**Paris, 23 October 2020**

**The French Data Protection Authority (La Commission Nationale de l'Informatique et des Libertés) “CNIL” extends its gratitude to the United Nations Special Rapporteur on the right to privacy (UNSRP) for the opportunity to submit a contribution on the subject of "the privacy rights of children and how this right interacts with the interests of other actors as the child develops the capacity for autonomy" in the context of his next report to the HRC in March 2021.**

Protecting children's privacy online has been identified as an overarching priority of focus for the members of the Global Privacy Assembly of Data Protection and Privacy Authorities (GPA) which has been included in its annual work plan, and by sharing information and experience from national initiatives focussed on children’s privacy online.

Raising children's awareness and teaching them how to protect their personal data, helping them to become responsible digital citizens and guaranteeing their rights in relation to parental rights determine the lines of action taken by the [Data Protection and Privacy Authorities Working Group on Digital Education (DEWG)](https://globalprivacyassembly.org/wgde-update/) led by the CNIL within the GPA. Since its creation in 2013 and within the framework of its mandate, in particular, aiming to "provide special protection for minors in their relations with the digital world", the CNIL has proposed on behalf of the DEWG several resolutions on Digital Education adopted by the GPA Conference[[1]](#footnote-1).

The CNIL like many other Data Protection Authorities in Europe has decided to initiate a reflection on the rights of minors with regard to their personal data. By introducing for the first time specific provisions for minors in European data protection law the General Regulation on Data Protection (GDPR), calls for greater consideration of the rights of minors in the digital environment and the establishment of specific guarantees to protect their personal data.

For this purpose, a *working group on the rights of minors in the digital environment* has been set up within the CNIL (conducting among other tasks a survey on a panel of children and parents in order to better understand children's practices and the perceptions they generate, a public consultation on its website, which has collected more than 700 contributions, monitoring work at the international level, conducting specific controls, consultations of law professors specialized in the subject of minors' rights, etc.).

**This work will result in the publication of conclusion by the College of commissioners of the CNIL, and eventually propose follow-up actions (such as additional work, priority awareness-raising actions).**

By introducing for the first time specific provisions for minors in EU data protection law, the GDPR creates new issues that need to be addressed. Several areas of thought have been identified:

1. The legal capacity of a minor to perform certain acts alone on the Internet;
2. The implementation of the application of the provisions of the GDPR concerning the protection of minors’ data;
3. The methods used to check the age of users and obtain parental consent;
4. The possibility - or not - for minors to directly exercise their rights with regard to their personal data;
5. The possible implementation of additional guarantees for the processing of personal data concerning minors.

These comments reflect part of legal analyses and avenues of reflection currently being conducted by our Commission on the subject.

The study carried out by the CNIL first of all consisted in taking stock of the current state of digital practices of young people and the evolution underway, and in looking at the economic and data protection issues raised by these practices. An analysis was also conducted of the legislation applicable to minors in relation to digital practices, at both international and national levels. Finally, the main issues identified in this regard have led us to inventory several possible approaches in terms of control and verification mechanisms and to submit concrete avenues aimed at improving the protection of minors' data.

1. **The current context and its limits**
2. **Young people's digital practices: widespread, early and poorly supervised by parents**

Two strong trends emerge from the survey conducted by the CNIL and other recent surveys on the subject: young people's digital practices are widespread and occur early, but also largely in an autonomous way poorly supervised by parents.

* **Widespread practices that occur increasingly early**

The European **Eu Kids Online 2020** survey shows that in many countries the **time spent online by young people has almost doubled since 2010**. In France, the daily average is around two hours during the week and three hours during the weekend for young people aged 9 to 16.

**Digital practices start increasingly early.** Parents of 8-9 year olds report that their child started using the Internet on their own at the **age of 7,** playing online games and watching videos on platforms such as YouTube. Children on average register to a social media later, around the age of 8 ½ while this age rises to 13 for parents whose children are between 15 and 17.

* **Autonomous practices, poorly supervised by parents**

**Browsing the Internet without parental supervision is widespread among young people. This phenomenon is certainly largely favoured by the generalisation of digital equipment for minors, who acquire their own device increasingly early.**

**Parents' lack of knowledge about their children's online lives reflects their level of autonomy**. Parents are aware of their children's earlier digital practices, but they are not aware of the extent to which these practices are becoming widespread: for example, parents underestimate on average the frequency with which their children play online alone.

The finding of de facto autonomy of minors online is corroborated by the **lack of widespread use of parental supervision systems, except for online shopping**. Younger **children seem to have their online practices more closely supervised** than their elders in their first online experiences.

1. **The personal data of minors: highly coveted data**

The personal data of children is of great interest to advertisers, since they make up one third of Internet users. The online advertising market for children could be worth **$1.7 billion by 2021[[2]](#footnote-2). Estimates show that more than 72 million pieces of data per child will have been collected by online** advertising companies before he or she reaches the **age of 13[[3]](#footnote-3)**. This data is collected[[4]](#footnote-4) at least as much when children visit sites aimed at adults as when they use services specifically designed for them.

* **A differentiated perception of the protection of personal data among minors**

Young people are often more aware than adults of the technical tools to protect their privacy. However, while they are more comfortable with their privacy settings, they do not seem to have **a full understanding of the issues and mechanisms surrounding the processing of personal data online**.

* + Children attach importance to the protection of the data they provide, but not to data that is captured without their knowledge or to data that is inferred from the information they have given[[5]](#footnote-5).
  + They do not see how this data can contribute to their long-term digital footprint.
  + Privacy is primarily approached by children in an interpersonal context: they expect companies to act as if they were their friends[[6]](#footnote-6).

Children are also **vulnerable to attention-grabbing techniques based on the exploitation of cognitive biases[[7]](#footnote-7)** (e.g. '*dark patterns*'), which are designed to influence users’ choice without coercion, through design or language choices.

* **The validity of minors' consent in the face of their lesser understanding**

A 2018 study by the BBC assessed the language used in the Terms and Conditions of Use and privacy policies of the main sites and applications used by young people. It concluded that of the 16 services tested, the reading level required to understand these texts was that of a university student.

**These gaps in understanding raise the question of the value of the consent of children, which often struggle to understand the scope and the purpose of the processing they are allowing.**[[8]](#footnote-8).

* **Risks related to commercial processing**

Children are very receptive to advertising and marketing messages. They are particularly vulnerable as they are generally **less equipped to distinguish between online advertising and information, especially in social networking environments**. This ambiguity is sometimes deliberately maintained by advertisers, for example when they use partnerships with popular bloggers.

* **Risks related to child development**

The pervasive presence of profiling and targeted advertising on the Internet poses a threat **to child development**. Economic incentives to keep users' attention for as long as possible lead publishers to lock them into more homogenous and personalised content, **"*filter bubbles*"[[9]](#footnote-9), which** can limit the development of children's critical thinking skills. Awareness of being monitored online can also lead children to modify their behaviour to minimise risks and may induce a **risk of social discrimination in the future**.

These issues are increasingly being taken into account by actors in the digital environment. In the private sector, **new business models** are **emerging** for **services for children that are more respectful of their personal data.** However, the impact of the development of these services is to be put into perspective: despite the introduction of YouTube Kids, 80% of children in the United Kingdom continue to use the general version of YouTube[[10]](#footnote-10).

1. **The place of minors in European data protection law**

These findings explain the special attention paid to children in the GDPR.

* **Recognizing the need for special protection**

While children should be able to enjoy all their rights, including the rights to data protection and privacy, they are **legally considered vulnerable,** although the degree of vulnerability of each minor depends on his or her age and level of maturity[[11]](#footnote-11).

This vulnerability justifies the establishment of **specific legal protection** for minors. It follows from Article 57 that **national protection authorities** are expected in their task of raising awareness among the general public, to pay ‘*specific attention*” to "*Activities addressed specifically to children* ".

Furthermore, the GDPR invites, **in the risk-based approach** that should guide any operator, to take into account the vulnerability of minors when assessing the proportionality of its data processing and determining the appropriate security measures. This has led the EDPB (European Data Protection Board) to include the processing of minors' data among the criteria to be taken into account in order to identify processing operations likely to be subject to a data protection impact assessment (DPIA).

Member States, supervisory authorities, the EDPB and the Commission are also invited to encourage the adoption of codes of conduct to harmonise the application of the provisions relating to minors (Article 40).

* **A range of specific protective devices**

These are underpinned by a **logic of empowerment of the minor**.

* ***Information tailored to minors on the nature and purpose of the processing of his/her data***

Article 12 of the GDPR states that all information and communication concerning the processing of children's personal data should be written in *"concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child*”

* ***Special vigilance regarding child profiling***

Recital 71 of the GDPR states that **exclusively automated decisions, including profiling, which produce legal effects or affect the data subject significantly in a similar way should not apply to children**.

The EDPB explains in his guidelines on automated individual decision making and profiling[[12]](#footnote-12) *"that this is not an absolute prohibition of such processing against children",* while recognising that "as *children are a more vulnerable group in society, organisations should, in general, refrain from profiling them for marketing purposes".*

* ***A reinforced right to be forgotten***

Whereas in European legislation this right appliesin the same way to all persons, recital 65 of the GDPR emphasises that **the right to be forgotten and the right of rectification are considered essential where consent to the** processing of information was **obtained during the** person's **minority,** "at a *time when he or she was not fully aware of the risks inherent in the processing*".

* ***The use of certain specified legal bases***

The GDPR more specifically provides certain legal bases for the processing of minors' personal data.

* **Consent**

Article 8 of the GDPR introduces a **capacity to consent to the processing of their data, when it is based on consent and is related to the provision of information society services, for children** between the ages of 13 and 16 years, the determination of the age threshold being left to the competence of States.

**Below the age of consent, the** processing of data concerning minors is lawful only insofar as **consent is given or authorised by the holder of parental authority on behalf of the child.** Article 8 of the GDPR states that the controller must endeavour to verify that such consent is indeed given by the parents, "having regard to the *technological means available*". Recital 38 of the GDPR allows for certain exceptions, for example in the context of preventive services offered directly to a child.

* **Legitimate interest**

Article 6 **introduces legitimate interest** pursued by the data controller or by a third party among the legal bases that authorise the processing of personal data. It is however specified that the **interests or fundamental rights and freedoms of the data subject prevail** over this legitimate interest, *"in* ***particular where the data subject is a child****. ».*

* **Protections specified in French Law**
* ***An adaptation of the modalities of consent for minors***

Article 45 of the Law of 6 January 1978 sets the ability to consent to data processing in France **at 15 years. Below the age of 15**, it introduces a mechanism of **double consent**: the processing of personal data *"is only lawful if the consent is given jointly by the minor concerned and by the holder(s) of parental authority".*

* ***Increased control of the minor over his or her health data***

Article 58 of the 1978 Law allows a minor under 15 years to oppose his parents' access to data concerning him that has been collected for **medical research** purposes. He may also object to his parents being informed of a preventive action, screening or diagnosis. The minor is then the only one to receive the information and, therefore, to be able to exercise his or her data rights.

* ***An enhanced right to be forgotten***

Article 51-II of the 1978 Law states *that "in particular, at the request of the person concerned, the* ***data*** *controller is required to* ***delete as soon as possible*** *personal* ***data that has been*** *collected in the context of the information society services offer* ***when the person concerned was a minor at the time of collection****.* «This right is guaranteed by the right to refer the matter to the CNIL in case there has been a lack of response from the data controller.

1. **The Legislation of Minors in relation to digital practices**
2. **At the international level: converging evolutions**

The **issue of the protection of minors' privacy online is at the heart of public debate in** many countries as well as at the level of international organisations. These developments, while not necessarily concerted or focused on the same issues, reveal **broad converging trends**:

* The guiding principle of the regulation must be based on the best **interests of the child,** which calls for reliance on the International Convention on the Rights of the Child (CRC), which was the first to recognise this standard.
* Regulation must **take into account the evolving capacities of children,** to make room for their gradual empowerment.
* The various texts, draft texts and positions expressed appear to be favourable to **the direct exercise of children's rights** inorder to ensure their effectiveness.

The **International Convention on the Rights of the Child has had a major impact on most national laws**. Its leading principle, the promotion of **the** **best interests of the child,** isnow the guiding principle of many national systems for the protection of minors. The direct effect of its provisions has gradually been accepted in France by the Council of State and the Court of Cassation. The **right of the child to respect for his or her privacy** was recognised in 1999 by the Court of Cassation and in 2004 by the Council of State. The protection of the best interests of the child was also enshrined in March 2019 as a constitutional requirement (Cons. Const., No. 2018-768 QPC).

**Work on children's rights in the digital environment has been undertaken** not only within the United Nations, but also in **various European and international initiatives that aim to shed new light** and give a more prominent place to the issue of children's rights**:**

* The European Commission,

A public consultation is currently underway until 8 December 2020 to develop a **new strategy on the rights of the child**. The issue of **children's rights in relation to the digital and information society has been identified as a priority**, in particular to include the risks associated with the use of new technologies and artificial intelligence. A communication is planned for thefirst quarter of 2021.

* The EDPB: The European Data Protection Board

The development of guidelines on the **protection of children's data** is part of its work programme. **Two other draft guidelines,** due to be adopted in the autumn, will *a priori* includeprovisions relating to minors: those **on the exercise of rights** and **on targeting users of social networks**.

* The Council of Europe

The Consultative Committee of Convention 108 of the Council of Europe has just prepared draft “Guidelines on Children’s Data Protection in an Education setting” **scheduled for adoption at the end of 2020**. The draft text states that the **interests of the child** should be at the heart of all actions relating to children in the digital environment, which requires taking into account the development of the child's capacities from birth to the age of majority. **The child's views should be recognised as increasingly important in accordance with his or her age and maturity**.

* The OECD

The revision of the 2012 Recommendation on the Protection of Children Online was initiated in 2018. It should lead to the **adoption at the end of 2020 of a new text**, which will strengthen the rights of the child online on the basis of the principles of the CRC.

Other work has been carried out by data protection authorities in other countries, such as the Age Code in the UK by the UK Commissioner, (ICO), the Irish authority, (DPC), which opted for a public consultation with a specific component devoted to the views of children and youth, and in the United States where the FTC (Federal Trade Commission) launched a public consultation in 2019 on the COPPA rule for the protection of minors online with a view to revising the US COPPA Act of 1998.

1. **At the national level: state of the law and prospects for evolution**

* **The rule of law: a complex articulation between parental authority and the rights of the child**

As a power exercised in the interests of the child, **parental authority must *a priori* beable to apply to all areas of the minor's life, including his or her privacy. However, the level of control over his or her privacy, in order to be legitimate, must be limited and proportionate to what is necessary to safeguard the best interests of the child**.

**Three legal techniques offer gradual autonomy to the minor: assistance, the pre-majority age threshold and the so-called “capacity island”**. They are **combined within article 8 of the GDPR**.

* The **assistance scheme is based on the** idea of joint consent of the minor and his/her parents. The use of this regime is widespread in a series of situations that have the common feature of affecting the person of the child (e.g., consent of a child over the age of thirteen is required to change his or her name).
* Another way of acting is based on **pre-majority thresholds** (e.g. in sexual matters). The goal may then be to **exclude parents from any decision-making power on a matter that affects their child's intimacy**.
* A final technique for empowering the youth is to offer  **islands of capacity for acts considered as not very dangerous, which** enables the juvenile to learn to exercise his or her autonomy.

The recognition of a minor's right to respect for his or her privacy raises fundamental questions: to **what extent is it consistent with the interests of the child, who, depending on his or her age and degree of maturity, has a sphere of intimacy that is enforceable against his or her parents?**

In the medical area, the legislator has enshrined a right to secrecy for minors by allowing them to oppose the transmission of certain information to holders of parental authority. **Case law has extended this right to the secrecy of minors** outside the situations mentioned by the law. These decisions open up a vast field of questioning applied to the digital environment. Indeed, adolescents find in the exposure of their intimacy on the Internet a ground for exploration and self-construction, from which one may wonder to what extent it should be possible to protect it from the eyes of adults.

* **CNIL and the protection of minors' data**

The CNIL has always paid particular attention to the protection of minors' data.

With regard to the recognition of the rights of minors, the decisions and opinions the **CNIL has issued on this subject, as well as its public communication illustrate its willingness to be pragmatic, to preserve the necessary empowerment of children, and to guarantee the protection of their privacy and intimacy**.

Thus, with regard to the applicable systems for selecting students for examinations, the CNIL opinion recognised that it was indeed the students, even underage, who are granted the right of access to information relating to the operation of the algorithm, and not their legal representatives, who were not mentioned at any time.

What is also very significant is the way in which the institution perceives young people. Indeed, the discourse and terms used by the CNIL in its relations with this young public and with the managers of sites aimed at young people is worth analysing so as to testify how its positioning on the subject reveals such important markers, e.g. the style used which reads as follows: "*Protect your freedom and your citizenship, exercise ... your rights",* as illustrated by a tab on the home page of the former CNIL’s Junior site[[13]](#footnote-13), it allowed minors to access a definition of the privacy rights and freedoms they are holding.

Moreover, another example produced by the CNIL’s complaints department, which although has rarely had to handle requests made directly by minors: in fact it duly proceeded with handling any request dealing with complaints as a matter of priority, and without referring to their legal representatives[[14]](#footnote-14). Strictly speaking, this is not a question of exercising rights, but the attitude of the CNIL shows an obvious openness to interacting directly with minors with regard to the protection of their privacy.

1. **Problems identified**
2. **Age verification and parental consent: a complex issue**

**The GDPR does not expressly mention any practical means of verifying parental consent and/or the age of the user in cases where these operations are required.** Article 8 states that the controller must then make "reasonable efforts", "taking into account the technological means available". Article 11 specifies that where the purpose of the data processing does not require the identification of the data subject, the controller is not obliged to collect additional information for the sole purpose of complying with the GDPR.

**Any age verification system needs to be effective and thus hard to circumvent, but also respectful of personal data protection and privacy, including sensitive data**. Children’s personal data could be combined with their online behaviour to form thorough profiles, which can in turn, have considerable impacts on them.

This is why it is necessary to consider the concrete implementation of such technologies:

\* In accordance with the principle of **proportionality**, could we have the mechanism to be used to verify the age considered with regards to **the intended purposes, the public targeted, the data processed, the technologies available and the level of risk associated with the processing?**

\* Shouldn’t such age verification system comply with the principles of **minimising the collection of personal data** and **limiting its storage period?**

\* Shouldn’t personal data collected as part of an age verification scheme and that transmitted to sites or applications **be used for any other purpose**, including commercial uses such as, profiling and behavioural advertising?

\* What about appropriately promoting "***standards*"** and a **certification mechanism** for verification systems to encourage the emergence of pooled solutions?

\* Whether would an age verification system based on the **intervention of a trusted third party providing initial verification of the identity of** individuals provide substantial advantages, by limiting the data available to each intervener?

\* However, few solutions appear operational in the short term, with the exception of parental control tools, which raise specific issues.

**B. Parental control: a balance to be defined**

Parental control arrangements however raise questions about the minor's privacy and data protection.

\* The installation of such devices may involve the collection of additional personal data concerning the minor. However, they do **not always imply the introduction of additional safeguards for the protection of personal data**.

\* The implementation of **supervision that is disproportionate to the age of the child and the risks to** which he or she is exposed may have counterproductive effects, **by altering the relationship of trust between the child and his or her parents**. Studies suggest that excessive monitoring of children on the Internet may limit their initiation to risk management, **delay their acquisition of digital skills** and lead them to make decisions based on the risk of punishment rather than on values.

\* UNICEF believes that too much parental interference may also **limit children's freedom of expression, access to information and critical thinking and affect how children will value their privacy in the future,** by making them accustomed to intrusive surveillance.

\* The tension between the benefits of parental control and children's right to privacy should be approached in the light of the 'evolving capacities of the child'.

\* Finally, the implementation of parental control **requires a dialogue between children and parents**.

1. **The possibility for minors to exercise their Privacy rights in the field of article 8?**

The GDPR does not address **how, on the basis of which evidence, a parent or legal representative can exercise the rights of the child,** nor **in which situations can the child directly exercise the rights applicable to his or her own data**.

**Recognising that minors have a certain capacity to exercise privacy rights on their own would** however seem appropriate for several reasons:

1° **The effectiveness of the minor's right to informational self-determination implies that the realisation of the child's digital rights cannot depend on his or her legal representatives**.

Indeed, the control by each person of his or her identity, particularly its digital identity, is becoming an essential component of privacy from a legal approach. Article 16 of the CRC recognises **the right of minors with respect for their privacy**. Giving substance to this right implies giving young people a certain amount of power over their privacy, to be articulated with respect for parental authority according to their age and degree of maturity.

In practice, the majority of **young people do not turn to their parents when faced with an online problem,** preferring for example, to ask for the removal of a publication that is problematic for them.

2° **Article 12 of the GDPR** requires that **children be informed of their rights in** a manner appropriate to their age. Itcan be argued that there is an **interdependence between information and the exercise of rights**. Should not the logic of these texts be given full effect by allowing young people to exercise the rights of which they would, through this information, be fully aware and knowledgeable?

**\* This recognition is in practice already widely accepted,** since the most **widely** used platforms allow minors to exercise their rights directly.

1. **Providing for additional safeguards in the use of data from minors?**

The protection of minors' data could be promoted by the implementation of additional guarantees by and on the sites, services and applications likely to be used by minors.

They could be encouraged by the development of guidelines on the protection of children's data, the adoption of good practices or the drafting of codes of conduct*:*

To illustrate, an *Age Appropriate* *Design Code* which has been developed and published by the Information Commissioner’s Office (ICO), UK on the design of online services that may be used by minors, provides for example, for the following:

* **Setting up a default reinforced confidentiality setting:**

(this setting could include protections such as the deactivation by default of all additional services that are not part of the "basic" service and which constitute processing operations, the non-transmission of the minor's data to a third party).

* **The default disabling of the underage profiling systems.**

1. **Integrating the design approach to better protect minors' data?**

The **need for information adapted to minors** is a requirement of the GDPR, a component of the specific protection they should benefit from. The information must be written in clear, simple and concise terms so that it is within the reach of the young people for whom it is intended.

However, **recent** studies and **initiatives suggest that in** order for **minors to be able to** effectively use this **information, further thought needs to be given to the form that this information should take and to the way in which the interfaces on which minors navigate are presented**. This leads us to affirm the need to integrate a design approach into the reflection on information and more generally on the rights of minors, and to look for concrete ways of deploying it.

It is a question of better understanding the way certain techniques are used today with regard to minors to encourage them to stay online (nudges, reward loops)**.** The question of appropriate design that respects the rights of minors is more than ever a field of analysis and debate that is expanding rapidly.

Observing the importance of integrating a *design* approach into the reflection on the rights of minors is in line with **work already carried out by the CNIL's digital innovation laboratory** (LINC)[[15]](#footnote-15) and **initiatives taken internationally** by various public or private stakeholders.

1. [Resolution A Digital Education for All (2013)](http://globalprivacyassembly.org/wp-content/uploads/2015/02/Digital-education-resolution.pdf)

   [Resolution for the Adoption of an International Standard for Personal Data Protection Education (2016)](http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-2016-on-Privacy-education.pdf)

   [Resolution on e-learning platforms (2018)](http://globalprivacyassembly.org/wp-content/uploads/2018/11/Résolution-2018-Plateformes-dapprentissage-en-ligne_VD-finale-23.10.2018.pdf) [↑](#footnote-ref-1)
2. Pwc (2019), Kids Digital Media Report, commissioned by Super [↑](#footnote-ref-2)
3. ABC News (2018), How your child's online profile is being captured and shared [↑](#footnote-ref-3)
4. A report by Oxford University researchers on mobile tracking estimates that applications for children transfer their personal data to about seven third parties, compared to five for the average application. [↑](#footnote-ref-4)
5. Stoilova, M., Livingstone, S. and Nandagiri, R. (2019) Children's data and privacy online: Growing up in a digital age. Research findings. London: London School of Economics and Political Science. [↑](#footnote-ref-5)
6. Johnson, Matthew, Valerie Steeves, Leslie Regan Shade and Grace Foran. Share or Don't Share: How Adolescents Make Privacy Decisions About Photos on Social Networks. Ottawa: HabiloMedia. [↑](#footnote-ref-6)
7. Kidron, B., Evans, A., Afia, J., Adler, J. R., Bowden-Jones, H., Hackett, L. & Scot, Y. (2018). Disrupted childhood: the cost of persuasive design. [↑](#footnote-ref-7)
8. Johnson, Matthew, Valerie Steeves, Leslie Regan Shade and Grace Foran. Share or Don't Share: How Adolescents Make Privacy Decisions About Photos on Social Networks. Ottawa: HabiloMedia. [↑](#footnote-ref-8)
9. Pariser, E. (2011). The filter bubble: What the Internet is hiding from you. London: Viking/Penguin Press. [↑](#footnote-ref-9)
10. Pwc (2019[) Kids Digital Media Report](https://www.superawesome.com/pwc-kids-digital-media-report-2019/), commissioned by Super Awesome [↑](#footnote-ref-10)
11. The European legislator thus considers that "children may be less aware of the risks, consequences and safeguards involved and of their rights related to data processing" (recital 38 of the GDPMR), while recognising a certain autonomy in their digital activities. [↑](#footnote-ref-11)
12. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 [↑](#footnote-ref-12)
13. Always accessible under [this link](http://www.ac-grenoble.fr/juniors/droits/droits.htm) [↑](#footnote-ref-13)
14. Complaints concerning minors are identified by a specific icon, and dealt with without delay. [↑](#footnote-ref-14)
15. <https://linc.cnil.fr/fr/ip-report-shaping-choices-digital-world> [↑](#footnote-ref-15)