Contribution of Maksim Burianov, Master of Law, author of two scientific monographs, expert of Generation Connection, head of Global Law Forum[[1]](#footnote-1) and initiator of the Declaration of Global Digital Human Rights – “Call for inputs on the solutions to promote digital education for young people and to ensure their protection from online threats”.

1. **What are the main challenges that young people in your country face in accessing digital education? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.**

In Russia, 53% of children spend between one to four hours per day on digital devices, with more than a quarter (26%) devoting all their free time to them[[2]](#footnote-2). Constant connectivity to the internet puts children in a vulnerable position where their rights can be infringed upon. Adults, often not fully aware of what their children are doing online and how they are doing it, need to be informed about the digital realities and risks. According to a new survey by Kaspersky Safe Kids[[3]](#footnote-3), over a quarter of parents in Russia (29%) do not know what information about their child is publicly available online (such as names, phone numbers, and other data). Moreover, 62% of parents do not ask their children for permission before posting content with them online for various reasons[[4]](#footnote-4).

Any technology should offer individuals a new measure of freedom, not control and restriction. Digital autocratic power, based on facial recognition, emotion, and action recognition systems, even in its early stages of development, can pose a threat to the realization of human and child rights. An ossified digital hierarchy will become a significant problem in the context of the unfolding digital technology AI race and has the potential to negate the achievements expressed in the universal establishment of human rights after World War II. Global digital human rights and digital child rights must be prioritized in the legal regulation of digitization and limit digital control, digital militarization, digital inequality, and cyber challenges. We will briefly define the key digital threats that will negatively impact digital transformation and the quality of life.

Digital surveillance is the unjustified and opaque collection of personal data (including biometric, medical, and genetic data) through facial recognition systems, GPS tracking, and online activity monitoring (using AI) by both public and private sectors, operating outside of legal frameworks and procedures, leading to human rights restrictions (especially for vulnerable groups, including children), discrimination, or improper data use. Human rights limitations include privacy, freedom of movement, free speech, the right to assemble, and protection from discrimination.

Digital militarization refers to the policy of developing, deregulating, funding, and implementing military digital transformation technologies (such as autonomous weapon systems, cyberattacks, including those using artificial intelligence and machine learning prediction models) by public sectors and military organizations. This leads to global existential threats (threats to sustainable human civilization development, including increased conflict likelihood, use of weapons of mass destruction, and cyberattacks on critical infrastructure) and violates states' obligations to protect human rights (right to life, security, or education) in the context of achieving unjust defense objectives, leading to digital escalation and increasing conflict unpredictability, with heightened risks for the most vulnerable groups (including children).

Digital inequality is the state where there is an uneven distribution and use of digital resources needed to meet people's needs, manifested in asymmetric access and usage of technological innovations and digital tools. This leads to disparities in opportunities and outcomes in education, healthcare, the economy, and other areas. Digital inequality is driven by socio-economic factors such as infrastructure availability, education, income, geographical location, and social inequalities, affecting quality of life (especially for vulnerable groups) both between and within states. Studies also show that digital inequality impacts access to education, healthcare, employment opportunities, and political participation. The availability of digital technologies, transparency in digitization (Govtech sector), and access to digital literacy education are key to bridging this gap.

Comprehensive cyber risks for children in the internet and smartphone era (during the third industrial revolution) encompass potential threats and risks associated with children's use of digital technologies, including the internet and smartphones. These risks cover a broad range of issues, including cybercrime (such as online fraud, cyberbullying, child pornography), cyber risks (such as exposure to inappropriate content, privacy breaches, identification risks), and internet regulation issues (including data protection, digital rights, and access to information). These risks can negatively affect children's physical, psychological, and social safety (impacting attention, memory, physical development), as well as their rights to privacy, information, and freedom of expression.

Risks to universal child rights (in the context of the fourth industrial revolution) include potential threats and challenges to children's rights, development, and well-being associated with the rapid development and dissemination of new technologies, including Web 3.0, metaverses, and generative artificial intelligence. These risks may involve issues related to privacy and data security, impact on mental health (affecting attention, memory, thinking, participation in the physical world), availability and quality of education, and digital control and uncertain impacts on children. Mentioned risks can also affect various aspects of children's lives, including participation, information, and protection from exploitation and violence.

It is noted that problems can significantly arise if digital risks reinforce each other, creating syncretic effects (composed of heterogeneous elements but presenting a holistic view). Therefore, this study introduces the term "syncretic digital risks." This term is formulated, firstly, by discussing the merging of the digital (virtual) and biological worlds, and secondly, by viewing this discussion through the lens of the exceptional potential of technologies, without having theoretical antipodes. "Syncretic digital risks" are defined as the most significant threats of the forthcoming digital transformation, arising at the intersection of Fourth Industrial Revolution technologies, Web 3.0, and science-intensive innovations, driven by progress in the scientific-technological, economic spheres and lagging in the ethical, public-legal, educational, political spheres, leading to the exponential digital transformation of outdated models of social relations. The term "generative panopticon echo chambers" is also proposed to characterize the worst-case scenario of digital transformation society development, combining digital surveillance, state internet sovereignty, manipulation through language models (such as sovereign or malicious versions of GPT), which will shape individuals' thought models in society with total oversight over it (reducing creativity and critical thinking ability).

Within the framework of "cognitive digital risks to the individual" in the 21st century, let's introduce the concept of "digital desubjectivation" – a multi-level process of regression of the fundamental foundations of personality and its essential capabilities through the rapid introduction of digital technologies, reducing the right to freedom of choice and decision-making to a minimum, leading to neurobiological consequences (dependence on technologies, objectification by technologies, humans as service to technology). These risks are conditioned by the digital footprint or imprint of a person in mass communication networks and the online environment, as well as by our species' biology and neurobiology. They include several stages: digital social mining and digital social programming.

Social mining is the process of extracting valuable information from databases, social networks, and other digital platforms for the purpose of analyzing user behavior and preferences. This allows organizations and businesses to better understand their audience and make more informed decisions, but at the same time exploits human basic needs (transforming them from stimuli to superstimuli, causing attachments, reducing the ability to choose). For example, a data analyst might use social mining methods to identify trends in public opinion or predict consumer behavior, with minors being particularly vulnerable in this respect since platforms are typically tailored to an adult audience (hence, it is critically important not to collect data from individuals under 18 years old). This concept is a part of the digital age economy and a key element in the attention economy, where the importance of information is determined by its ability to attract users' attention. In it, a human is a collection of fears, desires, preferences, passions, bodily sensations, hidden behind the framework of "individuality," instilled in them by media, mainstream, and pop culture, which replaced the function of education in the post-Enlightenment era, framed by likes and resonating comments, transitions through the World Wide Web and its hierarchy. Within this concept, any Data Scientist or data analyst - skillfully understands and extracts the nerve of the era, passing it into the hands of architects of large systems of startups and corporations, thereby granting control over human streams of codes to the capitalist visionaries of the era of the fifth power of data.

1. **What steps is the Government taking to ensure that digital education is accessible and promoted among young people? Please provide examples of specific laws and regulations, measures, policies, and programmes directed at ensuring young people’s universal access to digital education.**

The steps are insufficient.

1. **What steps is the Government taking to ensure that young people can realize their human rights online in a safe, empowering, and inclusive way?**

The measures are deemed insufficient.

**The Digital Right of a Child to Protection from Exploitation**: The Criminal Code provides for liability for physical and sexual violence, including cases involving minors, as well as crimes against the family and minors.

**The Digital Right of a Child to Information**: A cornerstone in this field is the Federal Law of December 29, 2010, No. 436-FZ "On Protecting Children from Information Harmful to Their Health and Development", covering virtually all information spheres: television, radio broadcasting, the internet, and print. The law categorizes all information into that which harms the health and development of children, including information that is completely prohibited from being distributed among children, and that which distribution among children of certain age groups is restricted, as well as other information that a child may encounter.

According to the federal law, information products are classified into the following categories: 1) Intended for children up to 6 years old; 2) For children from 6 years old; 3) For children from 12 years old; 4) For children from 16 years old; 5) Prohibited for children.

**The Digital Right of a Child to Privacy**: Let's analyze the digital right of a child to protect their photograph. According to the law described in Article 152.1 of the Civil Code of the Russian Federation, a citizen's image may be published and used only with their consent.

In line with this law, the faces of children on television and in digital media are usually blurred or concealed to ensure their anonymity and protect their private life. This rule applies to everyone capable of consenting to the use of their image, i.e., to all fully capable individuals.

This statement is supported by the decision of the Plenum of the Supreme Court of the Russian Federation of June 23, 2015, No. 25. It states that consent to the publication and use of an image is a legal transaction (according to Art. 153 of the Civil Code of the Russian Federation). From this, only a competent citizen, possessing full transactional capacity, can give permission for the use of their image. It's also worth noting that the rules on the transactional capacity of minors are applicable in this context. For example, minors under 14 years of age cannot independently give consent to the publication and use of their image. Therefore, their legal representatives must give consent on their behalf.

Citizens aged 14 to 18 have the right to independently give consent to the use of their images, but only with the permission of their legal representatives. However, one might wonder whether exceptions to the general rule, specified in Art. 152.1 of the Civil Code of the Russian Federation, can apply to minors, and if so, how these exceptions should be applied in light of the specified features. It's important to mention that there are exceptions to the main rule outlined in Article 152.1 of the Civil Code of the Russian Federation. According to this article, consent to use an image is not required if the action is carried out within the framework of state, public, or other public interests.

It's noted that consent to process personal data of individuals who have not reached 14 years of age can only be given by their parents, adoptive parents, or guardians. Since, on behalf of minor children under the age of 14, transactions are made by their legal representatives (para. 1 of Art. 28 of the Civil Code of the Russian Federation), except as provided in para. 2 of Art. 28 of the Civil Code of the Russian Federation. Accordingly, children can also legally register on social networks from the age of 14.

**The Digital Right of a Child to Protection from Information Creating Barriers to Development**: Another important document aimed at ensuring and protecting the rights of the child in the information environment is the Federal Law of July 24, 1998, No. 124-FZ "On Basic Guarantees of the Rights of the Child in the Russian Federation". Article 14 of this Law obliges the state authorities of the Russian Federation to take measures "to protect the child from information".

1. **What are the main gaps and challenges to young people’s protection from online threats in law, policy, and practice in your country and the impacts on young people’s human rights? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.**

The systemic issues in implementing the digital rights of children and youth include:

1. **At the Scientific-Theoretical Level**:
	* **Lack of Definitions**: There's no clear definition of the concept of children's digital rights and related concepts, such as various categories of digital risks affecting the realization of children's rights.
	* **Fragmented Approaches**: Digital rights of children are often substituted with protection in the digital environment instead of providing digital rights that would include elements of access, choice, protection, and security in the digital environment and technologies. They are also reduced exclusively to the informational rights of children (in the context of Industry 3.0, which includes the internet and smartphones), not considering the wide range of possibilities of scientific and technological progress (Industry 4.0, including generative AI, Web 3.0, etc.). Moreover, there's a lack of consideration for the wide spectrum of universal children's rights transformed in the era of digital transformation, leading to a new era of human rights and not considering new digital human rights, such as the right to be forgotten, and overlooking all stakeholders influencing the implementation of children's digital rights.
2. **At the Normative-Legal Level**:
	* **Unregulated Digital Challenges**: Digital militarization and threats to future generations, digital inequality among children, digital total control over children (including privacy issues), potential risks of artificial intelligence and machine learning algorithms, complex cyber risks for children in the context of the internet and smartphones, risks for universal rights of children in the context of modern technologies and the fourth industrial revolution, cognitive digital risks to the individual, and existential digital risks are not addressed adequately at both national and global levels. Internationally, treaties and principles do not incorporate concepts and principles of children's digital rights in the context of fourth industrial revolution technologies. The General Comment No. 25 (2021) on children's rights in the digital environment calls for the creation of an international legal treaty on children's digital rights, as it currently does not carry legal obligation.
3. **At the Law Enforcement Level**:
	* **Non-Human-Centric Enforcement Practices**: The application and implementation of digital technologies do not consider the unique interaction of children with the digital world. There's a lack of public oversight and parental involvement in decision-making regarding the digitalization of children's rights. Internationally, there's an issue with the duplication of programs and functions in separate agencies and addressing children's digital rights through a lens of declarativity, corporate self-regulation, and ethical, not legal, approaches, which affects the realization of children's rights. At the national level, there's a problem with insufficient training of personnel and human rights organizations in Russia to address the challenges of digital transformation, lacking knowledge and skills in digital technologies.
4. **What steps is the Government taking to ensure that young people are protected from online threats? Please provide examples of specific laws and regulations, measures, policies, and programmes.**

The situation analysis and proposals highlight the critical need for a paradigm shift in addressing the digital era's risks to human and children's digital rights. The declarative and ethical nature of current steps, including the adoption of a Code of Ethics in the field of artificial intelligence by major Russian technology companies and the outlined measures by the Commissioner for Children's Rights, underscores the insufficiency of ethical approaches and corporate self-regulation alone. The establishment of the Alliance for the Protection of Children in the Digital Environment in Russia is an important but insufficient step towards ensuring online safety for children.

**Proposals for a Paradigm Shift**:

1. **Legal Codification of New-Generation Rights**: It's imperative to legally enshrine the newest generation of human rights and digital rights for children. This requires moving beyond ethical approaches and corporate self-regulation to a framework that legally recognizes and protects these rights.
2. **Global Digital Rights of the Child**: The Global Law Forum's initiative to introduce the term "global digital human rights for 4IR" within the Declaration of Global Digital Human Rights project is a significant step. These rights encompass:
	* Access to global digital technologies and products generated by digital technologies.
	* Protection of personal information in the use of digital technologies.
	* Ensuring digital technologies enhance human capabilities and the realization of all human rights.
3. **Defining Core Digital Human Rights**: Essential digital rights should include:
	* The right to access the Internet and digital technologies for individualization and storage of digital assets.
	* The right to access reliable information.
	* The right to privacy and personal data protection (including personal, genetic, and biometric data).
	* Access to social services through techno-legal platforms.
	* Digital access to education and cultural values.
	* Rights to participate in property transactions, including digital transactions.
	* Prioritizing the use of technologies for the realization of human rights, including prohibitions against using technologies against individuals, particularly highlighting the use of artificial intelligence.

**Global Legal Framework for Sustainable Development**: The establishment of global digital human rights can pave the way for forming a global law that serves sustainable development interests. This approach aims to create a legal framework that not only addresses the immediate concerns around digital technologies but also ensures that these technologies are developed and used in ways that are beneficial to all segments of society, especially children, and are aligned with global sustainability goals.

The call by Maksim Burianov, a researcher and director of the Global Law Forum, an expert of Generation Connection, and an expert of the youth council at the Ombudsman's office in Russia, for the development of a unified theoretical model of children's digital rights highlights a critical approach toward addressing the complex challenges of the digital age. These rights are envisioned to prioritize and limit digital control, digital militarization, digital inequality, and enhance protection against digital threats to the security of individuals, society, states, and their communities. The principles formulated for the realization of children's digital rights include:

1. **Equality of Access**: Ensuring equal access to digital rights and technologies for all children.
2. **Best Interests of the Child**: The digital environment should serve the best interests of the child, ensuring their well-being and development.
3. **Digital Pluralism and Development Opportunities**: Promoting an environment that supports the diversity of digital content and allows children to explore and develop their potential.
4. **Special Care and Protection**: All children should receive special care, assistance, protection, and security in the digital environment.
5. **Long-term Perspective**: Legal regulations concerning children's digital rights need to be continually updated to reflect the rapidly evolving digital landscape.
6. **Inalienability of Rights and Freedoms**: Digital rights and freedoms of children should be inalienable and protected against any form of exploitation or abuse.
7. **Active Participation**: Children should be actively involved in the digital environment in a way that promotes their social, intellectual, and emotional growth.

Furthermore, Maksim Burianov underscores the necessity of adopting a Declaration of Global Digital Human Rights[[5]](#footnote-5) and Declaration (and Convention) on Global Digital Rights of the Child and proposes the establishment of an International Organization for Digital Freedoms and Rights of the Child. This initiative aims to avoid duplication of programs and functions among various agencies (UNESCO, UNDP, UNICEF, the Office of the Envoy of the Secretary-General on Technology), thus fostering a more coordinated and effective approach to safeguarding digital rights and freedoms for children globally. This proposal represents a significant step towards creating a comprehensive and cohesive framework for protecting children in the digital era, ensuring their rights are respected and upheld in the face of technological advancements and digital challenges.

For context, back in 2020, I proposed a global digital social contract - a Declaration of Digital Human Rights: <https://www.weforum.org/agenda/2020/08/here-s-why-we-need-a-declaration-of-global-digital-human-rights/>.

I launched a petition to support the adoption of the Declaration (which was signed by youth organizations in over 30 countries):<https://maxlaw.tilda.ws/un_digital_rights> . And I have written two books on this topic (so far available in Russian). The last book was written in the context of Web 3.0, generative AI, and the meta universe: [https://knorus.ru/catalog/yurisprudenciya/692081-cifrovye-prava-rebenka-aspirantura-bakalavriat-magistratura-monografiya/](https://www.litres.ru/book/maksim-sergeevich-bu/cifrovye-prava-rebenka-aspirantura-bakalavriat-magist-70023226/).

The best way to achieve digital sustainability is by committing to a Declaration of Global Digital Human Rights, which updates international law to take into account developments such as globalization and 4IR technologies. Such a declaration will fully articulate current international legal obligations of states and corporations in the field of human rights in the digital age.

 Their elements include:

 1. The right to exercise personal, social, economic, political, and cultural rights based on new technologies, without barriers built on the basis of new technologies.

 2. The right to freedom from digitalization of the military sphere and the right to digital neutrality

 3. The right to freedom from total surveillance through technology

 4. The right to personal data protection, including the protection of genetic information and health data (in the context of the rapid advances in biotechnology, bioengineering and telemedicine, for example).

 5. The priority of human beings - and their interests, integrity and quality of life - in the context of the creation, use, introduction, and development of artificial intelligence.

 6. Equal access to the opportunities offered by these technologies, including access to education, labor, healthcare, and basic social services based on new technologies.

 7. The right to take part in the management of social processes at the global, regional and national levels through digital technologies.

 8. The right of access to the global Internet for everyone.

1. Global Law Forum URL: <http://maxlaw.tilda.ws/digitalrights_globalshapers> (date of reference: 17.02.2024). [↑](#footnote-ref-1)
2. Digital habits in Russia: every fourth child spends all his free time in gadgets URL: https://www.kaspersky.ru/about/press-releases/2021\_cifrovye-privychki-kazhdyj-chetvyortyj-rebyonok-provodit-v-gadzhetah-vsyo-svobodnoe-vremya (date of reference: 17.02.2024). [↑](#footnote-ref-2)
3. Universal application for the protection of children in the digital world / URL: https://www.kaspersky.ru/safe-kids (date of reference: 17.02.2024). [↑](#footnote-ref-3)
4. Burianov, M.S. Digital rights of the child: a monograph / M.S. Burianov. - Moscow: RUSAINS, 2023. - 294 с. URL: : [https://knorus.ru/catalog/yurisprudenciya/692081-cifrovye-prava-rebenka-aspirantura-bakalavriat-magistratura-monografiya/](https://www.litres.ru/book/maksim-sergeevich-bu/cifrovye-prava-rebenka-aspirantura-bakalavriat-magist-70023226/) (date of reference: 17.02.2024). [↑](#footnote-ref-4)
5. Burianov М. Here’s why we need a Declaration of Global Digital Human Rights. World Economic Forum. Electronic resource. – URL: https://www.weforum.org/agenda/2020/08/here-s-why-we-need-a-declaration-of-global-digital-human-rights/ (date of reference: 04.02.2024). [↑](#footnote-ref-5)