Human rights in the ethical protection of youth in social networks - the case of Colombia and Peru

Jefferson Stewart Espinosa Vera*

jsev1986@hotmail.com

**KEYWORD**

Cyber-crime; specifically vulnerable victims

**ABSTRACT**

This work analyzes incidents of information technology and communications in the sphere of freedoms beginning with social contemporaneous changes. Later it will analyze the problems with chat and young people in the environment of parental education in the new technologies. Likewise, you can observe the importance of the legislation trying to protect kids, young people, and adolescents in their freedom, integrity and sexual development that can be made vulnerable by cyber criminals that look through different portals of the internet, to trick this special class of our population that must be protected constitutionally and criminally. Looking at this cyberspace framework that has revolutionized the world; and to be someone who uses it daily, it is of vital importance to have special care with children in respect to the use of this type of advanced technological tool, the role that parents, tutors, and society play is of great importance such that, they should grant space spaces where the youth can be guarded or guided to prevention so they don’t become victimized by cyber-crime. Also one of our points will speak of the risks associated with the web, INFOethics, parental education, and especially the general situation with regards to legislation in Colombia and Peru, as it is urgent that both countries take established and preventative measures with regards to the criminal law of each state, due to the vulnerable intimacy of social networks, and therefore because what is most being affected is the youth, which gravely affects their psychosomatic and social development, because there does not exist a correct or suitable use for cyberspace.

* Lawyer (Colombia), Universidad Autónoma Latinoamericana (Colombia), Master’s Degree in Procedural Law - National University of Rosario (Argentine), Diploma in University Teaching - Curriculum and Didactics Pedagogy - Universidad Pontificia Bolivariana (UPB - Colombia), Diploma in Human Rights and Conventional Control - ACDPC (Colombia) and University of Bologna (Italy). Presentation with public and oral defense presented in the Spanish language and later translated by Dr. Jefferson Stewart Espinosa Vera. International Speaker for Colombia at the XX Ibero-American Congress on Law and Informatics - Ibero-American Federation of Law and Information Associations - FIADI, held at the University of Salamanca - Spain - October 19, 20 and 21, 2016. Paper presented at Co-author in the Spanish language with Dr. Miguel Angel Vidalón Choque- Lawyer (Peru) - National University Hermilio Valdizán de Huánuco.
1. Human rights in cyber-space

The impact of information, communication technologies, as well as other new technologies in the sphere of freedoms, has configured a new generation of human rights. These new rights demonstrate that the catalog of freedoms never will be a closed or finished work. A free, pluralistic, and democratic society will always have to show sensitivity and openness to the needs required by new rights. While these have not been recognized by national or international law, they will act as vindictive, pre-normative, and axiological, but human rights are not mere simple postulation of what «must be». The theory of human rights cannot be insensitive to the urgency to take seriously the task of constructing a theory of open and responsibly committed freedoms with the response to the new needs and demands of human beings living in the era these new technologies. In our time, that that distinguishes the omnipresence of new technology in all aspects of life, both individual and collective, has amplified decisively the incidence of TIC in broad sectors of legal and political experience. Human rights as terminology, are relatively new concepts, and you can say that the term began having regular use at the beginning of the 20th century, and especially since the middle of that century, with the passage of the Universal Declaration of Human Rights, December 10, 1948. Already in 1945, The Letter of the United Nations had given expression to this term, which expressed one of its intentions, «to realize international cooperation in the solution to international problems of an economic, social, cultural, or humanitarian character, and in the development and stimulation in respect to human rights the fundamental freedoms of all, without distinction to race, sex, language, or religion…» (the highlighted is not from the original) In this context, New Technologies, have promoted new ways to exercise rights and, in fact, they can contribute to the strengthening of the participatory fabric of democratic societies. As it is, the cyber-citizenry and the tela-democracy are building a new horizon with respect to rights. The society, in which we live, is not the same in which they approved the Universal Declaration of Human Rights (passed in 1948, just after the second world war), International Pacts of Human Rights (passed in 1966, in the middle of the Cold War) and the rest of the international instruments of human rights protections. In this context, one of the aspects to have in mind, without a doubt, is the technological advance that there has been since. In the last decades—going back to the sixties, but above all in the last twenty years—have been characterized by the great development of technology and, certainly, by that today we refer to information and communication technology (TIC). The DUDHE makes reference to the TIC throughout its articles, for example in article 5. This technological advancement has assumed the emergency of new rights, many times in response to new aggressions. An example is the right to have personal data protected—also recognized by the DUDHE, article 5.9, that suggested the necessity to protect individuals from the dangers that could be imagined from information technology. On the other hand, day by day, the consumption and use of this unstoppable form of technology without control is realizing grave violations of human rights in all aspects of life in regards to the use of these electronic devices. Those of which have direct relations with liberty, integrity, formation, indemnity, and intangibility of boys, girls, and teenagers.

2. The problem of chat with young people-grooming and parental education in new technology

One of the most utilized services by users of the internet in general and especially with young people as means of communication, is without a doubt chats. Here is where they can easily be tricked by third-persons to obtain personal data and bank information, like account numbers, credit card numbers, passwords, etc.; parental belongings for purposes of committing later fraud. This practice has become known as grooming. Pedophiles and child abusers look, as a common tactic, to make contact through this electronic medium to take advantage of these same characteristics, pretending to be another child, in the majority of cases exchanging compromising photos. Once in possession of them, the stalker extorts the child in question telling him that they will send the
photos to their family members and/or friends, whose e-mail addresses they already have possession of previously, to pass into this first phase of trust.

The TIC in the service of education for underage youth

New technologies are taking on a great role in society, but at the same time in education, the role that Information and communication Technology (TIC) play in the world is more digitalized each day, it is very important for improving the quality of education, the benefits that contribute to the education model implemented since the TIC are innumerable, setting out several challenges to have in mind if you want to truly better the level of education that will permit the next generation (children), to be competitive in the digitalized world.

The illustrious American philosopher and linguist NOAM CHOMSKY\(^2\) has reflected about this section, the impact of the new technologies on education, he believes that to make good use of them, the first thing the student should have is a good point of reference, in which to move, search in an adequate manner, and to know how to differentiate from the true and correct information. The students need someone that can teach them all of this, and who better that their teacher? He says that to have so much information in the internet the only thing that can happen to the students if they do not follow the before mentioned steps is they will harm themselves, already objective data from distinct pages can be accumulated but at the same time they can be totally outside of reality.

Homeland power and education in respect to modern technologies. Special reference to the internet

Throughout history, children have occupied diverse status in the societies in which they would grow up. It is well known that up until the middle of the 18\(^{th}\) century the systems of raising children and education practices that existed protected the aggression of the adult against the child as a common denominator, considering them only as an objects of right and not, as they actually are, a subjects of right. It is by reason of this breakthrough that has produced the necessity that parents must educate their children in how to use these technologies correctly, the coat that grants them the exercise of parental responsibility. In this context it is necessary to establish between parents and children a fluid dialogue to achieve such an end.

Parental education, filters and tics

The conduct of man in society has many characteristics and many forms. In actuality with the advance of information and communication technology (TIC) the behavior of man has explored new horizons and new paths; one of them is the virtual world and especially that of the social networks.\(^3\) The grooming is a practice of bullying and sexual abuse against children and young people that, in the majority of cases, happens through social networks. Following, and in an exemplary mode, some minimal guidelines may be cited that parents should implement to instill in their children a responsible way to use the web:

a) Establish reasonable rules and norms in the use of the internet and digital devices to be utilized by children (for example: establishing time limits, spaces, and conditions of use).

\(^2\) In regards to technology in education, it should be said that technology is neutral. (…) For example: The internet is extremely valuable if you know what you are looking for; I use it all of the time in my investigation. If you know what you are looking for, if you have some type of reference point, that guides us to particular topics and allows us to leave many others on the periphery, then it can be a very valuable tool. Of course, one should always be prepared to question if the point of reference is correct: maybe we will find something that will question the manner in which we see things. You cannot pursue any type of investigation without a point of reference that is relatively clear that will guide the search and that can help to select what is significant and what is not, what you have to leave to the side, to what have to continue pursuing, to what deserves to be questioned or developed\(>) NOAM CHOMSKY (Text- The objective of the Education: The De-education). CONCEPT OF TECHNOLOGY AND EDUCATION-NOAM CHOMSKY.

\(^3\) Form of social interaction defined as a service on line focused on communities of people that share interests and activities, or that is interested in exploring the interests and the activities of others and that require the use of software.
b) Take privacy measures that are needed to prevent the youth from being a victim of a technical expert in deception.

c) Parents must become familiar with social networks so they know how they work, so they have the ability to anticipate potential risky situations.

d) Observe the state of mind of the youth. When a young person is a victim of abuse, violence, or blackmail, they will present abnormal attitudes.

e) Adults and parents must be examples of users so the children can learn from their parents example, and for this parents must assume the role of responsible user.

There are various filter systems, and between them we can mention the following:

1) The system called «black lists» or «lists of sites to block»;
2) The system of blocking sites by means of recognizing key word searches; and
3) The system called PICs (Platform for Internet Content Selection), which bases itself in a previous classification and the labeling web of page content using true invisible electronic «bar codes» that are read by the software that the user possesses.

3. Psychological and social behaviors of the victims (underage young people)

It is important to recognize that boys, girls, and teenagers that are victims of some type of information crime tend to present changes in their behavior.

- They show aggression towards classmates, teachers, friends, family members, or pets.
- Despite having shown enthusiasm for the internet, all of a sudden they lose interest in spending time in cyber-space.
- They become unsociable and timid people, that don’t discuss what happens to them, demonstrating stress, crying, or nightmares.
- Unarguably this phenomenon interferes with the scholastic performance of the boys, girls, and teenagers, manifesting itself in low grades without justification.
- Avoiding talking to parents about friends on social networks.

So, said situation will be analyzed accordingly in the Colombian and Peruvian cases, respectively:

4. The colombian laws

In the last decades the process of globalization has been presented at a world level, and has permitted technological, social, and cultural advances of a grand scale, leaving a glimpse of an increase in the utilization of information crimes as a way of criminally victimizing boys, girls, and teenagers, as the most vulnerable population within cyber-space. For this reason the necessity is seen to include the Colombian national legislation, by means of law 1273 of 2009 that realizes modification to the Colombian Penal Code where information crimes are characterized as «such conduct that relies on information tools calling themselves programs, computers, etc.; like those that avail themselves of those means to hurt the legally protected interests of others such as privacy, economic assets, public faith, etc.» It is like this that worry is generated by those institutions in charge of the Protection of Infancy and Adolescence by the use of this modus operandi, as a tool that facilitates sexual bullying, child porn, and child prostitution. Within this category it is important to highlight the methods they utilize to victimize boys, girls, and teenagers, as the cyber-bullying that is the use of electronic information and
methods of communication that are contained in email, social networks, blogs, instant messaging, text messaging, cellphones, and websites, to bully, intimidate, or scare a person with defamatory, degrading, and aggressive comments. Likewise there is *Grooming* and there is Sexting. The latter being the showing of suggestive photos through the web to each other.

### The Case of Colombia- Jurisprudence

With respect to the case of Colombia, it is important to highlight the ruling; uttered by the Honorable Supreme Court of Justice for the Republic of Colombia (Court of Criminal Appeals), the 29th of July, 2015- SP 9792-2015- Based: 42307- (Approved Act 259)- Judge Speaker: Dr. Patricia Salazar Cuéllar- Bogotá D.C.- Colombia that in other fundamental terms analyzes the right of privacy, the Protection of underage youth in social networks. (The Law of Infancy and Adolescence of Colombia- Law 1098 of 2006- Law 679 of 2001 by means which issues a statute to prevent and resist the exploitation, pornography, and the sexual tourism of minors, in development with article 44 of the Colombian Constitution and its regulation between other aspects of the use of global networks of information in relation to minors). The ruling of the Supreme Court of Justice of the Republic of Colombia, authorized by means of a judgment that indicated that the parent of the family will be able to have access to the passwords of the social networks and email accounts of their children, without being in violation of the right to privacy.

This way the parents remain authorized «to attend, orient, and control the communications of their underage children», according to the ruling of the high tribunal, now the parents of the family, have the authority to access information with the objective to protect the minors in cases in which they could be put at risk. This decision was taken by the Judges of Supreme Court of Colombian Justice, after the arrival of mail to their offices from an underage child inspected by his mother. This case was denounced as a violation of the right of privacy. The Colombian Constitutional Court has pronounced by means of a ruling of protection of June of 2016, with respect to the measures that the different education institutions should adopt, with respect to gender violence or cyber-bullying that is being generated through the social networks that are terribly scarring underage minors, including the suicide of a school girl, which was the reason that it was asked to have control of these things. The Court studied the case of a minor whose classmates had published a naked photo on a web page that was exclusively destined for bullying by his classmates. To the Court the publication of these intimate photographs are examples of gender violence through the social networks, given that no control exists in the education centers.

### 5. Ethics in social networks or information ethics, risks, and vulnerabilities on the Web

The social networks, being an information system like any other, come with dangerous vulnerabilities thanks in principal to its very same users. They are those who are exposed to different threats and their lack of knowledge many times can bring them to reveal personal information, probably recollected by those that do not have the best of intentions. The Social networks are, therefore, favorable stages for those that want to try and defeat the information security protections of a lot of people; additionally the users, in the majority of cases, are not conscience of the risks they run of divulging information openly that is of broad interest to the criminals, a situation that has helped to proliferate said practices. The vulnerabilities can have origin in some of the following aspects:

a) Spaces or physical elements: Work areas of the users, location of the server, wiring, between others.

b) The users: The people will be able to reveal important information many times without knowing it, including after being warned.

c) Passwords: The complexity of said combinations is essential, if it is something obvious and little changes, the element of security will become a vulnerability.

d) Bad programming: In some cases the developments are not focused in equipping your software with good security, this creates easy holes that can be taken advantage of by people with bad intentions.
e) Bad infrastructure: Some networks do not count on adequate equipment to avoid possible attacks.

f) Data integrity: Lack of a copy or redundancy that can cause lost data.

Ethics in social networks - Info-ethics

A philosophical discussion planted many years ago can leave the scope of an information investigation; it is where there will be a special focus in the related laws with said themes. However, it is necessary to have in mind some pertinent considerations for those that count on knowledge different from the common knowledge.

These are precisely the abilities of many of the software developers –an area that the majority of people do not have a strong command of-, and for them it is necessary to pay special attention thanks to these behaviors that technically are legal, but from an ethical point of view are quite reprehensible. The development of applications for the most popular social networks is an aspect that does not escape this discussion where the issue is raised and weather or not complying with the law in this manner is ethically incorrect. Social networks are not tools created to violate the law and commit all types of crimes, to the contrary, they are useful and powerful interfaces of interaction and entertainment that unfortunately some of its users have converted into a space where it is necessary to be very cautious with your personal data. After all of these considerations, we analyze an actual case, the theme of grooming in the Peruvian laws in a very critical way after already having analyzed the situation in Colombia and that can be applicable to various laws in a very general way in several aspects.

6. Critical analysis of article 5 of the law number 30096. «The violation of indemnity and sexual freedom through technology»

As a consequence of globalization and technological advances, society is the principal recipient of a progressive advance and evolution of codes that make life for humans modern and practical4. However, such technological advances have also awoken a sensation of insecurity in the political class, of such form that it has designed a technological advance as a channel that a threatening source of dangers travels through to a vulnerable sector of the population, in a manner that has opted to understand that such technological means put in danger, the specific validity of legal rights. The legislature has related the vulnerability of a certain indefensible sector of the population with this technological advance, following the little capacity that they have to discern and deter, with respect to, the dangerous activities [actions] that push others to damage their right [legal right] to the indemnity and sexual liberty in the Peruvian case of crimes against liberty, integrity, and sexual development in the Colombian case. Namely in such situation, we must affirm that once again the legislature relies on criminal law to justify a type of government criminalization that is to be geared and justified in the protection of the indemnity, the sexual liberty of boys, girls, and teenagers in the interacting technology, that are seized for sexual ends5. Such situation, without the intention to overshadow the good intentions and concern for that that must have been told to the legislature at the moment of design law number 30096, that represents –not withstanding- an expansive negative expansion of ius puniendi in the fight against crime, with the only end to be giving prestige and presence to the state, the same that undoubtedly was suggested by the media’s lawsuits. Facing such scenario, the state through criminal law has resorted once again to the criminalizing [general prevention] and the punishment [special prevention] of the injury to indemnity and sexual freedom of minor age children, figuring that is needless to say, that it now is protected by articles numbers 173, 175, and 183 – of the Peruvian Criminal Code.

4. On this matter: Art. Luis Gracia Martín. THE RANGE AND EXPRESSION OF MODERN CRIMINAL LAW.- «The criminal doctrine currently includes «Modern Criminal Law» to a plurality of penalties that broaden the criminal intervention to fields that, for example economic activity, that have traditionally been to a greater or lesser extent outside of its range.» In «ECO-NOMIC AND BUSINESS CRIMINAL LAW» Coordinators: Francisco R. Heydegger/Atahuamán P. Jhuliana. Idemsa, first edition March, 2013. P. 13-75

5. See article 5 of Law Number 30096.
7. The legally protected

To understand and justify the existence of the criminal law as the only manifestation of prevention and repression which the state has to punish conduct⁶, should ask the question what is it that it is intending to safeguard, or to say in another way, what is its object of protection, in a way that will have to establish what it is trying to protect are certain elevated values of a legal category. Article number 1 of law number 30096 [from now on the law] surrounding the object that has the law, has established that the same law has by object the prevention and sanction of conduct that affects systems, computer data, and other legal interests relevant to criminal law, committed through the utilization of information or communication technology with the end to guaranty the effective fight against Cyber-crime.

8. El iter criminis⁷

When article number 5 of the law makes a typical description, it also does it in respect to a chronological description of things that have happened and that have been tested in reality, in this sense, it should adjust the typical and chronological analysis that here it intends to do, in function in the following wording: «That through the information technologies of communication, contacts a child under the age of 14 to solicit or to obtain from him pornographic material, or to have sexual relations with him». Always emphasizing, that the only things put at risk are the legal aspects that are protected, but not its effective injury⁸.

The fas Subjective – Psyche of the Subject [ideation and preparation]

Every intentional crime also defines the verification of previous acts from those commonly known acts of application and resolution, those acts have been studied to illustrate psychological path of the crime in terms that it is understood that the cornerstone or substance of the crime will always be human conduct. A more familiar example would result if you imagined if A kills B [ideation] A buys the weapon [preparation] y finally grips the weapon and shoots B [application]; note that the verification of the forgoing examples, we can assign characteristics to the acts of preparation that differentiate from those acts of application, serving at the same time and for that they appear in reality. In this sense, the acts of preparation import a channel⁹ that always looks to connect the natural-subjective aspect [ideation] with the material-objective aspect [application], with such luck that the preparation creates the required peripheral conditions¹⁰ for the criminal idea of the agent to initiate the enforceable action, the same that has a direct connection with consummation of the devised plan.

The fas Objective - Material of the Subject [application and consummation]

With the base of being exposed to the previous section, the material aspects of the crime, the application of the acts, and the consummation of the facts all correspond with each other¹¹.

---
⁷ Ob. Cit. Raúl Peña Cabrera. P. 295. CAPITULO XIII - 1).- ITER CRIMINIS.
⁸ In respect. The Dr. Jorge Luis Salas Arenas. In «SEXUAL INDEMINITY - LEGAL TREATMENT OF SEXUAL RELATIONS WITH MINORS BETWEEN 14 AND 18 YEARS OLD». First edition. Lima - Peru, August of 2013. P. 38
¹⁰ Ob Cit. Raúl Eugenio Zaffaroni. P. 343. With respect to the professor Zaffaroni who has preferred to call them «attendant results».
9. The path and development of the supposed and contemplated in Art. Number 5 of law number 30096

Chapter III of the Law makes reference to information crimes against the indemnity and the sexual liberty, for such assertion, we could arrive at a first conclusion, and that is that the object or legal interest to protect with the type of penalty in mind would be the indemnity and the sexual liberty. Such idea appears to take itself further from reality when you take a glance at article number 5, it is evident that what is really punishable is the proposition with sexual ends, through technological channels, to boys, girls, and teenagers. It’s to say, when the article in reference demands as the first development el «contactor» to the victim «to» prepare the conditions of injury to this indemnity or sexual liberty, we can understand that such description, looks to punish the «proposals» with sexual ends to boys, girls, and teenagers through the technology.

The Subjective Phase-Psychological [internal phase of the crime]

In this sense, what we can try to establish is, that that is the «criminal idea» of the agent, attending to article number 5 of the law. While it is true that the wording of the article is written as a «done proposition of the agent, with sexual ends through the internet to boys, girls, and teenagers», we can’t conceive of such an idea, as the final desired object of the agent. It’s more reasonable to be in agreement and close down the debate on the issue, and affirm that the criminal idea here is to obtain pornographic material and/or have sexual activity with the victim, that is a boy, girl, or teenager.

The Objective Phase-material [external phase of the crime] If what is described in article number 5 of the law is understood to make reference to the previous acts, such as ideation and preparation, the acts of application and consummation are those that clearly can separate themselves from article number 173 of the penal code, the same that sanctions the adopted acts without need to wait of the consummation of the devised object in the psychological phase. In this sense, we consider that the punitive scope that describes article number 5 of the law technically falls short legislatively in the sense that it intends to punish with a punishment of acts that don’t correspond to objective-material phase.

10. Conclusions

– It is vital that the light of Colombian and Peruvian norms, are issues treated as so critical and at the same time of such great importance, just like the new technologies that have been at the height of their splendor in the last twenty years, and thanks to the speed of the information systems, the legislatures of each country should prevent the risks that are carried to both nations, like abuses of internet users or information criminals that take advantage of these advanced technologies to limit underage youth and adults in their personal and bank accounts; violating in this fashion their rights, such as the right to privacy and others, constitutionally and criminally embodied in the respective legal framework.

– The issue is based in the authority that parents have over their children; it is always important to teach children from an early age about the responsible use of these types of social networks.

– While it’s true that parental authority is by the parents; the rule of law is a guarantor also; every time that it takes over to legislate for the purpose of protecting its children (taxes). Educating young people at school about the scope of these technologies, that can be for good or can be for bad; obviously depending on the given use of these information tools.

– Technological advances are amplifying the field of action and every day the threats are more latent, however the solution will not be done without use of the new information and communication technologies, what is really important is to establish clear rules in the nuclear family to avoid possible problems with boys, girls, and teenagers, employing methods of which can help them avoid being victims of this type of crime. With respect to the filter mechanisms in media technologies, it’s not just the protection that they bring, but the mental filter that makes the young person thanks to his habitual or not-habitual conduct that
we deserve special attention at the determined moment, avoiding an emotional collapse or even suicide of the young person. The best filter is an attentive parent.

- The information risks will always exist and until we can compare it with the dangerous activity of driving a car, it is well known that as you drive and control your life, between them the personal information, you will be able to be run over by a cyber-criminal and easily make your information security vulnerable because it lacks predictability.

- The existence of the criminal law in Colombia and Peru, always attends to an object of protection, in a way that the law looks for the effective protection of certain elevated values as a category of legal interests. It’s as a limiting operational tax by the state intending to involve itself in the field of individual liberties.

- The object that is intended to be protected by the law 1273 of 2009 (January 05’) of Colombia and article number 5 of the law 30096 of Peru, lacks good legislative technique. To the contrary, in such cases, it is better to apply articles number 173, 175, and 183-A. The era of cyber-space, brings innovative aspects to the field of information technology, however it also create new criminal conduct, which affect the vulnerable population (underage minors), before a legal regulation should exist to prevent it.

- The grooming, the new way of operating by the pedophiles and child abusers, democratic states should quickly and efficiently raise the level of awareness in underage minors of this threat, to the end that they know the new methods of the criminals.

11. Bibliography


Rubinstein, J. L. In «Principals of psychology in general». 1967 Editorial Grijalbo, México D.F.


