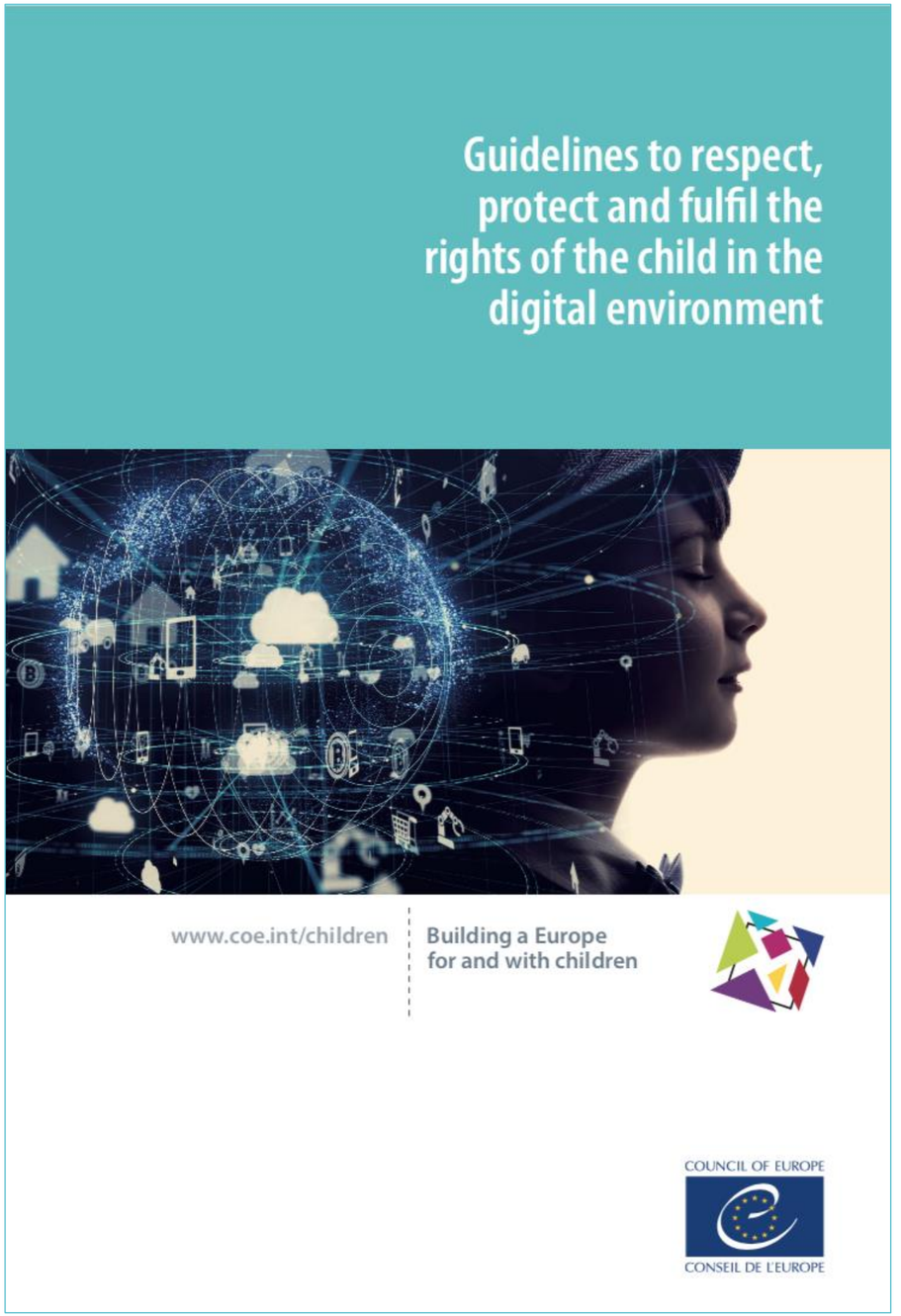
GHENT UNIVERSITY

Artificial intelligence, data protection and child rights policy

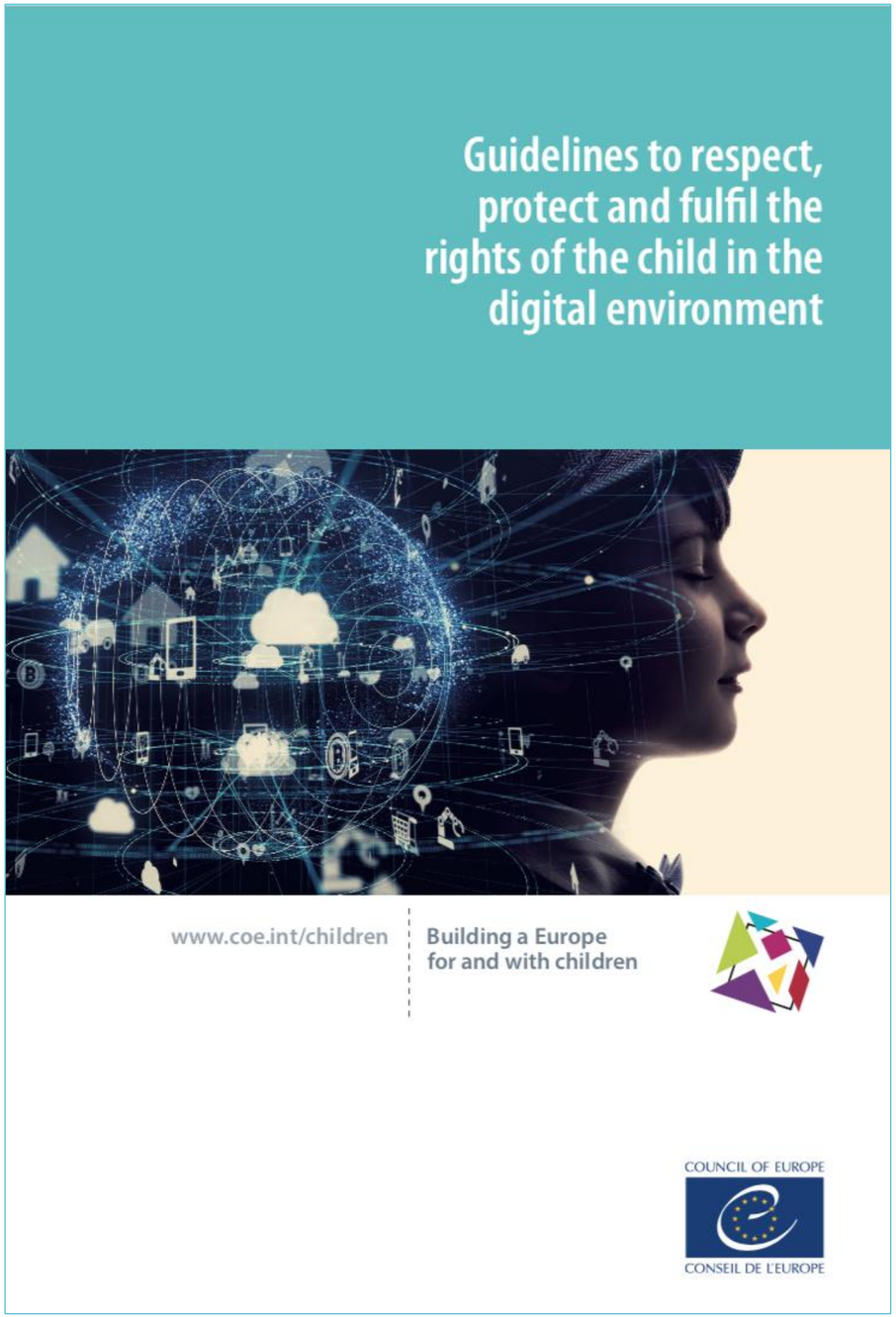
Prof. dr. Eva Lievens
Law & Technology
Ghent University



3.4. Privacy and data protection

26. Children have a right to private and family life in the digital environment, which includes the protection of their personal data and respect for the confidentiality of their correspondence and private communications.

27. States must respect, protect and fulfil the right of the child to privacy and data protection. States should ensure that relevant stakeholders, in particular those processing personal data, but also the child's peers, parents or carers, and educators, are made aware of and respect the child's right to privacy and data protection.



76. States should set up legal frameworks that apply to the processing of personal data of children and regularly evaluate the overall effectiveness of such frameworks. Due account should be taken of the relevant international and European instruments which refer to data-protection principles and rights, such as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

Handbook for policy makers on the rights of the child in the digital environment

www.coe.int/children

Building a Europe for and with children

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Profiling

Profiling is an automatic data processing technique that consists of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes. Profiling can be carried out for a variety of reasons, such as health reasons or marketing or advertising purposes.

Profiling is sometimes used to make **automated decisions** about an individual. According to Convention 108+, however, every individual shall have a right not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration.

The Committee of Ministers has acknowledged in its Recommendation that profiling of children may have serious consequences for them throughout their life, and given that they are unable, on their own behalf, to give their free, specific and informed consent when personal data are collected for profiling purposes, **specific and appropriate measures for the protection of children** are necessary to take account of the best interests of the child and the development of their personality in accordance with the UNCRC.[46]

Smart and connected toys and devices

An emerging concern relates to the way in which the Internet of Things (IoT) and, in particular, the Internet of Toys, affects children. New smart and connected toys directed at children (such as dolls, robots and watches) provide many positive opportunities for children, such as entertainment, enjoyment and reassurance, (informal) learning, identity-building and self-development. Yet, such devices may also pose serious risks to children's rights to privacy and data protection. These include corporate and government surveillance, data privacy and security issues, geolocation tracking, remote control of technologies and security failures. Moreover, connected toys are not the only internet connected devices that children are using today. Other IoT devices that impact children's lives and rights, such as smart home assistants, which are not directly targeted at children, but are present in their home environments, should also be the subject of regulatory compliance checks.

Sharenting

Parents are not only crucial in protecting their child's privacy online, but they may also pose a risk to their privacy. Sharenting is a word that is made up of 'sharing' and 'parenting'. It refers to the phenomenon of parents sharing information about their children, photographs for example, on blogs or social media, such as Facebook, Instagram or YouTube. Of course, most parents do this with good intentions, because they are proud of their children, or because they want to share experiences with other parents about the wonderful but sometimes also difficult aspects of being a parent. Some parents share only occasionally, other parents share almost everything that happens in their daily lives. Children, especially as they grow older, do not always feel comfortable with the information that their parents share. Sometimes conflicts arise between the child's right to privacy and the right to freedom of expression of the parent. Whatever the circumstances, parents should keep the best interests of the child in mind and discuss with their child what they share and why.

Handbook for policy makers on the rights of the child in the digital environment

www.coe.int/children

Building a Europe
for and with children

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Protect children's personal data in education setting

STRASBOURG | 27 NOVEMBER 2020


CAHAI
Ad Hoc Committee
on Artificial
Intelligence


INDEPENDENT
HIGH-LEVEL EXPERT GROUP ON
ARTIFICIAL INTELLIGENCE
SET UP BY THE EUROPEAN COMMISSION
AI
ETHICS GUIDELINES
FOR TRUSTWORTHY AI


Policy
guidance
on AI for
children
DRAFT 1.0 | SEPTEMBER 2020
unicef | for every child

IN FOCUS: Advances in Artificial Intelligence (AI) and implications for children's rights

Opportunities and risks related to AI in the context of children's rights in the digital environment

TYPE OF MEASURE	SPECIFIC PRINCIPLE/RIGHT	OPPORTUNITIES RELATED TO AI (EXAMPLES)	RISKS RELATED TO AI (EXAMPLES)
Fundamental principles and rights	Best interests / evolving capacities of the child	▶ AI technologies can adapt to children's maturity and capacities	▶ Children come into contact with AI technologies that are not designed with them in mind (e.g. AI devices in the home): risk of difficulty in use, exposure to inappropriate information or content
	Right to non-discrimination	▶ Empowering children with disabilities: AI can tailor products to children's individual learning, physical and other needs	▶ Bias if algorithms are designed in ways which overlook certain groups or when AI "learns" from biased or non-representative data input: risk of replicating or furthering inequalities
	Right to be heard	▶ Facilitating access to information for all children, including about their rights	▶ Law, policy and practice in relation to AI and AI technologies developed without input of children and child rights advocates, impinging on the right to be heard and overlooking their interests
	Duty to engage stakeholders	▶ Engagement with business enterprises: encourage development of AI technologies, services and policies which respect, protect and fulfil children's rights in the digital environment	▶ Lack of engagement with business enterprises: risk of development of AI technologies without consideration of the impact on children ▶ Lack of engagement with other stakeholders (parents/caregivers, civil society): risk of lack of capacity to protect and empower children in the field
Operational principles and measures	Access to the digital environment	▶ AI adaptive technologies can improve access to the digital environment, particularly for children with disabilities	▶ AI technologies may be prohibitively expensive: risk of further exclusion of certain groups of children (e.g. those in poverty, those with disabilities) in the digital environment
Operational principles and measures	Right to freedom of expression and information	▶ AI filtering systems can steer children towards appropriate online content, tailored to their interests or needs ▶ Filtering systems can block access to information disorder content	▶ AI filtering systems are automatic, usually carried out according to opaque criteria and algorithms: risk of unjustified interference with freedom of expression and information ▶ Information disorder produced through AI (e.g. "Deepfake" technology/programmes which create false or misleading stories): risk to accessing quality information ▶ Algorithms promoting non-diverse, low-quality or personalised content, based on user's viewing history and inferred interests, or content that is not age appropriate or adapted: risk to freedom to seek and receive information, freedom of thought, right to development

GHENT UNIVERSITY

Thank you!

Prof. Dr. Eva Lievens

Law & Technology

eva.Lievens@ugent.Be
@evalieve

www.ugent.be
https://www.Ugent.Be/re/mpor/law-technology/en

More about our research project:

A children's rights perspective on privacy and data protection in the digital age: a critical and forward-looking analysis of the General Data Protection Regulation and its implementation with respect to children and youth

https://www.ugent.be/re/mpor/law-technology/en/research/childrensrights.htm