Inputs for study on the solutions to promote digital education for young people and to ensure their protection from online threats

Submitted by MyData Global Thematic Group MyData4Children

MyData Global is an award-winning, international non-profit dedicated to empowering individuals by improving their right to self-determination regarding their personal data. As a membership association composed of over 100 organisation members and close to 400 individual members from over 40 countries on six continents, MyData Global brings together professionals and organisations from business, legal, technology and society perspectives to accelerate transformation for ethical and human-centric data sharing and use.

MyData4Children is a thematic group organised within the MyData community, focused on the special conditions, needs and possibilities for children's data. The group comprises academics, researchers, designers, developers, and experts on data, children's rights, digitalisation and education. We work to protect, empower and inspire children, their families and their circle of trust as they navigate and construct their digital world.

This input responds to questions 4 and 5 in the UNHCHR call for inputs, with a focus on contextualizing the main gaps and challenges to young people's protection online. Illustrative case studies, possible responses, references and background information on the MyData4Children thematic group are annexed for additional reference.

Gaps and challenges

> *Question 4 in the call for inputs asks: 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?*

Children today grow up with sophisticated digital products and services, their lives deeply embedded with data processing interactions that can facilitate profiling, behavioural analytics, and prediction. These functions can have an immense and unknown impact on children's futures, and digitising education can present risks related to constant screen time and distractions, dehumanizing the learning process and homogenisation of education with the introduction of automated systems for tutoring at scale (Blodgett and Madaio 2021).

The integration of highly intrusive and harmful surveillance systems is often justified through arguments about student well-being (Collins et al. 2021),[1] and recent studies find that arguments of equity are often used to justify the adoption of AI technologies in education and services used by children, especially those with precarious access to formal education, in the home (Cahn et al. 2020). The potentially negative consequences of these practices are rarely investigated (Holmes et al. 2021), but there have been numerous cases demonstrating that real-world harm can be caused by biased technology systems[2] and there is evidence that technologies tend to favor the already well-off, less so the most disadvantaged (Selwyn and Jandric 2020).

This has led to calls for better algorithmic auditing and trials for Product Certifications (The Edtech Equity Project, n.d.), but the power of the tech narrative persists. What attention has been paid to the potential harms of these technologies has tended to focus on individual or tool-specific impacts and has not consistently explored the potential for systematic, indirect, or societal harms (Young, 2020; Crooks, 2021). When digital education tools are found to be less efficient or effective than anticipated, this is often attributed to the limited abilities of children or teachers to use these technologies, paving the way for technological fixes (Convery, 2009).

Policy responses to these challenges are sporadic and inconsistent. Only 16% of countries globally have regulatory measures to address the unknown impacts of technology on children (UNESCO 2023), and regulatory measures are wildly inconsistent, with many countries adopting drastic measures such as wholesale bans (such as in schools) on the use of specific applications by children. For example, Denmark banned Google applications and Chromebooks (Schmiedt 2022); while France banned the free version of Microsoft Office 365 and Google Workspace (UC Today 2022), among others. There is little evidence that such measures are effective, and abuse of children's data is well documented even in countries where data privacy laws do exist (Human Rights Watch 2022; IDAC 2021). While the awareness around digital threats grows and governments take steps to create a safer digital future, there is a risk of focusing on technology applications without acknowledging the role of existing power imbalances in

[1] For example, the newly developed SELFIE tool has been specially designed to now measure the socio-emotional, physiological and health well-being of both students and teachers in highly digitized learning environments (see SELFIE [European Commission n.d.])

[2] For example, the use of facial recognition algorithms in exam settings that fail to recognise or falsely accuse cheating among black students' (VICE 2021), or non-native English bias in AI tools adapted to detect the AI-generated student text (Liang et. al. 2023).

exasperating online and leading to real-world harms such as false accusations and amplifying embedded biases (The Markup, 2020; Benjamin, 2019).

An obvious point of reference for navigating these challenges and effective regulation is found in the United Nations Convention of the Rights of the Child, which stipulates that:

> In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration" (UNCRC 2021:3)

Application of this principle can be complicated and requires a nuanced approach that enables children's agency. Some legal scholars have contended that this primary consideration should still be weighed against other interests, such as 'the interests of powerful companies that may very well be the direct opposite to those [interests] of children' (Van Der Hof et al. 2020: 841). Given the inherent power imbalance implied by these relationships, it is important to embed the primacy of children's interest in the technological and regulatory infrastructure of their increasingly digital lives. This commentary provides a proposal for how that might be pursued.

Potential solutions

The systemic challenges described above will not be solved by piecemeal approaches to specific governance regimes, regulations, or technical interfaces. We need a complete rethinking of how children's digital ecosystems work.

The human-centric model advanced in the MyData Declaration[3] provides a framework for understanding how this can be accomplished through technological, social and regulatory infrastructure that gives individuals agency and control over their data. This human-centric approach is the normative foundation for the European Data Strategy and subsequent landmark EU data regulation, and the MyData4Children thematic group applies this approach to children's protection and empowerment.

The below table shows how the principles articulated in the MyData Declaration can be applied to children's agency and protection, illustrated through a story from a day in the Michel family with 10-year-old Kim and parents Val and Pat.[4]

[3] The MyData Declaration articulates a commitment to working towards a just, sustainable and prosperous digital society, marked by the shift from formal to actionable rights, from data protection to data empowerment, and from closed to open data ecosystems. The declaration is available in 16 languages at https://mydata.org/participate/declaration/.

[4] See Appendix 4 for the scenario 'A day in the life of a family living in a MyData world'

MyData Principle	What this principle looks like in practice
HUMAN-CENTRIC CONTROL OF PERSONAL DATA	Kim has a personal digital ID and data wallet managed by guardians Val and Pat. The parents are empowered to control and manage the use of education data belonging to Kim until Kim is old enough to do it himself. Human-centric approach to Kim's data means it is used to make decisions in Kim's best interest by Kim, Val and Pat in collaboration with their circle of trust (educators, health suppliers, extended family, friends and service providers).
INDIVIDUAL AS THE POINT OF INTEGRATION	Kim is active at school, but also has many hobbies and some extra educational activities such as speech therapy. Many actors are generating data on Kim (e.g., school records, teacher's qualitative reports, therapy reports, hobbies badges, achievements diplomas, etc). Kim, Val and Pat have access to all the original data about Kim regardless of the actor generating it. It is Kim's data, for Kim.
INDIVIDUAL EMPOWERMENT	Kim - firstly through the parents and then by himself - has access and control of all scattered data generated about him throughout his life. Kim, Val and Pat use that data so they can turn it into actionable information and insights to facilitate Kim's development. It is not only grades, badges and assessments. Data from Kim's educational history is used for improving his present and plannig for his future.
PORTABILITY: ACCESS AND RE-USE	Decisions and processes about Kim's education and career are now comprehensive and faster as the same education data can be easily accessed and reused when needed. When Kim switches schools or applies for higher education, all the educational data is available and can be shared with institutions and actors as Kim sees fit. The data can also be shared with other service providers (e.g., health), family and friends.
TRANSPARENCY AND ACCOUNTABILITY	All educational actors (teachers, school boards, ed tech suppliers) are able to explain why and what certain education data is created and how it is used. Kim, Val and Pat can raise concerns if they are not comfortable with the handling of the said data. The education actors are held accountable for misuse of the trust deposited in them, as Kim, Val and Pat are able to easily revoke access and request redressing.
INTEROPERABILITY	Kim, Val and Pat are able to use different services from different education platforms as they see fit. They are not forced to use preselected services available only on one education platform. Technical interoperability allows them to share the data from one service or system with another and semantic interoperability allows them to make sense of that data and use it across different contexts.

A children-centric approach to regulating children's data ecosystems complements and is reinforced by existing regulatory frameworks and international standards,[5] but implies a fundamental and structural shift towards children's agency that can be applied across regulatory and cultural contexts. The application of this approach to the development and regulation of education technologies and other technologies can thus be a foundational and turn-key intervention to ensure that young people can realize their human rights online in a safe, empowering, and inclusive way.

Several companies and public institutions have committed to this approach by signing the MyData Declaration and being awarded the status of MyData operators. The endorsement of this approach by the Office of the High Commissioner could help further disseminate the model and support the proliferation of human-centric norms in the development of regulatory regimes across the globe.

In order to ensure the robust and thoughtful application of this model to digital education and technologies often used by children, we also call on national regulators to establish robust and systematic auditing regimes to ensure that their data practices prioritize children's well-being and human rights.

We openly and warmly invite the UN, its members and collaborators to join the MyData movement[6] and help us make our vision a reality: protect, empower and inspire children, their families and their circles of trust as they construct their digital worlds.

This commentary is submitted on 16 February 2024.

Contributors to this commentary include: Paula Bello (Ireland/Finland/Mexico), Gulsen Guler (UK/Turkey), Velislava Hillman (UK/Bulgaria), Eric Pol (France/Belgium), Marcelle Siewe Ngounou (Cameroon/Canada), Dixon Siu (Hong Kong/Canada/Japan), Meri Valtiala (Finland), Christopher Wilson (Norway/USA).

[5] There are many opportunities to roll out, together with accelerator programs, audits and training around ethical practices, children's rights and needs in digital education. The requirements for these audits as EDDS has piloted in the UK, are drawn from existing regulatory frameworks and standards such as the EU General Data Protection Regulation (GDPR), the Federal Trade Commission Act, the Children's Online Privacy Protection Act (COPPA), the Family Educational Rights and Privacy Act (FERPA), and standards including the Global Education Security Standard (GESS), WCAG 2.0 standard on web accessibility. The United Nations Convention on the Rights of the Child and comment 25 acknowledging children's rights in the digital environment, the EU Ethics Guideline for Trustworthy AI, the HRESIA model of assessment - Human Rights, Ethical and Social Impact Assessment (Mantelero 2023). Lastly, within the education domain, there are also enduring pedagogic theories and various good practices for assessing and evaluating edtech products and services across pedagogic baselines (e.g., the Education Alliance Finland https://educationalliancefinland.com/)

[6] Learn more about MyData Declaration, Principles and Community: https://mydata.org/