ELEARNINGNEWS ARTICLE

Year 6 - number 191 Wednesday 23 february 2022

# Child safety in the digital age

***How do we protect children from the "dangers" of digital exposure? Here are the risks young people may face and OECD recommendations to ensure the development of digital safety***

The digital environment has become a fundamental part of daily life, education and social interactions, even among **children**. This trend, already on the rise in previous years, received a major boost from the Covid-19 pandemic that struck the world, forcing people to turn to digital media to communicate with each other through a screen and schools to take advantage of distance learning. Today, more and more children and teens are embracing the Internet. According to UNICEF data, every day in the world 175,000 children and young people go online for the first time, an average of one every half second. And in general, one user out of three is a minor.

If, on the one hand, the Internet offers a multitude of possibilities, such as socializing and searching for information of all kinds, on the other hand it also exposes its users to a series of **risks** that, increasingly, also affect children and young people who, thanks to the use of mobile devices with Internet connection, go online more easily. Online risks can affect children's well-being and are, for the most part, online versions of the dangers that children face offline, such as bullying, racism and abuse. But the dangers of surfing the Web do not preclude taking advantage of the tremendous opportunities online. Rather, it is a matter of finding ways to promote the use of the Internet, without forgetting the importance of protecting the children who use it, by focusing on an increasingly effective digital education that keeps pace with technological change.

# Online risks

According to the report *Children in the digital environment. Revised typology of risks*, compiled in 2021 by the **OECD**, the Organisation for Economic Co-operation and Development, there are currently four categories of risk that can be encountered online. It must be borne in mind that the risks associated with surfing the Internet are very variable and can change over time. For this reason, the OECD decided to revise the three categories outlined in the 2019 report, which did not yet take into account conduct risks, considering children only as passive users of the network. Some of the categories identified years ago are still relevant today, although they may have evolved over time, while other possible risks that did not previously exist are now emerging more strongly, such as the dissemination of misinformation (fake news) or the participation of children who have become protagonists of the Web, in a peer-to-peer exchange that actively involves them.
The OECD's four updated broad categories recognize content risks, conduct risks, contact risks, and consumer risks. In addition, the report also identifies risks that go beyond these broad categories and can also have large-scale impacts on children's well-being, such as privacy risks, advanced technology risks and health risks.

**Content risks**

Content risks are where a child receives or is exposed to content that is also available to all other users of the Web. This category includes the risk to exposure of four types of content:

- **Hate speech content**, which can come in the form of images, words, videos, symbols, songs, and games. These types of content may target a certain religion, gender, sexual orientation or disability.
- **Harmful content**, such as online scams, pornographic advertisements, or violent and scary images.
- **Illegal content**, which may expose children to concepts that violate laws and social norms.
- **Misinformation content**, which reports fake news: children should be taught to recognize a fact that happened versus a misrepresentation.

**The risks of conduct**

In its previous report, the OECD ruled out the harmful actions of children on the Web when they create dangers. But this active position of children in the digital environment is becoming increasingly apparent. That's why the latest analysis includes the

category of conduct risks, a possibility that arises when children are actors in a peer-to-peer exchange and engage in conduct that is inappropriate or that may make them vulnerable. Specifically, a conduct risk "occurs when a child behaves in a way that contributes to the creation of risky digital content or contact." This type of possible danger affects not only children who are victims of these behaviors, but also those who engaged in them. The following types of conduct risks fall under conduct risks: hate behaviors, which involve using the Web to attack another child; harmful, unlawful, and problematic behaviors. The latter may consist of the exchange of sexual messages or images, which can turn into child pornography and be quickly disseminated on the Net.

**The risks of contact**

This category includes cases in which a child is the victim of a harmful situation on the Net. Examples of contact risks are:
- Cyber bullying, which is the intentional and repeated aggression over time, carried out through modern technologies, targeting a victim who is unable to defend himself;
- Sexting: refers to the exchange of sexual messages, which can spread rapidly online;
- Sextortion: refers to the threat of sharing and displaying a sexual image to coerce the victim into doing something.

**Risks to consumers**

Teens who connect to the Internet can also face consumer risks. Previously, the OECD defined consumer risks as those that children may face when they receive inappropriate marketing messages, are exposed to commercial messages that are not readily identifiable as such, and when their inexperience is exploited causing financial risk (online fraud). This definition may be considered still relevant today, although a number of new and emerging practices may add to the consumer risks faced by children, such as certain mechanisms that may be behind shopping apps.
In addition to these categories, the OECD has also recognized risks that cut across contact, conduct, commercial and content risks, and can significantly affect children's lives. These are:

- Privacy risks;
- Advanced technology risks;
- Health and wellness risks.

In fact, there are a number of steps you can take to protect your personal data, while trying to avoid privacy risks, to maintain **cyber security**.

# OECD Recommendations

In 2012, the OECD Council adopted a Recommendation for the Protection of Children Online, which was later amended in 2021 and renamed the Online Recommendation on Children in the Digital Environment. The document is intended to help teachers, parents and policymakers address technological advances and identify tools to support children and youth in pursuing and addressing online opportunities. The first recommendations address the need to ensure a "safe and beneficial digital environment for children" and are directed at organizations that provide services for children in the digital environment. This first category of recommendations is divided into:

- Core values, which consist of recognizing the best interests of the child and identifying their rights, which must be protected and respected;
- Empowerment and resilience, which involves supporting parents, guardians and children in understanding and being aware of their rights and legal services related to the digital environment;
- Proportionality and respect for human rights in measures taken to protect children online;
- Inclusion of children in the digital environment, taking into account their needs and age;
- Accountability and sharing across organizations to provide a safe and digital environment.

The second set of recommendations addresses the overall policy framework and aims to create policies that develop a safe and beneficial digital environment for children through the adoption of appropriate laws, digital literacy, and the promotion of research and development of privacy-protecting technologies. The document, in its third section, recommends the promotion of international cooperation, emphasizing the importance of collaboration among countries through **international networks** that defend children's interests in the digital environment and through the development of shared standards. Finally, the OECD Recommendations emphasise the need to promote guidelines for digital service providers to protect children surfing the Internet.

# Five tips for informed browsing

For children to be able to access the digital environment safely, it is critical to educate them and equip them with the tools they need to deal with the Internet and the issues they may face. Given the many possible risks to which the Internet exposes its users, UNICEF has provided children with five tips to help protect them from the dangers of the Internet:

1. Avoid droomscrolling, that is, the obsessive search for **bad news on the web**. In case of droomscolling is recommended to impose a time limit, devoting the rest to creative activities;
2. Use **sources that are reliable** in terms of information;
3. Pay attention to **security**: it is good to check your privacy settings, turning to a trusted adult in case of doubt or reporting the situation to the platform;
4. Put **kindness** first, to avoid using the digital environment to spread aggressive and offensive messages;
5. Keep the **real world** in mind, without forgetting personal relationships, which must be experienced without the presence of a screen.

*Translated with www.DeepL.com/Translator*