The Privacy Antidote: The importance of the right to privacy in countering the criminal use of ICTs to further strengthen the protection of children

Francis Monyango

CIPIT

Strathmore University
Centre for Intellectual Property and Information Technology Law

The Right to Privacy

The right to privacy is a enshrined in Article 12 of the Universal Declaration of Human Rights (UDHR), Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and in Article 16 of the Convention of the Rights of the Child (CRC).

Many national constitutions and human rights documents mention the right to privacy.

- Article 31, Constitution of Kenya
- Section 37, Constitution of Nigeria
- Section 14, Constitution of South Africa
- Article 17, Constitution of Senegal

Children's Right to Privacy

A child's right to privacy is a necessary antidote in countering the criminal use of ICTs.

The rights to privacy helps maintain appropriate social boundaries which are both physical and informational.

According to a Report of the Special Rapporteur on the right to privacy Joseph A. Cannataci, today's children are the first generation to be born into a digital age, while their parents are the first to rear 'digital children,'

Threats to Child Privacy

"Threats to children's privacy, both in the digital space and out of it, are increasing at alarming rates"

"Parents have a role to play in protecting their children's right to privacy, but it is not only up to them: States must safeguard children's rights by establishing appropriate practices and laws, and also ensuring information is available to children themselves on exercising their rights."

Threats to Child Privacy

- Adults' interpretations of children's right to privacy can impede the healthy development of autonomy and independence, and it can restrict children's privacy in the name of protection.
- Adults usually rely on surveillance to protect children is a case in point. It constrains children's rights to privacy and autonomy, yet children are increasingly subject to technological surveillance by Governments, corporations, parents, family and peers.
- Adolescents believe that privacy and private spaces away from judgment and monitoring allow them to explore ideas and creative expression and develop independent opinions. Parental controls need to be proportionate to the child's evolving capacity and views.

Perils of the digital world to children

- Child sexual abuse, whether offline or online, is a violation of bodily integrity and decisional autonomy. It has long-term consequences on personality and capacity, and the continued existence online of child sexual abuse material compounds those consequences.
- Sharenting is often described as any case in which an adult - who is responsible for the well-being of a child - "transfers private information about a child through digital channels". While the term is conventionally used to refer to social media and major telecommunication channels, information about children can also be fed into other data-tracking tools, such as fertility apps, smart toys, or personal cloud servers.

According to Meakin, due to the widespread accessibility of technology, the average child has a digital footprint before their first birthday, typically in the form of an ultrasound image or birth announcement photo. This information is not restricted to images, with birthdays, names, geographical locations and schools all susceptible to data brokers who very often sell personal information to advertisers

Young people's immersion in the ever-expanding range of digital technologies produces an ongoing stream of data, collected and enhanced by artificial intelligence, machine-learning applications and facial and speech recognition technologies. Children and their data fuel the business of the digital world.

Risks of processing children's personal data

Technological offerings need to be assessed against children's rights and best interests, as the processing of children's personal data can:

(a) Infringe privacy and data protection, including loss of autonomy and damage to personal reputation;

(b) Harm children's mental and emotional health and physical well-being;

(c) Result in economic harms or commercial exploitation.

Child Privacy Law

The European General Data Protection Regulation has provisions on protection of children's personal data which includes:

- special protection of minors by requiring information tailored to minors on processing of their data (art. 12); special vigilance regarding child profiling (recital 71); and
- a reinforced right to be forgotten (recital 65), and
- article 8 introduces a child's capacity to consent to data processing between the ages of 13 and 16.
- The general elements of data protection by design, privacy by default, the right not to be subject to automated individual decision-making (art. 22) and data protection impact assessments are worthy of wider application for protecting the personal data of children.

The Council of Europe's has adopted guidelines on children's data protection in an education setting broaden the definition of personal data processing to cover predictions about groups or persons with shared characteristics, and the definition of biometric data processing to cover those types of processing.

Child Privacy Law in Kenya

The Children Act, 2022

- Detention of children in conflict with the law, competent authorities shall take appropriate measures to facilitate humane treatment and respect for the privacy,
- Child Privacy. No person shall subject a child to arbitrary or unlawful interference with his or her privacy, family or private affairs, or correspondence, or to attacks upon his or her honour or reputation. Parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children.
- A child's personal data shall be processed in accordance with the Data Protection Act.
- Power to make orders relating to privacy in criminal proceedings.
- A child offender has the right to privacy during arrest, the investigation of the offence and at any other stage of the cause of the matter.

Data Protection Act, 2019

Processing of personal data relating to a child

(1) Every data controller or data processor shall not process personal data relating to a child unless—

(a) consent is given by the child's parent or guardian; and

(b) the processing is in such a manner that protects and advances the rights and best interests of the child.