EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Child protection on social networks in the era of Covid-19 confinement

VALERIA MANZO
Ph.D. (c) at University of Campania Luigi Vanvitelli
Lawyer in Naples

Abstract

While it is true that in the digital age minors have considerable tools to express their personality and exercise the rights recognised by international conventions (also through the use of technologies that allow new models of relationships), the continuous process of renewing applications inevitably results in a greater concentration of information with consequent exposure to greater risks for security and privacy.

In this context, due to the confinement measures caused by the COVID-19 pandemic emergency, children have become even more dependent on social media in order to stay in touch with their friends, to express their feelings, to study and to distract themselves.

The aim of this survey is to address the specific issue of children's interactions on social media and the impact in terms of privacy and data protection as their vulnerability has further increased in the light of the confinement emergency.

Keywords: Minors - social media - social networks - privacy - data protection - GDPR - COVID-19 - TWIGIS.it - Jonathan Galindo.

Summary: 1. The relationship between minors and social media. – 2. The protection of minors in the GDPR. – 3. Digital awareness. – 3.1 The TWIGIS.it platform. – 4. Social media in the COVID-19 era - The Jonathan Galindo case. – Conclusions.

1. The relationship between minors and social media.

The advent of social media has brought about a revolution in the ways of interaction and personal communication, which has had a profound impact on relational activities and a greater concentration of information with relative exposure to higher risks for the security and privacy of users.

Although living in a constantly evolving technological framework, some widespread processes can be identified that constitute the identifying traits of the social media[1] phenomenon.

In a study conducted in 2015[2] these were the four common characteristics identified:

--- the use of Web 2.0[3];

[1] R. Cafari Panico, *From Internet to Social Media*, (1nd edn, Maggioli 2013).

[2] J.A. Obar, S. Wildman, 'Social Media Definition and the Governance Challenge: An Introduction to the Special Issue' (2015) Telecommunications Policy, vol. 39, n. 9, 745-750.

[3] Web 2.0 means the phase of the Web following Web 1.0, characterised by the possibility for users to interact and modify the contents of the web pages of a site, portal or web platform.

--- the absorption of User-Generated Content (UGC)[4];
--- profiling users of the site or app;
--- the connection of profiles with those of other users or user groups.

If you do a Google search by writing "minors and social media" as first results you will see a series of articles and insights indicating the "risks" they run and a series of instructions for parents to protect and defend them.

For the digital natives, the net is not "one of the many means of communication", but "the main dimension of life" with the consequence that the relationships woven online, the sharing on social networks and the perception of the world increasingly mediated, impose new needs for protection, in the face of the inadequacy of the traditional categories of the law to regulate phenomena in continuous evolution.

As a vehicle of opportunities for growth and emancipation, the web risks, if lived in the absence of the necessary awareness, to expose increasingly fragile children to underestimated dangers, on the side between illusion of autonomy and introjection of rules and exercise of responsibility[5].

To give an example, these are the most frequent dangers:

--- sharing and dissemination of personal information and photographs;
--- violent content;
--- distortion of reality;
--- addiction;
--- use of the data for commercial purposes with consequent advertising bombardment;
--- social isolation[6].

Well, by catalyzing social media attention to phenomena such as those just mentioned, can it be considered that they are not the cause?

Starting from the children's sense of responsibility that inevitably passes for their parents, the problem must be placed in today's social and educational context where young people all too often find themselves facing the age-old problem of growth, even within a digital context, alone or in the company of false teachers.

Among the factors capable of positively influencing the awareness of minors, the role of teachers[7] and parents[8] remains fundamental, as well as the emulation of positive behaviour[9]. In particular, parents should be familiar with social tools and learn how to use them in order

---

[4] UGC, i.e. user-generated content, means any type of content made accessible through social platforms such as blog posts, wiki contributions, forum discussions, tweets and podcasts.

[5] Hearing of the President of the Guarantor for the protection of personal data, Antonello Soro, follow-up to the cognitive survey on forms of violence among children and against children and adolescents - Parliamentary Committee on Children and Adolescents (8 July 2020) on https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9434094.

[6] S. Weeden, B. Cooke & M. McVey, 'Underage Children and Social Networking' (2013) Journal of Research on Technology in Education, vol. 45, n. 3, 249-262.

[7] K. Davis, C. James, 'Tweens' Conceptions of Privacy Online: Implications for Educators' (2013) Learning, Media and Technology, vol. 38, n. 1, 4-25.

[8] S. Yusuf, M. Nizam Osman, M. Salleh, H. Hassan, M. Teimoury, 'Parents' Influence on Children's On-line Usage' (2014) Procedia - Social and Behavioral Sciences, vol. 155, 81-86; S. Livingstone, K. Ólafsson, E. J. Hel-Sperd, 'Maximizing Opportunities and Minimizing Risks for Children Online: The Role of Digital Skills in Emerging Strategies of Parental Mediation' (2017) Journal of Communication, vol. 67, n. 1, 82-105.

[9] Y. Seounmi, 'Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk- Benefit Appraisal Approach' (2005) Journal of Broadcasting & Electronic Media, vol.49, n. 1, 86-110.

to encourage children to use them consciously and, at the same time, monitor their online activities[10].
The "neutrality" of the web, understood as susceptibility to harmful or solidarity-based uses, charges users with responsibility for their online conduct and makes adults responsible for the delicate task of making children aware of how extraordinary, but also risky, the new dimension of life can be.
Rather than talking about the need to save children from social media, it should be about helping them to cope with growth problems by providing them with answers they can confront and learn to live the digital spaces available to them.
As the Council of Europe's Guidelines on the Rights of the Child in the Digital Environment underline, a real education, ethical and civic digital literacy would be the tool to enable children to draw all its extraordinary resources from the web in order to be "digital aware citizens".

2. The protection of minors in the GDPR.

Although *datafication* and connectivity simplify daily activities, the regulatory framework for the protection of minors, however articulated, does not seem sufficiently protective[11].
To counteract the vulnerability of data subjects, EU law grants them specific individual rights including the right to be informed of the fact that their data is being collected, the right of access to retained data, the right to object to unlawful processing and the right to rectification, erasure and blocking of data.
The Data Protection Directive requires that data subjects consent to data processing, regardless of the sensitivity of the data being processed (see Articles 7, 8 and 14).
A child-friendly consent procedure implies that the child's developing capacities are taken into account and, therefore, his or her progressive involvement.
The first step requires that the child's legal representative consults with the data subject before authorizing the processing; then, consent must be obtained from both the legal representative and the child; finally, consent is required only from the child when the latter is an adolescent[12].
In order to define the "risk" phenomenon it is necessary to recall the notion of *networked self* (i.e. the virtual projection of one's own identity) and identify the perception of minors themselves with respect to the threats connected to the use of social media.
The prolonged use of digital instruments that convey personal data, often without control, can well generate exponential risks that also involve the psychic-cognitive development of the child who does not yet have a fully trained understanding capacity[13].
From this point of view, among the negative effects of the so-called *privacy paradox*, as documented in the sociological literature, there is the tendency for the most fragile subjects

[10] According to the Wall Street Journal, Facebook is studying a technology to "link" children's profiles to those of their parents so that they can authorize their children's friendships and applications to use.
[11] D. Lupton, B.Williamson, 'The Datafied Child: The Dataveillance of Children and Implications for Their Rights' (2017) New Media & Society, vol. 19, n. 5, 780-794.
[12] FRA, *Handbook on European Law relating to the rights of the child* (2015).

[13] These include online communication with unknown subjects; exposure to content promoting anorexia, self-harm, drug use or suicide; cyberbullying; images of injuries to other children and exchange of sexual images.

to underestimate the dangers in terms of privacy and to underuse the tools made available[14]. While Directive no. 46 of 1995[15] made no distinction between the processing of children's and adults' data, as a consequence of the risk-based approach, the GDPR has taken a central role, having understood the protection of children's privacy as "data minimisation and computerisation".

Article 8 of Regulation (EU) 2016/679 specifically provides: "*Where Article 6(1)(a) ("when the data subject has given his or her consent to the processing of his or her personal data for one or more specific purposes") applies, with regard to the direct provision of information society services to minors, the processing of the child's personal data is lawful when the child is at least 16 years of age. Where the child is under 16 years of age, such processing shall be lawful only if and to the extent that such consent is given or authorised by the holder of parental responsibility.*

Member States may establish by law a lower age for these purposes provided that it is not less than 13 years old.

The data controller shall make every reasonable effort to verify in such cases that consent is given or authorised by the holder of parental responsibility for the child, in view of the technologies available.

Paragraph 1 shall be without prejudice to the general provisions of the contract law of the Member States, such as the rules on the validity, formation or effectiveness of a contract in relation to a minor".

The division made by the rule between the limits and conditions of the *privacy* consent and the contractual consent raises the following questions:

--- the minor could validly stipulate a contract and be "sub-threshold" for the provision of consent to the processing of data;

--- i.e. he could independently provide *privacy* consent without being able to validly enter into a contract, with the consequence that, in the first case, a valid contract (inasmuch as it complies with the requirements of personal development) will be opposed to unlawful data processing; while in the second case, a valid provision of consent for the lawfulness of the processing will be opposed to the cancellation of the contract itself[16].

When talking about children's "digital" rights, it should not be overlooked that access to web services is not only a right to exercise other rights (freedom to search, receive and disseminate information and ideas, to freely express one's opinion in terms of thought, conscience and religion, to associate and come together peacefully) but it is also the means by which certain rights can be protected where there is a real or alleged violation or where there is social discomfort related to the exercise of the child's freedoms.

For this reason, Recital no. 38[17], in stressing the greater risk associated with the processing of personal data of minors, has led to the strengthening of information tools (with a view to

---

[14] *Ex plurimis*, A. Thiene, 'The personality rights of children in virtual space' (2017) Annals online of Teacher Education and Training, vol. 9, n. 13, 26-39; A. Spangaro, *Minors and mass media: old and new means of protection* (1nd edn, Ipsoa, 2011), C. Perlingieri, 'La tutela dei minori di età nei social networks' (2016) Review of Civil Law, n. 4, 1324 et seq.

[15] It was first implemented by Law no. 675/1996 and then by Legislative Decree no. 196/2003.

[16] Childhood and Adolescence Watchdog, Note to the Prime Minister on the need to implement training programmes to develop digital awareness of underage people for digital consent, 10 September 2018 on https://www.garanteinfanzia.org/news/decreto- privacy-14-anni-il-consenso-ai-servizi-web-agia-ora-educazione-alla-consapevolezza.

[17] *According to* which: "*Children deserve specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards involved and their rights with regard to the processing of personal data. This specific protection should, in particular, cover the use of children's personal data for marketing purposes or the creation of personality or user profiles and the collection of personal data relating to children when using services provided directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of prevention or counselling services provided directly to a child*".

forming a conscious consent), as well as to the provision of rules for processing built as an objective imposed on the owner made responsible for the adoption of specific technical rules that achieve the protection of personal data.
According to a study on the cognitive development of minors conducted by the Stanford Children's Health paediatric centre, the typical phases in the growth of a child/adolescent were highlighted[18].
If between 6 and 12 years of age, we find the phase of the so-called concrete cognitive development, relative to the ability to think and reason, carrying out concrete operations on objects and actions, between 12 and 18 years of age, instead, the so-called complex thought develops, characterized by formal logical operations that allow the child to think about different possibilities, to reason from known information, to consider different points of view debating ideas and opinions, until reaching autonomous and personal decisions.
Sticking to the purely "medical-scientific" approach, the child, already at the age of 13, is in the midst of developing his or her personal identity and, therefore, normally "capable of discernment" also with regard to the use of information society services.
Although a child is "capable of discernment", can we share the concern of the European legislator when trying to make the web safer?

3. Digital awareness.

While increasing the minimum age of validity of consent, it can certainly not prevent access to "harmful" content circulating on the web.
In fact, to consider the issue resolved after preventing access to digital services means to reason in the abstract, denying a phenomenon.
On the occasion of the XIII Safer Internet Day 2017, the Safer Internet Day set up and promoted by the European Commission, the Blue Telephone has organised a special event at the Chamber of Deputies, an event entitled "The relationship between young people and the internet" in which a survey carried out by Doxa Kids was presented as a preview. The survey showed that, in Italy, among the under 13 respondents (out of a sample of over 600 adolescents) 73% habitually use WhatsApp, 44% Facebook, 35% Instagram, 13% Snapchat and 11% Twitter.
This data clearly shows how digital natives are able to circumvent the limitations of the network to create profiles or accounts even in the 9-12 age group.
If, therefore, the problem seems to be the non-existence of a training programme included in education that educates children to use digital technologies safely, preventing them from accessing information society services would only generate a greater sense of curiosity.
On balance, keeping the age of autonomous digital consent high would not help to prevent risks if the rise was not accompanied by appropriate training of those to whom consent is given.
But is it realistic to think that these measures are a form of protection for children?
A recent study carried out by EU Kids Online[19], which coordinates and stimulates surveys on how children use new media, with particular reference to risks and web security measures, said that the more children use the Internet, the more they acquire digital skills and are able to seize opportunities on the Internet, comparing content and websites and assessing the

[18] On https://www.stanfordchildrens.org/en/topic/default?id=cognitive-development-90-P01594.

[19] On http://eprints.lse.ac.uk/60512/1/EU%20Kids%20onlinie%20III%20.pdf.

reliability of information.
Education in the use of digital platforms is not, however, the only aspect to be considered in terms of learning, as there is also education through digital platforms.
During her speech in New York on July 12, 2013, in the UN Headquarters, Malala Yousafzai, the youngest Nobel Peace Prize winner because of her commitment to the affirmation of civil rights and the right to education, was asked: "What would you recommend to someone who believes that an injustice is happening in her community but who does not know how to start making a real impact to remove it?
Such is the answer: "I think it's easy. It's full of people who would start wondering 'Who do I have to meet to say what's going on? Where do I have to go to do it? '. But the tool in front of you is social media. Use them. [...] It is difficult to stand up and tell a Taliban that what they are doing is wrong if they are in front of you in your house. It is easier to start a peaceful protest on Facebook".
Well, teaching is also applicable to children's use of social media and web services: not everyone is in a position to ask their parents for consent, not everyone would get it, yet often the first step to remove physical and mental injustice is to create a social profile or to join a virtual space where they can express their opinion freely and without parental interference in their personal sphere. After all, privacy is also this.

3.1 The TWIGIS.it portal.

If in the beginning there were the late digital immigrants (who grew up without technology and were sceptical about its use), digital immigrants (born in an analogue world but adapted to use technology) and digital natives (who from birth have had to deal with technology), today the eyes are focused on the "mobile- born" or children who, even before learning to walk, already know how to move easily on PCs, smartphones and tablets[20]
Paul Holland, general partner at the Foundation Capital, wondered what the "mobile-born", once grown up, expect from technology.
According to Holland, their approach to furniture will force them to rethink ways and timescales of the traditional day in the office, including new interfaces, software and hardware to be refurbished; assuming that offices, as we know them today, will still exist.
Whether it is work or leisure, the key word will be interactivity, since, according to the "mobile-born", everything can be implemented with software.
At the moment, the curiosity of children for tablets and the like represents a new challenge, especially for companies.
If Intel has acquired Kno, a startup specialising in the construction of educational software whose flagship product is interactive textbooks to browse on mobile, Facebook, along with other big names, from Google to Yale University, in Panorama Education, a startup that uses online surveys to collect data that will then be processed and used to improve the school environment, trying to solve problems such as bullying.
There are also those who, like the Israeli startup Twigis, have tried to create child-proof versions of tools already used by adults, launching a social network and an information portal for children between 6 and 12 years of age which, while safeguarding their privacy, provides a space in which they can develop their creativity and share experiences.
On Twigis:

[20] According to a Common Sense Media study conducted in the USA, if the percentage of two-year-olds using a mobile device is 38%, this rises to 63% in children under the age of eight.

--- minors have a personalized profile on which they cannot post pictures but only create avatars;
--- it is necessary to insert the email of your parents, who will have to give their consent;
--- all content and messages are screened in advance by a group of moderators in an anti-bullying manner that provides for the suspension (from two days to one month) from the social if one user targets another[21];
--- personal information is not disclosed, not even through cookies.
The portal consists of two sections: in the news section minors can read articles and comics (for which it is also possible to create new ones to share with the community), as well as follow interactive videos and tutorials aimed at doing DIY jobs; in the games section there is a large collection divided into categories such as adventure, action, sport, board games and cards.
This gives children the opportunity to experience virtual worlds in a safe digital environment that stimulates their skills and creativity.

4. Social media in the COVID-19 era - The Jonathan Galindo case.

While lockdown confinement has forced many children to make further use of social media in order to stay in touch with each other, it has also exposed them to increased vulnerability to violence, abuse and online grooming.
According to the Lanzarote Committee's "Declaration on the Protection of Children from Sexual Exploitation and Sexual Abuse during the COVID-19 Period", adopted on 15 May 2020, it is essential to assess the impact of the pandemic crisis management measures in place and to adapt the responses of child protection systems to the new situation by ensuring that all children are confined to safe environments.
As recently stressed by the Global Partnership to End Violence against Minors and UNICEF, together with partners in the Alliance for the Protection of Children and Adolescents in Humanitarian Action, the prevention of exploitation and abuse and safe reporting of concerns should be an integral part of all COVID-19 prevention and control measures.
In the document, the Committee recalls how the measures taken by States to contain the pandemic have exposed "*children to a greater risk of abuse, neglect, exploitation and violence*".
It reads as *follows:* "As a *result of the confinement measures, children are increasingly online and depend on social media to stay in touch with friends, express feelings, study, distract themselves": a large number of children are therefore likely "to be lured online and become victims of sexual extortion, cyberbullying or other sexual exploitation facilitated by technology*".
For the Committee, therefore, it becomes "of the *utmost importance that helplines and hotlines are known both to minors and to the general public and that they are made available 24 hours a day, including through online platforms*" and that States ensure that they have adequate human resources and equipment so that no request for help is left unanswered.
Attention is also asked for initiatives "*that inform children and young people, in a manner appropriate to their age, of the assistance and support services, both physical and psychological, to which they still have a right of access*" and states are invited to provide forms of support for parents and guardians in the management of children's emotions and behaviour during the crisis situation.

[21] It is no coincidence that important partnerships have been signed in Italy with the Telefono Azzurro and the Moge (Italian parents' movement) who have participated in the analysis and definition of the structure of Twigis.it's contents, in addition to the collaboration of the State Police.

The Council of Europe, for its part, has developed a series of awareness-raising documents focusing not only on the detection and reporting of violence against children, but also on issues such as how to talk to children about COVID-19, how to manage time spent in front of a screen during an emergency, how to assist during confinement and how to ensure online safety at a time of social distancing[22].

The isolation to which minors have been forced in recent months has led some of them to adopt bolder online behaviour, making them even more vulnerable.

On 30 September last, the main Italian newspapers reported the tragic news of an 11-year-old Neapolitan minor who took his own life.

The victim, before killing himself by jumping off the balcony, would send a message WhatsApp to the mother of the following tenor: "*Mommy, Daddy I love you. Now I have to follow the man in the black hood. I am running out of time. Forgive me.*

What is most frightening is the lucidity with which an unavoidable deadline and an appointment with an irreversible death are put off.

The reconstructions carried out led to identify in "Jonathan Galindo" the referee of a deadly online game from the image of an anthropomorphic dog (a sort of Walt Disney's Goofy with a sinister smile) whose objective would be to convince the interlocutor to take part in the so-called "game".

Such is the consolidated dynamic: the referee of the challenge would begin by sending a request for friendship to minors on social networks and then write them a private chat message of the following tenor: "Do you want to play a game?

Any positive response would start a game of tests of courage to the point of self-harm.

But who is hiding behind Galindo? The truth is that anybody can wear his clothes on social networks and it is difficult to think that behind the many profiles created there is only one person hiding.

Through Google Trends it has been possible to observe how the first mentions of this *creepypasta* phenomenon with a terrorist background were made in January 2017, with epicentre in Latin America and India, and how interest in the "Jonathan Galindo" search key began to grow in May 2020, and then exploded in July.

While the deadly challenge on TikTok has become a summer trend (demonstrating the proliferation of videos in which users dance against the background of screens captured from conversations with the one who is supposed to be an occult persuader), on Facebook, Instagram and Twitter profiles there has been a split between users who have raised the alarm[23] and users who, instead, have publicly announced that they want to play the role of the anthropomorphic dog in order to scare their friends.

The question arises, therefore, spontaneously: what motivates minors to accept the challenge?

According to some reconstructions, the victim would be "frightened" by demonstrating to the referee that he knows his location and IP address.

What if it is a spirit of emulation? or a viral phenomenon of fashion"? And above all, why

---

[22] On https://www.coe.int/en/web/children/covid-19.

[23] A tweet from @uh_xsh on July 2nd, which went viral, is a perfect example of how these online dynamics work. The text of the tweet is as follows: *"*WARNING* If you are reading, you are obliged to rewire. Make your friends stay alive. Circulating an account called Jonathan Galindo, they are the masters of the Blue Whale Challenge whose intent is to convince you to commit suicide. If someone sends you a dm ("direct message") or interacts with you, block it".*

do children feel "obliged to continue rehearsing"?
Analysing the elements of the challenge in question, it is easy to see quite a few similarities with other deadly online games developed since 2017; Think of the Blue Whale phenomenon (a 50-day course - coordinated by a tutor - which involves challenges of increasing difficulty aimed at destroying children's self- esteem to the point of convincing them that their life is worth nothing and therefore leading them to suicide), the Tide Pods Challenge (challenge to eat capsules of washing machine detergent), the Bird Box Challenge (challenge to perform actions such as driving blindfolded), the Balconing (challenge to dive from a balcony of a flat or hotel room into a swimming pool only after taking drugs or alcohol), or the Momo Challenge (challenges ranging from watching horror films to self-harm).
The real danger of these "games" is the so-called "Werther effect" (or Copycat suicide), a phenomenon of emulation that leads to an increase in suicides after the news of a suicide published in the media.
How, then, can we combat the phenomena of deadly games online? The World Health Organisation has published a *vademecum* for the press which calls for a "responsible presentation of information" avoiding sensationalism, excessive amplification of the news and details on suicides[24]".
The answer seems, therefore, aimed at containing, as far as possible, the high mediaticity in order to avoid the emergence of new emulative phenomena and the protagonism that, too often, minors hide within themselves.
But can this be considered sufficient? In the writer's opinion, no, because at a time when the network has become an inseparable companion, starting from the fragility and emotional instability of children, it is all too often forgotten how fundamental the active presence of parents is through dialogue (in order to understand whether their children are aware of what Social Challenges actually are and what they entail) and careful monitoring (aimed at noticing suspicious behaviour or bodily injury).

Conclusions.

Never as in the current era have families, schools and civil society been called upon to recognise and share their educational skills and knowledge respectively, in order to enhance the growth of children and strengthen the influence of their role as active citizens, aware adults capable of becoming reference points for future generations[25].
The web is no longer just a virtual place to visit, but an atmosphere that surrounds reality itself, constantly bringing new possibilities and concerns closer together.
Therefore, the challenge for the educational, social and family system becomes the constant updating on the evolution of technologies by spreading the culture of "media education" and educating minors to a responsible and conscious use of the web and social networks without, however, neglecting the non-virtual reality of which they should not be spectators, but actors, becomes an activity of considerable importance.

[24] On https://www.who.int/mental_health/prevention/suicide/resource_media.pdf.
[25] A. Alesina, A. Ichino, *Homemade Italy. Survey on the real wealth of Italians*, (1nd edn, Mondadori 2009).