digital Parenting: *The Challenges for Families in the Digital Age. Göteborg: Nordicom,* pp. 31–39.

10. Livingstone S., Byrne J. (2018) Parenting in the digital age. The challenges of parental responsibility in comparative perspective. In: G. Mascheroni, C. Ponte and A. Jorge (eds.) Digital Parenting: The Challenges for Families in the Digital Age. Göteborg: Nordicom Press, pp. 19–30.

11. Livingstone S., O'Neill B. (2014) Children's rights online: challenges, dilemmas and emerging directions. In: S. van der Hof, B. van den Berg and B. Schermer (eds.) Minding Minors Wandering the Web: Regulating Online Child Safety. Berlin: Springer, pp. 19–38.

12. Macenaite M. (2016) Protecting children's privacy online: A critical look to four European self-regulatory initiatives. *The European Journal of Law and Technology*, vol. 7, no. 2, pp. 1–26.

13. Morgan A. (2018) The transparency challenge: making children aware of their data protection rights and the risks online. The Communications Law, vol. 23, no. 1, pp. 44–47.

14. Naab T. (2018) From media trusteeship to parental mediation: The parental development of parental mediation. In: G. Mascheroni, C. Ponte, A. Jorge (eds.) Digital Parenting: The Challenges for Families in the Digital Age, pp. 93–102.

15. Ogrodnik-Kalita A. (2022) Protection of the child's right to privacy in the Convention on the Rights of the Child, the General Data Protection Regulation and Polish law. In: E. Marrus, P. Laufer-Ukeles (eds.) Global reflections on children's rights and the Law: 30 years after the Convention on the Rights of the Child. New York: Routledge, pp. 171–181.

16. Oswald M. et al. (2017) Have "Generation Tagged" lost their privacy? University of Winchester: Centre for Information Rights. Available at: https://cris.winchester.ac.uk/ws/portalfiles/portal/356432/826826_Oswald_GenerationTagged_original.pdf (accessed: 04.01.2022)

17. Phippen A. (2017) Online technology and very young children: Stakeholder responsibilities and children's rights. *The International Journal of Birth and Parent Education*, vol. 5, no. 1, pp. 29–32.

18. Clark L., Brites M. (2018) Differing parental approaches to cultivating youth citizenship. In: G. Mascheroni, C. Ponte and A. Jorge (eds.) Digital Parenting: The Challenges for Families in the Digital Age, pp. 81–89.

19. Schreiber A. (2014) Family-based rights in privacy and other areas of law — an Israeli perspective. *The International Family Law, Policy and Practice*, vol. 2, no. 2, pp. 13–27.

20. Steinberg S. (2017) Sharenting: Children's privacy in the age of social media. *Emory Law Journal*, vol. 66, pp. 839–884.

21. Trajkovska M. L. (2015) Privacy, freedom of expression and the Internet. In: Essays in Honour of Dean Spielmann. Oisterwijk: Wolf Legal Publishers, pp. 335–342.

22. Van der Hof S., Lievens E. (2018) The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR. The Communications Law, vol. 23, no. 1, pp. 33–43.

23. Wildhaber L. (2004) The European Court of Human Rights in action. *The Ritsumeikan Law Review*, vol. 21, pp. 83–92.

24. Williams K. (2003) On controlling Internet child pornography and protecting the child. Information and Communications Technology Law, vol. 12, no. 1, pp. 3 –24.

Information about the author:

N.V. Kravchuk — Senior Researcher, Candidate of Sciences (Law).

The article was submitted to the editorial office 18.04.2022; approved after reviewing 17.05.2022; accepted for publication 19.05.2022.