Building Trustworthy AI for Children: Advancing Digital Civic Education and Risk Governance within the EU AI Act

Good afternoon everyone.

First of all, I would like to express my deep appreciation to the Personal Data Protection Service of Georgia, and in particular to the President Lela Janashvili, for hosting us here in Batumi and for organizing such an important event.

And, of course, a warm thank you to Lika Kobaladze and all distinguished speakers, it is an honor to share this stage with you and to be part of such a rich and timely conversation.

* * *

Before diving in, let me ask you to picture this:

A child, barely two years old, easily swiping through videos on a touchscreen, long before he or she can read, speak or even less understand what "privacy" means.

This is not the future, it's our present.

We are no longer talking about "digital natives". Today's children are truly **"mobile born"**, growing up in a world where digital platforms and AI systems are not tools they learn to use later in life, but the very environment they are raised in which **shapes their relationships, emotions and minds.**

In light of this, we are here to confront a question we can no longer postpone:

If children learn to interact with technology before they can fully understand the world around them, how can we ensure that the digital environments they live are truly safe, fair and respectful of their rights?

Platforms, which are more and more AI-powered, determine the content they see, the games they play, the interactions they experience and, most of all, **the logic** that guides all the choices they can make within them.

These platforms can support learning and creativity, but they also nudge behaviors, often in subtle, invisible ways.
When **nudging begins in early childhood**, it risks **undermining the individual's ability to develop independent and critical thinking**.
As recently highlighted by the **G7 Privacy in Rome**, the new generation - Generation Alpha - will be the first to grow up in a world deeply influenced by AI at every level: learning, health, communication, decision-making.

This makes it imperative to **adopt a child-centric perspective in the design and governance of AI systems**.

Beyond general online exposure, **social media and video games** represent powerful ecosystems where AI is used to influence children's behaviors in ways that are often opaque and deceptive.
On **social media**, nudging powered by AI can expose children to a wide range of risks.
They may come across inappropriate or harmful content, experience cyberbullying, develop unhealthy patterns of social comparison, or fall victim to the spread of misinformation, all within environments that are specifically designed to maximize their engagement without fully considering their well-being.

The **Italian Data Protection Authority** has already taken hard measures on multiple occasions to protect children from online risks**.**
This includes the **immediate blocking of TikTok** in 2021, after the tragic

case of a 10-year-old Italian girl who died for the so-called *"blackout challenge"*. The video had been uploaded on TikTok, leading the Garante to suspend data processing for users whose age could not be verified.
Further interventions followed, including the **ban on the AI chatbot Replika**, due to the serious risks it posed to minors and emotionally vulnerable individuals; more recently by urging firstly to OpenAI and then to DeepSeek to adopt stronger safeguards especially for age verification.

Also, in the world of **video games** dark patterns enhanced by AI algorithms are becoming increasingly common.
These manipulative design techniques, which prioritize profit and retention, exploit children's cognitive vulnerabilities to keep them playing for longer periods, encouraging them to make in-app purchases and to foster addictive behaviors often tied to competitive or social dynamics.

Such practices, over the long term, **shape the very choice architecture on which the thought and life of the adult individual will develop**, affecting their right to self-determination.

Recent studies, including research on **Fortnite and Minecraft**, two of the most popular online games among millions of adolescents, reveal the complexity of gaming's social impact. Video games are not simply harmful or beneficial, their impact depends heavily on **how they are designed**, **how they are played** and **how they are experienced by players**.

That is why children and adolescents need to be able to understand not just the entertainment value of games, but also their social and psychological implications.

Thus, while gaming can offer opportunities for connection and learning, it must be approached with careful governance to mitigate risks and maximize its positive potential.

It is clear that any reflection on digital platforms is closely connected with the issue of data. After all, **at the heart of every AI system is data**.

And in the case of children, data is not just information, it is a record of their development, their interests, their vulnerabilities.

Children's data is **doubly sensitive**.

It reflects who they are today and anticipates who they may become, impacting their future opportunities.

Moreover, the digital traces a child leaves behind are permanent and constantly updated. This dynamic exposes minors to **permanent profiling** that can impact their future decisions, such as university admissions, job opportunities or access to health services.

A youthful preference or a mistake made without full awareness can become a defining factor across a lifetime, limiting the right to redefine one's identity.

Yet, if obtaining valid consent is challenging even for adults, how can we expect children - even teenagers - to give truly free, informed, and conscious consent?

Children, due to their developmental stage, are particularly easy to influence. They trust friendly designs, gamified environments and interactive avatars, without necessarily understanding the broader consequences of sharing personal information.

As you all know, **Meta** has announced that, from the end of this May, it will use publicly data from its platforms (such as posts, comments and photos) to train its AI models. While Meta states that data from users under 18 will be excluded, there is a significant risk that images and information about minors, shared by parents or friends online, could be included in these datasets. This is especially concerning given that, in Italy, children under 14 are not legally capable of providing consent and their digital presence is often managed by adults who may not fully realise the implications of sharing such content online.

From this stage, I would like to share a proposal for your consideration: that any data related to children - especially when shared by third parties - should be excluded by default from AI training datasets.
Such a measure would reinforce the principle of data minimization and reflect a strong commitment to the best interests of the child, ensuring that children's rights are not silently compromised in the name of technological progress.

When children themselves disclose their personal data in these environments, they often do so **without full awareness** of how this information will be collected, used, combined with other datasets, and retained indefinitely.

Thus, the lack of informed consent from minors is not just a legal gap, it is an **ethical failure** that undermines the very autonomy and dignity that we are obliged to protect.

We shall also remember that, according to Article 29 of the UN Convention on the Rights of the Child, education must develop every child's personality, talents, and abilities to the fullest.

Closely linked to this, let me shift your attention to what I firmly believe is the key challenge of our time: we **must reshape how we educate children to live in a digital world**.

Digital civic education must become a national, European and even global priority and a democratic necessity.
Children shall learn to:

- navigate platforms safely, critically, responsibly and consciously;
- understand privacy risks and commercial manipulations;
- defend themselves against dark patterns and data exploitation;
- build a strong and resilient digital identity.

As both the **UNICEF Policy Guidance on AI for children** (2021) and the most recent **EU Commission Recommendation** on the same topic (n. 1238/2024) make clear, education in the digital age must evolve to address a broader and more urgent set of priorities.
It must foster **early awareness** of how their personal data is collected, shared and used and teach them to protect it with the same care as their physical identity.

Let me briefly refer to a global trend that confirms the growing awareness of how crucial AI will be for future generations.
In recent months, countries like **China** and the **United States**, as well as several European nations, have begun to integrate **AI education** directly into their school systems.
For instance, Beijing has introduced mandatory AI instruction from primary to secondary education and the U.S. administration has launched federal programs to promote AI literacy among students and teachers.

However, I would suggest that before we teach children how AI works, we must first teach them how to behave in the digital world**.**
In other words, **AI education must be built on a solid foundation of digital civic education**.

In this context, the **role of educators** is absolutely fundamental.
If we expect children to navigate the digital world with awareness and responsibility, we must first ensure that **teachers themselves are properly equipped, even more so than their students**.

The most recent data show that, as of today, many educators are not yet ready to take on this crucial role.

According to the latest report of the International Digital Education Working Group of the GPA, a survey conducted in five countries revealed that between 40% and 81% of teachers had not received any training in data protection or digital citizenship. Moreover, many educators reported not knowing where to access appropriate teaching resources. This highlights the urgent need to support teachers not only with institutional guidance but also with practical, high-quality educational tools.

Because in a world where AI systems can generate content, summarize texts, and even suggest decisions, what becomes truly valuable is the **human capacity to think critically**, to challenge assumptions, to make ethical judgments and to ask uncomfortable or unexpected questions.

This means that we must educate children **not for shortcut answers**, but for **deep, reflective inquiry**: an education that promotes reasoning, reflection, and empathy.

Because the most transformative questions are still - and will always remain - entirely human.

Finally, let us reflect on the policy framework we are building in Europe nowadays.

The **EU AI Act** represents a historic commitment to govern AI technologies in line with fundamental rights and democratic values.
The AI Act, in particular at Recitals 28 and 48, explicitly addresses risks of manipulation, exploitation, and social control and also the impacts on rights such as privacy, education, non-discrimination, and mental health.
Moreover, the AI Act also aligns with the broader EU strategy of building integrated child protection systems that include the digital dimension.

It is clear that EU AI Act marks a step forward to integrate ethics, children's rights and protection into the foundations of the AI-driven world.

Regulation alone will never be enough. It must be paired with education, cultural change, awareness and investment in digital citizenship for our youngest generations.

Building trustworthy AI for children is not only about avoiding risks and damages.
It is about **actively promoting children's development, autonomy, participation and dignity**, offline and online.
It is about ensuring that today's digital ecosystems encourage critical thinking, civic responsibility and human prosperity.

To truly achieve this vision, we must act now.

We must urgently launch concrete projects and study programs focused on digital civic education.

Children must not be passive consumers of technology.
They have to be empowered to understand, question and shape the digital world they live in.
They must be given the tools to protect their rights, express their views and participate as full digital citizens.

Embedding digital citizenship into early education is how we defend our fundamental values: **freedom, equality, dignity and democracy**.

If we fail to invest in civic education now, we risk raising generations who live in a world of algorithms but are unable to govern it.

If we succeed, we will build a future where technology serves humanity and not the other way around.

Thank you very much.