

# Beyond the horizon: a new era for the rights of the child

## High-level Launching Conference for the new Strategy for the Rights of the Child (2022-2027)

### Artificial intelligence: maximising opportunities while minimising risks

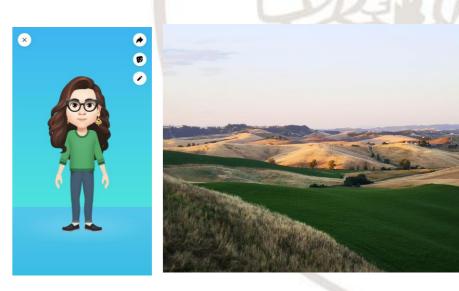
Dr. Denise Amram Assistant Professor LIDER Lab - Scuola Superiore Sant'Anna (Pisa, Italy) email: <u>denise.amram@santannapisa.it</u>

#### **Short Bio**



- LLB (UNIPI), JD (UNIPI), PhD in Law (SSSA), Attorney at Law (Italy), ISO DPO certified 11697:2017 (TUV), Italian Qualification as Associate Professor of Comparative Law.
- Assistant Professor at LIDER Lab –DIRPOLIS Institute, Scuola Superiore Sant'Anna. Affiliate researcher at EMbeDS Department of Excellence.
- **Coordinator** of the Permanent **Observatory on Personal Injury Damages** EThics and law witH and fOr reSearch (**ETHOS**) at LIDER Lab. **Co-coordinator of Family law and children's rights Area.**
- **Teaching / research activities** in Italy and abroad, including France (Université Panthéon-Assas and Université Panthéon-Sorbonne), The Netherlands (Utrecht University), Ireland (University College Dublin), Malta (University of Malta), and USA (Columbia Law School, Harvard Law School).
- Authored ~110 publications in Italian, French, English, and Spanish, including **a book** and 2 co-editions.
- H2020 ongoing Funded Projects @LIDER Lab: LeaDS, reCreating Europe, Valkyries, SoBigData++. National Funded Projects: 5GSOSIA, OPT-HEPAC under Bando Salute 2018.
- Several interdisciplinary projects in collaboration with other SSSA's Departments and Institutes (eg Predictive Justice)
- Interests: Fundamental Rights Protection & New Technologies, Data Protection, Family Law, Tort Law.





www.lider-lab.it

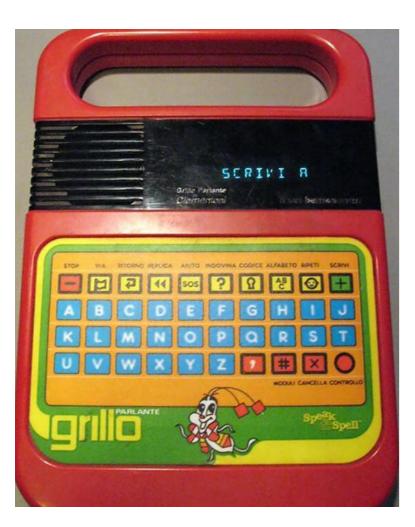




- Are children to be considered as a particularly vulnerable category when it comes to AI?
- How can we improve protection of children against harmful effects and risk assessment of AI?



### Why Children are Vulnerable towards Al-Solutions?









### Why Children are Vulnerable towards Al-Solutions?

#### Vulnerab\* = 40 times in the CoE Strategy 2022-2027

#### Access to and safe use of technologies for all children section:

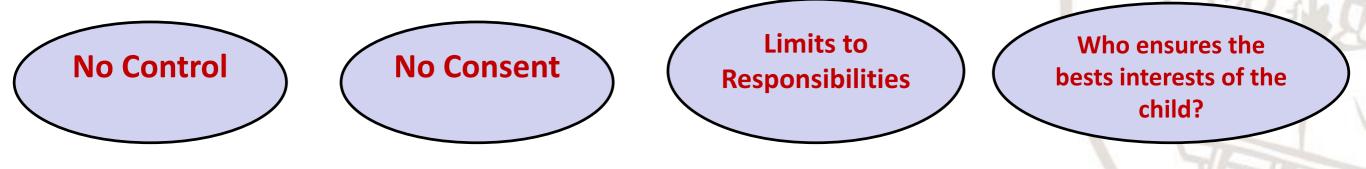
"Many children **in vulnerable situations**, such as children belonging to national minorities or children with disabilities, and children having no or limited access to the Internet and other digital technologies, are not familiar with these and are **left out of digital education**. As recognised by the CRC in its General Comment No. 25

"if digital inclusion is not achieved, existing inequalities are likely to increase, and new ones may arise"."



## Why Children are Vulnerable towards Al-Solutions?

 Al-solutions may process (=collect) personal and non-personal data and share them without control from parents/adults and/or interact with children without control from parents/adults and/or connect/cross to other processed information without control from parents/adults



From latin respondere (to have the legal obligation to protect and promote children's rights and act in their bests interests)



### If parents have no control, who shall be accountable?

- AI-solutions developers according to the AI Act shall be accountable → to assess risks of their product and implement mitigation measures.
  - To inform about data processing.
  - To highlight functionalities and envisaged reactions.
  - To provide opt-in and opt-out options
  - To contribute to create awareness for **digital parenting support**
- Before putting the AI-based solution on the market tests engaging end-users (children and their parents) shall be performed
- To provide **consistency mechanisms** to apply tailored standards certification.

#### **CoE strategy 2022-2027**

**IMPLEMENTING** its standards, by continuously:

3.1.1 **Protecting children online**,<sup>42</sup> e.g. from violence, including grooming, sexual and peer violence and cybersexism, from exposure to pornographic and other harmful content, cyberbullying, online hate speech and interference with right to privacy and personal data protection (including in the context of education settings), thus following the "4C" approach (content, conduct, contact and contract risks).<sup>43</sup>

3.1.2 Raising awareness about sexist misuse of social media and online threats for children (including online child sexual exploitation and abuse).

3.1.3 Ensuring that cases of **online child sexual exploitation and sexual abuse** are reported, investigated and prosecuted promptly, efficiently and appropriately.

3.1.4 **Supporting** families, teachers and other professionals, volunteers as well as children, to **prevent** cases of **cyberbullying and online hate speech**.

3.1.5 Providing **digital citizenship education** for children, carers, professionals and volunteers work-ing with children.<sup>44</sup>

3.1.6 Providing positive digital parenting support.

3.1.7 Fighting digital exclusion and ensuring an **equal access to the digital environment**, including for children with disabilities, children in the context of migration and children belonging to national minorities, in particular Roma and Traveller children, as well as in the context of distance learning.

#### INNOVATING, by:

3.2.1 Inviting business and industry to fulfil their responsibilities towards children, including by undertaking child impact assessments, ensuring the participation of children in the assessment stages, as well as involving them in the design of digital services and products.

3.2.2 Tackling the use of internet and social media for spreading disinformation, hate speech and violent radical ideas including for the purpose of terrorism among children.

3.2.3 Providing guidance and training to **build** capacities for professionals on the rights of the child in their relation to technologies, engaging children in the development and delivery of capacity-building and digital education for teachers and other professionals or volunteers.

3.2.4 Enhancing child participation through technologies and in decisions related to the digital environment and technologies, in light of promising practices and mechanisms, including by facilitating exchanges between existing child participation mechanisms and institutions at different administrative levels (local, regional, national and European).

3.2.5 Analysing the risks posed by and possibilities to benefit from the use of **artificial intelligence technologies**.

3.2.6 Promoting safe and enabling spaces for children to freely search for information and express their views online.

3.2.7 Exploring new issues impacting children's well-being, i.e. online gaming, online marketing and online influencing.

3.2.8 Ensuring the rights of children to online play, leisure and association.

#### **Action Points**



#### Gaps to be covered in generalized Al-related legislative initiatives and EU Data Strategy

- To introduce mechanisms of **participation** to highlight children's perspectives
- To properly allocate roles and responsibilities among adults, developers, data controllers, institutions
- To introduce incentives for harmonization procedures for standards development
- To introduce mechanisms of reporting and monitoring in a continuous assessment
- To develop tailored awareness initiatives and educational paths for target groups and stakeholders

#### **Our Contribution**



- To develop **multi-level assessment tools**
- To extract **best practices** and legal enablers from the gap analysis
- To design contractual clauses, self-regulation mechanisms for companies, institutions, adults
- To propose **law reforms** at International, EU, national levels
- To promote consistency mechanisms between legal formants, authorities, and policy makers
- To develop educational paths, training modules and deliver them



#### **Questions?**

#### Thank you for your attention!

Email <u>denise.amram@santannapisa.it</u> <u>https://www.santannapisa.it/it/denise-amram</u> <u>www.lider-lab.it</u>