Children and teenagers on social networks: a Latin American and Caribbean perspective¹

Carlos G. Gregorio
Instituto de Investigación para la Justicia, Argentina

Introduction

Protecting the rights of children and adolescents on digital social networks (and generally-speaking within the context of the new communication and information technologies) is a worrying issue and a concern that is accompanied by some tragic stories and poor expectations in terms of control in some parts of the world. Two entirely opposite points of view are emerging; some see a world of opportunities while others become anxious over the resulting conflicts and use of their personal data. However, the strongest reaction concerns a warning about the risks and vulnerability of children and adolescents in cyberspace; almost everyone agrees on the need for education, prevention and legislative reforms that provide a degree of regulation. On more than one occasion arguments have been heard claiming that children and adolescents (and the sympathy surrounding the promotion of their rights) are being used as a vehicle that, in short, would result in the destruction and withdrawal of the free space that has been created (through numerous Internet applications) where the main expectation is the utmost manifestation of the freedom of expression.

Analysing this predicament is not easy; not only because of the complexity involved in establishing a balance between children's rights, personal data protection and freedom of expression but also because public expectations (of a varying nature depending on the country) exert a range of different emphases and demands.²

This paper will attempt to present an optimistic view of the problem, trying to include the arguments with the most weight in the debate and fundamentally arguing that a balance to satisfy all interests is not impossible if a certain degree of research and creativity is applied in a participatory manner.

¹ This paper makes numerous references to the conclusions of a research project entitled *Rights and justice on digital social networks* [Derechos y justicia en las redes sociales digitales], funded by the International Development Research Centre (IDRC) and the Canadian International Development Agency (CIDA).

² In some countries, social demand is for proxies or mechanisms to avoid the censorship that some governments intend to impose on certain ideas and certain websites. In other countries, the demand is for filters so that certain content is not accessible to children and adolescents (depending on the content in question) or for certain websites to be blocked in accordance with applicable legislation, such as child pornography, and even some online casinos to be blocked because they evade tax laws.

1. Freedom of expression

New technologies have generated a great deal of expectation since their appearance and expansion. Among these expectations is a broader right to express oneself, to communicate, to access knowledge and public information and to receive less costly services that are less susceptible to corruption. Significant progress has been made in many of these fields. Freedom of expression has enjoyed its fair share of this progress, which has essentially created the need for new balances to be found, particularly regarding one's right to a private life, the protection of personal data and the rights of children.

One important example of the tension and the need for a balance between freedom of expression and the rights of the child can be found in the case of Free Speech Coalition v. Ashcroft, 535 U.S. 234 (2002) in its ruling of 16 April 2002 by the US Supreme Court. The legislation in question was the Child Pornography Prevention Act of 1996 (CPPA), 18 U.S.C. § 2251 et seq., which extended federal prohibitions on child pornography to sexually explicit images in which child representations were produced virtually, without the participation of a real child.

The Government argued that virtual child pornography fed the appetite of paedophiles and encouraged them to become involved in illegal conduct. This argument was not accepted by the judges due to the reasoning quoted below:

"The Government may not prohibit content because it increases the possibility that an unlawful act may be committed "at some indeterminate future time." Hess v. Indiana, 414 U.S. 105, 108 (1973) (per curiam). The Government may suppress content for advocating the use of force or a violation of the law only if "such advocacy is directed at inciting or producing imminent lawless action and is likely to incite or produce such action" Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (per curiam). Here there is no attempt, incitement, solicitation or conspiracy. The Government has shown no more than a remote connection between content that might encourage thoughts or impulses and any resulting child abuse. Without a significantly stronger, more direct connection, the Government may not prohibit content on the ground that it may encourage paedophiles to engage in illegal conduct."

The expression "significantly stronger, more direct connection" is used in the text in an attempt to paraphrase the ruling.

A clear sign of the tension is that the PROTECT Act (Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act) was sanctioned one year later, which establishes criminal sanctions on the production, distribution, receipt or possession of sexually explicit representations of a child, whereby it is not required that the child present in the images actually exists³.

 $^{^3}$ 18 USC Section §1466a. The regulation expressly includes when such representation is a cartoon and has generated the same reaction as the previous regulation. In Brazil, Law 11,829 establishes criminal sanctions in the event of simulated images and a difference of opinion exists regarding its application to cartoons. However, it has been established that cartoons with explicit scenes are used by pederasts to get close to and prepare their victims (grooming).

2. Exploratory studies regarding children and adolescents online

The US Supreme Court ruling in 535 U.S. 234 (2002) Free Speech Coalition v. Ashcroft allows a standard to be inferred in some way to establish the balance that should exist between the freedom of expression and the rights of the child in the sense that the mere chance of generating a risk is not sufficient but rather that it would be necessary, for example, for there to be a direct and significantly strong connection between an application aimed at facilitating the freedom of expression and the risk for children and adolescents.

The Internet concept as a space of freedom is present in many ideological and commercial arguments and has been directly expressed in numerous forums, such as the debates in the Internet Governance Forum where certain attempts at regulation were described as indirect censorship.

In a recent study, Gasser, Maclay and Palfrey analysed the online vulnerability of children and adolescents according to the country from which they access the Internet.⁴ The focus of the study accepts the existence of a wide range of new opportunities for children and adolescents in new technologies but also makes an exhaustive analysis of the risks that were detected. The study repeatedly highlights that there is a great deal of anecdotal information and one-off cases that have been picked up by the press but that very little data has been systematically obtained.

The study also contains an underlying hypothesis postulating that the risks for children and adolescents in industrialised nations are not the same as the risks for children in developing nations. Within this area of the study, a series of considerations arise (such as those that refer to "highly contextual risks" and a series of "tragic stories covered by the press") that are complemented by the weakness of the rule of law and the lack of robust institutions. The arguments basically point to a need to gather empirical data on victimisation in order to justify an effect on the balance between the rights of the child and other fundamental rights (and eventually the freedom of expression).

It is true to say that the risks for children and adolescents in the use of new information and communication technologies are not new risks but rather, for the most part, a redistribution of pre-existing risks that now affect different populations to different degrees and are fundamentally expanding within an atmosphere of excessive trust and, therefore, less caution and prevention. For this reason, security policies are more critical in developing nations, given that local risks are compounded by global risks, and the meagre local prevention measures receive little support from industrialised nations.

Although it is true that there are insufficient data to appreciate the full extent of the victimisation that is generated online, which can be seen to be affecting the real lives and rights of children and adolescents, on the other hand there are many cases to be found in the courts, claims made to child protection agencies and stories reported in the press. It can also be felt that empirical data will not be forthcoming from developing nations in the short term (for various reasons) and that a response from the law, the governments and civil

⁴ URS GASSER, COLIN MACLAY & JOHN PALFREY, "Working towards a deeper understanding of digital safety for children and young people in developing nations: an exploratory study by the Berkman Centre for Internet & Society at Harvard University, in collaboration with UNICEF" (16 June 2010).

society is being delayed, probably due to the existence of higher priorities.

There is also debate surrounding the ways in which the risks and preventative measures should be considered legally (to a certain extent as nascent as they are polarised) in developing nations. It would seem essential that they be examined in order to define the precise nature of the public policies to be developed, but it is always difficult to seek local solutions to global problems.

2. Sound estimates and cases that reach the courts

As part of a research study that began in 2009, supported by the European Union and undertaken by the London School of Economics and Political Science, an exhaustive study was performed in 25 European countries that included questionnaires and face-to-face interviews of more than 23,000 children aged between 9 and 16, and their parents. Conversely, there have been very few studies in Latin America and the Caribbean of a similar nature. Probably the most similar study is the one performed by SaferNet of Brazil in 2009 in three Brazilian states, as well as other studies restricted to limited areas in other countries.

More limited studies have been performed in Latin America and the Caribbean however, but they have been used "to listen to children and adolescents" in their perception and opinion regarding the use of new technologies. Although it is recognised that this type of empirical study and estimation based on representative sampling does throw light on a complex reality and are of great use in the decision-making process, when looked at from the perspective of certain developing nations, they seem somewhat unworkable due to the magnitude of economic resources and regional coordination required but not available in those countries. However, a comparison of results from studies completed in other regions reveals more similarities than discrepancies.

One of the greatest issues and concerns regarding carrying out this type of study is the way in which Internet accessibility and applications are constantly changing. For example, it is known from the studies performed in Latin America and the Caribbean that cybercafés (public spaces of a mainly commercial nature) play an important role in access to the Internet. However, the use of mobile telephones in Latin America and the Caribbean has possibly achieved greater penetration than in the industrialised nations and it is expected that access to social networking applications will relocate to mobile telephones over the coming years. Furthermore, the applications used by children and adolescents are rapidly changing, whether this be due to the offer of new functionalities or the regional dominance gained over time by each particular offer.

These changes are too fast and significant to assume that the data obtained from interviews and surveys can maintain their validity over time. Furthermore, the cost of these studies (already significant for

 $^{^5}$ Sonia Livingstone, Leslie Haddon, Anke Gorzig & Kjartan Olafsson et al., "Risks and safety on the Internet: the perspective of European children (initial findings from the EU Kids Online survey of 9-16 years old and their parents" (21 October 2010).

⁶ SaferNet and the Federal Public Ministry, "Relatório da pesquisa online no Estado do Pará: hábitos de navegação na Internet; será que nossos alunos e educadores navegam com segurança na Internet no Estado do Pará?" and similar for the States of Rio de Janeiro and Paraíba.

such regions as the European Union) becomes prohibitive for regions with fewer resources and even more so if they need to be updated in the face of new technological scenarios.

In some way, it seems impossible to speak (at least in the short term) about sound estimates of the risks and perceptions of children and adolescents online, and less so if a certain continuity over time is sought.

In addition, a series of conflicts have arisen in Latin America and the Caribbean that have reached the courts, the public authorities, the police, the child protection agencies and the lines or websites used to report incidents⁷. All these mechanisms receive the most serious expressions of vulnerability and certainly fuel the debate for much more drastic reactions and political proposals. It is also true that many more conflicts remain hidden from view, whether due to a lack of trust in the reporting process (which tends to victimise the victims even more and generally provides very few solutions) or because many of the victims are unaware of their condition (in many cases, vulnerability is associated with silent discriminatory attitudes, some of which will happen in the future while others will simply never be felt).

3. The Memorandum of Montevideo

Despite the fact that the situation of children and adolescents online in Latin America and the Caribbean has very few fundamental differences from the situation existing in other regions of the developing world, there are certain factors that become more relevant when defining public policies.

By June 2009, the situation of children and teenagers online had generated sufficient concern at a global level as to generate various regional actions and documents defining principles and formulating recommendations.

Within the social, cultural, political and legislative diversity that exists in each region, it is possible to refer to the following documents: Acordo que põe fim à disputa judicial entre o Ministerio Público Federal de Brasil e a Google (of 1 July 2008)8; the Child Online Protection Initiative by the International Telecommunications Union (of 18 May 2009)9; Opinion 5/2009 on online social networking from the European Article 29 Working Party (of 12 June 2009)10; and the Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. 11 / Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. (of 16 July 2009)12.

In light of these documents, the idea has arisen to produce a specific document for Latin America and the Caribbean that is in line with the

⁷ Such as the complaint website SaferNet Brasil (<u>www.safernet.org.br</u>) or the website of the Colombian cyber police (www.delitosinformaticos.gov.co/ChatDicri/).

^{*} http://www.prsp.mpf.gov.br/sala-de-imprensa/noticias prsp/noticia-7584/?searchterm=google

http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html

¹⁰ http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163 es.pdf

http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm

¹² http://www.priv.gc.ca/cf-dc/2009/2009 008 0716 f.cfm

progress already made in other regions and at an international level but also applying certain factors that are specific to the region, mainly related to the characteristics of developing nations.

The Memorandum is the result of an initiative from the "Derechos y Justicia en el movimiento social en Internet" project [Rights and Justice in the Internet social movement] coordinated by the Instituto de Investigación para la Justicia in Argentina and which received funding from the International Development Research Centre and the Canadian CIDA. In order to document the unique characteristics of the region and in order to listen to the voice of children and adolescents (the most vulnerable victims but not necessarily the only victims), six field research programmes were initially undertaken in Argentina, Brazil, Colombia, Costa Rica and Peru¹³.

Based on these studies, following analysis of the above-mentioned documents, and after an exchange of opinions with authorities on the topic, a seminar-workshop was organised in the city of Montevideo to discuss and come up with a series of recommendations for the public policy managers in the region. Experts on personal data protection, the rights of the child and the management and regulation of new technologies were involved in the work with backgrounds in academia, the public sector, as experts for international bodies, judges and public policy-makers.

The result was the Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes¹⁴ [Memorandum on the protection of personal data and privacy on Internet social networks, specifically in regard to children and adolescents], perhaps interpreting that the protection of data is the first step towards a comprehensive guarantee of rights.

The Memorandum is intended for use as a document to seek consensus, with an authority deduced merely from its rationality; essentially a non-binding body of law (a *soft law* to use modern terminology) that may be capable of guiding all public and private actors, including industry, in the immediate future.

It begins by stating that the Internet and the Knowledge Society represent extraordinary progress, a window of opportunity for access to information and knowledge, for communicating, participating and exercising freedom of expression. In this respect, tackling the risks and vulnerabilities is seen as a necessary task. Without express mention thereof, the Memorandum was structured according to the consensus felt in its recommendations. Firstly, a recommendation was made regarding preventative and educational actions for safe and responsible use of new technologies. Secondly, the development of programmes to support victims is believed to be of an urgent nature. In this regard, a legislative solution and suitable institutional framework is not discarded but the need to receive collaboration from

¹³ SERGIO BALARDINI and other authors from the CHICOS.NET Association, "Hacia un entendimiento de la interacción de los adolescentes con los dispositivos de la web 2.0. El caso de Facebook". Laura León Kanashiro "Adolescentes y web 2.0: privacidad y riesgos"; Zareth Díaz García and Raúl Rojas Niño; "Significados e implicaciones del protagonismo sexual de los adolescentes de provincia en internet"; Milena Grillo River, Jeannette Durán Alemán and Walter Esquivel Gutiérrez, "Expresiones de violencia interpersonal y social en el ciberespacio desde la vivencia adolescente: estado del arte de la investigación' in "Datos personales y libertad de expresión en la redes sociales digitales", F. Barindelli and C.G. Gregorio (eds.) Ad-Hoc, Buenos Aires (2010).

industry in order for those corrective measures deemed necessary to be applied without delay was confirmed.

4. Vulnerability and risks in Latin America and the Caribbean

The term 'contextual risks' would seem at first sight to be appropriate for the reality in Latin America: poverty, weak institutionality, Internet access mainly from cybercafés and a concept of anonymity that is usually viewed in the region with ties to impunity, among other characteristics that are specific to developing regions. Within this context of uncertainty, certain Internet applications (such as social networks) are viewed as a globalised abstraction.

On the other hand, the region of Latin America presents the highest rates of expected growth in terms of connectivity, Internet use and adhesion to social networks and other applications. Mobile telephony, which is not altogether unrelated to these issues, is also experiencing exponential growth in the region, particularly pay-as-you-go mobile telephony. As an additional note, there are almost as many mobile telephone lines as there are inhabitants in some countries of the region.

Using a more analytical risk map, it is possible to ask whether certain Internet applications have intrinsic risks and whether it is possible to settle for a definition of "contextual" regarding all the risks that are found to be present. One alternative hypothesis consists of considering the conjunction of intrinsic risks with contextual risks that can explain many of the events witnessed in the region.

In order to explain this conjunction, it may be worth mentioning a series of conflicts that have arisen in recent years in Brazil and that are associated with the use of the *Orkut* social network. These conflicts have resulted in a series of both criminal and civil legal proceedings¹⁵. Initial reactions from the Public Ministry in Brazil arose after discovering that *Orkut* was being used to share images of child pornography, a situation that was later investigated by the Federal Police in Brazil. The large number of offences identified within the context of *Orkut* and the criminal actions arising therefrom led the company Google to sign an agreement with the Federal Public Ministry and with the organisation SaferNet to collaborate with the authorities (under the threat of significant fines) in stamping out these offences¹⁶.

At the same time, a series of civil actions were brought in Brazil, the majority of them for defamation, personal image rights and some for child pornography, in which Google was sued for pain and suffering 17 .

 $^{^{15}}$ The Orkut social network is owned by Google and is mainly used in Brazil and India.

¹⁶ See www.safernet.org.br/site/sites/default/files/TACgoogleMPF_0.pdf, Termo de a ajustamento de conduta, entre La Procuradoria da Republica no Estado de São Paulo, Google Brasil Internet Ltda. e SaferNet Brasil (2 July 2008)

 $^{^{17}}$ Similar actions were brought in Argentina, several years earlier, such as S. M. y L. E. v. Jujuy Digital y Jujuy.com, but in much lower numbers, relatively-speaking. The difference lies in the greater degree of access to justice that exists in Brazil, which enables action to be brought for significantly lower sums of compensation.

These legal actions all share a number of characteristics: (1) they are brought in small claims courts known as *Juizados Especiais* in Brazil, without formalities, they do not require the presence of a lawyer and there are no legal costs. The claimant files a claim against a user of *Orkut* who is only known by a nickname or pseudonym and in a subsidiary nature against Google in order for the same to reveal the identity of the user; (2) the judge instructs Google to report the identity of the user behind the nickname or pseudonym under threat of a 5,000 Brazilian Real fine per day until such information is provided¹⁸.

To begin with, Google claimed that the users accepted the US courts when signing up as users of <code>Orkut</code>. The response to this from the Brazilian justice system was that such acceptance was void and that the jurisdiction of the Brazilian courts is absolute. Secondly, Google do Brasil (against whom the actions were brought) argued that it simply acts as a representative. The Brazilian justice system replied that the use of the name Google and its capacity of representation, as well as the capacity to collect payment for advertising services provided, made it jointly liable and therefore the subject of any action.

In a significant number of cases, Google do Brasil has been unable to identify the individual behind the social network profile. In these cases, the judges ruled against Google do Brasil, ordering it to pay compensation for pain and suffering, which amounts to approximately 10,000 Brazilian Real per case.

At the time of drafting the Memorandum, it was appreciated that both processes in Brazil (civil and criminal) represented one of the most noteworthy experiences in Latin America and was decisive in the signing of partnership agreements between the company Google and the legal authorities. For that reason, the chapter entitled "Recommendations on the Application of the Law by the State" included the following paragraph:

10.1. ... The use of strict liability is to be strengthened as a form of regulatory mechanism for guaranteeing fundamental rights in the applications of the Information and Knowledge Society, Internet and online social networks. Judicial penalties that can be applied to the derived damages have the advantage of being a quick, efficient response capable of dissuading dangerous designs. This type of civil liability is founded on the child's best interests. ¹⁹

 $^{^{18}}$ This is an average fine. There is some variation from one court to another. It is the equivalent of some 2,000 euros per day. Google do Brasil is not always the defendant in these cases. There have also been cases against Fotolog and Facebook, and against individuals when they have been identified. ¹⁹ Clearly inspired by the 'Declaration of principles on freedom of expression' approved by the Inter-American Commission on Human Rights (October 2000): "10. Privacy laws should not inhibit or restrict investigation and dissemination information of public interest. The protection of a person's reputation should only be guaranteed through civil sanctions in those cases in which the person offended is a public official, a public person or a private person who has voluntarily become involved in matters of public interest. In addition, in these cases, it must be proven that in disseminating the news, the social communicator had the specific intent to inflict harm, was fully aware that false news was disseminated, or acted with gross negligence in efforts to determine the truth or falsity of such news". [Approved during the 108th Ordinary Period of Sessions of the IACHR]. Source: http://www.cidh.oas.org/declaration.htm

This paragraph mentions several concepts that are necessary in order to analyse the regulatory framework. Therefore, the following is considered relevant: (1) the recommendation is limited to those cases in which a child or adolescent is the victim; (2) the term 'dissuade dangerous designs' alludes to liability for specially designed products and not simple liability for content.

In this regard, the most recent legal rulings in Brazil base their decision on a dangerous design (liability for specially designed products) found by the judges in the Orkut application, in short when seeing that absolute anonymity was violated, and on the fact that the application is a lucrative activity for the company²⁰.

The arguments from Google against the judicial rulings in Brazil refer to Section 230 of the US Communications Decency Act, in which the service providers are immune to judicial action for content - called protection for the good Samaritan²¹. However, the rulings in Brazil are for liability for specially designed products, applications that include the possibility to operate in an anonymous fashion, and not necessarily for any specific content. It should also be considered that the Political Constitution of Brazil guarantees freedom of expression but excludes anonymity.

Article 5. All persons are equal before the law, without any distinction whatsoever, Brazilians and foreigners residing in the country being ensured of inviolability of the right to life, to liberty, to equality, to security and to property, on the following terms: ... 4. the expression of thought is free, and anonymity is forbidden; 5. the right of reply is ensured, in proportion to the offence, as well as compensation for property or moral damages or for damages to the image;

It is also said that a system of civil sanctions could create indirect censorship and the consequent loss of freedom of expression. However, the amount of the compensation paid in Brazil is relatively moderate and could be interpreted as a gentle incentive to improve security conditions in the applications and is very far from representing an economic risk for the company — it is more just a minimal part of the negative press received by any industry.

Even though the majority of these cases involve defamation from adults, some cases involve so-called 'cyber-bullying' 22. In almost all

See R. S. B. v. Google do Brasil Internet Ltda. Regarding anonymity as a means of protection for those who exercise their right to express themselves, see John Doe v. Cahill 884 A.2d. 451, 456 (Del. 2005) where the service provider is aware of but unable to reveal the identity of the user until presented with a judicial order. However, the anonymity to which the Orkut cases refer is created when a user of a social network can create their profile in a cybercafé and operate in such a way as to make it impossible for them to be identified.

www.law.cornell.edu/uscode/html/uscode47/usc sec 47 00000230----000-.html
There is a draft law in Peru to combat cyber-bullying. On 28 October this year, Draft Law N° 4406/2010-CR was presented to the Congress of the Republic. The text proposes to pass a Law that promotes healthy cohabitation and school discipline and punishes bullying and violence among schoolchildren; the Antibullying Act. The measure is being taken within a context in which school violence is becoming increasingly more serious, in which the victims are suffering irreversible psychological and physical harm and, in some cases, death. Physical and psychological violence, as well as all forms of hostility and bullying among students committed by any means, particularly virtual, telephonic, electronic and other similar means, within the educational

the cases, the risks in Latin America and the Caribbean can be associated with the flow of personal data, the non-existence of data protection authorities in most countries being of a decisive nature (they only exist in Argentina, Mexico and Uruguay, and in Brazil it falls under the competency of the Public Ministry in its capacity as public ombudsman) 23 .

Children and adolescents, communication and freedom of expression

It should be emphasised that the style used in this paragraph contains a certain measure of quixoticism, insofar as that Internet applications will not be described precisely as they are today in terms of the offer but rather as they could be if a balance of rights is sought. This mantra of optimism under which rights, expectations and designs are sheltered is an exercise in imagination to demystify the concept whereby the best possible scenario for new technologies is to only develop under the control of market rules.

Since the Internet became more widely available, one of the expected impacts in democratic institutions is undoubtedly that Internet applications would produce a notable increase in the right to free expression 24 .

	INTER- PERSONAL COMMUNICATION	GROUP COMMUNICATION	UNMEDIATED EXPRESSION	MEDIATED EXPRESSION
EXPECTED RIGHTS	right to communication right to the privacy of those communications		freedom of expression image rights	
EXAMPLES	Telephone	Facebook Orkut	Twitter, blogs,	
	mobile telephone e-mail		Wikileaks, YouTube, "comment on this article"	`media' in the classic sense
CONTENT AND ACCESS	No invasion of privacy in communications without a judicial	lack of indexing ²⁵ robots identify violations	indexed - (sometimes with a moderator who applies	indexed - (with an editor holding responsibili

Table 1. Digital social applications

community, because this phenomenon has recently been taking place via these media (through which the attacker hides behind anonymity or impunity), taking the name of 'cyber-bullying'. National Institute for the Defence of Competency and the Protection of Intellectual Property (INDECOPI) www.indecopi.gob.pe in its role as overseer of the suitability of the educational services defined by the Protection and Defence of the Consumer Code. The regulations establish obligations for schools, teachers and students, which include compulsory reporting and educational and preventative actions.

See www.bibliojuridica.org/libros/3/1407/12.pdf : Carlos G. Gregorio, Protección de Datos Personales: Europa v. Estados Unidos, todo un dilema para América Latina, in Transparentar al Estado: la Experiencia Mexicana de Acceso a la Información, Hugo Concha Cantú, Sergio López-Ayllón, Lucy Tacher Epelstein (eds.), (2004)

 24 The freedom of expression implies two rights, viz. the right to free expression and the right to not express oneself, to remain silent and to withhold your own information.

withhold your own information.

25 In reality, this is not always the case. Depending on the social network and the selected level of privacy, the content can be indexed by universal Internet search engines (Google, Yahoo, Bing, etc.)

	order	of the website rules ²⁶	forum rules)	ty)
IDENTIFICATION	Caller ID IMEI - SIM card ²⁷ public telephone ²⁸	possible pseudonym (subject to acceptance by friends)	possible pseudonym	anonymity almost impossible
INTEREST OF CHILDREN AND TEENAGERS	high	very high	low	almost nil
RISKS FOR CHILDREN AND TEENAGERS	low	high	average	almost nil

In fact, a positive transformation in the free expression of ideas and opinions has been observed in recent years; from a model mediated by typical companies of the past to a series of Internet applications that allow the expression and manifestation of ideas in a direct manner (such as blogs, the ability to comment on articles in virtual newspapers and to a certain extent in some social networks such as Twitter).

The result of this process is still not fully known. Despite the fact that there are many more ways to express oneself today, it has also become apparent that there is less chance of being heard, of causing an impact and generating significant change. The impact of an idea published in an article on the pages of a widely-distributed newspaper (read by many people) or broadcast on television, is not the same as one that appears in a *blog* that, in the majority of cases, is known only to those who think alike and that is very difficult to find due to the saturation of search results on the Internet.

This analysis leads to a discussion of which available Internet applications are generically known as social networks, how they are used (i.e. what are the expectations of the user) and which rights would they be trying to enhance.

The main expectation from users of certain social networks could be defined as "a means for asynchronous group communication". For example, in the interviews with children and adolescents about who they think reads their content on social networks and who looks at their photos, the immediate response is "my friends".

IMEI (International Mobile Equipment Identity) and the SIM card (Subscriber Identity Module) tend to make it possible to identify any mobile telephone (and generally associate it to a person). In some countries, changing these codes is considered an offence.

Robots are included in many applications that analyse private content in order to send commercial advertising. This represents a reduction in personal data rights and the privacy of communications. Their acceptance is arguable but their widespread nature also opens up the possibility of using these robots to detect situations of bullying, defamation or illegal content. ²⁷ IMEI (International Mobile Equipment Identity) and the SIM card (Subscriber

codes is considered an offence.

28 The public telephone certainly opens up the possibility of making totally anonymous calls that generate a certain risk; however the low level of associated conflict makes this risk relatively admissible, particularly because whoever receives the call has sufficient control to end it.

Other social networks, such as *Twitter* and *blogs*, have a clear expectation to exercise the right to express oneself (even when some people create closed accounts only for their friends).

The difficulty in designing an application (a "means for communication" in the broader sense within the Internet context) that also maximises the privacy of communications and the freedom of expression would seem to be difficult and it is probably true that the applications available at the moment are still a little confused about which expectation they satisfy. In this regard, the concerns of the Article 29 Working Party are clear when seeing that the "domestic exception" may have lost meaning when referring to users of social networks who have thousands of friends, as well as regarding the contradiction to be found in the indexing by the large search engines of the content of social networks²⁹.

In practice, children and adolescents are not very interested in social networks of expression, such as Twitter or the blogs, because they are more attracted by social networks that make it easier for them to socialise with their friends³⁰. In Table 1, the column regarding group communication is the one that concentrates the risks and the interest from children and adolescents. It is highly probable that the offer of safer communication applications (including mobile telephony) would favour the Rights of the Child without affecting freedom of expression.

Returning to the civil actions in Brazil, it is possible to see that they only exist within the context of social networks of communication, whereas a recent ruling in Argentina in the case Protectora Asociación Civil v. Facebook, Inc. recognises that the expectation was for "expression" and does not apply civil liability³¹.

6. Children, adolescents and mobile telephony

In August 2010, Telefónica de España S.A. announced its acquisition of the social network *Tuenti* with the intention of expanding its operations in Brazil, Argentina and other Latin American countries, particularly in the sector of adolescents and young people. This news forewarns and explains a change in Internet connectivity, which in Latin America will migrate from a mainly cybercafé environment to the more widespread use of social networks from mobile telephones. It is highly likely that the entire risk scenario will change should this migration come about. At the same time, it could be excellent news for the children and adolescents of Latin America and their rights; especially because *Tuenti* has expressed its commitment to applicable legislation by signing an agreement with the Spanish Data Protection Agency and also because Telefónica already has social responsibility policies established in the region.

²⁹ Opinion 5/2009

 $^{^{30}}$ See in Livingstone et al. (work cited supra n. 4) Table 5 that states that the interest of children between 9 and 12 in blogs represents 5% of boys and 6% of girls, whereas among teenagers between 13 and 16, it represents 13% of boys and 16% of girls. 31 See the case Protectora Asociación Civil v. Facebook, Inc. (ruling of 11 May

³¹ See the case Protectora Asociación Civil v. Facebook, Inc. (ruling of 11 May 2010). This involved a group of adolescents who created a Facebook profile to encourage their school companions to refrain from going to school on a specific day and gather in a public space to celebrate their rebellion. The judicial ruling limited itself to ordering Facebook to remove the content. In Italy, criminal sanctions have been applied to five Google executives for the publication on YouTube of a video ridiculing a child with Down's Syndrome, see http://speciali.espresso.repubblica.it//pdf/Motivazioni sentenza Google.pdf

In most countries of Latin America to some degree, connections via a mobile telephone are identifiable with an individual. In other words, it is more probable that a social network profile will be identified with a particular user when using mobile telephony than with previous methods. If we accept that absolute anonymity and identity fraud in chatrooms, social networks and other Internet applications is one of the causes of vulnerability among children and adolescents, a greater level of identification will reduce the risks for children and adolescents. Clearly, this reduction will not be absolute because there are many unidentified mobile telephones (either because they are old or because they are purchased from a second-hand market) but this aspect can be improved upon with the collaboration of companies and responsible actions from users. Certain design aspects of the social networks could also reduce the risks, such as safer criteria for the acceptance of new friends.

It is also known that mobile telephones introduce new vulnerabilities for children and adolescents; GASSER, et al. describe the method of exchanging images (in some cases of child pornography) in exchange for credit balance, a risk that has also been reported in several countries of Latin America and which joins other risks associated with video cameras and the possibility to transfer files between mobile telephones³². Civil liability may also be applied but would have a positive impact when considering that the alternative designs are much more feasible.

In a ruling by the *Tribunal de Justicia del Estado de Rio de Janeiro*, Brazil, a mobile telephony operator was found to be responsible for the pain and suffering caused to a particular female customer of the operator who received insults in the form of anonymous text messages sent via the company's website.³³

Over the coming years, it will be necessary to maintain a constant process of risk identification and highly-fluid dialogue with the companies that provide mobile telephony services because the design risks can be controlled better in this market but the need for prevention and education is greater. 34

7. Prevention, education and corporate social responsibility

It is highly likely that the debate on the balance between the rights of the child, freedom of expression and the protection of personal data will continue for a long time. It will also be quite some time before mechanisms are implemented in the region to generate sound data regarding the victimisation of children and teenagers on digital social networks, on mobile telephony and on other Internet applications. As long as there are no empirical data that enable it to be established whether there is a "direct and significantly strong link" between vulnerability and the design of the applications supported by digital social networks, education and prevention (the

 $^{^{32}}$ When associating social networks with mobile telephony, this also breaks the illusion that these applications are free. In reality, the 'free' services we find on the Internet are paid for with our own personal data and the receipt of advertising. This new method would seem to include yet another application in the price of the connectivity package.

 $^{^{33}}$ See $\hat{C}.M.P.$ v. Nextel Telecomunicações Ltda (18 October 2010) it can be seen that the risk lies in a flaw in providing a service to users that enables anyone to send messages via the Internet without identifying themselves, thus failing to offer consumers the level of security to which they are entitled. The sentence (4,000 Brazilian Real) is insignificant.

³⁴ See: www.safernet.org.br/site/sites/default/files/Teles.pdf

priority recommendations according to the Memorandum of Montevideo) seem to be the only feasible alternatives.

Although prevention and education for safe and responsible use is one recommendation that is widely agreed upon by the international community³⁵, that does not necessarily make it a simple task in Latin America and the Caribbean. Several countries in the region have embarked on "a computer for every child" programmes³⁶, but these public policies have not been accompanied by their inclusion in the standard education programmes aimed at teaching the safe use of new technologies. This lack of cohesion is accompanied by the difficulty in training teachers and educators and the lack of economic resources in education budgets to respond to these needs. There are NGOs operating in the region that offer prevention workshops in schools, but it is an external offer and must be paid for by the schools that receive them. This system leads to a greater impact being felt by those private schools with additional resources.

Although corporate social responsibility policies could be a highly valuable resource for at least resolving the initial stages of generating educational content and training teachers, many operators (connectivity, Internet applications and mobile telephony providers) do not demonstrate the same standards of corporate social responsibility in this region as those expressed in their countries of origin.

Conclusions

Practically every industry involves some kind of risk. Under this premise, the management of progress involves maximising opportunities and minimising risks and, in this case, maintaining the risks within the realm of possible control by children and adolescents, and their families.

The development of applications in cyberspace is as fast a process as it is complicated. It not only requires several fundamental rights to be rethought but also requires an understanding that there are a range of business activities involved with significant economic interests. Even though there is a legitimate expectation to maximise freedom of expression through Internet applications, not all applications should be aimed at expressing oneself. Provided there is a sufficient offer of applications for expressing oneself, this expectation will be sufficiently met. However, by introducing a certain degree of order (which could be achieved through minor changes in the design of these applications), it is possible to create safe spaces where the rights of children and teenagers are quaranteed, and that would seem to not be limiting freedom of expression. For example, getting the offer to distinguish between social networks for communication and social networks for expression (in a design where one set excludes the other) could be one form of solution, even though that may seem like utopia at the moment.

 $^{^{35}}$ This objective was included as Goal N° 24 in the Plan de Acción sobre la Sociedad de la Información

y del Conocimiento de América Latina y el Caribe (eLAC2015) [Action Plan on the Information and Knowledge Society in Latin America and the Caribbean] approved in the city of Lima on 23 November 2010 at the Third Ministerial Conference organised by CEPAL.

³⁶ Several countries in the region have embarked on "un ordenador por niño" [a computer for every child] programmes, the Ceibal Plan in Uruguay is the most advanced.

The truth is that there will be many outstanding issues that need to be discussed, such as protection against defamation on social networks for expression and the precise nature of the mechanisms of civil liability to discourage such practices and compensate any damage incurred by possible victims. However, at least excluding a significant majority of children and adolescents from unsafe environments could be a starting point from where to begin moving forward.

It is highly likely that the expansion of digital social networks into the field of mobile telephony will enable improvements to be made to security conditions; (i) mobile telephony risks are not so closely related to the business model as they are in the case of Internet applications; (ii) self-regulation is possible and especially the regulation of mobile telephony within national legislation; (iii) it will be possible to minimise the ability to remain anonymous in communications without significantly affecting services; and (iv) the corporate social responsibility of telephony operators is much more mature than that of those companies offering online applications.

The protection of the Rights of the Child within a virtual context is truly a challenge that needs to be tackled from many angles. The Memorandum of Montevideo offers boundaries and priorities from a regional perspective; a contribution that is open to international debate.

The existence of sound data on the victimisation of children and teenagers in virtual scenarios seems to be a problem in developing countries. However, that does not justify any delay to policies that could be based on data from other countries or regions and a careful examination of the cases to have reached the courts can be undertaken at any time. Education and prevention for the safe and responsible use of new technologies stand out from among these policies. It is believed that corporate social responsibility today is an essential aspect for the implementation of policies in the education sector – at least in developing countries.

The Rights of the Child (being as they are Human Rights) are now facing a dilemma in which a new balance must be found. It is a volatile situation in which the media and information and communication technologies have changed and will continue to change. The polarisation of arguments is senseless and simply leads to a lack of progress; research, monitoring, creativity and corporate social responsibility seem to be the right paths forward.

Other websites visited

Legislation

United States

18 USC Section \$1466a

www.law.cornell.edu/uscode/18/usc sec 18 00001466---A000-.html

Communications Decency Act

www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000230----000.html

Brazil

Brazil: Political Constitution

http://www.senado.gov.br/legislacao/const/con1988/CON1988_13.07.2010/CON1988.pdf

Peru: Draft bill on cyber-bullying

 $\frac{\text{http://www2.congreso.gob.pe/Sicr/TraDocEstProc/TraDoc}}{\text{d99575da99ebfbe305256f2e006d1cf0/10caeda48c4022e4052577ca0074d2a5/$FIL}}{\text{E/04406.pdf}}$

Court rulings

[16 April 2002] Free Speech Coalition v. Ashcroft, 535 U.S. 234 (2002)

http://supreme.justia.com/us/535/234/case.html

[30 June 2004] S. M. y L. E. v. Jujuy Digital y Jujuy.com

www.iijlac.org/jurisprudencia/components.php?name=Articulos&artid=37

John Doe v. Cahill 884 A.2d. 451, 456 (Del. 2005)

www.citizen.org/documents/DoevCahillSupremeCourtOpinion.pdf

[12 February 2009] R. S. B. v. Google do Brasil Internet Ltda.

www.iijlac.org/jurisprudencia/components.php?name=Articulos&artid=100

[11 May 2010] Protectora Asociación Civil v. Facebook, Inc.

www.iijlac.org/jurisprudencia/components.php?name=Articulos&artid=104

[18 October 2010] C.M.P. v. Nextel Telecomunicações Ltda

www.iijlac.org/jurisprudencia/components.php?name=Articulos&artid=105

Studies

Studies by SaferNet and the Federal Public Ministry

http://www.safernet.org.br/site/prevencao/pesquisas

Risks and safety on the internet: The perspective of European children. Initial findings from the EU Kids Online survey of 9-16 year olds and their parents.

www2.lse.ac.uk/media@lse/research/.../Initial findings report.pdf

News

[21 September 2010] Telefónica lanzará Tuenti en Brasil y Argentina e impulsará la integración móvil

http://www.marketingdirecto.com/actualidad/social-mediamarketing/telefonica-lanzara-tuenti-en-brasil-y-argentina-e-impulsarala-integracion-movil/

[2 April 2009] Tuenti se compromete con la AEPD a implantar sistemas efectivos de verificación de edad y a depurar los perfiles de menores de 14 años

https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2009/n
otas prensa/common/abril/020409 Tuenti AEPD reunion.pdf

[23 November 2010] Países aprueban plan para lograr una sociedad de la información de acceso universal: autoridades de América Latina y el Caribe acordaron el plan eLAC2015, que busca fomentar el uso de las TIC como instrumentos para alcanzar un desarrollo más inclusivo.

www.eclac.cl/elac2015