e-Youth before its judges

Poullet, Yves

Published in:
Computer Law and Security Report

Publication date:
2011

Document Version
Publisher's PDF, also known as Version of record

available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

e-Youth before its judges – Legal protection of minors in cyberspace

Yves Poullet

CRIDS, University of Namur, Belgium

Keywords:
e-Youth
Protection of minors
Cyberspace law
Profiling
Data protection
Privacy
Social networking
Privacy by design

ABSTRACT

The present paper[1] aims both at introducing the legal aspects of the protection of minors in cyberspace and analysing and criticizing certain main features embedded in this legal approach of young people protection. After a short *introduction* underlining the concept of child's rights and the reason why this right has been particularly proclaimed in the context of the cyberspace, the *first section* describes the new technological features of the ICT environment and linked to this evolution the increasing risks the minors are confronted with. A typology of cyber abuses is proposed on the basis of these considerations. A list of EU or Council of Europe texts directly or indirectly related to the minors' protection into the cyberspace is provided. The *second section* intends to analyse certain characteristics of the legal approach as regards the ways by which that protection is conceived and effectively ensured. Different principles and methods might be considered as keywords summarizing the legal approach and to a certain extent, fixing a partition of responsibilities taking fully into account the diversity of actors might be deduced from the different regulatory documents.

The *third section* comes back to the different complementary means by which the Law is envisaging the minors' protection. The obligation to create awareness about the potential risks minors might incur definitively is the first one. The omnipresent reference in all the legal texts to the role of self-regulatory interventions constitutes another pillar of the protection envisaged by the Law. After having described the multiple instruments developed in the context of this self-regulation (labels, codes of conduct, hotlines, ODR...) or even co-regulation, the paper examines the conditions set by the European legislators as regards these instruments. Technology might be considered as a fourth method for protecting children. Our concern will be to see how the Law is addressing new requirements as regards the technological solutions and their implementation. The present debates about the liability of the actors involved in applications or services targeted or not vis-à-vis the minors like SNS or VSP operators are evoked. As a final point the question of the increasing competences of LEA and the reinforcement of the criminal provisions in order to fight cyber abuses against minors will be debated. In *conclusion*, we will address final recommendations about the way by which it would be possible to reconcile effective minors' protection and liberties into the cyberspace.

[1] This paper in notably based on the CRID's research achieved in the context of the TIRO research project carried out in the context of the programme launched by the Federal Ministry of Science and Policy (BELSPO) and conducted together with SMIT (VUB), Department communicatiewetenschappen (UA), CITA and CRID (University of Namur). See the report TIRO, Teens and ICT: Risks and Opportunities (Cyberteens and cybertools), published by BELSPO, 2008.

0267-3649/$ – see front matter © 2011 Professor Yves Poullet. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2010.11.011

1. Introduction

A quotation of the 2/2009 opinion of the Art. 29 WP (WP 160) enacted in February 2009 about Data Protection and Minors illustrates the main reason why legislators are particularly concerned about granting protection to minors:

> "*From the static point of view, the child is a person who has not yet achieved physical and psychological maturity. From the dynamic point of view, the child is in the process of developing physically and mentally to become an adult. The right of the children and the exercise of these rights, including that of data protection, should be expressed in a way which recognizes these two perspectives*."

In other words to take again the NUSSBAUM's approach,[2] the Law has to ensure the conditions for the development of human capabilities, that is to say not the actual achievements of persons but the freedom of persons to achieve the development of his or her personality (his or her *ipse*).[3] Insofar as the child's development may be favoured by the use of ICT, at the same time it can be compromised by it. Consequently, the Law has to take certain initiatives to avoid events which might jeopardize this development. If it is not contested the overwhelmingly positive potential of the Internet is evident: that is to inform, entertain and educate children. At the same time a totally free internet for children and young people might lead to obvious harms including sexual abuse of children, harassment, grooming, potential contact abuses and financial damage.[4] Even if children are to a certain extent "*expert users of online technologies and aware of both risks and ways of dealing with them, they are not mature in the sense of being able to evaluate the situations they encounter and the possible consequences their decision might have*".[5]

The EU regulatory Action as regards the e-Youth protection takes place in the context of the EU Commission Declaration on Children's rights dated from 2006[6] designated as a priority for the EU: "*A particular priority must be effective protection of the rights of the children against economic exploitation and all forms of abuse, with the Union acting as a beacon for the rest of the world*". This Declaration pleads in favour of effective measures around different tools:

- more comprehensive analysis of the needs and priorities and of the impact of relevant EU actions undertaken so far;
- more efficient mainstreaming of children's rights in EU policies, strategies or programmes and enhanced coordination within the European Commission;
- better cooperation with key stakeholders, including children;
- stronger communication and increased awareness of children's rights and of EU actions in this field.

In that context, protection of young people is considered as a major issue. According to data released by the EU Commission,[7] in the UK during the period 1997–2005, the number of sites with child abuse material increased by 1.500 percent and Interpol's Child abuse Image Database contains 550.000 images of 20.000 children. All these abuses are obviously perpetrated against children, but what must be noticed is that children are not the only victims but increasingly the perpetrators themselves. Before addressing a typology of these abuses, it would be interesting to understand the causal link one might establish between the new technological features of online services and the increasing risks incurred by young people.

Different trends might be underlined as regards the development of ICT. New significant characteristics are often developed, but besides this there are also new applications and roles played by new actors exploiting these technological

[2] See notably, M. Nussbaum, Capabilities and Human rights, *Fordham Law review*, 66 (1997), 273–290.

[3] Under our opinion, Law is achieving this task through the privacy concept in the broadest sense. "The two aspects – freedom from unreasonable constraints (from the State or from others) in the construction of one's identity, and control over (some) aspects of the identity one projects to the world – are at the heart of what the various 'facets' of privacy are all about. Yet, more fundamentally, and against the common view that the 'freedom in the construction of one's personality' and 'control over information about oneself one projects on the world' pursue different, though complementary, normative goals, we would like to argue that their common normative justification and objective, or, to say it more plainly, the final value they are meant to advance, is the capacity of the human subject to keep and develop his personality in a manner that allows him to fully participate in society without however being induced to conform his thoughts, beliefs, behaviours and preferences to those thoughts, beliefs, behaviours and preferences held by the majority. Privacy and data protection regimes should thus be understood as 'mere' tools (evolving when required by the new threats that socio-economic, cultural, and technological changes impose on individual and democratic self-determination), meant to pursue that one single common goal: sustaining the uniquely human capacity for individual reflexive self-determination and for collective deliberative decision making regarding the rules of social cooperation." (A. Rouvroy and Y. Poullet, The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy, in Reinventing Data Protection, Proceedings of the 2nd CPDP Conference, Brussels 2009, Gutwirth, Poullet et al (eds), Springer Verlag, 2010, p. 59 and ff).

[4] See SAFER INTERNET FORUM REPORT, "*Safer Internet and Online Technologies for Children*", 20–21 June 2007.

[5] Proposal for a Decision of the EU Parliament and of the Council establishing a multi-annual Community Programme on protecting Children using the Internet and other communication technologies, Brussels 27. 2.2008 COM (2008)106 final, Explanatory Memorandum, p. 2. See also, the JRC Scientific and Technical report published in 2009 about "*Young people and Emerging Digital Services – An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks*", p. 9.

[6] Communication from the Commission - Towards an EU strategy on the rights of the child {SEC(2006) 888} {SEC(2006) 889}/*COM/2006/0367 final.

[7] See the Explanatory Memorandum of the Proposal mentioned footnote 4. For other alarming ciphers, see http://www.eukidsonline.net/.

features. As regards these characteristics, four major points might be identified:

- *About Moore's Law* - The development of ICT can be firstly described in a continuous and tremendous growth of computer and communication systems capacities. The so-called Moore's Law predicts that every 18 months the storage capacity of a computer is multiplied by two for the same price, which implies the multiplication by 1000 in fifteen years. It is becoming possible to store on a personal computer the records of all the events of my life and to set-up a central GRID collecting the basic identification data of all people around the world. This capacity of storage doubled by an increasing capacity of processing and transmission explains how Google can validate your request, scanning in less than 10 s more than a thousand million sites worldwide. It explains also the development of what we call the Web 2.0 multimedia applications like YouTube, Dailymotion, etc.
- *Internet revolution* - The Internet revolution might be described from different points of view. The global character of this network has a double meaning. It means not only the universal dimension of this infrastructure, implying the interoperability of technical norms.[8] Internet also leads to the convergence of all networks, which were traditionally clearly separated like TV channels and mobile infrastructure and thus the possibility to cross match the data created by all these communication activities. That convergence is doubled by the convergence of the terminal. Our mobile devices and computers are achieving today activities like voice telephony services, TV or radio programmes reception, e-mails communications, etc. which 30 years ago were reserved to specific and dedicated terminals. The fact that a younger generation fans of these kinds of terminals might use them without parental and teacher control creates new risks everywhere.
- *Ambient Intelligence* - Ambient Intelligence[9] is perhaps the most recent outcome of the ICT evolution. With the miniaturization of terminals into "smart dust" and their implantation into objects, clothes and even on or within our own bodies, it is now possible to conceive interaction among human beings and their environment through the "Internet of Things". The technology is becoming ubiquitous covering all the events of our everyday life. We also speak of a "learning technology" insofar as it is able to adapt its functioning to the data obtained through its use. The networks created by the dialogue between things, among things or between things and people create a space progressively invested by ICTs.
- *Digital identities* - "Digital identities" are increasingly linked to individuals or to be more precise with their bodies (biometric data); or with objects under their control or use e.g. the personal computer or the communication means employed (cookies or IP addresses); tag numbers as regards RFID[10] enshrined in clothes etc…) or simply with works or things whether or not belonging to the individuals concerned.[11] One underlines the different roles of these "digital identities". They firstly might be used as "authentication" tools, especially to permit the access to certain resources. Secondly they are essential for the reconstruction of an informational image about a person – whether identified or not - apart from pieces of information scattered in databases and geographically dispersed through the network and without limitation of borders. In other words they permit the traceability (the capacity to follow the movement of a person, a good or a message) and more the ability to establish links among different databases in order to retrieve the information concerning the same individual identified or not (e.g. cookies, RFID tag number, etc).[12] Digital identifiers (like IP address, RFID tag number) permit also contact with people by sending appropriate messages. That triple characteristic of digital identifiers, linkability, traceability and contactability, explains why special attention must be given to that kind of data, which at first glance seem less sensitive than biographic data. Finally, it should be noted that biometric data are available during the entire life of the individual, precisely because they are directly linked to the body, in which traces revealing DNA can be found very easily (blood, hair, etc).

As regards now the applications and the actors, the following points can be made:

- *User Generated Content* - User Generated Content's applications definitively constitute, from the Internet users' point of view, the most prominent new applications on the Web. About 60% of the content available on the web is coming from these new applications, like social networks,

[8] An additional effort to coordinate infrastructure is being propelled by the European Organization for Nuclear Research (or "CERN", Europe's scientific consortium where the World Wide Web was born). CERN's Large Hadron Collider Computing Grid project includes a plan "to integrate thousands of computers worldwide into a global computing resource," or Grid. The project's most enthusiastic proponents contend: "*The Grid goes well beyond simple communication between computers and aims ultimately to turn the global network of computers into one vast computational resource.*"

[9] "*The central idea of these networks is to create environments in which people are surrounded by intelligent intuitive interfaces that are embedded in all kinds of objects. It is an environment that is capable of recognizing and responding to the presence and actions of different individuals in a seamless, unobtrusive and often, invisible way using several senses*".

[10] RFID = Radio Frequency IDentifier.

[11] See the Object Names System (ONS) put into place by GSI in the context of a large development of RFID and in a way quite similar to that chosen for the DNS operated by ICANN with the cooperation of Verisign. ONS will permit to trace a product to know exactly the producer, distributor, the ingredients, etc. Placed at a certain distance of a reader which might be the mobile, it permits a consumer to know exactly the product he or she is purchasing.

[12] Digital identities might be considered as "matching identifiers". "Matching identifier" refers to an item of information making it possible to identify the same individual in two data processing operations, each of which has a different file controller or a distinct purpose. Items of personal data include matching identifiers such as cookies which enable individuals to be recognised and their actions or movements to be tracked over time, whether in cyberspace or not.

Wikipedia, online games or YouTube, generally grouped under the concept of Web 2.0 applications. These emerging applications radically transform the relationships among the actors. In the traditional scheme, the role of the information service provider on one side and the role of the Internet users on the other are quite distinguished and the regulation available is normally reserved only to professionals. At issue is what happens when Internet users, including young people, in the context of these new applications, play the same role as traditional information providers when posting news on their blogs or on YouTube and become data controllers by putting information online about themselves and about third parties? Can we consider that the author of a blog is a journalist or an editor, subject to the same deontology and legal duties that the press must adhere to? New risks and threats derive from the very sensitive nature of the data they are posting, and the illicit or harmful information they are diffusing, etc. The privacy risks created by the use of these data by third parties in the context of certain secondary uses *must be highlighted*.

- *Profiling techniques* - More specifically profiling techniques[13] seem to be more and more used by companies or administrations. Profiling might be defined as a computerised method involving data mining from data warehouses, which may facilitate the placing of individuals, with a certain degree of probability, and hence with certain induced error rates, in a particular category in order to take individual decisions relating to them. Taking the opportunity of the huge number of traces generated by Internet users in addition to their use of communications services and using data collected just-in-time - thanks to the technologies and coming from a large variety of sources - companies or administrations are defining profiles and apply these profiles to individuals in order to take decisions towards individuals whether identified or not. "Adaptive pricing" is often quoted in that context. According to the profile of the customer, the information service provider might decide to adapt the price of a service or a product. One-to-one marketing is largely based on that technique and more and more administrations are detecting presumed smugglers or terrorists using that method.
- *New actors: the intermediaries* - Before discussing the implications of these applications as regards our fundamental liberties, we would like to underline the increasing role of *intermediaries*. By intermediaries, we mean all the activities which render useful the usage of the applications. It might be platforms offering the Web 2.0 services, search engines or all communications services providers as well as operators intervening in support of these communication services like certification providers. These persons play a decisive role by providing added-value services, but at the same time might be considered as gatekeepers to the information provided by or to Internet's users. They are ranking the information, facilitating the access to that information and, in certain cases, selecting the information offered.

To what extent might they be held liable in case of diffusion of illicit or illegal messages by their platform? The question has recently been raised after the diffusion on YouTube of images provided by a future Finnish killer.[14] Two additional remarks need to be made: firstly, the economy of the functioning of these services is often quite obscure, since they are using the information they collect for their own benefit or the benefit of a third party by developing marketing operations or other added-value services; secondly, law enforcement authorities might be tempted to cooperate with such services providers in order to find potential suspects in criminal affairs.

Starting from that short overview of technological features and actors, we list different cyber abuses youngsters might suffer in a cyberspace environment. It is quite clear that the borders between these different abuses are unclear and that there are a lot of overlaps.

- As regards the *financial and economic* interests, we have pinpointed how companies might use one-to-one marketing techniques in order to solicit adequately the young people. Beyond that a lot of services (videogames, phone…) are 'offered' taking advantage of childhood addictions. The instantaneous character of Internet transactions enhance the risk that children will not resist to the temptations so easily accessible. Finally, we pinpoint the risks linked with transactions at distance (lack of knowledge as regards the vendor, the quality of the product and the security of payment) which are increasing since everybody now, including young people, sell products or services on the net through developed transactional platforms.
- As regards *human dignity*, as previously said (see above,), paedophilia, sexual abuses including grooming activities, xenophobia, moral or sexual harassment are more and more committed through Internet applications.
- As regards *data protection and privacy*, firstly, it is clear that particularly with web 2.0 applications each of us but particularly the children are invited (and more and more feel obliged by social pressure) to be present on the net with a maximum of data about themselves and the events of their social life, including data about their friends, relatives and more generally about their social environment. Secondly, the huge capacities of data storage and processing are multiplying the possibility of profiling

[13] R. Brownsword, 'Knowing Me, Knowing You—Profiling, Privacy and the Public Interest' in M. Hildebrandt and S. Gutwirth (eds), *Profiling the European Citizen*, Dordrecht, Springer, 2008, pp. 362–382. The Council of Europe has adopted very recently a recommendation about profiling: Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, *Adopted by the Committee of Ministers on 23 November 2011*.This recommendation is published at: https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282010%2913&Language=lanFrench&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

[14] The 18 year old Pekka-Erik Auvinen in November 2007, see for instance timesonline, "Finish" YouTube Killer "was bullied at school", 8 November 2007.

individuals and archiving the data such images, Internet uses, profiles or messages for an unlimited time without taking into account the 'right' granted to each of us to be forgotten.
- As regards now *reputation*, cyber-bullying and defamation are becoming more and more frequent by the use of the new applications like blogs, SNS, etc.
- As regards *psychological damages* caused for instance by violence sexual nudity, self-mutilation or suicide websites, their number is increasing not only by the multiplication of these websites but also because young users are using their devices in an uncontrolled and isolated environment and thus might not refer immediately to their parents or peers.

These offences when compared with their perpetration in an offline context take on another reality in an online environment when the unique scope and facilities offered by Internet technologies come to the fore.[15] So the messages are often more implicit than in an offline environment: for instance, xenophobia messages might be delivered under the format of a game or through apparently scientific studies and it must be emphasised that these abuses are easier to commit since their author remains to a certain extent anonymous and since the technology gives them an opportunity to disseminate very easily to a large population without the additional distribution costs that their cyber hate messages would normally induce. Finally we must also pinpoint the fact that, due to the interactivity of the Internet technology, the authors are not necessarily fully cognisant of the impact of their online messages compared to the reaction they would observe if they were facing their victims or presenting them with a written page.

2. Section 1: the legal environment and its main principles

In order to face to all these risks, the EU and Council of Europe have promulgated regulations directly or indirectly aimed at protecting young people. As regards the first category the following texts can be identified:

- The Council Recommendation 98/560/EC on the protection of minors and human dignity in audiovisual and information services (1998) that makes recommendations and gives guidelines on the protection of minors
- This was followed by the *European Parliament and Council Recommendation 2006/952/EC on the protection of minors and human dignity and on the right of reply*, that takes into account recent technological developments and the changing media landscape
- The *Audiovisual Media Services directive* adopted in December 2007 which includes rules for the protection of minors
- The Council of Europe *Convention on cyber crime* (2001) which aims to facilitate international cooperation in the detection, investigation and prosecution of cyber crime
- This was followed by the Council of Europe *Convention on the protection of children against sexual exploitation and sexual abuse* (July 2007), which establishes forms of sexual abuse of children as criminal offences
- The *Council Framework decision 2004/68/JHA on child pornography* (2004) which sets out the minimum requirements for Member States in the definition of offences and appropriate sanctions concerning the production, distribution, dissemination, transmission, making available as well acquisition and possession of child abuse material. On 25 March 2009 the Commission published the text of a proposal for a revised Council Framework decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework decision 2004/68/JHA. This text is before the EU Parliament (see Brussels March 29, 2010, COM (2010)94 final)
- The Commission's communication COM (2007) 267, 22.5.2007 *'Towards a general policy on the fight against cyber crime'* aimed at strengthening operational law enforcement cooperation in the field of online child sexual abuse material, improving international cooperation.
- The Commission's communication COM (2006) 367, 4.7.2006 *'Towards an EU strategy on the Rights of the Child'* addresses internal and external policies on children's rights in a coherent way, fully consistent with the already existing Community action plans and programmes.
- The EU "Guidelines for the Promotion and Protection of the Rights of the Child" (Council Conclusions 16457/07, 12 December 2007) serve as framework for protecting the rights and integrity of children in third countries.

As regards the legislation indirectly relevant as regards the protection of children, one can list:

- The directive 95/46 on Data Protection and the more recent directive 2009 called the e-privacy directive deal with questions about processing of personal data which is a major issue in the context of the use by youngsters of web 2.0 applications. Article 29 working Party addressed in Feb. 2009 a Working Paper[16] analysing certain issues about the application of data protection legislations to this specific question. We might also refer to EDPS opinion on Safer Internet for Children.[17] Among a long list of questions, we list the following: First, to what extent the "consent" requirement might be used to legitimate processing about youngsters? On that point, the answer is unclear and perhaps it would be interesting to take example from the US

[15] See Y. Poullet, «La lutte contre le racisme et la xénophobie sur Internet», in *J.T.*, 2006, n° 6229, pp. 401–412, available on the website: http://www.droit-technologie.org/dossier-146/la-lutte-contre-le-racisme-et-la-xenophobie-sur-l-internet.html

[16] Working paper 160 already mentioned above.

[17] EDPS, Opinion on the proposal for a decision of the European Parliament and of the Council establishing a multi-annual Community programme on protecting children using the Internet and other communications technologies, June 23, 2008 (O.J. 7.1. 2009 (2009/C 2/02)).

COPPA legislation,[18] which imposes a requirement for parental consent as regards children under 13 years.[19] Second, it can be argued that the right to be anonymous has to be enacted quite strongly as regards children since in the context of the development of their personality it would be dangerous to keep data over their past and to infer there from certain information about their present personality? Other questions arise: can we forbid the profiling of users registered as under the age of 18?[20] Are youngsters to be viewed as data controllers in the context of Facebook applications or blogs containing data about relatives, friends or other people?

- The Directives on electronic commerce, on distance contracts[21] and so on are also relevant to children's activities on the net. So the question to what extent their consent might be considered as valid due to their minority remains questionable and solved differently by EU member state jurisdictions. Minors' use of e-payments in the case of electronic transactions can also be questioned. It needs to be stated that the 2005 Directive on unfair commercial practices[22] introduces the need to take into account the categories of population targeted when judging the unfair character of specific practices. That might be of interest in case of certain advertisements.
- Finally we have to consider the Directive on IPR and Internet,[23] particularly the Directive on a better reinforcement of the IPR in cyberspace[24] which gives the member states new tools for identifying and fighting illegal copies of protected materials.

Art. 29 WP in its opinion about privacy and protection of children identifies three major principles followed by such legislation and in general the regulatory initiatives coming from the European Union. The three principles might be developed as follows.

Best interest: *"The principle of best interest requires a proper appreciation of the position of the child. This involves recognising two things. First, a child's immaturity makes them vulnerable, and this must be compensated by adequate protection and care. Second, the child's right to development can only be properly enjoyed with the assistance or protection of other entities and/or people (family, society and state)"*. This clear recognition of parental, societal and public authorities' duties leads to the recognition of responsibilities as will be discussed below.

Special attention is reserved by recent texts to discuss the delicate question of young people profiling or "online preference marketing"(OPM).[25] As said above young people are uploading a lot of data on the web which might be of great interest for service providers or third parties, like employers or law enforcement authorities, for addressing targeted advertisements and/or taking decisions about them. The profiling techniques might be used in that context. That usage might lead to harm since the youngster is identified to a profile at a moment when his or her personality is not yet fixed resulting in possible harm to his or her development. Another point to be underlined is that this storage of past events in this life period might create prejudice since certain past bad actions might be stored which might consequently affect the judgement of third parties. That is why the right to be anonymous and to be

[18] "There is a United States federal law, located at 15 U.S.C. §6501–6506 (Pub.L. 105–277, 112 Stat. 2581–728, enacted *Children's Online Privacy Protection Act of 1998 (COPPA)* October 21, 1998). The act, effective April 21, 2000, applies to the online collection of personal information by persons or entities under U.S. jurisdiction from children under 13 years of age. It details what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities an operator has to protect children's privacy and safety online including restrictions on the marketing to those under 13. While children under 13 can legally give out personal information with their parents' permission, many websites altogether disallow under age children from using their services due to the amount of paperwork involved. This legislation is to be distinguished from the COPA, The *Child Online Protection Act (COPA)* was a law in the United States of America, passed in 1998 with the declared purpose of restricting access by minors to any material defined as harmful to such minors on the Internet. The United States federal courts have ruled that the law violates the constitutional protection of free speech, and therefore have blocked it from taking effect. As of 2009, the law remains unconstitutional and unenforced." (Wikipedia). The COPPA is in course of revision. FTC has launched debates about a certain number of questions to be addressed due to the Internet evolution and the way children are now using and accessing the Internet. On that debate and the issues identified by FTC, see FTC website (http://www.ftc.gov/opa/2010/03/coppa.shtm).

[19] In Europe, a child is defined as a person below the age of 18 years as in the UN Convention on the rights of the Child (UNCRC) of 20 Nov.1989 (see notably on that point the Communication from the Commission, *"Towards an EU Strategy on the rights of the Child"*, Brussels 4.7.2006, COM(2006) final).

[20] On that point see the Art. 3.5 of the recently adopted Council of Europe recommendation: "'The collection and processing of personal data in the context of profiling of persons who cannot express on their own behalf their free, specific and informed consent should be forbidden except when this is in the legitimate interest of the data subject or if there is an overriding public interest, on the condition that appropriate safeguards are provided for by law." (Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, adopted by the Committee of Ministers on 23 November 2010). *See also the Council of Europe recommendation's preamble*: "Considering that the profiling of children may have serious consequences for them throughout their life, and given that they are unable, on their own behalf, to give their free, specific and informed consent when personal data are collected for profiling purposes, specific and appropriate measures for the protection of children are necessary to take account of the best interests of the child and the development of their personality in accordance with the United Nations Convention on the Rights of the Child;"

[21] Electronic Commerce Directive of June 8, 2000 and Distance Contracts Directive of May 20, 1997.

[22] Unfair Commercial Practices Directive of May 11, 2005.

[23] Directive of May 22, 2001 on copyright and related rights in the information society.

[24] Directive of April 29, 2004 on the enforcement of intellectual property rights.

[25] FTC speaks about "OPM" rather than "profiling" because the process involves "collecting data over time and across Web pages to determine or predict consumer characteristics or preferences for use in and delivery on the Web".

forgotten[26] and the prohibition on the use of profiling for young people[27] must be proclaimed.

Adaptation and participation: *"Since the child is a person who is still developing, the exercise of their rights must adapt to their level of physical and psychological development. Not only are children in the process of developing, but they have a right to this development"*… and progressively to participate fully in the decisions concerning themselves and therefore to have their own privacy increasingly protected including against their traditional protectors (parents or educators). All sociological reports reveal that the use of Internet applications, the perception of risks and the negative impact as regards illegal or harmful materials considerably vary in function among the different age groups. Common sense tells us that a ten year old child has to be protected in a different way from someone who is 18 years old. Particularly it would seem that beyond 13 years of age, male users are better than female users in identifying risk; they are web 2.0 'experts' and develop strategies especially as regards the use of e-Id technologies for avoiding privacy threats. JRC report[28] pinpoints that they consider that the protection of their data is their own responsibility: *"They do not attribute responsibility for the protection of their data to governments or police and courts. Instead they are asking for tools that give them more direct control of their own identity and data"*. That consideration leads to a view that the adoption of stricter regulations, like the US COPPA, for minors 13 years aged or less is appropriate. In the same way it might be useful to consider the importance of systems verifying the age-appropriateness of users according to the financial or moral harm they might suffer. So it is important to distinguish between different age groups when child audiences are targeted, starting from a much younger age (6 years old) until the age of civil majority (18 years). For instance, to participate in auction platforms this must be restricted to youngsters of 16 years or more. As regards the legal validity of children's consent, it must be taken into consideration both the age of the minor and the economic value of the transaction. It is the responsibility of the service provider to ensure that their service are age appropriate for the potential audience and to take the needed precautions and measures in order to avoid any disproportionate risks. On the contrary we have to consider that certain minors, due to their age, ought to be viewed as adults since they are able to take their own responsibility therefore suggesting that their consent is valid.

As regards the *participation principle*, it means at the micro level that the point of view of minors must be heard through appropriate means. The recent debate launched by FACEBOOK about a new version of its privacy policy is an exemplar. It shows clearly that youngsters are concerned by the way the digital services are creating new risks and have certain ideas about the way to manage them. At the macro level and according to Art. 12 of the UNCRC (United Nations Convention on the rights of the Child), children need to express their views in dialog with other stakeholders on decisions affecting their life. It means that they must be represented in an appropriate manner in the different institutions in charge of defining Information society policies.[29]

Responsibility: Shared responsibilities must be established between all the actors following the principles of (i) the increasing responsibility of the children and (ii) the best placed actor for avoiding the damage or the cause of the damage suffered by children. The recently adopted Safer Social Networking Principles for the EU, drafted by SNS providers in consultation with the EU Commission in the context of the Safer Internet Programme "*Empowering and Protecting Children Online*", illustrates the concrete significance of this principle: "In order to achieve an appropriate protection, assignation of different levels of responsibilities and competences to different actors (multi-*stakeholders approach) is required*:

- *Parents, teachers and other carers: have an important role to play in both educating and fostering an ongoing dialogue with children and young people in their care about safe and responsible online behaviour*
- *Service providers should provide targeted, easily accessible and up-to-date information and tools to assist them in doing so. Providers should also explore ways to work with educators, governments and other stakeholders to create resources and other educational vehicles. They must cooperate with governmental authorities and provide to them an updating as regards the new applications developed.*
- *Governments and public bodies should provide children and young people with the knowledge and skills to navigate the Internet safely. Governments should ensure that e-safety curricula that accurately reflect current Internet services and behaviours are delivered in schools. Governments should also ensure that law enforcement agents and those working in the criminal justice system are equipped with the appropriate training tools and resources necessary to effectively combat criminal activity conducted online. Governments should work together to ensure that the frameworks for cross-border coordination are effective and efficient*
- *Police and other law enforcement bodies: should ensure that officers have appropriate and relevant training and resources for investigating and prosecuting the illegal use of online services. Service providers and law enforcement bodies should work collaboratively to share their knowledge of their services and to support investigations in line with applicable laws.*
- *Civil society: as a whole, and through bodies such as child protection agencies, youth organisations and, counselling services, should collaborate with SNS providers and governments through consultation, dialogue or working groups that address their mutual target groups and challenges online. Increasingly,*

[26] A. Rouvroy, «Réinventer l'art d'oublier et de se faire oublier dans la société de l'information?», in *La sécurité de l'individu numérisé. Réflexions prospectives et internationales.*, 2008, pp. 249–278.

[27] As it is the case in the Safer social network principles (on these principles, see hereinafter). Under these principles, SNS providers must "*take steps to ensure that private profiles of users registered under the age of 18′ are not searchable*". The same idea is submitted by the FTC.

[28] JRC Report mentioned above footnote, p. 58.

[29] As proposed by the Communication from the Commission (COM(2006))367 final: "*Towards an EU Strategy on the rights of the Child*". See also, the point 2.2 of the Annex 2 of the Safer Internet programme 2009–2013: "*Stimulating the involvement of children and young people in creating a safer online environment*".

social networking platforms are being harnessed by mental health, social care and support organisations to raise awareness, educate and to deliver counselling and support to young people online, a development which potentially has many positive outcomes."

Undoubtedly, children as users have to accept greater responsibility that increases with their progressive maturity. They have to respect the terms of use and other guidelines to the extent they are aware of their existence (or should have been since appropriate means to draw the individual's attention to them have been used by the service provider) and are able to correctly understand these documents. They must use the different tools and mechanisms offered to them for protecting themselves, people and communities in which they form part and participate.

3. Section 2: how the law is promoting different regulatory tools?: an inter-normative approach of the Children's protection

In order to achieve the protection of children, *four main complementary types of tools* are prescribed by European Institutions. At the EU level, the Safer internet Programme was recently renewed for the period 2009–2013.[30] This aims at empowering and protecting children and young people when in charge of the coordination, overview and assessment of all these relevant tools. Awareness definitively constitutes a first line of EU and Council of Europe concerns. All the texts about the topic mention the need to develop self-regulation and technological solutions (Children's Protection Enhancing Technologies, CPETS) as the most adequate way to formulate evolving and innovative ways to ensure the adequate protection. Complementary to this second approach is the need to better define and strengthen the liability of service providers, especially the new intermediaries such as the search engines, the Web 2.0 platform operators. This is clearly envisaged. Finally, the reinforcement of criminal provisions and the increasing LEA powers are considered as essential in last recourse to fight against the most serious infringements. Each of these means will be the object of the following relevant developments:

3.1. *Awareness*

Point 3 of the Safer Internet Programme addresses the issue in these terms: "*The activities will be aimed at increasing the awareness of the public*" by providing adequate information about risks and ways to deal with them. A major and positive role needs to be attributed to the schools through an adequate mandatory educational programme (need for teachers' education) and to ensure that what Council of Europe calls "Media Literacy" or "Info-competencies" is taught.[31] Besides that initiative, different actions are envisaged which are listed by the Safer Internet Programme: exchange of best practices, provision of contact points where parents and children might receive information about how to stay safe in an online environment, financial support for awareness tools, etc. The programme also underlines the obligation of each of the actors intervening in the provision of online services accessible for young people to deliver specific information related to the activities and services provided by them. The online public consultation[32] launched in the context of the preparation of the Safer Internet programme had proposed a lot of other actions, notably the involvement of public media (Press, radio, TV). The consultation countenanced the interesting idea of using peers for disseminating appropriate information about risks and solutions in the cyber community and suggested a "five steps approach" for specific target young people groups (i) Knowledge, (ii) Approval, (iii) Intention, (iv) Practice, and (v) Advocacy.

3.2. *Self and co-regulation*

Already, the 1998 recommendation on the protection of minors[33] considered that either self-regulation and/or co-regulation (to be defined as an effective mix of public and private initiatives) ought to be the pillars of an effective protection in cyberspace:

> *"The industrial sectors and parties concerned are encouraged to cooperate with the relevant authorities in setting up structures representing all parties concerned; the aim is to facilitate participation in coordination efforts concerning the protection of minors and human dignity on both a European and an international level; cooperate in drawing up* ***codes of conduct*** *for the protection of minors and human dignity applying to online services; develop on a voluntary basis new means of protecting minors and informing viewers; collaborate in the follow-up and regular evaluation of initiatives carried out on a national level concerning the application of this recommendation".*

[30] The 2009–2013 Safer Internet Programme (Budget 655 millions) has as ambition to tackle new issues like the raise of web 2.0 application, mobile technologies, infringements like grooming and cyber bullying. In order to ensure a better coordination and a better awareness between all stakeholders, the Programme sets up (Point 4) a "Knowledge Base" identifying all activities about online safety of young people.

[31] Recommendation Rec(2006)12, Sept 27 2006 empowering children in the new ICT environment *"Recalling Recommendation Rec(2006)12 of the Committee of Ministers on empowering children in the new information and communications environment, which underlines the importance of information literacy and training strategies for children to enable them to better understand and deal with content (for example violence and self-harm, pornography, discrimination and racism) and behaviours (such as grooming, bullying, harassment or stalking) carrying a risk of harm, thereby promoting a greater sense of confidence, well-being and respect for others in the new information and communications environment;" On that issue and the need to envisage differently the education to the use of new media, see our TIRO report, p. 266 and ff.*

[32] "*Safer Internet and online technologies for children*", Summary of the results of the online Public consultation and 20–21 June 2007 Safer Internet Forum Report, EU Commission, Report available on the Safer Internet website.

[33] Council Recommendation 98/560/EC on the protection of minors and human dignity in audiovisual and information services (1998). That assertion is repeated by a lot of other EU and Council of Europe documents, see on that issue the list proposed by us in the TIRO report (p. 239 and ff., footnotes 152 and ff).

The Council of Europe has the same preference for self-regulation[34]:

> "*Aware of self-regulatory initiatives for the removal of illegal content and the protection of users against harmful content taken by the new communications and information industries, sometimes in cooperation with the state, as well as of the existence of technical standards and devices enabling users to select and filter content; Desirous to promote and strengthen self-regulation and user protection against illegal or harmful content,*"

All official EU documents are promoting and stimulating at all the levels self-regulatory or co-regulatory initiatives.[35] For instance, on May 26, 2003, the EU Council decided to extend for two years the previous Decision and Action Plan for promoting the safer use of the Internet by combating illegal and harmful content on global networks. The Decision focused on the need to reinforce a certain number of actions, deemed as co-regulatory measures, insofar as their enforcement required the full support, including financial and administrative support, of the Member States. This included completing and improving the existing network of hotlines, ensuring cooperation between self-regulatory initiatives, development of quality site labels, benchmarking of filtering software and services, promotion of self-rating systems,[36] etc. So in particular the EU Commission "*has always supported of industry self-regulation which enables industry to create a system by which they can deal rapidly with any kind of new issues that might come on*".

A broad range of means might be developed in that perspective. One might distinguish different types amongst these means. Certain are aimed to produce norms so best practices and codes of conduct or companies' privacy policies or terms of use are defining the way the service provider will act. Others are developed to oversee whether the self-regulated bodies are effectively respecting their own commitments. On that point, labelling systems, rating systems or hotlines (mechanisms put at the disposal of users to report violations of terms of use by other users) have to be evoked. Beyond that, in case of evidence of non-compliance, initiatives like ADR (alternative dispute resolution mechanisms) or ODR (Online Dispute Resolution systems) might be set up by the actors themselves. Finally, infringements might be fought by internet blocking, or other penalties and that without the intervention of public authorities or jurisdictions.[37]

In the context of Safer Internet, two major co-regulatory initiatives[38] must be highlighted since they represent an original way to deal with the problems created by advanced applications:

- *European Framework for Safer Mobile use by Young Teenagers and Children (Feb.2007)* signed by mobile operators. This framework agreement promotes a self-regulated code of ethics for industry stakeholders. It contains principles and measures that the signatories commit themselves to implementing. It seems, according to a report published by the GSM industry, that 90% of the code has been enforced through national codes of conduct.
- *Safer Social Networking Principles for EU (Feb. 2009)* voluntarily adopted by the industry in February 2009 and signed by most of the major players. Seven principles are enacted through this code. These include: 1. Work towards ensuring that services are age appropriate; 2. Raising awareness of safety messages and acceptable use policies to users, parents, teachers, …, 3. Empowering users through tools and technology, 4. Responding to notifications of illegal content and conduct, … Furthermore it must be underlined that the document contains a "self-declaration form" which describes exactly the way by which the signatory plans to fulfil his obligations.

To what extent can it be said that these self-or co-regulatory solutions are valid from the legal point of view, to be considered as valid instruments and enforced as such by the judges in case of conflict. Previous papers[39] have elaborated upon the criteria of legal validity of self-regulation in the ICT environment and, taking fully into account the plurality of the norms,[40] we now propose three criteria, as follows[41]:

[34] Recommendation Rec(2001)8 of the Committee of Ministers to member states on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services) *(Adopted by the Committee of Ministers on 5 September 2001)*.

[35] Co-regulation is defined by the Inter-institutional Agreement "*Better Lawmaking*" concluded between EU Commission, EU Parliament and EU Council of Ministers (Sept. 18, 2003 as follows: "*Co-regulation means the mechanisms whereby a Community legislative act entrusts the attainment of the objectives defined by the legislative authority to parties which are concerned and recognized in the field*").

[36] See on that point, the Council of Europe recommendation on profiling techniques, already quoted: "*Member states should encourage the design and implementation of procedures and systems in accordance with privacy and data protection, already at their planning stage, notably through the use of privacy-enhancing technologies. They should also take appropriate measures against the development and use of technologies which are aimed, wholly or partly, at the illicit circumvention of technological measures protecting privacy*" *(Art. 2.2)*.

[37] See on that issue particularly the report on cross media rating and classification and age verification solutions, Safer Internet Sept 2008.

[38] The two self-regulatory texts might be found on the Safer Internet Programme website: http://ec.europa.eu/saferinternet.

[39] Y. Poullet, How to regulate Internet? New Paradigms for Internet Governance, in *Variations sur le droit de la société de l'information*, Cahier du Crid, p. 130 and ff. See also, C. Marsden (ed.), *Regulating the Global Information Society,* Oxford Institute, 2001.

[40] About the « pluralisme normatif », that is to say the multiple possible sources of the norms and their recognizance by the legal systems, see M. Coipel, Quelques réflexions sur le droit et ses rapports avec d'autres régulations de la vie sociale, in *Gouvernance de la société de l'information*, Cahier du Crid, Bruylant-Bruxelles, p. 44 and ff.; See also, M. Vivant, Cybermonde: droit et droit des réseaux, *Semaine juridique*, 969, 1996. L. Senden, SOFT LAW, SELF-REGULATION AND CO-REGULATION IN EUROPEAN LAW: Where Do They Meet? *ECJL*, 2005 available at: www.ejcl.org/91/abs91-3.html.

[41] Y. Poullet, "ICT and co-regulation: towards a new regulatory approach?", in *Starting points for ICT regulation. Deconstructing prevalent policy one-liners*, The Hague, TMC Asser Press, 2006, pp. 247–259 (Information Technology & law series; 9).

- "*Legitimacy*" is "source-oriented[42] and underlines the question raised by the authors of a norm and its transparency. To what extent, might the legal system accept a norm elaborated outside of the actors designated by the Constitution or under constitutional rules? This quality of the norm means that the authorities in charge of its creation must be recognised for their authority by the community or communities required to abide by the rule that has been enacted. This legitimacy is obvious as regards the traditional State authorities acting in conformity with the competence devoted to them by the Constitution. It is less obvious when the regulation is the expression of private actors as is the case with self-regulation, particularly when the latter comprise obscure associations or even private companies able to impose their technical standards. On that point we agree with the Safer Internet approach[43] since it insists on the participation of all the stakeholders mentioned above and it must be re-emphasised that the two documents just quoted have been discussed together by the industry, NG0 and the EU Commission. According to the Participation Principle, it would have been wise to enlarge at least from now on, the dialog with Children's representatives.
- "*Conformity*" is "content oriented" and designates the compliance of normative content vis-à-vis fundamental societal values; those embedded undoubtedly in the legal texts but also beyond that to ethical values that need to be taken into account by the legal system. Again this criterion is quite easy to satisfy and to verify in case of traditional texts issued by governmental authorities insofar as these texts take into consideration existing rules with superior values. It seems more intricate to satisfy this criterion when the compliance with existing legislative text is not systematically checked insofar as these texts are not existing or not clearly identified. Indeed self-regulation is often a way to avoid the traditional and constitutionally foreseen regulatory methods and procedures of rule-making.
- Finally, there is "*effectiveness*" which is "respect oriented". To what extent, will a norm be effectively respected by those to whom the norm is addressed? The questions about information, about the existence of norms, about the sanctions and the way in which they might be obtained are central for determining the effectiveness of a norm. By this criterion, one means that the addressees of a norm need to be aware not only of its content but also of the consequences of non-compliance by addresses who would otherwise be stimulated to follow the rule. The requirement of predictability of the norm emphasises that clear rules, easily accessible and made public by appropriate means, must be developed.

On that point, it is quite clear that technology, as Joel Reidenberg[44] has pointed out, and self-regulatory mechanisms like codes of conduct, labelling systems or ODR might produce additional ways to promote and enforce normative instruments.[45] On that issue, authors insist as to the need, according to article 6 of the C. of E. Human Rights Convention, for procedural fairness to be ensured.[46] In the case of the two above mentioned documents it is pitiful that nothing has been mentioned as regards the sanctions a company, signatory of the self-regulatory document will be subjected to for non-compliance.[47]

3.3. *Technological measures*

In addition to the other tools, technical solutions are considered to be essential. Effective mechanisms to trace, filter, analyse or block websites or individuals acting in an illegal or harmful way must be found in order to ensure effective protection within the cyberspace environment. Examples include: PICS solution with automated analysis of the content; automated systems of age control; and filtering systems with automated blocking of access to websites. In the alternative, technological measures might be implemented to ensure that young users surf safely on the Net. In regard to this issue E-id, allowing an anonymous surfing, encryption mechanisms, access control mechanisms or other PETS, …must be highlighted. Once again, the implementation of these various technological measures is clearly supported by the EU and C.

[42] See, on this distinction between "source-oriented tests", "content oriented tests" and "effectiveness-oriented tests", R. Summers, Towards a better general theory of legal validity, in *Rechtstheorie*, 1985, 16, p. 65 and ff.

[43] See also the permanent C of E request for a multi-stakeholder approach in the drafting and evaluation of the codes of ethics and other self-regulatory documents. On that requirement, H.J. Kleinsteuber, The Internet between Regulation and Governance, in *Self-regulation, Co-regulation and State regulation*, at www.osce.org/item/13570.html?ch=93, p.61 and ff.

[44] J. Reidenberg, Lex Informatica: the Formulation of Information Policy Rules through Technology, 76 Texas Law Rev., 1998, 553–593. On the same point, Y. Poullet, "Technology and Law: from challenge to Alliance", dans *Information quality regulation: foundations, perspectives, and applications*, Baden–Baden, Nomos Verlagsgellschaft, 2004, pp. 25–52; and definitively the LESSIG's fundamental reflections in "*Code and other Laws of Cyberspace*", New-York, Basic Books, 1999.

[45] See particularly, B. du Marais, Autorégulation, régulation et co-régulation des réseaux, in Le droit international de l'Internet, G. Chatillon (éd.), Bruylant, 2002, p. 296 et s. About the characteristics of the Internet which justify a self-regulatory decentralized approach rather than the traditional top–down approach based on a legislative and nationally bounded approach, see D. POST and D.R. JOHNSON, The New Civic Virtue of the Net, available at: http://www.stbr.stanford.edu/STLR/Working_Papers/97_Post1/contents.htm: "The ideal of national debate among wise elected representatives regarding the overall public good may be replaced, online at least, by a new architecture of governance that allows dispensed and complex interactions among groups of individuals taking unilateral actions and seeking more local goods and solutions. Instead of attempting to rely even upon the best of our democratic traditions to create a single set of laws imposed on the net from the top–down …".

[46] N. Suzor, The role of the Law in virtual communities, forthcoming *BTLJ*, 2011, p. 43 and ff.

[47] See in that sense the declaration in the Safer Social Networking Principles for the EU: "*While providers will support all seven principles, it is for each provider to judge where and how far they will apply the document's specific recommendations. These principles are aspirational and not prescriptive or legally binding, but are offered to service providers with a strong recommendation for their use.*"

of E.[48] *institutions*. To be more precise, it is recommended: (i) to empower users through tools and technology implementing protective solutions by default; (ii) to make a prior assessment to determine the technological measures to be implemented in relation to the services offered and the targeted audience; and (iii) to make recourse to protective measures, whenever it is reasonable to foresee potential damage.[49]

Beyond the call for robust and valid technological systems protecting children, it is conceivable, on the basis of what might happen within current privacy regulatory debates, that new ideas might be introduced that extend far beyond the limited sphere of data protection. Let us return to the privacy debates. Progressively, grounding their reasoning on the Preamble 2 Directive 95/46: "*Data processing systems are designed to serve man: (…) they must … respect their fundamental rights and freedoms, in particular the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of the individuals*": the Article 29 Working Party in its Opinion on RFID (Jan. 19, 2005) and the EU Commission's Recommendation of May 2009 are asserting a liability not only as regards data controllers or providers as specified in the Data Protection Directive but also as regards information systems designers and terminal equipment producers. It is their duty to embed in their products and in the design of their information systems the tools needed to comply with privacy legislation requirements.

This approach, called "Privacy by Design",[50] is thus based on some early thinking in the area first framed in French law in 1978 and recalled by the Recital 2 of the EU Directive 95/46: "*Information technology should be at the service of every citizen. Its development shall take place in the context of international cooperation. It shall not violate human identity, human rights, privacy, or individual or public liberties*". Based on these texts, Data Protection Authorities have consistently confirmed the principle that the responsibility for protecting the data of any users lies with the suppliers of terminal equipment and those creating the infrastructures, as they are responsible for the risks they have created. The DPA[51] and EU Commission[52] have gone a step further when dealing with the emerging RFID technology. In order to measure the privacy risks linked with the dissemination of RFID and its use, they have placed on the shoulders of the RFID operators[53] an obligation to "*conduct systematically an assessment of the applications and implementation for the protection of privacy* ***and***[54] data protection, including whether the application could be used to monitor an individual. The level of detail of the assessment should be appropriate to the privacy risks possibly associated with the application; take appropriate technical and organisational measures to ensure the protection of personal data ***and*** privacy; designate a person or group of persons responsible for a continuous assessment…; make available the assessment to the competent authority at least six weeks before the deployment of the application; (…)".

This obligation to produce a 'Technology Assessment' on privacy risks[55] and to make this assessment publicly and individually available constitutes, in our opinion, the first regulatory assertion of the necessity to take fully into account, at an early stage of conception of an information system, the privacy risks linked with the deployment of such technology. It is quite interesting to see how far this obligation will be enlarged to embrace all invasive and ubiquitous technologies that put people at risk and which will characterize our future Information Society.

To what extent this trend imposes data protection by design and a privacy assessment might be more deeply embedded in today's debate that it is currently. To what extent can it be said that by creating information systems affecting children in particular that the operator of these complex systems like SNS, Video service providers or mobile

[48] See particularly the Council of Europe Recommendation Rec (2001)8 of the Committee of Ministers to member states on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services), *Adopted by the Committee of Ministers on 5 September 2001*: 9. "*Member states should encourage the development of a wide range of search tools and filtering profiles, which provide users with the ability to select content on the basis of content descriptors*". 11. "*Member states should encourage the use of conditional access tools by content and service providers in relation to content harmful to minors, such as age-verification systems, personal identification codes, passwords, encryption and decoding systems or access through cards with an electronic code*".

[49] See for instance the Art. 27 of the Audio Visual Media Service (AVMS) Directive about content which might seriously impair minors.

[50] As asserted by Anne CAVIOUKAN, DPA Commissioner from Ontario (Canada) in its introductory remarks to the Privacy Guidelines for RFID Information Systems available on the website: http://www.ipc.on.ca: "*Privacy and Security must be built in from the Outset – at the design Stage*". Examples of privacy by design include the road per-use payment system proposed in DE JONGE and JACOBS ("Privacy-friendly electronic traffic pricing via commits", *Proceedings of the Workshop of Formal Aspects of Security and Trust (FAST 2008)*, Springer Verlag Lecture Notes in Computer Science, 5491) in which the car journeys are not sent to a central server for fee computation but kept on the on board computer (and still auditable in case of dispute). Another illustration of the approach is the ambient intelligence architecture put forward in Le METAYER ("A formal privacy management framework", *Proceedings of the Workshop of Formal Aspects of Securiy and Trust (FAST 2008)*, Springer Verlag Lecture Notes in Computer Science, 5491, pp 162–176) which involves "privacy agents" in charge of managing and protecting personal data.

[51] *Working paper on the questions of data protection posed by RFID technology*, January 19, 2005, WP No. 105 available on the European Commission website: http://www.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_fr.pdf.

[52] Commission Recommendation of May, 12, 2009 (C (2009) 3200 Final) on the implementation of privacy and data protection principles in applications supported by radio-frequency identification.

[53] The 'operator' is defined by the Commission Recommendation as '*the natural or legal person, public authority, agency, or any other body, which alone or jointly with others, determines the purposes and means of operating an application, including controllers of personal data using on RFID application*". It must be underlined again that this concept designates a category of persons broader than the 'data controllers' and might definitively target RFID information systems or RFID terminal producers.

[54] We underline. See infra, our conclusions.

[55] On "*Privacy Impact Assessment*", see R.Clarke, "Privacy impact assessment: Its origins and development, [2009] 25 *CLSR* 123 and ff. This article provides in two appendices a list of exemplars of PIA documents and references to guidelines describing different PIA methodologies.

operators[56] should be required to observe the same duties? Certain assertions present in documents we have referred to, clearly are going in this direction. So, in the Safer Social Networking Principles, the third Principle enunciates:

> "*Providers should employ tools and technologies to assist children and young people in managing their experiences on their services, particularly with regards to inappropriate or unwanted content and conduct. Service providers should make an assessment of what measures, to implement based on the services being offered* and the intended audience These measures that can help to minimize the risk… may include for example …".[57]

The importance given in the 2009–2013 Safer Internet Programme to the need for the operators and information systems designers to develop "*technical solutions for dealing adequately with illegal and tackle harmful conduct online*" illustrates the same concern.

If both technological solutions and self- and co-regulation might be considered as positive ways to deal with problems raised by the online services and bring adequate solutions to protect young people, their impact and validity in certain cases are questionable, since they might affect fundamental liberties. So the EDPS[58] has delivered a quite interesting opinion about the proposal submitted by the Commission concerning the new Safer Internet Programme and has underlined the absolute need to take fully into consideration the privacy issues of all actors, not only children when certain self-regulatory measures are taken. EDPS notably states that "*In an area where freedom of speech, access to information, privacy and other fundamental rights are at stake, the intervention of private actors raises the questions of proportionality of the means used*". Very recently[59] the EDPS questioned quite severely the possibility envisaged by the proposal for a Directive on combating the sexual abuse, sexual exploitation of children and child pornography already discussed, raising strong concerns about the envisaged enactment of voluntary action by Internet Services Providers to block the Internet pages on the basis of code of conduct and guidelines: "*The EDPS has in previous opinions expressed his concerns regarding the monitoring of individuals by private sector actors (e.g. ISP's or copyright holders), in areas that are in principle under the competence of Law enforcement authorities.*"

In the same line of argument the Council of Europe Recommendation (2008) on measures to promote the respect for freedom of expression and information with regard to internet filters denunciates certain negative impacts that Internet filters might have on freedom of expression.[60] Although generally supporting "voluntary and responsible use of Internet filters," the Council[61] agreed that filters could legitimately be deployed in public places such as schools or

[56] See as regards mobile operators, certain recommendations proposed by the EU Framework for Safe Mobile Use by younger Teenagers and Children: "*Individual mobile providers should offer capabilities which can be used by parents to customize access to content by children using mobiles….*".or "*Appropriate means to control access to content should also be applied where content is supplied by contracted providers of third parties, commercial content which would be classified as only suitable for adult customers in equivalent media*".

[57] The enumeration contains provisions about measures for forbidding searches concerning people registered as under age 18, setting the default for full profiling, giving users control over who can access their profile, giving users the option to pre-moderate comments of other users before being published on their profile.

[58] EDPS, Opinion on the proposal for a Revision of the EU parliament and of the Council establishing a multi-annual Community Programme on protecting children using the Internet and other Communication technologies. June 23, 2009, OJ 7.1.2009.

[59] EDPS, Opinion on the proposal for a Directive cn combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework decision 2004/68/JHA, May 10, 2010.

[60] Y. Akdeniz, Who watches the watchmen? The role of filtering Software in Internet Content regulation, in *Self-regulation, Co-regulation and State regulation*, available at www.osce.org/item/13570.html?ch=93 p. 101 and ff. See also, the US decision of the Supreme Court in Aschcroft Attorney General v. Aclu et al, June 2004 at http://supct.law.cornell.edu/supct/html/03-218ZS.html: "*Filtering software is not a perfect solution because it may block some materials not harmful to minors and fail to catch some that are*".

[61] "*In this context, member states should*:

i facilitate the development of strategies to identify content carrying a risk of harm for children and young people, taking into account the diversity of cultures, values and opinions;
ii. cooperate with the private sector and civil society to avoid over-protection of children and young people by, inter alia, supporting research and development for the production of "intelligent" filters that take more account of the context in which the information is provided (for example by differentiating between harmful content itself and unproblematic references to it, such as may be found on scientific websites);
iii. facilitate and promote initiatives that assist parents and educators in the selection and use of developmental-age appropriate filters for children and young people;
iv. inform children and young people about the benefits and dangers of Internet content and its filtering as part of media education strategies in formal and non-formal education.

Furthermore, the private sector should be encouraged to:

i develop "intelligent" filters offering developmental-age appropriate filtering which can be adapted to follow the child's progress and age while, at the same time, ensuring that filtering does not occur when the content is deemed neither harmful nor unsuitable for the group which the filter has been activated to protect;
ii. cooperate with self- and co-regulatory bodies in order to develop standards for developmental-age appropriate rating systems for content carrying a risk of harm, taking into account the diversity of cultures, values and opinions;
iii. develop, in co-operation with civil society, common labels for filters to assist parents and educators in making informed choices when acquiring filters and to certify that they meet certain quality requirements;
iv. promote the interoperability of systems for the self-classification of content by providers and help to increase awareness about the potential benefits and dangers of such classification models.

Moreover, civil society should be encouraged to:

i debate and share their experiences and knowledge when assessing and raising awareness of the development and use of filters as a protective measure for children and young people;
ii regularly monitor and analyse the use and impact of filters for children and young people, with particular regard to their effectiveness and their contribution to the exercise and enjoyment of the rights and freedoms guaranteed by Article 10 and other provisions of the European Convention on Human Rights".

libraries, but suggests that strict limits should be placed on such filtering to prevent it from becoming overbroad. Those limits are sensible. So we note that users must be able to signal when content is being filtered and have a simple way to challenge the accuracy of the filter. Manual overrides should be put in place when practical so that users can quickly obtain access to blocked material, etc.

Transparency about the filtering methods used; which criteria; which procedure for fixing these criteria; how the system functions; and who is responsible for it: i.e. who developed the filtering systems; who controls their functioning and what auditing methods are available all have to be ensured. This paper will return to the delicate question of the need for balance between different values and the need to protect children, on the one hand and the importance of respecting fundamental liberties like privacy or freedom of expression on the other.

3.4. *Liability*

As stated previously the new Internet applications, particularly Web 2.0 such as social network services and video posting or e-gaming services (for instance: YouTube, Dailymotion, Myspace, Facebook, Wikipédia blogs, Second Life) are the new intermediaries. Their responsibility in case of harm provoked by users of their services is questionable. Is Art. 14 of the e-commerce Directive, for example, which provides a large exoneration of liability for hosting services providers, applicable to these new categories of service providers? To solve that question, we must take into consideration that the service provided by these new categories of intermediaries is not limited to technical activities such as is true in the case of pure hosting providers. The limitation of activities grounded upon the specific regime of liability enacted by the article 14 and 15 of the e-commerce directive may not then sit so easily upon these new categories of intermediaries. Indeed the latter are classifying and storing received information and, according to that information, are either addressing advertisements to those users themselves or permitting third parties to do so who have entered into a contract with them, as well as putting at the disposal of users access to a certain number of applications that create additional risks for them and any other recipients of the information posted. It is submitted that, taking these additional activities into account, these new intermediaries bear more liability than hosting providers for their actions. It does not mean that they are liable each time a harmful or illegal content is posted and provokes damages. It is quite obvious that we have to fix this liability according to the means developed or required according to the specific service being delivered. So it is quite clear that if YouTube, who is responsible for classifying videos posted by its users, fails to block a priori access to videos with paedophilia content, that it will be liable for not having used adequate filtering and screening systems to control such postings. The same occurs if YouTube fails to use recognised systems for controlling the age of users and allows young people to access content rated as 'adults only'. The obligation to use appropriate and reasonable self-regulatory means and technical tools for diminishing the risks or for avoiding them is their responsibility and the failure to respect of this obligation should lead to their liability, unless evidence can be adduced that the use of these tools in the particular circumstances was not sufficient to avoid the harms incurred by the user.

What do we mean by 'appropriate self-regulatory measures and technological tools? The court might refer to codes of conduct, such as the principles enacted by the EU Safer Internet Programme as a "rule of art". It might also refer to standards developed by institutions like INHOPE or other recognised standardisation authorities.

Furthermore, it could well be that the service provider is liable under other specific legislation. For instance, an SNS provider has personal data controller obligations[62] to inform users about processing purposes and to use adequate security measures as regards the integrity, availability and confidentiality of the personal data. SNS has to obtain from the user his or her informed free and specific consent for marketing uses of his or her data. The access to the data stored including the profile must be offered through easy and user friendly mechanisms. The data must be deleted upon the termination of the contract concluded with the user. Under the e-commerce directive, certain information must be given about the service provider, advertisements must be clearly identified and access to the terms of use offered through easy to use mechanisms.

3.5. *Criminal provisions and LEA competences - major trends:*

"Prime responsibility for fighting against any illegal activities and illegal content, such a child sexual abuse material, should rest with the police. The capacity of law enforcement bodies need to be strengthened in this role so that they can take a more proactive approach and participate in cross-border cooperation such as in the organisation of more sting operations and in respect of hotlines and policy generally to combat online child abuse".[63] The recently adopted *Treaty on the European Union* underlines the importance of protecting children by enacting in its article 29:

> *"Without prejudice to the powers of the European Community, the Union's objective shall be to provide citizens with a high level of safety within an area of freedom, security and justice by developing common action among the Member States in the fields of police and judicial cooperation in criminal matters and by preventing and combating racism and xenophobia. That objective shall be achieved by preventing and combating crime, organised or otherwise, in particular terrorism, trafficking in persons and offences against children …"*

[62] On the SNS obligations see the Opinion 5/2009 of the Art. 29 W. P dated from June 12, 2009 on Social Networking, W.P. 163. The opinion contains a specific chapter on the problem of children.

[63] "*Safer Internet and Online Technologies for Children*", Summary of the results of the online public consultation, Safer Internet Forum report, EU Commission, June 2007. p.7.

The Framework Decision on the sexual exploitation of children and child pornography is in course of revision[64] and is an illustration of this trend towards a "*high level of security through measures to prevent and combat crime which includes child sexual abuses and child sexual exploitation*".

Three main points need to be emphasised as regards the increasing competence granted to LEA. First, new texts are enlarging the number of offences by criminalising new forms of abuse using the Internet. So, for instance, the amendments proposed by the Commission defines new criminal offences related to the use of IT such as online pornographic performances, or knowingly obtaining access to child pornography, even in cases where there is no downloading or storing of the images and thus without any "possession" traditionally required by the criminal provisions. It includes also the criminalisation of "grooming" activities, that is to say solicitation of children for sexual purposes. Second, based on the Council of Europe Convention on Cyber crime,[65] a better international cooperation between LEAs grounded on a common definition of offences is foreseen.

This cooperation constitutes an adequate answer to the global nature of the Internet. In the recently approved EU Youth Strategy (Council Resolution Nov. 27, 2009), the EU authorities anchor their policy into a global policy protecting children. This strengthened and duly established cooperation between LEA is regarded as absolutely necessary when the offending content is located or removed to websites outside of EU. The proposal to allow blocking of websites with child abuse content, developed by the EU Commission, responds also to the concerns raised by the global character of the Internet. Another suggestion is to create interoperable national databases of websites containing child pornography materials. Third, as regards investigative methods, cooperation between e-communications service providers and certain service providers like SNS on the one hand and LEA on the other is foreseen by legislative provisions or by codes of conduct.[66] Furthermore, the obligation for e-communication services providers to keep storage of traffic data during a period between six months and two years as prescribed by the Directive on Data retention[67] will facilitate the investigation of LEA.

Certain of the extensions to these LEA prerogatives raise questions as regards the respect of fundamental liberties, particularly privacy, freedom of expression and human dignity. EDPS[68] commented quite forcefully about the Safer Internet Programme for children as follows:

> *"The European Parliament has recently adopted a Resolution[69] stressing the need for a solution in compliance with the fundamental Rights of individuals. In point 25 of its resolution, it states that 'the Internet is a vast platform for cultural expression access to knowledge and participation in European creative, bringing generations together through the information society, the Parliament calls on the Commission and the Member states to avoid adopting measures conflicting with civil liberties and human rights and with the principles of proportionality, effectiveness and dissuasiveness, such as the interruption of the Internet'. The EDPS considers that a balance has to be found between the legitimate objective to fight against illegal content and the appropriate nature of the means used. It recalls that any action of surveillance of telecommunications networks, where necessary in specific cases should be the task of law enforcement authorities."*

What EDPS has clearly in mind is what authors call the "public order clause" which seeks to balance conditional fundamental freedoms such as the liberties or human rights mentioned above with the rights or interests of third parties. For instance, if a blocking measure is envisaged against a child having violated a copyright, the judge according to the Council of Europe Convention, will need to assess to what extent a child's right to freedom of expression and to privacy might be counterbalanced by the violation of the IPR of the author? To solve that problem, a three step evaluation is needed for validating the interference with conditional human rights[70]:

- respect for the principle of lawfulness constitutes the first condition: the Law must be accessible and a norm cannot be viewed as a law if its content is not formulated with sufficient precision to enable people targeted by the law (which might be *in casu* a child) to regulate his or her conduct. It is of course true that only public regulation and not self-regulatory measures can hinder or limit the exercise of a freedom;
- the obligation to pursue a legitimate aim is a second criterion of the validity of any interference. So it might be

[64] Council Framework Decision 2004/JHA of Dec. 22, 2003 on the sexual exploitation of children and child pornography. See the Commission proposal for a Council framework decision combating the sexual abuse, sexual exploitation of children and child pornography, March 29, 2010, See also the Council of Europe Convention CETS, n°201 on the protection of children against sexual exploitation and sexual abuse which is at the basis for the improvements suggested by the Commission.

[65] Council of Europe Convention on Cybercrime STS n°185, Nov. 15, 2001. It is quite interesting to denote that this Convention is opened to the signature of non member states of the Council of Europe. US and Japan for instance have ratified the CoE Convention which might be considered more and more as an international global standard. That situation allows an international cooperation far beyond EU or even Council of Europe countries.

[66] See Principle 5 of the Safer Social Network Principles (already quoted): "*Service providers should have in place arrangements to share reports of illegal content or conduct with relevant law enforcement bodies and/or hotlines… Providers may consider including links to other local agencies or organisations, for example relevant InHope services and LEA…*"

[67] Directive 2006/24/EC of March 15, 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

[68] EDPS, Opinion already quoted sura footnote 54.

[69] European Parliament Resolution, April 11, 2019 on cultural industries in Europe (2007:2153 (INI) point 25).

[70] About a similar approach, read C. Callanan et al, *Internet blocking balancing cybercrime responses in democratic societies*, Report prepared within the framework of Open Society Institute Funding, 2009, 33 pages.

considered that certain measures, especially blocking measures, will only be taken if the aim is to protect the sensibilities of weaker persons like children, but in that case the restriction must target only children and not other adults.
- The last point concerns the principle of "necessity in a democratic society"; what the Court of Strasbourg has defined as responding to a pressing social need and proportionate to the legitimate aim pursued, that is to say that no alternative, less intrusive, or limited incursion upon liberty is possible.

4. Conclusions

Let us try to summarize the reflections in this paper. Definitively we have tried to demonstrate that privacy, as a capability and condition for self development in a democratic society, might be seen as the 'red thread' operating throughout the analysis. We consider that even if children (or young people) are vulnerable, due to their immaturity, access to the Internet and its multiple applications do represent an essential tool for the development of their personality. Information Communication Technologies (ICTs), with their ubiquitous and universal characteristics, are drastically modifying our environment as well as our economic and social relationships. This trend will increase in the future in a way which is only partially predictable at this time. ICT are used in an increasing number of contexts and are offering to each of us a place without limits where we are able to better express ourselves, where we have access to more and more personal services, but also where the physical or social barriers which separated the various visions of the world tend to disappear. In this sense, ICTs create a unique opportunity to develop ourselves and to enter into a dialog founded on the recognizance of a large diversity of opinions. This might contribute to a cultural, economic, intellectual, democratic and human enrichment of the global society. Even if restrictions to that access are needed for obvious reasons and if protective measures have to be taken, these restrictions and protective measures must be limited according to the proportionality principle and definitively a positive approach fostering awareness and participation of youngsters.

Having recalled that fundamental privacy concern, we have tried to demonstrate that the EU policy is founded on threefold approach characterized as follows:

- A multi-stakeholder approach
- A multi-normative approach taking fully into consideration and assessing the technological landscape and applications
- The fundamental roles of the State not only to promote the dialog between all these stakeholders and to encourage them to fix appropriate and evolving rules for the virtual communities. Overall, beyond that, to recall our fundamental liberties including those in development as regards young people and therefore the need for their protection, to fix by sound compromise the problem whereby liberties are in conflict and foster continuously its maintenance as an evolving context.

As SUZOR[71] concluded "*So too, in virtual communities, the* boundaries of private law doctrine mediates the relationships between participants and providers (as they do in disputes between participants and non participants). The rule of law, as a discourse that emphasises the legitimacy of governance and appropriate limits on the exercise of power, provides a useful framework as a first step to reconceptualising and evaluating these tensions in communities at the intersection of the real and the virtual, the social and the economic, and the public and the private."

"*Why we need lawyers?*" becomes obvious at the end of these findings. Law has not to be regarded as a system intervening only for sanctioning. Law is the appropriate tool for creating the conditions of the dialog between all interested people in children's protection, to promote both a multi-normative methodology at the service of such protection. Meanwhile, the law has to sustain overall control of these other means for maintaining the conditions for progress within the limits imposed by the fundamental principles and liberties of our democratic societies, while paying attention to their effective enforcement.1

Yves Poullet *(yves.poullet@fundp.ac.be) Member CLSR Editorial Board, Former Director CRID (University of Namur) Professor at the Faculties of Law and Rector, University of Namur, Belgium.*

Based on a paper presented at the e-Youth conference 2010: http://www.ucsia.org/eyouthAntwerpen, May 27–28 2010.

[71] N. SUZOR, article quoted above footnote 45, p. 52. See on the same point, M. Risch, Virtual rule of the Law, draft available at: http://ssm.com/abstract=1463583: "*Market based regulations such as contracts lack neutral and consistent enforcement mechanisms. Code based constraints are often implemented arbitrarily and without notice. Community norms are often vague, unwritten and are enforced by mob rules. Autonomous self-regulation is too complex and costly. Real world laws, no matter how clear and impartial in real space, do not have a history that gives any confidence about how they might apply in the virtual activity*".