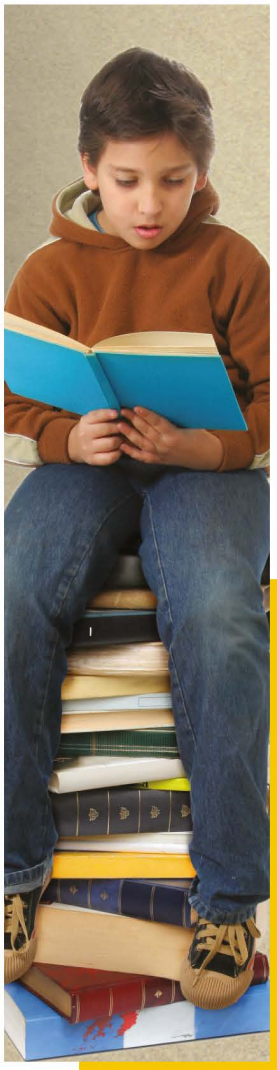
European Parliament

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT B
STRUCTURAL AND COHESION POLICIES



Agriculture and Rural Development

Culture and Education

Fisheries

Regional Development

Transport and Tourism

Research for CULT Committee - Solutions and policy dilemmas regarding minors' protection online

IN-DEPTH ANALYSIS

EN

2018

European Parliament

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

Policy Department for Structural and Cohesion Policies

CULTURE AND EDUCATION

Research for CULT Committee - Solutions and policy dilemmas regarding minors' protection online

IN-DEPTH ANALYSIS

This document was requested by the European Parliament's Committee on Culture and Education.

AUTHOR

Ghent University: Eva Lievens

Research manager Katarzyna Iskra
Project and publication assistance Lyna Pärt
Policy Department for Structural and Cohesion Policies, European Parliament

LINGUISTIC VERSIONS

Original: EN

ABOUT THE PUBLISHER

To contact the Policy Department or to subscribe to updates on our work for the CULT Committee please write to: Poldep-cohesion@ep.europa.eu

Manuscript completed in February 2018

Print	ISBN 978-92-846-2582-6	doi:10.2861/430640	QA-02-18-071-EN-C
PDF	ISBN 978-92-846-2581-9	doi:10.2861/32780	QA-02-18-071-EN-N

This document is available on the internet in summary with option to download the full text at: http://bit.ly/2nQkltI

For full text download only:
http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA(2018)617455

Further information on research for CULT by the Policy Department is available at:
https://research4committees.blog/cult/
Follow us on Twitter: @PolicyCULT

Please use the following reference to cite this study:
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
Please use the following reference for in-text citations:
Lievens (2018)

DISCLAIMER

European Parliament

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

Policy Department for Structural and Cohesion Policies

CULTURE AND EDUCATION

Research for CULT Committee - Solutions and policy dilemmas regarding minors' protection online

IN-DEPTH ANALYSIS

Abstract

This briefing paper addresses the various regulatory instruments that may be adopted to realise the full range of child rights in the digital environment, and identifies a number of policy dilemmas that arise in this context.

IP/B/CULT/IC/2017-144 February 2018

PE 617.455 EN

CONTENTS

LIST OF ABBREVIATIONS

ARIs	Alternative Regulatory Instruments
AVMSD	Audiovisual Media Services Directive
CoE	Council of Europe
CULT	Culture and Education Committee
EP	European Parliament
EU	European Union
GDPR	General Data Protection Regulation
UN	United Nations

EXECUTIVE SUMMARY

The full range of the rights of the child is impacted by the digital environment in which children grow up. To ensure that those rights are respected, protected and fulfilled, a range of regulatory instruments is available. These instruments can be situated along a '**regulatory continuum**', differentiated by the actual involvement of different actors and the role they play in the different phases of the regulatory process. **Self-regulation**, **co-regulation** and **legislation** have been used in the past to shape the digital environment, and, hence, influence how children navigate risks and opportunities therein. In addition, **technology**, **education** and **digital literacy** have significant potential to support the regulatory mechanisms along the continuum.

Whereas much emphasis has been put on the use of self-regulation in the past, gradually, a **shift to more sophisticated types of co-regulation** can be observed. Recent legislative instruments (or review procedures thereof), such as the General Data Protection Regulation or proposals for a new Audiovisual Media Services Directive, require for instance that codes of conduct that are drafted by industry actors are approved by regulatory authorities or impose more stringent procedural safeguards and evaluation mechanisms. Such an approach is especially suitable to reach delicate policy goals, such as the realisation of children's rights in the digital environment.

In order to support existing regulatory instruments and adopt a holistic approach to ensure that resilience is built, **technology and digital literacy** are indispensable. At the same time, it is important to assess the impact of the use of technical tools on all rights of the child – such as freedom of expression or the right to privacy –, to acknowledge that different types of technology are suitable for different ages, and not to overestimate the effectiveness of technology. Providing children (and parents) with **digital literacy skills** and **information,** for instance by means of (consistent) rating and labelling schemes, must therefore be a key element of any regulatory strategy.

If, at the EU level, a consistent and coordinated regulatory strategy on the rights of the child in the digital environment is to be adopted, a number of **policy dilemmas** should be considered.

All rights of the child – **protection**, **participation** and **provision** rights – must guide EU policymaking. Rights are often **interlinked**, and may at times **conflict** with each other. Measures to protect children's privacy or right to data protection may have unforeseen consequences for their right to freedom of expression and association; and for older children, conflicts may, for instance, arise between their right to the development of their sexual identity and their right to protection. **Child rights impact assessments** are therefore required before adopting policies that may affect the rights of the child.

Equally, policies should, where necessary, be differentiated on the basis of **age, maturity and evolving capacities** of the target group, or on the basis of the **vulnerable** situations in which certain children find themselves. This entails that policies should be **adaptable and flexible** to take into account the needs of vulnerable children, and also ensure that they are provided with equal and non-discriminatory access to the digital environment, high-quality and child-friendly content and services, and digital citizenship and literacy skills.

When designing regulatory policies, the **roles and responsibilities** of a variety of actors must be carefully considered. Governments (at different levels), civil society organisations, industry, educators, parents and children themselves all carry a certain degree of responsibility, although the weight of the responsibility for each actor is still shifting today. In addition to the unquestionable added value of **EU** level policies in an inherently cross-border digital world, the responsibility – and accountability – of powerful actors, such as **industry** and **data controllers** has been increasingly emphasised over the past few years. Moreover, the increasing shift towards co-regulation engages **(state) legislators**, **regulators** and **industry**. When such regulatory mechanisms are based on impact assessments, constructed in a careful manner, with clearly-defined aims, sufficient safeguards, monitoring and evaluation systems in place, and where there is a constructive cooperation between (co-)regulators and regulatees, there is a significant potential for reaching policy aims. Actors that could, and should, be engaged more in policymaking processes are **civil society** and **children** themselves. Children want to be involved in policymaking processes that aim at shaping the digital environment and their use thereof, and could contribute significantly.

Finally, all policymaking should be grounded in an **up-to-date evidence base** that monitors children's experiences with and use of digital technologies, both from a qualitative and quantitative perspective. This, of course, requires resources and a mandate to commission such – interdisciplinary and participatory – research that encompasses all EU Member States.

1. INSTRUMENTS ALONG THE REGULATORY CONTINUUM

KEY FINDINGS

- A wide range of regulatory instruments is available to ensure that the rights of the child are respected, protected, and fulfilled in the digital age, from **command-and-control state regulation** to alternative regulatory instruments, such as **self- and co-regulation**.
- A **shift to co-regulation,** with increasing attention for regulatory backstops, and monitoring and enforcement tasks for regulatory authorities, may provide important guarantees to realise the rights of the child in the digital environment.
- For certain risks that children are faced with in that environment, such as **sexual abuse** or **intrusive types of personal data processing**, legislation is the appropriate regulatory instrument, although the implementation thereof requires continued consideration of the full range of the rights of the child, on top of clarity and legal certainty.
- **Technology** has significant potential to shape children's activities in the digital environment, but should not be seen as an isolated panacea. It should rather be part of a regulatory approach that also encourages industry accountability, and that promotes **digital literacy and skills** to navigate risks and opportunities.

A wide range of regulatory instruments is available to ensure that the rights of the child are protected, promoted and fulfilled in the digital age, from command-and-control state regulation to alternative regulatory instruments (ARIs). ARIs can lean towards 'self-regulation', where there is no government involvement (which will be very rare) or a very limited level of government involvement (such as, for instance, the encouragement of self-regulation, symbolic support or low-key cooperation with government agencies). Or, ARIs can incline towards 'co-regulation', where there is a higher degree of government involvement, which can vary widely – from soft varieties to more elaborate types of co-regulation. Objectively establishing the exact required level of government involvement for an instrument to be categorised as self- or co-regulation is not feasible nor desirable, since so many different nuances can be incorporated into ARIs which, incidentally, is one of the assets of their use. Instead, the various regulatory instruments can be situated along a '**regulatory continuum**', differentiated by the actual involvement of different actors and the role they play in the different phases of the regulatory process: **creation**, **implementation** and **enforcement** of rules that aim to achieve a **goal of public interest**. In addition, regulatory tools such as **technology**, **education** and **digital literacy** can be part of or supporting the regulatory mechanisms along the continuum.

Since the mid-1990s, policies aimed at a safer internet for children have significantly relied on the use of ARIs (Lievens, 2010; McLaughlin, 2013). This was reflected in the 2012 Commission Communication on a European Strategy for a better internet for children, which stated that *"[l]egislation will not be discarded, but preference will be given to self-regulation, which remains the most flexible framework for achieving tangible results in this area*" (European Commission, 2012a). The use of ARIs has also increasingly been put

forward as a means of implementation for obligations included in legislative instruments. The following sections of the briefing paper focus on **developments** in this context since the adoption of the 2012 strategy, and the report by the European Parliament on protecting children in the digital world (European Parliament, 2012). The various regulatory instruments are described and their use is illustrated with examples from recent policy initiatives, moving from instruments with low levels of government involvement to command-and-control regulation, and ending with examples of supporting or empowering tools.

1.1. Alternative Regulatory Instruments

1.1.1. Self-regulation

Self-regulation entails the creation, implementation and enforcement of rules by a group of actors, industry in particular, with minimal or no intervention by the state (Lievens, 2010). This type of regulatory instrument is better adapted than traditional legislation to fast-changing, complex environments (Cave et al., 2008), such as the ICT and media sector, and can thus help to reach important policy goals. **Advantages** of self-regulation that are often acknowledged are flexibility, the capacity to adapt quickly to fast developing technologies and increasingly global issues, the high degree of expertise of the players that are involved and a lower cost (Mifsud Bonnici, 2008; McLaughlin, 2013; de Haan et al., 2013). Notwithstanding these assets, there are also a number of **drawbacks** such as the lack of effective enforcement and non-existent or mild sanctions in case of non-compliance. Other criticisms are limited transparency and a lack of accountability and legal certainty, resulting in a decrease in democratic quality of regulation (Latzer et al., 2012; de Haan et al., 2013). More fundamentally, it has been argued that self-regulation does not always protect fundamental rights of citizens in the same adequate way as traditional government legislation does (Price and Verhulst, 2000; Lievens, 2010) or that it may interfere with the effective exercise of fundamental rights by internet users (Angelopoulos et al., 2016).

A number of self-regulatory initiatives specifically aimed at children in the digital environment have been set up at the level of the European Union, ranging from the **Safer Social Networking Principles** for Europe,[1] the **CEO Coalition**[2], the **ICT Coalition for Children Online**;[3] to, more recently, the **Alliance to better protect minors online**.[4] These initiatives gather industry (in different constellations) that commits to make the digital environment safer for children. They have worked on, for instance, promoting privacy-friendly default settings, encouraging age-appropriate content, offering reporting mechanisms, implementing content classification and providing parental controls. This engagement fits within their responsibility to respect and support children's fundamental rights. Although these initiatives have undoubtedly led to **important actions** by private actors vis-à-vis the risks and opportunities that children face in the digital environment, a number of the **drawbacks** mentioned above have also been observed (de Haan et al., 2013). Independent assessments of the implementation of the Safer Social Networking Principles, for instance, showed that the commitments by the social networking sites were not put into practice in an adequate manner (European Commission, 2011b). Moreover, the

1 http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf.

2 http://ec.europa.eu/information_society/activities/sip/docs/ceo_coalition_statement.pdf.

3 http://www.ictcoalition.eu/. This coalition was formerly known as the ICT Principles Coalition or ICT Coalition for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU.

4 https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online. For the statement of purpose of the Alliance, see: http://ec.europa.eu/newsroom/document.cfm?doc_id=42408; for the individual company statements, see https://ec.europa.eu/digital-single-market/en/news/individual-company-statements-alliance-better-protect-minors-online.

organisational processes of the CEO Coalition have been opaque to outsiders. Although it was claimed that regular meetings were held, companies engaged in research and realisation of new ideas and actual progress was being made, at least to outsiders, there was a lack of transparent information on the working methods and the collaboration with civil society and other actors, reports were brief and communication by the Commission remained superficial. The ICT Coalition for children online undertakes a greater effort to be transparent about the commitments that companies engage in and to assess its own impact. The first report on the implementation in 2014[5] was largely based on self-reporting and did not carry out actual tests, for instance as to the actual reaction or feedback users get when they have reported something. Since then no independent evaluations have been undertaken, but companies do fill out implementation reports themselves. When the Alliance to better protect minors online was launched in February 2017, a commitment was included to perform an independent and transparent review after 18 months. This is promising, and in line with the **Principles for Better self- and co-regulation**.[6] These principles were adopted in 2013, as the result of a process of public consultation, and focus on the conception of self- and co-regulation on the one hand, and the implementation thereof on the other hand. The latter part includes recommendations with respect to iterative improvements, monitoring and evaluation. According to the principles, participants in such regulatory schemes should, for instance, regularly and collectively evaluate performance both against output commitments, and as to impact.

Another (less child-specific) initiative that could be considered self-regulatory - although the European Commission takes up a strong monitoring role - is the **Code of conduct on countering illegal hate speech online** which the European Commission agreed on in May 2016 with four companies: Facebook, Microsoft, Twitter and YouTube.[7] The implementation of this code of conduct has been assessed by the Commission at regular intervals, a first time in December 2016,[8] and a second time in May 2017.[9] According to the results of the second evaluation, significant progress was made, but some challenges remained, for instance with regard to speed of reviewing notifications and the quality of the feedback that is provided to users on how notifications have been assessed. On January 8, 2018, the Commission demanded that more efforts and faster progress were to be made, and that, although, the Commission would "*continue to promote cooperation with social media companies to detect and remove terrorist and other illegal content online", "if necessary", "legislation would be proposed to complement the existing regulatory framework".*[10]

1.1.2. Co-regulation

Co-regulation consists of a combination of non-state and state regulation in such a way that a non-state regulatory system links up with state regulation (Hans Bredow Institut and EMR, 2006). This regulatory instrument combines advantages of both these instruments, provided that it is carefully structured within the legal framework with attention for procedural guarantees. On the one hand, co-regulation has the advantages of being flexible, adaptable, and being built on the expertise and involvement of the sector, and on

5 The report is available here: http://www.ictcoalition.eu/gallery/75/ICT_REPORT.pdf.

6 https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/CoP%20-%20Principles%20for%20better%20self-%20and%20co-regulation.pdf. A Community of Practice (CoP) for better self- and co-regulation was established at the same time. More information on the functioning of that Community can be found in a 2016 Report on the CoP Stakeholders Survey, see Commission, 2016d.

7 http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf.

8 http://ec.europa.eu/newsroom/just/item-detail.cfm?&item_id=50840.

9 http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300.

10 http://europa.eu/rapid/press-release_STATEMENT-18-63_en.htm.

the other hand, more legal certainty, democratic legitimacy and more (effective) enforcement can be provided. As such, it is a more **refined** instrument, and one that is especially **suitable** with respect to a **delicate policy goal** such as **realising children's rights in the digital environment** (Lievens, 2010).

1.1.3. Self- and- co-regulation in the context of the GDPR and the AVMS

Important recent legislative instruments (or review procedures thereof) that relate (in part) to the protection of minors online explicitly refer to the adoption of self- and co-regulatory instruments to implement the principles and obligations therein.

The **General Data Protection Regulation** (GDPR; below), which will prove to be of the utmost importance in respect of children's right to data protection, contains in its article 40 a possibility for associations or industry bodies to draft codes of conduct, for instance in relation to "the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained". According to article 40, the supervisory authority shall provide an opinion on whether such a draft code (or amendment or extension thereof) complies with the GDPR, and shall approve that draft code if it finds that it provides sufficient appropriate safeguards. Such a mechanism is clearly co-regulatory in nature.

The **Audiovisual Media Services Directive** (AVMSD; below) contains explicit references to self- and co-regulation. Moreover, almost all provisions with regard to the protection of minors in the Commission proposal for a new AVMSD explicitly refer to the use of self- and/or co-regulation as a means for implementation. In relation to video-sharing platforms, only co-regulation is mentioned (Article 28a). The study on the 'Effectiveness of self- and co-regulation in the context of implementing the AVMSD', commissioned by the European Commission in the review process of the AVMSD, found that in the context of self- and co-regulation[11] with regard to the protection of minors and to commercial communication, the actual implementation of these instruments still left **room for improvement** with regard to the fact consumer and civil society groups were often not represented; certain schemes lack a systematic process for implementing improvements; in certain schemes no systems are in place which specifically monitor the scheme objectives, and indicators and targets are often missing; and the fact there were few evaluation systems in place which undertake regular assessments of the scheme, its performance, possible areas for improvement, as well as its broader impact (Panteia and VVA Europe, 2016). This is why it is crucial that Article 4, para. 7 AVMSD of the Commission proposal requires the codes of conduct that are adopted in the framework of self- and co-regulation to "*clearly and unambiguously set out their objectives*", "*provide for regular, transparent and independent monitoring, and evaluation of the achievement of the objectives aimed at*", and "*provide for effective enforcement, including when appropriate effective and proportionate sanctions*". The European Parliament (EP) amended this paragraph by adding that it is the **"[r]egulatory authorities and/or bodies**" that "shall provide for regular, transparent and independent monitoring and evaluation of the achievement of the objectives aimed at in those codes". Moreover, the EP clarified that "[t]he codes of conduct shall provide for effective and transparent enforcement **by the regulatory authorities and/or bodies**, including […] effective and proportionate sanctions".[12] Again, this is clearly a prominent **shift to co-regulation**, where audiovisual media service providers play an important role in drafting

[11] The study did not make explicit distinctions between self- and co-regulatory schemes when collecting schemes (Panteia and VVA Europe, 2016).

[12] Council of the European Union, Mandate for negotiations with the Parliament, 17 November 2017, http://data.consilium.europa.eu/doc/document/ST-14409-2017-ADD-1/en/pdf.

the content of the codes of conduct, but where there is a regulatory backstop, and an important task for regulatory authorities with regard to monitoring and enforcement.

1.2. Regulation

Command-and-control regulation entails that the state performs all regulatory tasks: creation, implementation, monitoring and enforcement. It is evident that this type of regulation has inherent shortcomings in complex and fast-moving sectors such as the media and ICT sector. This does not mean, however, that this cannot be an **appropriate** regulatory instrument in relation to certain risks that children are faced with it in the digital environment.

1.2.1. Child sexual abuse

With respect to illegal content, criminal legislation is of course key. As regards child sexual abuse material (CSAM) in particular, **Directive 2011/92/EU** of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA addresses a number of **online risks**, such as solicitation of children online for sexual purposes (grooming) (Article 6) as well as webcam sexual abuse and online viewing of child abuse images without downloading them (Article 5, in particular paragraph 3). Furthermore, Article 25(1) imposes an obligation on Member States to ensure prompt removal of webpages containing or disseminating child pornography in their territory and to work to obtain removal if hosted outside their territory, and Article 25(2) provides Member States with the option to block access by users in their territory to webpages containing or disseminating child pornography through different means, including public action and self-regulation by the industry, subject to a number of safeguards. The 2016 implementation report by the Commission found that, in general, the Directive had led to substantive progress, but that there is still **considerable scope** for the Directive to reach its full potential through complete implementation of all of its provisions by Member States (European Commission, 2016b). In respect of Article 25 in particular, the Commission concluded in a similar manner, indicating that "key **challenges** ahead include ensuring that child sexual abuse material in Member States' territory is removed promptly and that adequate safeguards are provided where the Member State opts to take measures to block access to Internet users within its territory to web pages containing child sexual abuse material" (European Commission, 2016c).

The importance of addressing the risks related to online child sexual abuse by means of legislation has also been acknowledged at the level of the **CoE**, where the current monitoring round of the Lanzarote Convention focuses on 'The protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs)' and was reaffirmed by the **UN** General Assembly in its Resolution on the Rights of the Child of December 2017.[13]

1.2.2. Data protection

A second important legislative instrument in relation to children's rights in the digital environment is the **General Data Protection Regulation**. In its 2012 Report the European Parliament welcomed the (then still) proposal and the provisions in relation to the processing of personal data of children, but stated that "these provisions need to be clarified and developed in a way that ensures that they are clear and fully operational once the new legislation is adopted and do not undermine internet freedom". It has been argued

[13] http://srsg.violenceagainstchildren.org/sites/default/files/2017/L.21Rev.1asorallyrevisedandamended.pdf.

by a number of scholars and civil society organisations that this demand has not been met (Lievens and Verdoodt, 2017; Macenaite, 2017; Milkaite et al., 2017; van der Hof, 2017). The explicit acknowledgement in the GDPR that children merit specific protection with regard to their personal data (recital 38) can only be applauded. Yet, there are few clear provisions that really zoom in on the best interests of children and the specific measures that should be taken by data controllers to guarantee a 'fair' level of protection (for instance in relation to article 8 GDPR on child and parental consent in the context of a 'direct' offer of an 'information society service' to a 'child', or regarding profiling of children). This results - contrary to recital 7 GDPR which acknowledges the importance of legal and practical certainty - in uncertainty, not only for data controllers, but also for children and parents. Moreover, it is essential that the implementation of the policy that aims to protect children's right to (data) protection does not undermine their rights to participation (such as their right to freedom of expression or their right to freedom of association) (see below).

1.3. Technology

The use of technology has been advocated as a regulatory solution since the very first policy documents concerning the protection of minors in the digital environment. Technological tools have thus been implemented into the architecture of browsers, websites, social media, and apps, shaping children's navigation and use (van den Berg, 2014). However, whereas such tools have significant potential in this area, in certain cases they also display drawbacks, in particular with respect to effectiveness and the impact on fundamental rights. Hence, the use of technical measures should not be seen as an isolated panacea but rather as part of a regulatory approach that also encourages industry accountability, and that promotes digital literacy (Zaman and Nouwen, 2016).

1.3.1. Filtering and other restrictions on access

Content that is considered inappropriate for children can be filtered, blocked or protected by paywalls or PIN codes. The latter happens for instance in the context of video-on-demand services (Cappello, 2015). Filtering can happen in a variety of ways, such as on the basis of rating or labelling of content (see below), keywords, or black or white lists of websites. When it comes to filtering content that is considered harmful to children (but not illegal),[14] it is important to be aware that filters may suffer from over- or under-inclusiveness (van den Berg, 2014) and are not equally suitable for all children under the age of 18. As children grow older, their right to freedom to receive information and explore content that might be of importance to the development of their identity might override the rationale behind the deployment of filtering technology.

1.3.2. Parental control, monitoring and notification software

Parental control tools have been promoted in the context of the European Commission's 2012 Communication on a European Strategy for a better internet for children as well as in the new AVMSD proposal (article 12 and 28a Commission proposal). Such tools may include filtering options, tracking functionalities or time restrictions that parents can enable. Yet, research with regard to the effectiveness of such tools, on the one hand, and statistics about the uptake of parental controls (where action by parents is needed), on the other hand, is respectively inconclusive and scarce (Zaman and Nouwen, 2016). In this context, Zaman and Nouwen, for instance, have argued for "more nuanced approach towards parental controls that lies beyond a one-sided focus on child protection to avoid over-

[14] For more information on filtering of illegal content, see Swiss Institute of Comparative Law (2015).

controlling and over-protective parenting, which is found to negatively affect the development of the child".

1.3.3. Identification and age verification mechanisms

Age verification mechanisms may be useful (or even necessary) to enforce restrictions on certain types of content that children should not have access to, such as adult sexual content (as required e.g. by the UK Digital Economy Act 2017)[15], or illegal gambling websites. There are different methods that can be used, for instance through self-affirmation, delivery point validation, credit or debit card use or electronic checks of age verification databases and identification documents (Cappello, 2015). In many cases, however, it is not necessary to identify an individual, it is sufficient to determine whether or not the individual has reached the age threshold of 18 years.

Questions related to age verification also arise in the context of the **GDPR**. Although the GDPR does not explicitly require age verification of data subjects, it appears that it will be necessary to check the age of data subjects as relying on the consent of an underage child will entail that the processing of his or her personal data will be unlawful (Article 29 Working Party, 2017). Data controllers will need to assess which methods are appropriate to check the data subject's age, taking into account the risks of the processing and the principle of data minimisation. The age that needs to be verified may differ across EU Member States as the age of consent will differ from one Member State to another (either under article 8 GDPR or because national interpretations of legal capacities differ).

1.4. Supporting (or empowering) mechanisms

1.4.1. Education and digital literacy

The use of supporting mechanisms such as **education, media or digital literacy, and awareness**, is of the utmost importance. Providing children (and parents) with skills to navigate risks and opportunities in the digital environment should be an essential part of regulatory strategies. This is acknowledged in many policy documents at various levels (including the United Nations, OECD, EU and Council of Europe). The importance of media literacy was emphasised by the EP in one of their amendments to the AVSMD proposal. The Internet literacy handbook[16] launched by the Council of Europe in December 2017, also acknowledges this approach and aims (among other things) to enable children to "*embrace the multitude of possibilities that the Internet has to offer, at the same time as building up their digital resilience, conscious of their own capabilities and responsibilities*".

1.4.2. Rating and labelling

The purpose of rating and labelling systems is to provide parents and carers with reliable and useful information so that they can make **informed and well-balanced decisions** about which content is appropriate for their children (Wauters et al., 2016). Children as well might be empowered to make decisions on whether or not they want to access certain content. Rating and labelling systems may be merely informative, may be part of filtering solutions or may be integrated in regulation and enforced by regulators. In many Member States rating and labelling mechanisms are used. One of the most prominent examples is the Dutch *Kijkwijzer*-system, a single content classification system for television

[15] See HM Government (2017): Part 3 of the Digital Economy Act 2017 requires a person making available pornographic material on the Internet to persons in the UK on a commercial basis to do so in a way that ensures that the material is not normally accessible by persons under the age of 18.

[16] https://rm.coe.int/internet-literacy-handbook/1680766c85.

programmes, videos, films, games and mobile content.[17] For games, the PEGI system functions across the EU, and is also applicable to small online games (PEGI OK label). Aside from the PEGI system, other rating and labelling systems remain predominantly national and are often restricted to 'traditional' media content. There are initiatives that attempt to make labels machine-readable and interoperable, such as the MIRACLE-project,[18] or that let users rate content on online video portals, such as YouRateIt, but it is currently not clear whether these initiatives are still ongoing. Furthermore, what types of content are considered 'harmful' still varies from country to country, and across Member States different ages are used in age rating systems (Cappello, 2015).

The **AVMSD** proposal introduces a new Article 6a which requires Member States to ensure that AVMS providers provide sufficient information to viewers about content that may impair the development of minors, by means of a **system of descriptors** indicating the nature of the content. The introduction of a requirement to implement such systems across all EU Member States does fit in with an approach that aims to empower parents as well as children (recital 9 AVMSD proposal). However, as similar approaches are adopted in related areas, such as the promotion of a wider use of age rating and content classification in the Strategy for a better internet for children, **consistency** should be ensured across policy areas.

17 http://www.kijkwijzer.nl.
18 https://www.miracle-label.eu.

2. POLICY DILEMMAS

KEY FINDINGS

- As the digital world is the world that children live in, with every aspect of their lives impacted by technology, it is clear that a **consistent child rights approach** must be adopted at the EU level. All rights of the child – **protection, participation and provision** rights – must guide EU policymaking in this area.
- The rights that children should be able to exercise in the digital environment may, at times, **conflict** with each other or need **balancing**. **Child rights impact assessments** are therefore required before adopting policies that may affect a variety of rights.
- Also with respect to the digital environment, concepts such as '**age and maturity**' and '**evolving capacities**' play an important role in deciding on which (regulatory) measures are appropriate for children from zero to eighteen.
- Policies should be adaptable and flexible to take into account the needs of children in **vulnerable** situations.
- All actors that are involved – from **governments (at different levels), industry, civil society organisations** and **educators** to **parents and children** – must take up their responsibility in the digital environment. Constructive cooperation between (co-)regulators and regulatees, the accountability of powerful actors and participatory policymaking with children are of particular importance in this respect.
- Policymaking should be grounded in an **up-to-date evidence base** that monitors children's experiences with and use of digital technologies, both from a qualitative and quantitative perspective.

The 2012 EP report stressed "*the need for children's rights to be mainstreamed across all EU policy areas, by analysing the impact of measures on the rights, safety, and physical and mental integrity of children, and for this to include Commission proposals regarding the digital world, drafted in a clear manner*". As the digital world is the world that children live in, with every aspect of their lives impacted by technology, it is clear that a **consistent child rights approach** must be adopted at the EU level when legislative or regulatory initiatives are taken that concern the digital environment. Now more than five years later, two main points of attention can be identified. First, it can hardly be argued that the full range of child rights have been thoroughly and carefully considered in recent review processes in this area, such as the data protection reform.[19] Second, still too often the focus of EU policy is solely on the *protection* of children in the digital environment, whereas **the UNCRC attributes not only protection rights to children but also *participation* and *provision* rights** (Livingstone and O'Neill, 2014). In this regard, the Council of Europe (CoE), who identified 'Children's rights in the digital environment' as one of the five priorities of its Strategy on the Rights of the Child 2016-2021 (Council of Europe, 2016b),

[19] Aside from issues related to the GDPR which are described below, the Commission Proposal for a new e-Privacy Regulation does not contain one reference to children and their rights (Verdoodt and Lievens, 2017).

is now preparing a comprehensive and holistic Recommendation on guidelines for member States to promote, protect and fulfil children's rights in the digital environment.[20] If also at the EU level a consistent and coordinated approach on child rights in the digital environment is to be adopted, a number of policy dilemmas should be considered.

2.1. Balancing (children's) rights

The various protection, participation and provision rights that children should be able to exercise in the digital environment are very much interlinked, and may, at times, conflict with each other or need balancing.[21] Children's right to **freedom to receive and impart information** may, for instance, sometimes necessarily be restricted, but in other instances restrictions imposed on their use of digital media in schools, communities and other public or private locations will be excessive (Lievens et al., 2018). Such restrictions may be imposed both by State authorities and by private actors for legitimate reasons, but should always be proportionate and accompanied with sufficient substantive and procedural safeguards (Council of Europe, 2008). Moreover, in addition to conflicts between children's right to **protection** and children's right to freedom of expression, there may be conflicts between the first and adult rights to freedom of expression, for instance when access to certain content is restricted for everyone (e.g. by imposing age verification to gain access to online adult content) in order to prevent access by minors. Also, 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**).[22] It has been claimed, for instance, that the implementation of article 8 GDPR might lead providers of services that are used by large numbers of children today to decide to stop offering their services to the group of children that are under the age of consent determined in that article (Lievens and Verdoodt, 2017). Other conflicts may arise between older children's **sexual rights** and the right to protection in the context of policies that address phenomena such as sexting, in that criminalisation of sharing of sexually suggestive pictures on a consensual basis might infringe on the legitimate exploring of adolescents' sexual identity.[23] Finally, it is important to be aware that **participation rights** may also have a protective function, meaning that children can only be truly empowered, supported and resilient in the digital environment if they are actively and meaningfully involved in the formulation, implementation and review of policies directed at their protection (McLaughlin 2013; Lievens et al., 2018).

These reflections entail that when considering policies that aim to realise the full range of rights of the child in the digital environment, detailed **child rights impact assessments**

[20] https://www.coe.int/en/web/children/-/call-for-consultation-guidelines-for-member-states-to-promote-protect-and-fulfil-children-s-rights-in-the-digital-environment.

[21] This idea has been incorporated into recital 31 (situated within a range of recitals related to the protection of minors on video-sharing platforms) of the Commission AVMSD proposal which states that when taking measures to protect minors from harmful content […], the applicable fundamental rights, such as the right to respect for private and family life and the protection of personal data, the freedom of expression and information, the freedom to conduct a business, the prohibition of discrimination and the right of the child, as guaranteed by the CFEU, must be carefully balanced.

[22] See also the 2011 EU Agenda for the Rights of the Child which emphasised that "[t]he Commission aims at achieving a high level of protection of children in the digital space, including of their personal data, while fully upholding their right to access internet for the benefit of their social and cultural development" (European Commission, 2011a).

[23] Directive 2011/92/EU contains the possibility to exclude certain consensual activities in certain instances from criminalisation, but only a limited number of Member States chose to implement these in national legislation (European Commission, 2016b).

must be carried out, taking into account all the rights that might be at stake. This also includes less obvious reflections such as taking into account the right to protection from economic exploitation or the right to development when considering phenomena such as behavioural profiling or targeted advertising (Verdoodt and Lievens, 2017).

2.2. Different ages, different rules

The UNCRC defines a child as a human being below the age of eighteen years. As children develop during the timeframe between birth and majority, concepts such as '**age and maturity**' and '**evolving capacities**' play an important role in deciding on which (regulatory) measures are appropriate for which groups of children. The UN Committee on the Rights of the child (2016) has recently emphasised that "[a]pproaches adopted to ensure the realization of the rights of **adolescents** differ significantly from those adopted for **younger children**". Although this unequivocally applies to the digital environment, regulatory approaches thereof do not always acknowledge this to a sufficient extent. Where the **GDPR**, for instance, addresses issues related to children, it is not always clear whether those provisions apply to all under-18s as the text does not contain a definition of a child. At the same time, it is unclear whether decisions on the age of consent, laid down in article 8 GDPR, are rooted in scientific theory or **evidence** on children's commercial literacy (Livingstone, 2017). It has been argued in this respect that data controllers should differentiate between young children and adolescents in their data processing activities (Montgomery and Chester, 2015). Furthermore, when technology is used to implement policies in relation to the digital environment, certainly for teenagers and adolescents policymakers could consider a shift from techno-regulatory solutions (such as filtering) towards **persuasive and nudging solutions** (such as self-monitoring or the use of default settings); the latter ensure that their freedom to experiment and discover is enhanced, while in the process, they become more competent, risk-aware and resilient (van den Berg, 2014).

2.3. Enhancing and strengthening opportunities for all children

Taking policies beyond protection entails a stronger emphasis on participation and provision rights and the opportunities that the digital environment encompasses. It is up to policymakers to carefully consider the drivers and incentives of such an approach. Furthermore, similar to the fact that policies towards children in the digital environment might sometimes be 'age-blind', policies also tend to address children in the same manner, regardless of the fact that certain children find themselves in **vulnerable situations** for a variety of reasons. This may include children with disabilities (Alper and Goggin, 2017), children living in poverty, children from minority groups, child refugees or those displaced by armed conflict, children of imprisoned parents, and other vulnerable groups who may not be reached by schools or supported by parents (Lievens et al., 2018). Although research on how vulnerable children are impacted by the digital environment is scarce, there are findings that indicate that often children that are vulnerable offline are also vulnerable online (Livingstone and Haddon, 2009). At the same time, for children in such situations the digital environment might offer enhanced opportunities to exercise their rights (Alper and Goggin, 2017). This entails that policies should be adaptable and flexible to take into account the needs of vulnerable children, and also ensure that they are provided with equal and non-discriminatory access to the digital environment, high-quality and child-friendly content and services, and digital citizenship and literacy skills.

2.4. A shared responsibility

Multi-stakeholder involvement has been one of the **cornerstones of EU policy** in relation to the digital environment. It is clear that many actors are involved in the realisation of child rights in this environment: governments (at different levels), industry, civil society organisations, educators, parents and children themselves. Each and every one of these actors carries responsibility in achieving this aim, although the weight of the responsibility of certain actors is still shifting today.

First, the responsibility of powerful actors, such as **industry** and **data controllers**, for instance, has been increasingly emphasised over the past few years. This fits in with a larger awareness of industry or private sector responsibility regarding human and child rights, such as laid down in the UN General principles on human rights and business, the UN Children's rights and business principles, the UN General Comment on state obligations regarding the impact of the business sector on children's rights, and the CoE Recommendation on human rights and business. These documents confirm that although it is the State's duty to protect human rights, business enterprises have the responsibility to respect human rights. In complex environments, such as the digital, it is of the utmost importance that these actors take up their responsibility, as children and parents are often at loss about the impact of certain technologies on their rights. An example thereof is the enhanced accountability of the data controller in the context of the **GDPR**, which, together with the implementation of the principles of privacy by design and default into practice and the carrying out of Data Protection Impact Assessments, could lead to a greater de-responsabilisation of parents and children. A second example can be found in the recent Commission **Communication on Tackling illegal content online**, which aims to move towards enhanced responsibility of online platforms.[24] Also with respect to combating online child sexual abuse material these platforms can play a crucial role, in cooperation with state authorities and other stakeholders.

Second, the increasing shift towards co-regulation, as discussed above, engages (**state) legislators**, **regulators** and **industry**. When such regulatory mechanisms are based on impact assessments, constructed in a careful manner, with clearly-defined aims, sufficient safeguards, monitoring and evaluation systems in place, and where there is a constructive cooperation between (co-)regulators and regulatees, there is a significant potential for reaching policy aims.

Third, within policymaking and regulatory processes, there are actors that are sometimes 'forgotten', although they also bear responsibility. This not only is the case in relation to **civil society**, whom could be enabled to play a bigger role, but it is undoubtedly so when it comes to children themselves. Actual participation of **children** themselves in the policymaking process (not only through associations that defend their interests) should also be encouraged and realised (Lievens, 2017). Participatory research with children regarding their rights in the digital age has shown that children want to be involved in conversations with policymakers on how to use digital media to support children's rights and want to take responsibility (Third et al., 2014).

Fourth, there is an important responsibility at the **EU** policymaking level, as the digital environment is inherently a cross-border one. This means, on the one hand, that enforcement and jurisdiction issues in relation to important challenges in relation to child

[24] https://ec.europa.eu/digital-single-market/en/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms.

sexual abuse material and other illegal content, can only be addressed through enhanced cooperation at European (and international) level. On the other hand, both for providers and users of cross-border services legal certainty is crucial. One example of confusion in relation to children is the fragmented landscape that is emerging as governments across the EU implement article 8 of the **GDPR** and choose different ages at which children are capable of giving consent to process their personal data.

2.5. Grounding policy in up-to-date evidence

Given the speed at which the digital environment moves forward, with children often being early adopters and primary consumers of services in manners that are unintended, all policymaking should be grounded in an **up-to-date evidence base** (Lievens et al., 2018) that monitors children's experiences and use, both from a qualitative and quantitative perspective. This, of course, requires resources and a mandate to commission such research that encompasses all EU Member States.

REFERENCES

- Alper, M. and Goggin, G. (2017) "Digital technology and rights in the lives of children with disabilities", *New Media & Society*, 19(5), 726–740

- Angelopoulos, C., Brody, A., Hins, W., Hugenholtz, B., Leerssen, P., Margoni, T., McGonagle, T., van Daalen, O. & van Hoboken, J. (2016), *Study of fundamental rights limitations for online enforcement through self-regulation*, http://www.ivir.nl/publicaties/download/1796

- Article 29 Working Party, *Draft Guidelines on consent under Regulation 2016/679* (WP 259), 28 November 2017

- Cappello, M. (ed.) (2015), The protection of minors in a converged media environment, IRIS plus, Strasbourg, European Audiovisual Observatory, http://publi.obs.coe.int/documents/205602/8261715/The+protection+of+minors+in+a+converged+media+environment.pdf/bc80d13a-eedc-4b0a-8824-40bc2cdd6e47

- Cave, J., Marsden, C., & Simmons, S. (2008), *Options for and effectiveness of internet self- and co-regulation*, http://www.rand.org/pubs/technical_reports/TR566.html

- Council of Europe (2008), *Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters*

- Council of Europe (2016a), *Recommendation CM/Rec(2016)3 of the Committee of Ministers to member States on human rights and business*

- Council of Europe (2016b), *Strategy for the rights of the child (2016-2020),* https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM%282015%29175&Language=lanEnglish&Ver=final&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F 5D383&direct=true

- de Haan, J., van der Hof, S., Bekkers, W., and Pijpers, R. (2013), "Self-regulation", 111-129, in: B. O'Neill, E. Staksrud and S. McLaughlin, *Towards a better internet for children? Policy pillars, players and paradoxes*, Göteborg, Nordicom

- European Commission (2011a), *Communication: An EU Agenda for the Rights of the Child*, COM(2011) 60 final

- European Commission (2011b), *Digital Agenda: social networks can do much more to protect minors' privacy*, http://europa.eu/rapid/press-release_IP-11-1124_en.htm

- European Commission (2012a), *Communication on a European Strategy for a Better Internet for Children*, COM(2012) 196 final

- European Commission (2012b), *Principles for Better Self- and Co-regulation*, https://ec.europa.eu/digital-single-market/en/principles-better-self-and-co-regulation

- European Commission (2016a), *Commission Staff Working Document Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities*, SWD(2016) 168 final

- European Commission (2016b), *Report from the Commission to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography*, COM (2016) 871 final

- European Commission (2016c), *Report from the Commission to the European Parliament and the Council assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography*, COM (2016) 872 final

- European Commission (2016d), *Report of the CoP Stakeholders Survey*, https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/dae-library/results_cop_stakeholders_survey_0.pdf

- European Parliament (2012), *Report on protecting children in the digital world*, 2012/2068(INI)

- Hans Bredow Institut and EMR (2006), *Final Report Study on Co-Regulation Measures in the Media Sector*, https://ec.europa.eu/digital-single-market/en/news/study-co-regulation-measures-media-sector-2007

- HM Government (2017), *Internet Safety Strategy Green Paper*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf

- Latzer, M., Just, N., and Saurwein, F. (2012), "Self- and co-regulation: Evidence, legitimacy and governance choice", 373-397, in: M. Price and S. Verhulst (Eds.), *Routledge Handbook of Media Law*, Oxford, Routledge

- Lievens, E. (2010), *Protecting children in the digital era: The use of alternative regulatory instruments*, Leiden/Boston, Martinus Nijhoff Publishers

- Lievens, E. (2017), "Children's rights and media: imperfect but inspirational", 231-250, in: E. Brems, W. Vandenhole and E. Desmet, *Children's rights in the global human rights landscape: isolation, inspiration, integration?*, Routledge

- Lievens, E., & Verdoodt, V. (2017), "Looking for needles in a haystack: key issues affecting children's rights in the General Data Protection Regulation", *Computer Law & Security Review*, https://doi.org/10.1016/j.clsr.2017.09.007

- Lievens, E., Livingstone, S., McLaughlin, S., O'Neill, B., and Verdoodt, V. (2018), "Children's rights and digital technologies", in T. Liefaard and U. Kilkelly (eds), *International Human Rights. International Children's Rights Law*, Springer (forthcoming)

- Livingstone, S., and Haddon, L. (2009), *EU Kids Online: Final report*, EU Kids Online. (EC Safer Internet Plus Programme Deliverable D6.5), London, LSE

- Livingstone, S. and O'Neill, B. (2014) "Children's rights online: challenges, dilemmas and emerging directions", 19-38, in: van der Hof, S., van den Berg, B. and Schermer, B., *Minding minors wandering the web: Regulating online child safety*, Asser Press Springer

- Livingstone, S. (2017), *Children's commercial media literacy: new evidence relevant to UK policy decisions regarding the GDPR*, http://blogs.lse.ac.uk/mediapolicyproject/2017/01/26/childrens-commercial-media-literacy-new-evidence-relevant-to-uk-policy-decisions-regarding-the-gdpr/

- Macenaite, M. (2017), "From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation", *New Media & Society* 19(5), 765-779

- McLaughlin, S. (2013), "Regulation and legislation", 77-91, in: O'Neill, B., Staksrud, E. and McLaughlin, S. (eds.), *Towards a better Internet for children? Policy pillars, players and* paradoxes, Gothenborg, Nordicom

- Mifsud Bonnici, J. (2008), *Self-regulation in cyberspace*, The Hague, T.M.C. Asser Press.

- Milkaite, I., Verdoodt, V., Lievens, E., and Martens, H. (2017) *Roundtable Report: The General Data Protection Regulation and children's rights: questions and answers for legislators, DPAs, industry, education, stakeholders and civil society*, https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=2018677

- Montgomery, K.C. and Chester, J. (2015), "Data Protection for Youth in the Digital Age – Developing a Rights-based Global Framework", *European Data Protection Law Review* 1(4), 290

- Panteia and VVA Europe (2016), *Effectiveness of self- and co-regulation in the context of implementing the AVMS Directive: A study prepared for the European Commission DG Communications Networks, Content & Technology*, https://ec.europa.eu/digital-single-market/en/news/audiovisual-and-media-services-directive-self-and-co-regulation-study

- Price, M. & Verhulst, S. (2000), "In search of the self: Charting the course of self-regulation on the Internet and global environment", 57-78, in: Marsden, C. (ed.), *Regulating the global information society*, London, Routledge

- Swiss Institute of Comparative Law (2015), *Comparative study on blocking, filtering and take-down of illegal internet content*, 2015, https://rm.coe.int/168068511c

- Third, A., Bellerose, D., Dawkins, U., Keltie, E. & Pihl, K. (2014), *Children's rights in the digital age: A download from children around the world*, http://www.unicef.org/publications/files/Childrens_Rights_in_the_Digital_Age_A_Download_from_Children_Around_the_World_FINAL.pdf

- Unicef (2013), *Children's rights and business principles*, http://www.unglobalcompact.org/docs/issues_doc/human_rights/CRBP/Childrens_Rights_and_Business_Principles.pdf

- United Nations (2011), *Guiding principles on business and human rights*, http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

- United Nations Committee on the Rights of the Child (2013), *General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights*

- United Nations Committee on the Rights of the Child (2014), *Report of the 2014 day of general discussion 'Digital media and children's rights'*

- United Nations Committee on the Rights of the Child (2016) *General comment No. 20 (2016) on the implementation of the rights of the child during adolescence*

- van den Berg, B. (2014) "Colouring inside the lines: Using technology to regulate children's behaviour online", 67-85 in: van der Hof, S., van den Berg, B. and Schermer, B., *Minding minors wandering the web: Regulating online child safety*, Asser Press Springer

- van der Hof, S. (2017), "I agree. . . or do I? – A rights-based analysis of the law on children's consent in the digital world", *Wisconsin International Law Journal* 34, 409

- Verdoodt, V. and Lievens, E. (2017), "Targeting children with personalised advertising: How to reconcile the (best) interests of children and advertisers", 313-341, in: Vermeulen, G. and Lievens, E. (eds) *Data Protection and Privacy under Pressure: Transatlantic tensions, EU surveillance and big data*, Maklu

- Wauters, E., Lievens, E. and Valcke, P. (2016), "Empowering Children through Labelling in Social Networks: Illusion or Solution?", 227-247, in: Walrave, M., Ponnet, K., Vanderhoven, E., Haers, J. and Segaert, B. (eds), *Youth 2.0: Social Media and Adolescence: Connecting, Sharing and Empowering*, Springer

- Zaman, B. and Nouwen, M. (2016), *Parental controls: advice for parents, researchers and industry*, http://eprints.lse.ac.uk/65388/

CAT: QA-02-18-071-EN-C (paper)
CAT: QA-02-18-071-EN-N (pdf)

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT B
STRUCTURAL AND COHESION POLICIES

Role

The Policy Departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- Agriculture and Rural Development
- Culture and Education
- Fisheries
- Regional Development
- Transport and Tourism

Documents

Visit the European Parliament website:
http://www.europarl.europa.eu/supporting-analyses

PHOTO CREDIT: iStock International Inc., Photodisk, Phovoir

ISBN 978-92-846-2582-6 (paper)
ISBN 978-92-846-2581-9 (pdf)

doi:10.2861/430640 (paper)
doi:10.2861/32780 (pdf)

Publications Office