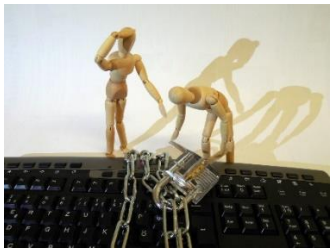
50th EPRA meeting

Athens, 23-25 October 2019

Plenary Session 1 – Protecting minors in the online world: What are the common challenges between NRAs and DPAs?

Introductory document[1]

Géraldine Denis, Emmanuelle Machet, EPRA Secretariat


Contents

[1] **Disclaimer: this document has been produced for an internal meeting by EPRA, an informal network of 53 regulatory authorities in the field of audiovisual media services. It is not a fully comprehensive overview of the issues, nor does it represent the views or the official position of EPRA or of any member within the EPRA network.**

1. Introduction

Protecting minors in the online world is a key regulatory objective with considerable practical challenges. In 2019, EPRA members therefore made the protection of minors in the online world a major theme of the network's yearly Work Programme, with two sessions scheduled focusing respectively on research and evidence of harm (in the spring) and on the interplay between with data protection and media regulation (in the autumn). This paper aims to highlight some of the themes of that latter topic, and the areas of intersection between data protection and media regulation, ahead of our discussion in Athens.

The European Data Protection Supervisor has characterised "Finding a balance between security and privacy" as the one of the recent strategic objectives of his field; meanwhile striking a balance between the protection of minors and freedom of expression is the core mission of audiovisual media regulators.

Over the last 25 years, technology has transformed our lives and the lives of children in positive ways nobody could have imagined, generating a plethora of new kinds of content, facilitating world-wide interactions and opening unprecedented avenues for accessing and sharing content.

By the same token, the protection of minors poses a serious concern across all types of content in Europe, and even more since the digitisation of the media and the spread of the Internet. Recent research has, to a large extent, confirmed that the concerns of the public were well founded even though they need to be balanced with the benefits and opportunities that the use of the Internet bring to children. Preliminary findings of the EU Kids Online network show that, since 2014, challenges and exposure to experiences that bothered children have increased significantly with cyber bullying on the rise, sharp increases in reported potentially harmful UGC content, a higher proportion of children reporting having seen sexual images and received sexual messages, and more children claiming to have been in contact with someone they had not met before and more children report meeting someone following an online contact[2]. In parallel, recent findings from the less explored field of harms specifically related to children's data revealed that children struggle to grasp the commercial interest behind a content in the online context and they usually assume that "the others" will not collect or use their private data. Understanding grows with experience but there's no "magic" age of capacity[3].

In our spring meeting in Sarajevo, EPRA looked at recent and on-going research and evidence with a view to assessing the levels of online harm and to understanding how regulators are likely to go about developing remedies that are proportional to the level of harm. The session emphasised that a better understanding of children's online experience helps identify and assess situations involving content, contact or conduct-related risks, for the sake of better regulation. It is crucial to involve children in research and to fill current knowledge gaps, especially regarding very young children. Key conclusions from the session included that:

[2] See the presentation of Brian O'Neill at the EPRA meeting in Sarajevo in May 2019, accessible here: https://www.epra.org/attachments/sarajevo-plenary-1-protecting-minors-in-the-online-world-presentation-by-brian-o-neill-technological-university-dublin

[3] Children's data and privacy online Growing up in a digital age, LSE and ICO research, S. Livingstone, M. Stoilova and R. Nandagiri: http://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-presentation-for-web.pdf

- in order to be effective, the response needs to focus on the well-being and the rights of children, which requires not only protecting minors against harmful content but also providing appropriate positive content and listening to their needs.
- evidence-based research on online harms is vital for regulators to justify actions undertaken and get public approval. Audiovisual media service regulators also have a responsibility to use evidence in an appropriate way and balance it with freedom of expression.
- sharing knowledge, methodologies and findings is essential, as is working in partnership at the European level.

The next logical step after researching and understanding online harms to children is to focus on mechanisms and policies to protect and empower minors, and we have chosen to look at this through the lens of data protection and intersection between exposure to harmful content and harms stemming from misuse of children's data. This decision is underpinned by recent developments in European policy. In the revised Audiovisual Media Services Directive, AVMS providers and video-sharing platforms (VSPs) are required to implement concrete – direct and indirect – measures to protect minors from accessing harmful content such as age verification tools. In that context, important new provisions, such as Art. 6a par. 2 and Art. 28b par. 3 specifically introduce the concept of protecting children's data and their use for commercial purposes while protecting them from harmful content. Therefore, for the second session of our yearly plenary theme on the protection of minors against harm in the online environment, we will focus on issues relating to children personal data and identify the common challenges for audiovisual media service regulators and data protection authorities before exploring potential paths for a meaningful cooperation between NRAs and DPAs.

By way of background to this session, it is worth reflecting on why EPRA felt that it was particularly timely to devote a plenary session to the protection of minors in the online environment and common challenges for NRAs and DPA. EPRA Work Programmes in recent years have heavily focused on the disruption of the media ecosystem and the need for audiovisual media regulators to adapt to the changed environment. This involves, among other things, reinforced dialogue with stakeholders and the need for stronger dialogue and cooperation with other regulatory and self-regulatory authorities, notably Data Protection Authorities**.**

The ad hoc Working group on 23 May 2018 in Luxembourg[4], which convened on the day of the coming into force of the EU General Data Protection Regulation, tentatively explored areas where concerns about privacy and data protection might meet and encouraged interaction between broadcasting regulators and privacy/data protection regulatory bodies through the organisation of a session in the future. In Barcelona in May 2016, a Working group on "Data Protection & Big Data - What impact on media regulation?" [5] raised the awareness of EPRA members as to why media regulators should care about the use of massive data and consider their possible impact on freedom of expression, pluralism of information and editorial independence and responsibility. In December 2015, the European Audiovisual Observatory and EPRA co-organised a workshop on the grey areas between data protection and media regulation[6]. In bringing together experts in both fields in a workshop, the idea

[4] https://www.epra.org/attachments/luxembourg-wg-iii-new-challenges-for-privacy-introduction
[5] https://www.epra.org/attachments/barcelona-wg3-data-protection-big-data-introductory-document
[6] https://www.epra.org/news_items/the-grey-areas-between-media-regulation-and-data-protection-outcome-of-second-joint-obs-epra-workshop

was to develop a discussion on practical case studies focusing on the underlying regulatory framework in the respective areas with the view of gathering findings as to possible gaps or overlaps which might undermine the legitimate expectations of adequate protection of European citizens. More recently, several EPRA sessions (on algorithms, news in the Digital Age, commercial communications 2.0, Elections and Social Media and on Artificial Intelligence) also addressed issues in which the use of personal data feature prominently.

2. Protecting minors in the online world: the inevitable involvement of personal data

2.1. The new ecosystem of content consumption: the limit of linear rules

The days when the TV set was the only means to access audiovisual content are long past. Audiovisual content can now be produced by anyone, can be accessed by anyone, anywhere in the whole world, without prior editorial control, at any time and through a large variety of online services. Audiovisual content is often delivered via recommendation systems based on the user's profile. Any online navigation allows providers to collect data, providing them with details on the preferences, opinion and sensitivities of the user. The nature of audiovisual commercial communications has also radically changed, with data collected from the individual user at the core of the business model. Search engines, content recommendations and targeted content: everything tends to be based on the user's profile resulting from his/her browsing history, his/her preference settings or the purchases he/she made. The ecosystem shifted from a mass marketing to an "one-to-one" marketing[7].

As a result, traditional protection tools that have proven effective in the audiovisual linear world, such as the time of broadcast (watershed), editorial control or the ban on advertising during specific programmes, can rapidly reach technical limits: in the online environment, how can we adapt the measures to effectively protect children from harmful content?

This is not the first time that emerging new media has presented challenges to practical regulation: with the development and take-up of on-demand audiovisual media services, PIN codes, pay walls or other age verification systems became the most relevant instruments for the protection of minors. However, such non-linear services remained under the editorial responsibility of a media service provider. This is not the case any longer for content on video-sharing platforms.

Compounding this problem, many VSPs which are popular with children, such as YouTube, have not designed their content standards and the personal data terms to be, in principle, suitable to children. Effectively protecting minors against harm on these services would have to be proportionate and take due regard of their primary business model of data collection for advertising purposes. The obvious solution would be to require the service provider to identify a user as a child, and then adapt its service as a result.

And this would necessarily involve children's data processing. Protecting minors against harmful content in the online world requires diving into the black box of personal data.

[7] See annex 3

2.2. Online content consumption: collecting data

Online navigation creates data that can be collected and processed. In order to understand the impact and the reality of data processing, a short inventory of the situation is required: which kind of data are collected by the providers?

Personal data is any information which allows to identify, directly or indirectly, a person. It could be a name, an identification number, a location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[8]. For instance: a picture, an IP address, a pseudonym, an invoice, a telephone number, a comment, the "like" or any other actions of a user through its account…

We can distinguish between three kinds of data collected through online content consumption, as suggested by Dr Sonia Livingstone[9]:

- The "*data given*": the data that people give directly, intentionally or not. It includes the information given on an account profile or also the pictures and videos posted on social network (about themselves or someone else). Children's data can then be collected directly or through their friends or parents' activities (photos or videos of their children…).
- The "*data traces*": the main example is the "cookie". Mostly unknowingly, any visit of a website leaves some traces such as geo-localisation, browser fingerprinting, IP address…
- The "*Inferred data*": the analysis and combination of all the data collected, namely, the profiling (which leads to recommended contents or websites/apps and microtargeted advertisements).

As Veronica Barassi highlighted[10], data collection itself is not the problem. The danger remains mainly in the data inference (as seen above, the process of collecting and cross-referring data to infer a "profile"). Indeed, gathering and analysing all the data collected leads to a perfect knowledge of the user, potentially invading privacy and creating a perfect target for advertisement, propaganda or recommended content, for instance.

3. Protecting minors in the online world: the legal framework

3.1. The legal obligations as enshrined in the AVMS Directive

In the revised AVMS Directive of November 2018, the protection of minors appears as an essential obligation for any audiovisual media services (i.e. traditional broadcasters and providers of video on demand services must ensure that children do not normally see or hear harmful content) and for the video-sharing platforms (VSPs must take appropriate measures to protect children against harmful

[8] Art. 4 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance): https://eur-lex.europa.eu/eli/reg/2016/679/oj

[9] 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: http://www.lse.ac.uk/media-and-communications/research/research-projects/childprivacyonline

[10] https://blogs.lse.ac.uk/parenting4digitalfuture/2019/07/17/social-media-data/

content) – see annex 1. The revised Directive on the one hand, aligns, the standards of protection for TV broadcasting and on-demand services and, on the other hand, creates a new obligation to VSPs:

→ *Harmful content*. According to the new provisions, appropriate measures shall be taken to ensure that minors will not normally hear or see audiovisual media services (linear TV or VoD) that may impair the physical, mental or moral development of minors. Moreover, even though it is acknowledged that VSPs cannot be held responsible as an editor for the content published by users on their websites, VSPs shall also take appropriate measures 'to protect minors from programmes, user-generated videos and audiovisual commercial communications which may impair their physical, mental or moral development in accordance with Article 6a(1)'.

→ *Harmful commercial communications*. The danger of commercial communications regarding children (Article 9. 1) and Article 28b) is also emphasised. All audiovisual media providers, including VSPs, are required to prevent on their services any commercial communications which may cause a physical, mental or moral detriment to minors.

→ *The use of data for marketing purpose*. The Directive prohibits the processing of children data collected through the protective "appropriate measures" undertaken to protect minors, for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising. The Directive indirectly acknowledges the danger of such commercial practices for minors.

In these circumstances, regulation is comfortable that in an editorially controlled world the balance between protection and freedoms (of expression and privacy) can be maintained – but that the risk becomes greater when you are effectively mechanising/automating the means of protection.

3.2. The legal protection of data

All the data collected or processed in a member State of the European Union shall comply with the principles set by the GDPR[11], which entered in force in May 2018. Its very broad scope of application gives these rules a quasi-world-wide influence. A lot has been written on this new regulation, which has raised a lot of reactions, revealing the crucial relevance and concern of society with regard to personal data issues.

As a result, any data collection and/or processing shall comply with the following principles:

Lawfulness, fairness and transparency	Processing must respond to one of the legal grounds laid out in the GDPR (*Consent of the data subject / Performance of a contract/ Legal obligation / vital interest of the person / public interest*) and to the legitimate need and purpose described to the data subject.
Purpose limitation	Data can only be collected for specified, explicit and legitimate purposes.
Data minimization	Only data strictly necessary for the explicit legitimate purpose can be collected.

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance): https://eur-lex.europa.eu/eli/reg/2016/679/oj

Accuracy	Data must be kept accurate and updated.
Storage limitation	Data shall only be stored for the necessary length of time.
Integrity and confidentiality (security) of the data	Personal and technical measures must be taken by the data controller and processor for this purpose.
Accountability	The data controller must be in capacity to prove the compliance with the previous principles.

→ And what about minors?

First of all, the GDPR does not refer to "minors" but to "children". However, the DPAs agree that "children" must refer to the definition provided by the article 1 of the UN Convention on the rights of the children[12], meaning all children under 18.

The GDPR acknowledges that children need a specific protection and states that:

- **Consent**: if you provide an information society service and if you rely on consent to process the data, the consent for children under the required age needs to be provided by the holder of parental responsibility (Article 8). Each State may set down the required age between 13 and 16.
- **Use of data for marketing purpose**: specific protection is required when children's data are used for marketing purpose or creating personality or user profile (Recital 38). In line with this, children should not be subject to decisions based solely on automated processing (including profiling[13]) if these have a legal or similarly significant effect on them (Recital 71).
- **Transparency**: information addressed to a child regarding its personal data should be in a concise, transparent, intelligible and easily accessible form, using clear and plain language, adapted to the age of the child (Art. 12, 40 and Recital 58).
- **The promotion of digital literacy** (Art. 57).

In general, a child-friendly data protection by default and by design is encouraged: the data protection requirements must be integrated in the processing activities and business practices, from the design stage, and high personal data protection standards should be set up by default.

While the GDPR acknowledges the vulnerability of children and creates specific provisions in this regard, it does not provide a very detailed and established framework of rules or technical restrictions.

However, by superimposing the AVMS Directive and the GDPR, it appears that audiovisual media regulatory authorities and data protection authorities do share some common objectives with regard to the protection of minors online and that their respective missions are, in some way, interconnected.

4. Protecting minors in the online world: common challenges of NRAs and DPAs

[12] The 1989 United Nations Convention on the Rights of the Children: https://www.unicef.org/child-rights-convention/convention-text

[13] The use of data to evaluate certain aspects related to the individual. The purpose is to predict the individual's behaviour and take decisions regarding it.

There seems to be scant research on the common challenges faced by NRAs and DPAs. In line with this remark, the results of the online survey[14] conducted among EPRA members reveal that the examples of structured cooperation between NRAs and DPAs are rare so far.

However, when reviewing audiovisual regulation issues in a digital world, the idea of a stronger collaboration with DPAs is worth considering.

We have identified below several common challenges that point at potential benefits of a cooperation between NRAs and DPA.

4.1. Restricting access without infringing children's and adults' rights

One of the current tools to restrict children's access to harmful content is to encourage the application of access control tools or age filters which would allow the providers, according to the age of the user, to filter the accessible contents and adapt the service or even, to deny access to the entire website.

Apart from the issue of identification of online harmful content, the use of such tools raises the following concerns:

4.1.1 The first challenge is to secure access control tools which are efficient and fully compliant with personal data regulation.

The age control tool system	Audiovisual Regulation challenges (*)	Data Protection requirements
The identification of the child	The identification tool should be accurate and efficient to secure a justified restricted access to the content. It should not prevent other users to access content.	The data processing must be accurate and must not infringe the child and the other user's rights to the protection of their personal data.
The data collected	The data must not be used in a commercial way.	DPA must control that the data are only used for the specific purpose of protection (and not in a commercial way). Data must be secured, confidential and compliant with the GDPR principles such as the principle of minimisation.
The length of conservation of the data	The tool should respect the evolution of the child as media is a crucial part of the child's development and should not prevent him to have access to content suitable for his actual age.	DPA must determine the legitimate length of conservation: the length must be strictly as long as necessary – principle of the GDPR.

(*) General principles inferred, directly or indirectly, from the AVMSD.

[14] Survey Protecting minors in the online world: focus on personal data issues: https://www.epra.org/surveys/protecting-minors-in-online-world-focus-on-personal-data-issues (only accessible to logged-in EPRA Members)

We are facing a paradox: children deserve specific protection with regard to their personal data processing but their identification as a child requires processing their personal data.

How is it possible to *effectively identify a child, while fully complying with the GDPR*?

What kind of data are *strictly necessary to be collected and how to ensure compliance with the principle of minimisation*?

How can we make sure *that it would not prevent access for other users of the same shared device*? What should be *the length of conservation of those data*?

Indeed, as the child grows up and evolves, his access to content must evolve as well and the system of access control tool must be designed in a way that does not jeopardize the child evolution and participation in the community.

As stated by Eva Lievens, "*policies that require age or identity verification of children require consideration for children's right to privacy and compliance with data protection principles, such as data minimisation (Article 5(1)(c) GDPR). In the same vein, policies that aim at protecting children's right to data protection should not undermine their rights to participation (such as their right to freedom of expression or their right to freedom of association*)"[15].

4.1.2 <u>The second challenge is to prevent excessive and unjustified blocking access tools.</u>

"*A company that is damaging the environment is not acceptable. Similarly, a company that harms children is not acceptable. But the question is: have we established precisely what harms exist online for children? Or do we need to establish first what rights need to be acknowledged and protected*?"[16]

Most of the VSP services used by children are not child-specific (such as YouTube). There is in this context a risk that the intersecting requirements of the AVMS Directive and GDPR relating to the data of children creates incentives for some VSPs to simply prevent children from accessing their services, therefore sidestepping difficult problems of identifying content likely to harm children and the risk of excessive blocking for adult users. These problems are explored below.

- The difficult identification of harmful content

In order to comply with the legal requirements of the AVMSD and of the Directive 2031/EC on information society services, online media service providers should first, identify what content is harmful to children if the programme is released under its editorial responsibility (VOD services for instance), or otherwise analyse any content flagged as harmful by a viewer (in case of user-generated content), and then, take appropriate measures to prevent access for children under a certain age. Moreover, they are required to protect children against any harmful commercial communications. This may be a difficult task and it would be easier to simply deny access to the entire service.

- The unwillingness to apply general high-privacy standards

[15] Lievens, E 2018, Research for CULT Committee – Solutions and policy dilemmas regarding minors' protection online, European Parliament, Policy Department for Structural and Cohesion Policies, Brussels

[16] G. Polizzi – Meeting report 24 June 2019 on behalf of the Children's Data and Privacy Online project: http://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Report-launch-event.pdf

Moreover, the GDPR encourages a child-friendly privacy by design and by default standards for children data's processing. It also tends to prohibit, regarding children, "any form of automated processing of personal data evaluating the personal aspects relating to a natural person" (and so, profiling). This would require that an online media service provider should first identify the age of the user, with a compliant data processing system, and then adapt its all website with appropriate standards (*information related to the data processing given to the user in a clear and accessible language suited to his age and limited commercial collection and use of the data*).

An ideal solution would be to apply the highest privacy and child-friendly by design and by default standards to every user and to switch off any profiling process. This solution, however, seems hardly realistic as it may seriously reduce the data collected and will oblige the industry to review its business model, based essentially on personal data processing.

Here again, it would definitively appear easier for a service provider to simply prevent children accessing the service with the use of an age control access tool.

- The danger of an excessive use of blocking access tools

An excessive use of blocking access tools could seriously restrict essential rights of children, such as freedom of expression and opinion. Children must have access to media, an essential part of their development, and they must be in capacity to be part of the society.

"*For now, there are no real options to "giving consent" when using online platforms, as the only alternative is to be excluded from the world*" S. Livingstone[17].

"*It would be problematic if children were to be faced with the decision either to lose access to a service they value or to lie about their age to retain access (and, thereby, find themselves treated as an adult rather than benefiting from the protections due to them as a child)"*[18].

An excessive use of access control tools can seriously infringe children's rights and both NRAs and DPAs could then be entitled to monitor such use by the media service provider in order to make sure that children's rights are respected.

4.2. Protecting children against the danger of profiling and the use of their data for marketing or other profiling purposes

Point 37 of the Appendix to the Council of Europe Recommendation on Guidelines to respect, protect and fulfil the rights of the child in the digital environment states that "*Profiling of children, which is any form of automated processing of personal data which consists of applying a "**profile**" to a child, particularly in order to take decisions concerning the child or to analyse or **predict his or her personal preferences, behaviour and attitudes**, should be prohibited by law. In exceptional circumstances,*

[17] G. Polizzi – Children's data and privacy online: challenges and solutions - Meeting report 24 June 2019 on behalf of the Children's Data and Privacy Online project: http://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Report-launch-event.pdf

[18] Children: a special case for privacy? SO. Livingstone – InterMEDIA July 2018 Vol 46 Issue 2 – www.iicom.org

States may lift this restriction when it is in the best interests of the child or if there is an overriding public interest, on the condition that appropriate safeguards are provided for by law"[19].

Recital 38 of the GDPR: "*Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the* ***purposes of marketing or creating personality or user profiles*** *and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child"*.

The AVMSD, for its part, requires the protection of minors against harmful content and harmful commercial communication.

Indeed, harm may not only come from the content itself (inappropriate products, HFSS products…), but also from the way it is brought to the child's attention. For instance, personal data collected through the online media website would allow advertisers to identify the child's preferences and to target him regularly with the same type of ads, amplifying the harmful impact on him. Some online media providers may also take advantage of the very "easy to influence" character of children for marketing purposes (with repeatedly inappropriate recommended content for instance) or even to lead them to harmful content such as hate speech. If it is possible to get the profile of a person (his interests, his opinions), influencing this person would become a "child's play". The use of children's personal data may thus enhance the negative influence of harmful content on them.

Therefore, in an online ecosystem which relies a lot on the processing of data (recommended content, targeted advertisements…- See annex 3 for an illustration of a targeted advertisement system), monitoring harmful content cannot be achieved without monitoring the media provider's processes around the publication of content.

According to Sonia Livingstone, "*in future, it may work better for data controllers to protect the rights (and limit the commercial exploitation) of all users than to try to identify children (and other vulnerable users) so as to treat them differently (not least because the very process of identifying children may undermine the principle of data minimisation which protects their privacy*)"[20].

How can we assess the harmful impact on children of such processes? How can we protect children against harmful communication if they are not identified as children?

Some important regulatory and legal developments are emerging:

→ In the US, YouTube (Google) has been fined $170 million in September 2019 for having collected personal data from children on its YouTube video streaming website for the purpose of targeted advertisement, as prohibited by the Children's Online Privacy Protection Act (COPPA). In response, "the digital video giant will treat data from any YouTube user who watches children's content as if it comes from a child, regardless of their actual age, and will stop serving personalized ads on the

[19] Recommendation CM/Rec(2018) of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment: https://www.coe.int/en/web/children/-/new-recommendation-adopted-on-children-s-rights-in-the-digital-environment

[20] Children: a special case for privacy? S. Livingstone – InterMEDIA July 2018 Vol 46 Issue 2 – www.iicom.org

content. YouTube will ask creators to self-identify children's content and use artificial intelligence to find videos that target kids"[21]. As already mentioned, the task of identifying content targeting children could prove quite arduous. In this instance, YouTube intends to transfer such responsibility to the user/creator of the content. As stated by the American Federal Trade Commission, "*this settlement now makes Defendants responsible for creating a system through which content creators must self-designate if they are child-directed. This obligation exceeds what any third party in the marketplace currently is required to do. It represents the first and only mandated requirement on a platform or third party to seek actual knowledge of whether content is child-directed"*[22].

→ The initiative from the ICO, the Data Protection Authority from the UK, goes in a stricter direction and recommends, in an age appropriate design code (cf. Annex 2):

- the application of high-privacy by design and by default standards, **for all websites likely to be accessed** by children (not just for services targeted children);
- therefore, to switch off, by default, any profiling and geo-localisation processing;
- and to prevent any data processing that may be detrimental to the well-being of a child.

What should be the criteria to identify the scope of application of such standards and how would the media providers react to such impact on their business system?

Those initiatives demonstrate that the issue of harmful micro-targeted content related to children is beginning to be a major subject for stakeholders and DPAs. No fully satisfactory solutions have been found so far and it could thus be in the interest of all to gather the stakeholders and the relevant authorities, in particular the NRAs and the DPAs, in order to discuss current challenges and share experiences with a view to assessing more precisely the actual harmful impact of such practices from the industry.

As noted in the meeting report of the LSE's Children's Data and Privacy Online project: "*Are children not already subject to offline advertising about junk food, for instance, which is in itself harmful? How is it different online? We need to assess who is causing what type of harms and how particular business models are leading to such harms. But the problems we face offline should not discourage us from regulating the digital environment*"[23].

4.3. Educating children for a safer digital consumption

Minors are an easy and vulnerable target for commercial communications, but also any other forms of harmful speech and information disorder. As highlighted in the previous paragraph, the use of children's personal data may enhance the negative influence of harmful content on them. It is therefore crucial to enable children to understand the mechanisms and to raise the awareness of

[21] Hollywood reporter 'Google Fined $170M for Violating Children's Privacy Law on YouTube', 9/4/2019 by Natalie Jarvey, Ashley Cullins: https://www.hollywoodreporter.com/news/google-pay-170m-fine-violating-kids-privacy-law-youtube-1236620

[22] https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations

[23] G. Polizzi – Meeting report 24 June 2019 on behalf of the Children's Data and Privacy Online project http://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Report-launch-event.pdf

parents and guardians about the possible dangerous use of the data. Indeed, data of children can also be given away by their parents, friends or any other person (through a video or any other mean of identification of the minor).

It is therefore vital to focus on ways to give children the necessary skills to understand the functioning of the online world, both for a thoughtful use of the online information and for a better communication and presence on the Internet. Children cannot be taught how to protect themselves against content without understanding how and why such content reaches them.

Studies show that children are worried about their privacy when they realise what happens to their data but most of them do not have a clear map of what is really going on when they are online[24]. As pointed out by the project 'Children's data and Privacy Online', they "notice that advertisements start appearing across platforms as soon as they show some commercial interest in something […]" but "while children understand how their data is recorded on some platforms, cross-device identification, metadata and profiling are hard to grasp[25]". The joint research of Ofcom and the ICO also underlines the concern of parents and children regarding the use of their personal data for commercial purpose or recommended content[26].

Providing tools for the vulnerable public, and especially children, to help them understand how media work and interact with them in an appropriate way is the aim of Media Literacy, which has become an important mission for many audiovisual media regulators in Europe. This is also the aim of the Digital literacy projects undertaken by the Data Protection Authorities. The initiative of the French CNIL with the launch of the website educnum.com[27] is particularly worth mentioning. Children must, for instance, get familiar with the mechanism of targeted advertisement in order to understand why those commercial communications are addressed to them.

Understanding children's use and attitude of online media is not an easy task. Against this backdrop, sharing knowledge and experience regarding children's online harms – in respect of the content they are exposed to and the way their data is used – would seem like a good idea in order to get a clearer picture of what are the real challenges and issues at stake and for the sake of a consistent approach to implementation.

5. Opportunities for cooperation

Whereas most of the research and projects related to the protection of minors online tend to treat in a separate way the question of media regulation on the one hand and the question of personal data regulation on the other, there have been several calls for cooperation to share experience and know-how.

[24] See above note 19

[25] 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: http://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf

[26] Ofcom (UK) report - February 2019 "Children and parents: media use and attitudes report 2018": https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/Children-and-Parents-Media-Use-and-Attitudes-2018.pdf

[27] CNIL website on Digital literacy: https://www.educnum.fr/

For instance, in the Guidelines to respect, protect and fulfil the rights of the child in the digital environment[28], the Council of Europe underlines, regarding the protection tools, the need to take into account "children's evolving capacities", children's right to privacy and right to information (point 54). The Guidelines also encourages a "*strategic and co-ordinated multistakeholder approach […] including national, regional and local law-enforcement and other authorities, educational and social-service agencies, independent human rights institutions, data-protection authorities, professionals working for and with children, civil society, including child and youth-led organisations, business enterprises, industry associations, researchers, families and children, in ways which are tailored to their roles and functions*" (point 111).

The GDPR, in its Article 57 §1-g, encourages DPAs to collaborate with, "*including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation*".

As pointed out by Prof. Eva Lievens during the ERGA workshop, all the fields are becoming increasingly interlinked and there are advantages of closer cooperation "between media regulators and data protection authorities when it comes to the mechanisms and tools used for processing information about children"[29].

The brief EPRA online survey[30] on this topic, which gathered 24 responses, showed that the majority of audiovisual media regulators do not cooperate with their counterparts in the field of data protection.

Nevertheless, the survey has revealed a number of best practice examples:

Regular meetings: The Norwegian Media Authority has regular meetings with the Data Protection Authority, both for advisors and at an executive level; the Dutch CvdM has a cooperation agreement with the Data Protection Authority and meet once a year - and ad hoc if necessary. In Switzerland, OFCOM contacts the Swiss Federal Data Protection and Information Commissioner if needed on a case-by-case basis; the cooperation is deemed efficient and fruitful. In the UK, Ofcom has monthly meetings with ICO (the DPA) and CMA (the competition and market authority) at senior level, supported by weekly working level meetings.

Joint Research: In France, the CSA and data protection authority CNIL have produced joint reports and studies – together with other sectoral regulators (on vocal assistants and smart speakers 2019; on new regulation and data regulation). In the UK, ICO and Ofcom have signed a Memorandum of Understanding to support collaborative research into consumers experience of online harms and data related issues and conduct a yearly joint study.

Media Literacy: In Norway, several actions regarding Media Literacy projects, were jointly organised with the DPA, such as seminars on age limits, privacy and children on social media. Both authorities

[28] Recommendation CM/Rec(2018) of the Committee of Ministers https://www.coe.int/en/web/children/-/new-recommendation-adopted-on-children-s-rights-in-the-digital-environment

[29] ERGA Academy 2018 Workshop: Protecting Children in Audiovisual Media Services -The effectiveness of age verification and media literacy (Activity Report): http://erga-online.eu/wp-content/uploads/2018/02/Protecting-Children-in-Audiovisual-Media-Services-Current-and-Future-Measures.pdf

[30] Survey Protecting minors in the online world: focus on personal data issues: https://www.epra.org/surveys/protecting-minors-in-online-world-focus-on-personal-data-issues/results

produce feature articles and and a joint leaflet for parents is also developed. In Portugal, the ERC has jointly organised a seminar with the Portuguese DPA. The DPAs are also participating in the media literacy networks/working groups facilitated by media regulators in France, Norway and North Macedonia. In France, a partnership agreement is being developed between the CSA and CNIL as well as other sector regulators to provide reference documents on the various subjects within the area of competence of each authority.

Regulatory convergence: 15 EPRA members (out of 53) are convergent authorities, with wider regulatory competences than just the audiovisual field. However, the Gibraltar Regulatory Authority (GRA) is the only body who is competent for audiovisual media and data protection. It seems that the French government toyed with the idea to create a single body responsible for audiovisual and data protection, but is likely to opt for a merger between the CSA and the Copyright body HADOPI instead in the new draft audiovisual law ("projet de loi relatif à la communication audiovisuelle et à la souveraineté culturelle à l'ère numérique") expected for November 2019.

The aim of this session is to debate and to reflect on the challenges faced by NRAs and the DPAs and to explore how a meaningful cooperation and a structured engagement could look in order to share the knowledge, the experience and the know-how regarding children's online experience.

6. Structure of the session

After an introduction by EPRA Board sponsor and Vice-chairperson Maria Donde, the session will commence with a keynote address by an academic and researcher expert in online child safety and personal data, Professor Eva Lievens.

Professor Eva Lievens is an assistant professor at the Law Faculty of Ghent University in Belgium since 2015. Her research focus on the legal challenges posed by new media and ICT phenomena, related to children's rights, cybercrime and alternative regulatory instruments. She is a member of the Flemish Regulator for Media, the Strategic Advisory Committee for Media, the Belgian Film Evaluation and the Advisory Committee for Telecommunications.

The keynote will then be followed by a panel discussion with representatives of DPAs, who will share their practical experience and views first through a short presentation of their respective key findings and then through interactive exchanges with the audience.

9:30-9:40 Introduction by Maria Donde

9:40-10:00 Keynote speech by Eva Lievens

After an introduction to the topic, Eva Lievens will provide an overview of the main principles of the GDPR and identify the common areas raised by the new link between the AVMS Directive and the GDPR. Eva will then elaborate on Children's Rights and present best practice recommendations, including the forthcoming recommendations from the Council of Europe on GDPR implementation. Eva will also provide an insight into the findings of her ongoing research with children and how they deal with online challenges.

10:00-10:20 Short Presentations by panellists

10:20-11:20 Interaction with keynote and panellists and with the audience

The regulatory panel will be composed of:

- **Elanor McCombe**, Group Manager in the policy team at the Information Commissioner's Office (ICO), the UK's DPA. She has been working specifically on the development of the ICO's Age Appropriate Design Code.

- **Pascale Raulin-Serrier**, Senior advisor and Coordinator of the International Digital Education Working Group of the CNIL (Commission Nationale de l'Informatique et des Libertés - the French DPA): she joined the CNIL in 2005 and is specialised in Digital Education. She promotes collaborative projects in digital education for all ages, and, on behalf of CNIL, leads an international working group in Digital Privacy Education, helping share teaching resources and projects among 50 DPAs.

7. Bibliography

1. Legislation:

Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive): https://eur-lex.europa.eu/eli/dir/2018/1808/oj

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): https://eur-lex.europa.eu/eli/reg/2016/679/oj

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance): https://eur-lex.europa.eu/eli/reg/2016/679/oj

Recommendation CM/Rec(2018) of the Committee of Ministers https://www.coe.int/en/web/children/-/new-recommendation-adopted-on-children-s-rights-in-the-digital-environment

2. Reports of regulators and networks

European Data Protection Supervisor, Annual Report for 2018, published in 2019: https://edps.europa.eu/sites/edp/files/publication/ar2018_executive_summary_en.pdf

ERGA Academy 2018 Workshop: Protecting Children in Audiovisual Media Services -The effectiveness of age verification and media literacy (Activity Report): http://erga-online.eu/wp-content/uploads/2018/02/Protecting-Children-in-Audiovisual-Media-Services-Current-and-Future-Measures.pdf

Ofcom (UK) report - February 2019 “Children and parents: media use and attitudes report 2018”: https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/Children-and-Parents-Media-Use-and-Attitudes-2018.pdf

EPRA background document (2019): Protection of minors in the online world: focus on evidence of harm":
https://www.epra.org/attachments/sarajevo-plenary-1-protection-of-minors-in-the-online-world-introductory-document

EPRA Comparative background document (2013): The Protection of Minors in a Connected Environment:
https://cdn.epra.org/attachments/files/2156/original/protectionofminors_final.pdf?1367573493

3. Research

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: http://www.lse.ac.uk/media-and-communications/research/research-projects/childprivacyonline

http://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf

Blog The London School of Economics and Political Science – Parenting for a digital future: https://blogs.lse.ac.uk/parenting4digitalfuture/2019/07/17/social-media-data/

G. Polizzi – Children’s data and privacy online: challenges and solutions - Meeting report 24 June 2019 on behalf of the Children’s Data and Privacy Online project: http://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Report-launch-event.pdf

Lievens, E 2018, Research for CULT Committee – Solutions and policy dilemmas regarding minors’ protection online, European Parliament, Policy Department for Structural and Cohesion Policies, Brussels:
http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA(2018)617455

Children: a special case for privacy? S. Livingstone – InterMEDIA July 2018 Vol 46 Issue 2 – www.iicom.org

Hollywood reporter ‘Google Fined $170M for Violating Children's Privacy Law on YouTube’, 9/4/2019 by Natalie Jarvey , Ashley Cullins: https://www.hollywoodreporter.com/news/google-pay-170m-fine-violating-kids-privacy-law-youtube-1236620

8. Annex

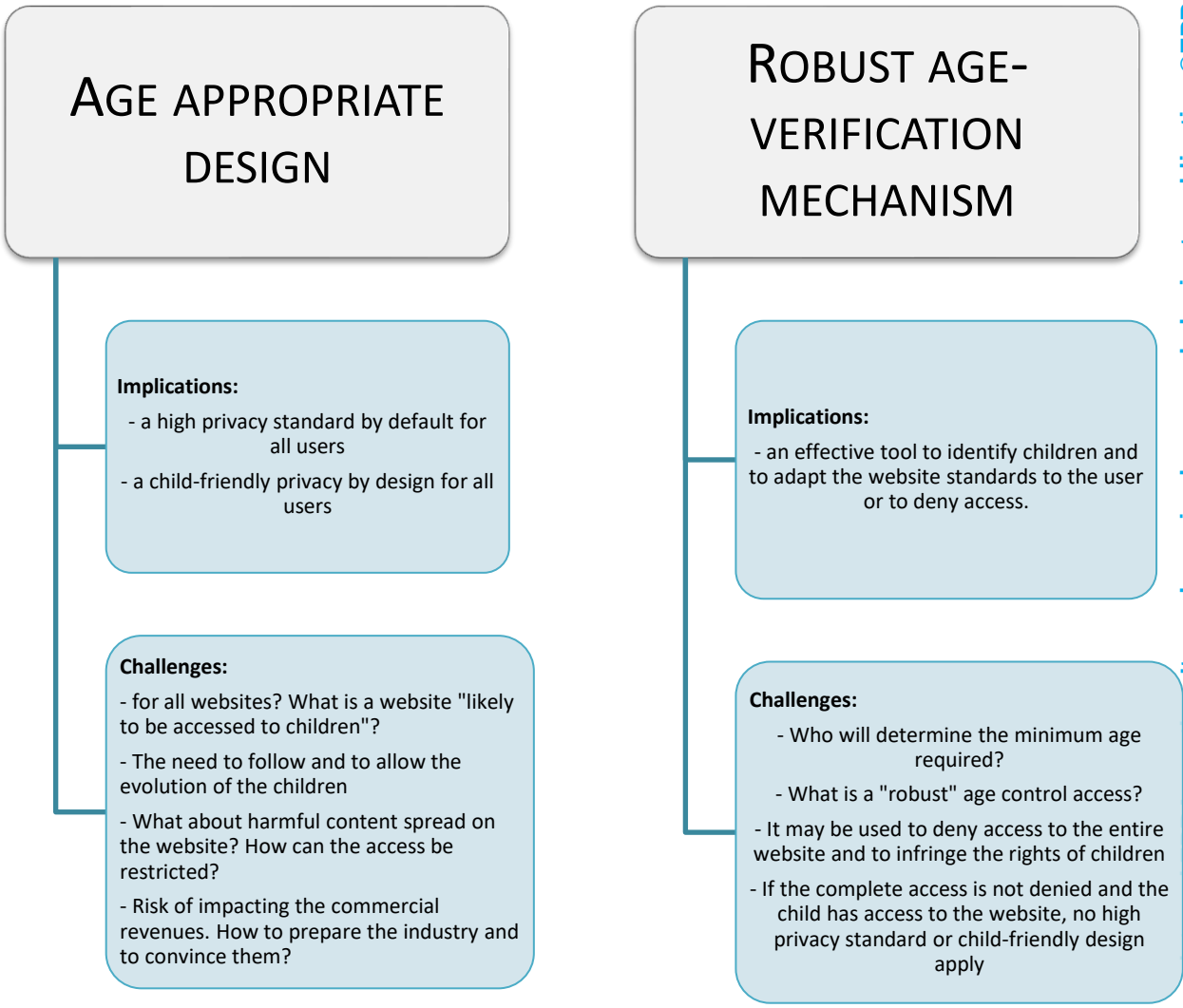
Annex 1:

Protection of minors: the AVMSD changes	
AVMSD 2010	**AVMSD 2018**
BROADCASTERS: *Article 27*: 1. Member States shall take **appropriate measures** to ensure that television **broadcasts** by broadcasters under their jurisdiction ***do not include*** any **programmes which *might seriously impair* the physical, mental or moral development of minors**, in particular programmes that involve pornography or gratuitous violence. 2. The measures provided for in paragraph 1 shall also extend to other programmes which are **likely to impair the physical, mental or moral development of minors**, except where it is **ensured**, by *selecting the time of the broadcast or by any technical measure*, that minors in the area of transmission **will not normally hear or see such broadcasts**. VOD Services: *Article 12*: Member States shall take **appropriate measures** to ensure that on-demand audiovisual media services provided by media service providers under their jurisdiction **which might seriously impair the physical, mental or moral development of minors** are only made available in such a way as to ensure that **minors will not normally hear or see such on-demand audiovisual media services**. *Article 9 §1g)*: **audiovisual commercial communications** shall not cause **physical or moral detriment to minors**. Therefore, they shall not directly exhort minors to buy or hire a product or service by exploiting their inexperience or credulity, directly encourage them to persuade their parents or others to purchase the goods or services being advertised, exploit the special trust minors place in parents,	BROADCASTER + VOD Services: *Article 6a §1*: Member States shall take **appropriate measures** to ensure that **audiovisual media services** provided by media service providers under their jurisdiction **which *may (~~seriously~~) impair* the physical, mental or moral development of minors** are only made available in such a way as to **ensure that minors *will not normally hear or see them***. Such measures may include selecting the time of the broadcast, age verification tools or other technical measures. They shall be proportionate to the potential harm of the programme. The most harmful content, such as gratuitous violence and pornography, shall be subject to the strictest measures. 2. **Personal data of minors collected** or otherwise generated by media service providers pursuant to paragraph 1 **shall not be processed for commercial purposes**, such as direct marketing, profiling and behaviourally targeted advertising. 3. Member States shall ensure that media service providers provide sufficient information to viewers about content which may impair the physical, mental or moral development of minors. For this purpose, media service providers shall use a system describing the potentially harmful nature of the content of an audiovisual media service. *Article 9 §1g)*: **audiovisual commercial communications** shall not cause **physical, *mental* or moral detriment to minors**; therefore, they shall not directly exhort minors to buy or hire a product or service by exploiting their inexperience or credulity, directly encourage them to persuade their parents or

teachers or other persons, or unreasonably show minors in dangerous situations.	others to purchase the goods or services being advertised, ***exploit the special trust minors place in parents, teachers or other persons***, or unreasonably show minors in dangerous situations. VIDEO SHARING PLATFORMS: *Article 28b*: 1. Without prejudice to Articles 12 to 15 of Directive 2000/31/EC, Member States shall ensure that video-sharing platform providers under their jurisdiction take **appropriate measures** to protect: (a)minors from **programmes**, user-generated videos and **audiovisual commercial communications which may impair their physical, mental or moral development** in accordance with Article 6a(1);

Annex 2:

The options considered by the ICO in the Age appropriate design code.



Annex 3:

The advertising scheme: Real Time Bidding