Human Rights under Cyber Space with special reference to Indo-French Legal Regime : A Comprative Analysis

Indrajeet Singh, PHD Research Scholar,
School of Law, Manipal University Jaipur

Abstract

The tremendous development of Information and Communication Technologies (ICTs) in the last few decades has led to the creation of a cyberspace (the space of interaction formed by the global network of computers which compose the internet[1]), where new opportunities are opened for connections, interactions between all kinds of actors and individuals. Individuals can use online mediums to express or inform themselves and communicate freely and instantaneously worldwide. More and more people have access to these technologies and use them to a large extent, hence slowly changing the ways in which people express themselves, communicate, and behave on cyberspace. Hence, this paper's aims are to look at the challenges raised by infringements of individual's human rights committed on cyberspace in particular. Focusing on four areas that are particularly important to the individual's ability to exercise his rights freely in the cyberspace, we will first study the source of those rights and internet's impacts on their exercise, then study the violations and the legal provisions relevant to the offenses, comparing the French and Indian legal frameworks.

Keywords: Information and Communication Technologies, cyberspace, technologies, infringements, French and Indian legal frameworks.

INTRODUCTION

The tremendous development of Information and Communication Technologies (ICTs) in the last few decades has led to the creation of a cyberspace (the space of interaction formed by the global network of computers which compose the internet[2]), where new opportunities are opened for connections, interactions between all kinds of actors and individuals. Individuals can use online mediums to express or inform themselves and communicate freely and instantaneously worldwide. More and more people have access to these technologies and use them to a large extent, hence slowly changing the ways in which people express themselves, communicate, and behave on cyberspace.

Internet constitutes an important vehicle for the promotion and exercise of human rights. The speed of communication, the sharing of information, the platforms provided for expression and action are all features

[1]Cyber Law, Cyber Crime, Internet and E-commerce, professor VimlenduTayal, Bharat Law publications, p. 63
[2]Cyber Law, Cyber Crime, Internet and E-commerce, professor VimlenduTayal, Bharat Law publications, p. 63

that enhance the opportunities provided for people to actively exercise their freedom of speech and expression. However, misuses by any actor (be it an individual, a corporation, the government) can also happen online, leading to infringements and violations of one's fundamental rights. The interaction between cyberspace and human rights has created new challenges as far as human rights abuses are concerned, because although these abuses existed in the form of conventional crimes, their existence in the context of cyberspace raises questions about the need of specific provisions regulating human rights exercise and protection online.

Hence, this paper's aims are to look at the challenges raised by infringements of individual's human rights committed on cyberspace in particular. Focusing on four areas that are particularly important to the individual's ability to exercise his rights freely in the cyberspace, we will first study the source of those rights and internet's impacts on their exercise, then study the violations and the legal provisions relevant to the offenses, comparing the French and Indian legal frameworks. We will then look at the ways in which laws are enforced so that individuals can protect the exercise of their rights online and compare the French and Indian systems, so as to be able to further make suggestions to empower individuals to exercise their rights more freely, to improve the protection of human rights in the digital space and to improve Indian and French national cyber legal framework in dealing with human rights.

Hypothesis

The specific nature and the spread of the use of online mediums calls for special protection against violations of human rights on the cyberspace, as current legislation do not sufficiently protect their free exercise. Furthermore, there is a need for enhanced international cooperation.

Research questions

- What individuals' human rights are the most challenged by the cyberspace and what are the impacts of cyberspace on those human rights?
- What cybercrimes are specifically related to infringements of those rights and what are the corresponding legal provisions in France and in India?
- What is the process of law enforcement in cases of violations of those human rights on cyberspace in France and in India?
- What suggestions can be made to improve the Indian and French systems as far as protection of human rights on cyberspace is concerned, and what suggestions can be made to improve the protection of human rights on cyberspace?

1.1. HUMAN RIGHTS AND THE CYBERSPACE

1.2. Human rights impacted by cyberspace's development

The United Nations have strongly contributed to the recognition and combat to guarantee human rights at the international scale through the Universal Declaration of Human Rights (UDHR), 1948 and the International Covenant on Civil and Political Rights, a multilateral treaty still open for signature and

ratification. Although these two legal texts are not directly enforceable, they have a major symbolic importance as 167 countries ratified the latter, including France and India. Following the dynamic launched by the UDHR, regional human rights declarations were created such as the European Convention on Human Rights, 1950. As co-writer, France is a founding member of the Convention enforceable through a complaint process to the European Court of Human Rights.[3]

However, the question of human rights in the international community has been raised rather recently and was preceded by national concerns to guarantee fundamental rights to their citizens. Nowadays, constitutions are considered as the most efficient legal instrument for this purpose. Hence, as this paper aims to analyze the protection of three human rights threatened by the development of cyberspace, it is essential to go through constitutional provisions providing the right to dignity, the freedom of speech and expression and the right to privacy as well as through sections protected vulnerable sections of society especially children.

1.2.1. Right to dignity

The right to dignity is the first, as violation of other human rights will automatically endanger the dignity of victims. This right is particularly broad as it guarantees to people the freedom from discrimination[4] as well as the freedom from cruel, inhuman and degrading treatment.[5] In India, the State has the obligation under Art. 21 of the Constitution to guarantee to its citizens a life with human dignity free from exploitation. In France, the right to dignity was recognized by the Constitutional Council in its decision from 27th July 1994.[6]

1.1.2 **Freedom of speech and expression**

The freedom of speech and expression is a fundamental right at the foundations of democracy as observed by the Indian Supreme Court in *Romesh Thapar v. State of Madras*: Patanjali Shastri : " *Freedom of speech and of the press lay at the foundation of all democratic organizations, for without free political discussion no public education, so essential for the proper functioning of the process of popular government, is possible*."[7] The freedom of speech and expression include the freedom of opinion and to express these opinions without worry. It is guaranteed in India by Art.19(1) of the Constitution and in France by Art. 10 and 11 of the Declaration of the Rights of Men and the Citizens (DRMC) which has constitutional value. However, this fundamental right comes with reasonable restrictions in the interest of the State or citizens. Regulations of the freedom of speech and expression are provided in Art. 19(2) of the Constitution of India and by Art. 11 of the DRMC.

[3] "UN Treaty Collection : International Covenant on Civil and Political Rights", United Nations, updated data on 11th December 2013 *available at* http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en (Last visited 12th December 2013)
[4] Art. 2, International Covenant on Civil and Political Rights, 1966
[5] Art. 7, International Covenant on Civil and Political Rights, 1966
[6] Constitutional Council, Decision n°94-343/344 DC, 27th July 1994
[7] AIR 1950 SC124

1.1.3 **Right to privacy**

The right to privacy corresponds to the right of people to be protected by the law against "arbitrary interference with [their] privacy, family, home or correspondence, nor to attacks upon [their] honor and reputation."[8] In India, Art. 21 of the Constitution protecting life and personal liberty includes the right of privacy. It was confirmed by the Supreme Court in *Govind vs State of Madhya Pradesh & Anr on 18 March*, 1975.In France, Art. 2 of the DRMC and Art. 9 of the Civil Code guarantee the right to privacy which can be legally violated only in case of a legal investigation.

1.1.4. **Rights of children**

Finally, the extreme vulnerability of children requires particular legal protection; therefore, both Constitutions provide special fundamental rights for children. As far as internet is concerned, especially because this technology is increasingly accessible to unsupervised children, children's dignity is particularly threatened. Aggravated penalties have been provided as a means of deterrence in order to better protect them.

1.2. POSITIVE AND NEGATIVE IMPACTS OF THE CYBERSPACE ON THE EXERCISE OF THOSE RIGHTS

1.2.1. **Internet as a platform for freedom of speech**

As said in the introduction, Internet has been a vehicle providing and expanding a large panel of opportunities for individuals to exercise their human rights worldwide. Especially regarding freedom of speech and expression, the cyberspace allows for individuals to become much more active and proactive because they can, thanks to the Internet, communicate instantaneously worldwide, reach information, actively collect, publish and share news and data. Access and dissemination of information is fast and widespread, it empowers people, broadens possibilities of debates, discussions, education material availability, all consistent with right to information, to education… The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression ended his report by saying that "*Unlike any other medium the Internet facilitated the ability of individuals to seek, receive and impart information and ideas of all kinds instantaneously and inexpensively across national borders. By vastly expanding the capacity of individuals to enjoy their right to freedom of opinion and expression, which is an "enabler" of other human rights, the Internet boosts economic, social and political development, and contributes to the progress of humankind as a whole*"[9].

[8] "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks", Art. 12, Universal Declaration of Human Rights

[9] F La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Report to the Human Rights Council, 17th session, UN Doc A/HRC/17/27 (2011), p 19, *available at*http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx (Last visited on December 11, 2013.)

1.2.2. **Cybercrimes violating human rights**

However, cyberspace does not only have positive impacts. Like any platform open to the public at large and where everyone is free to participate, Internet is a space where misuse can easily happen, subsequently leading to offenses, abuses and violations of other's rights. Conventional crimes, that already existed before the appearance of cyberspace, are now committed online and their impact differs depending on the way they are conducted and on the public they target and reach. Human rights can be infringed upon by an individual, a corporation, a government scheme etc. online.

For instance, offenses violating the freedom of speech and expression on cyberspace will be ones such as bullying, hate-crimes, racist or homophobic discourse, defamation, sexual harassment, stalking, obscene material dissemination which are offenses likely to be committed by other individuals and concerned with far-reaching content deemed illegal, while others could be the restriction of online content (a debate exists as to whether these precautions limit or protect users from infringements of their rights).

Above-mentioned content-wise offenses also impair on the human right of dignity and the freedom from discrimination. Consequences of such content-offenses can have tremendous impacts on one's life and health, especially when they target children.

Also, violations of the right to privacy online are quite diverse, and serve different purposes (commercial, advertisement, fraud, harassment...). Some common offenses are the tracking of personal information by stalking, hacking into a computer system, identity theft, unauthorized disclosure of data to other actors etc.

In this first part, we have looked at the sources and the ways in which human rights have been impacted by the cyberspace, as well as the kind of offenses that can be committed in general. In the next part, we will focus on the legal provisions providing for protection from and punishment of these offenses in the Indian and French legal contexts.

2. THE PROTECTION OF HUMAN RIGHTS IN CYBERSPACE

2.1. Cyberspace's legal frameworks

In India, there is one main body of law dealing with regulations of the cyberspace: The Information Technology Act 2000 amended in 2008 (IT Act, 2008). It addresses amongst other topics a list of offenses committed on cyberspace and their sanctions, as well as the law enforcement process for cybercrimes. Adding to this Act, the Indian Penal Code (IPC) provisions apply for a number of conventional offenses committed on the cyberspace. Further, several particular acts may apply depending on the cybercrime committed.

By contrast in France, there is no unique legislation regulating cyberspace but a set of laws composed by new laws focusing on specific issues raised by the development of internet, and by older ones. Insofar, the Law on the Press, 1881 is the main tool to protect the freedom of speech and expression including in cyberspace. In this case, internet is a means to commit crimes that have always existed; therefore, the

provisions of the Law on the Press remain applicable. On the other hand, new laws have been enacted in response to the emergence of new crimes. The Law on Information Technology, Data Files and Civil Liberties, 1978 is a case in point. It guarantees the access to personal data as a human right and regulates their protection[10]. To do so, it establishes the Commission Nationale de l'Informatiqueet des Libertés (CNIL), an independent regulatory body that aims to inform subject and controllers of their rights and duties and ensure that the processing of personal data is in conformity with this Act.[11] The Godfrain Act relative to computer fraud as well as the 1991 Act relative to secrecy of messages emitted via telecommunications are also two main elements targeting the regulation of cyberspace and the guarantee of human rights to French citizens. These laws have modified the Penal Code; whose provisions have to be analyzed.

2.2 CYBERCRIMES RELATIVE TO THE FREEDOM OF SPEECH AND EXPRESSION ON CYBERSPACE AND VIOLATION OF DIGNITY

2.2.1 Cyber harassment

In France, on September 12, 2013, the Senate[12] voted an Amendment of the Equality between Women and Men Bill establishing cyber harassment as a crime that should be punished by two years of imprisonment and a fine of 30 000€.[13] While the Bill is pending, the current legislation on sexual harassment is applicable for crimes committed online. It is composed by the Law on Sexual Harassment, 2012 and Art. 222-33 of the Penal Code which first section defines sexual harassment as "imposing on a person, repeatedly, remarks or behavior of a sexual nature that is impairing its dignity because of their degrading or humiliating character, or create against him a daunting situation hostile or offensive."[14] However, the current legislation does not recognize other forms of harassment. Moreover, cyber-bullying is not an offence punishable as such.

In India, there is no one specific provision applying to cyber sexual harassment. However, section 509 of the IPC[15] which makes the intent to insult the modesty of a woman illegal and punishable by a possible one-year jail sentence and/or a fine comes close to the possible contents of cyber sexual harassment offense. Also, cyber-stalking (also called online harassment), which can be defined as "the repeated acts of harassment or threatening behavior of the cybercriminal towards the victim by using internet services" comes under

[10] "Information technology should be at the service of every citizen. Its development shall take place in thecontext of international co-operation. It shall not violate human identity, human rights, privacy, or individualor public liberties." Art. 1, Law on Information Technology, Data Files and Civil Liberties, 1978

[11] Chapter III: The Commission Nationale de l'Informatique et des Libertés (CNIL), Law on Information Technology, Data Files and Civil Liberties, 1978

[12] French higher House of the Parliament

[13] http://www.pcinpact.com/news/82356-le-cyber-harcelement-bientot-infraction-a-part-entiere.htm

[14] The penalties are two years of imprisonment and a fine of 30 000€. Heavier penalties may be imposed in specific cases (minor, person abusing the authority conferred by his functions, etc.), Art. 222-33, PENAL CODE

[15] Sec. 509, IPC, "Whoever, intending to insult the modesty of any women, utters any words, makes any sound or gesture, or exhibit any object, intending that any such word, sound should be heard, or that such gestures or objects shall be seen by such women, or intrudes upon the privacy of such women, shall be punished with simple imprisonment for a term which may extend to one year, or with fine or with both.

section 503 of the IPC[16], as criminal intimidation committed through the use of computers. Put together, those two sections provide for the criminalization of cyber harassment, be it stalking, sexual harassment, cyber-bullying (which comes under criminal intimidation) Adding to that, section 66 A of the IT Act, 2008 provides punishment for sending offensive messages through communication services, whose nature can be that of what is used for cyber harassment and stalking.

2.2.2 **Cyber-racism, hate crimes**

In France, Art.24 of the Law on the Press states that: "Those who, by one of the means set forth in Art. 23 have led to discrimination, hatred or violence against a person or group of persons because of their origin or their membership or non-membership of an ethnic group, nation, race or religion, shall be punished by one year of imprisonment and a fine of 45 000€ or one of these penalties." In 2007, the Law on the Prevention of Crime has been enacted. Its Art. 40 modifies Art. 6 of the Law on Trust in Digital Economy to include racial hatred and Holocaust denial documents in the list of illegal content. Art. 227-23 of the Penal Code provides penalties for these crimes.

In India, the IT Act itself doesn't deal with cyber hate-speech or cyber-racism, but sections 153 A and 505 of the IPC clearly state that statements creating or promoting enmity, hatred or ill-will between different groups or classes based on race, language, place of birth, caste, community, region, religion… are criminalized and punishable[17].

2.2.3 **Cyber homophobia**

In France, Art. 24(2) of the Law on the Press also prohibits any act inciting "hatred or violence against a person or group of persons because of their sex, orientation or gender identity or disability caused or will, in respect of the same persons." Penalties are provided in Art. 225-2 and 432-7 of the Penal Code.

No such specific provision is provided in Indian legislation, though such offences, when committed, could fall under provisions providing penalties for cyber-defamation, cyber hate-crimes, or even cyber-bullying and cyber harassment.

2.2.4 Cyber defamation

The Law on the Press prohibits any form of defamation through any means of communication. Defamation is defined as "any allegation or imputation of a fact that undermines the honor or reputation of the person or body to which the act is attributed."[18] Defamation of individuals by any means is punishable of a fine of 12 000€ whereas defamation committed against a person or group of persons because of their origin

[16] Sec. 503, IPC, "Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of anyone in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation."

[17] Sec. 153A & 505, IPC: sanctions to be detailed

[18] Art.29, Law on the Press, 1881

or their membership or non-membership of an ethnic group, nation, race or religion is punishable by one year imprisonment and a fine of 45 000€ or one of these penalties.[19]

In India, the IPC provides dispositions for defamatory offenses in section 499 and 500, defamation consisting of "whoever, by words either spoken or intended to be read, or by signs or by visible representation, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm the reputation of such person".

2.2.5 **Dissemination of obscene material –including indecent representations**

In France, the Law on the Prevention of Crime established Art. 222-33-3 of the Penal Code which prohibits and punishes the saving or downloading of any images relative to the violation of a person's dignity. It constitutes a voluntary act of complicity with the integrity of the person under Art. 22-1 to 222-3 to 222-31 and 222-14-1 and is liable to fifteen years of imprisonment. The dissemination of registration of such images is punishable by a five-year imprisonment and a fine of 75 000€. This particular offence was created to deal with the practice of happy slapping which corresponds to the practice of filming the physical assault on a person using a mobile phone, in order to then distribute the corresponding video.

In India, sections 67 and 67 A of the IT Act deal with the punishment for publishing or transmitting obscene material and obscene material containing sexually explicit act in electronic forms (obscene material being defined as lascivious or appealing to the prurient interest or having as effect to tend to deprave and corrupt persons who are likely to read, see or hear the matter[20]) which consists of conviction for up to respectively five and seven years and or a fine. Adding to that, section 292 of the IPC also deals with the sale and dissemination of obscene material. Also, section 66 E of IT Act punishes the violation of privacy of individuals by the publication or transmission of the image of a private area without their prior consent, which amounts, once published or transmitted, to a violation of the dignity of the person and indecency of their representation. Further, the Indecent Representation of Women Act, 1986 prohibits any advertisements or publications (sections 3 and 4) that contain any indecent representation of women[21]. An amendment bill[22] currently seeks to explicitly widen the scope of the Act to cover Internet and cyberspace based-communications.

2.3 CYBERCRIMES RELATIVE TO THE RIGHT TO PRIVACY ON CYBERSPACE

2.3.1 **Cyber stalking – tracking of personal info**

Cyber-stalking violates the right to privacy when the stalker tracks and gets access to information they shouldn't. In France, cyber-stalking is not an offense punishable as such, but the author of acts for this purpose

[19] Art. 32, Law on the Press, 1881
[20] Section 67, IT Act 2008
[21] as defined in section 2(c), Indecent Representation of Women Act, 1986 ("the depiction in any manner of the figure of a woman, her form or body or any part thereof in such a way as to have the effect of being indecent, or derogatory to, or denigrating women, or is likely to deprave, corrupt or injure the public morality or morals"
[22] The Indecent Representation of Women (Prohibition Amendment) Bill, 2012

may be held liable on the basis of civil or criminal liability. For instance, the violation of the right to image is punishable by one year imprisonment or a fine of 45 000€ or both[23].

It is not an offense as such in India either, but it can be included in the reading of sections 503 and 509 of the IPC as mentioned in the above section on cyber-harassment.

2.3.2 **Hacking**

Hacking means unauthorized access to a computer system, and was defined in the IT Act 2000 as the fact of destroying or deleting or altering any information residing in a computer resource or deleting its value or utility or affecting it injuriously with the intent to cause or knowingly being likely to cause wrongful loss or damage to the public or any person[24].

The Godfrain Act, 1988 relative to computer fraud prohibits unauthorized access to a computer system, even without modification or use of data made available. It is punishable by two year imprisonment or a fine of 30 000€ or both.[25] These penalties are increased in case of theft or destruction of data.

In India, section 66 of IT Act, 2008 read alongside section 43 of the Act provides for the offense of hacking if it is done "dishonestly or fraudulently" and punishment can amount to a term of three years of jail and or a fine when there is criminal liability (for that to happen, the dishonest or fraudulent intent has to be proved). If not, only section 43 providing for civil liability and compensation for damages (not exceeding one crore) is to be used.

2.3.3**Identity theft**

Identity theft is the act of taking the name of a third party. The initial article of the Penal Code criminalizing identity theft was impractical on the internet because an offense had to be committed with the identity of the third party. Hence, art. 226-4-1 has been created in 2011 in response to the increasing number of identity thefts on cyberspace. It states that identity theft or the use of one or more data of any kind of a third party's identity to disturb its tranquility or others, or to damage his honor or his account is punishable by one-year imprisonment and a fine of 15 000€.

In India, identity theft consists of "fraudulently or dishonestly make use of the electronic signature, password, or any other unique identification feature of any feature of any person"[26] and is an offense punishable by a three-year jail sentence and or a fine in the IT Act (section 66 C). Further, section 66 D also provides sanctions in the case of such impersonation undertaken for cheating by using computer devices alongside sections 416 and 419 of the IPC.

2.3.4 **Unauthorized disclosure/storage of information and privacy**

Art. 226-1 of the Penal Code defines the offence of violation of privacy which can take either the form of capture, recording or transmission of words spoken in private or confidential capacity, in a public or private

[23] Art. 226-1 & 226-2, Penal Code, 1994
[24] Sec. 66, IT Act 2000.
[25] Art. 323-1, Penal Code, 1994
[26] Section 66 C on identity theft, IT Act 2008

place, without the consent of the author or the form of fixing, recording or transmission, the image of a person in a private place without the consent of their subject.

In India, there are several diverse provisions within the IT Act, 2008 dealing with privacy: section 69, 69 A and 69 B provide the Government and notified agencies with powers to order possible interception, monitoring, decryption, blocking from public access of information, collecting traffic data etc. through any computer resource if need in the interest of the security of the nation, public order, the prevention of a cognizable offense. Hence effectively infringing on individuals' right to privacy. Section 67 C complements this as intermediaries have to retain information as prescribed by the government or be liable for punishment.

Otherwise, as mentioned above, section 66 E protects from offenses of voyeurism and obscene photography that obviously violate individuals' privacy. Concerning breaches of privacy, section 43 A provides for corporate liability when failing to protect sensitive personal data (neglect being the trigger causing wrongful loss or gain to any person) and unlimited compensation, while section 72 deals with the breach of confidentiality and privacy by disclosure of information / data relative to a person without their consent (and sets a liability of two years of jail and or a fine); and section 72 A sets punishment of up to two years of jail and or a fine for disclosure of information in breach of a lawful contract operated with the intent or the knowledge of being likely to cause wrongful loss or wrongful gain (intent has to be proven for the section to apply).

As well, sections 65 and 66 relatives to tampering and hacking into computer systems and modifying, possibly deleting data and information, are also sections covering offenses violating the right to privacy.

2.4 Cybercrimes relative to children's fundamental rights

2.4.1 **Child pornography**

In France art. 227-23 of the Penal Code prohibits pornography for any person below the age of 18. Recording, saving or sending pornographic images or videos of children in order to publish them is punishable of five years of imprisonment and a fine of 75 000€. In cases where children are below the age of 15, these actions are punishable even if they did not aim to be published. The penalty is increased to seven years of imprisonment and a fine of 100 000€ when the dissemination of the image or representation of minors are used in an electronic network of communications for an unspecified public. Moreover, a frequent or monetary consultation of online website providing such an image or representation of children is punishable by two year imprisonment and a fine of 30 000€. Last but not least, the attempt of offences provided under this section is liable to the same penalties.

In India, cyber child pornography - the publication or transmission of material depicting children in sexually explicit or obscene manners in electronic form, the enticement of children to online relationship etc.- is punished under section 67 B of the IT Act 2008 by a penalty up to ten years of jail and or a fine.

2.4.2 **Special provisions and protections for children**

The French Penal Code punishes the action of making violent or pornographic information available for children online.[27] Moreover, it increases the penalty for sexual assault when the child victim was brought into contact with the perpetrator through the use of an electronic network of communications for an unspecified public. The penalty is brought to seven years of imprisonment and a fine of 100 000€.[28]

Concerning child pornography in India, section 294 of the IPC sanctions any person letting children access any obscene material as described in section 293 with a conviction for a term up to three years and a fine, and increases the sentence in case of second conviction, hence protecting children from the access to obscene and pornographic material.

In this second part, we have listed some of the cyber offenses violating human rights exercise and looked at what were the provisions that applied in France and in India. in the next part, we will study the mechanism of law enforcement in the particular case of human rights violations on cyberspace in both countries.

3. Law enforcement in India and in France

3.1. French complaint process

In France, the judicial system is divided in two different orders: the criminal order and the civil order. Criminal courts are competent to settle disputes between private individuals and to punish the perpetrators of the criminal laws whereas civil courts deal with disputes but do not impose penalties (rent, divorce, eating, etc.). The offenses above-mentioned engaged the criminal liability of perpetrators. Offenses are organized in three categories according to the level of gravity of the offense and determining the tribunal which will judge it. Hence, the first degree of complaint is composed by the Tribunal de Police, the Correctional Tribunal and the Courd'Assises. Tribunal de Police's and Correctional Tribunal's judgments can be appeal in the Appeal Court whereas Courd'Assises' judgments can be appeal in the Courd'Assisesd'Appel. The last resort for any offense is the Cour de Cassation, the highest court. France being a member of the European Union, the complainant can bring an action in annulment before the Court of Justice of the European Union only if after being through all the national judicial level. This action enables the Court to review the legality of the contested act or sections and to annul it if in contradiction with the European Law.

As a member of the Council of Europe, France is a part of the European Convention of Human Rights. Any citizens of a member of the Council of Europe victim of the law can complain before the European Court of Human Rights by claiming that the national legislation is in contradiction with any articles of the

[27] Art. 227-4, Penal Code, 1994
[28] Art. 222-28, Penal Code, 1994

Convention. The Court may sentence France and ask to change the legislation. A case in point is *Söderman* v. *Sweden* in which the EuropeanCourt of Human Rights sentenced Sweden to fail to provide effective appeal possibility while the complainant was filmed naked when she was a child, action violating Articles 8 and 13 of the Convention.

In India, the liability of internet service providers is reinforced compared to France in so far as intermediaries have to publish strict and clear rules and regulations addressed to the users of their services listing a number of items that cannot be hosted on the server[29]. Shall any of these items come to the knowledge of any ISP, they are to remove them. The list itself is quite large and ranges from deceiving messages and impersonation to violation of property rights or information that could infringe one's right to dignity, the law and the freedom of speech by going too far (cases of obscenities, racial and hate speeches…). Hence the scope where ISPs can and are encouraged to intervene in India differs greatly from France.

4. SUGGESTIONS

4.1. Comparison of judiciary systems

The main difference between the French and the Indian judiciary systems is that there exists a Cyber Appellate Tribunal in India, a specific court for appeals, whereas there is no special court for cybercrimes in France. The lack of expertise and knowledge of judges has been raised and criticized leading to a self-initiative of judges in Appeal Courts. Some of them followed trainings and specialized themselves in cybercrimes. We suggest that the Minister of Justice makes compulsory the allocation of a judge specialized in cybercrimes in each Appeal Court. Moreover, a national study should be conducted in order to determine whether or not a special court, as the Indian one, is required. At first glance, it would make sense, especially after the official opening of the European Cybercrimes Center in 2013.

4.2 A CNIL in India

Regarding the protection of privacy in cyberspace, the creation of a specific law regarding data protection solely (like the one existing in France: Law on Information Technology, Data Files and Civil Liberties, 1978) would clarify the situation for the protection of personal data and hence for citizens' privacy rights in cyberspace whereas data protection as of now in India is covered by provisions present in several acts such as the Indian Contact Act (1872), the Indian Telegraph Act (1885), the Credit Information Companies Act (2005), the IT Act (2008 - sections 43 A & 72 A), the Public Financial Institutions Act (1993); hence many critics say that India lacks a proper data protection legislative framework and needs one to be more effective and ably focus on violations and infringements of privacy rights.

Also, there is no Data Protection Authority in India, as opposed to the presence of the CNIL in France (created by the above cited data protection law). It is an independent regulatory body whose aim is to ensure protection of personal data. To this effect, it has power of control and can issue sanctions (warnings or fines)

[29] IT (intermediary Guidelines) Rules, 2011

in case of infractions. Further, its missions also include informing people about their rights and obligations, protecting the exercise of those rights, and anticipating evolutions of technology to adapt regulation of data protection by giving advice and recommendations to the government on legislation of this topic. In the absence of a specific data protection legislation, such a body, if set up in India, could centralize demands and complaints regarding data privacy and protection.

4.3 Improving the legal frameworks

In France, there is no legislation regulating cyberspace but a set of laws composed by new laws focusing on specific issues raised by the development of internet and older once in opposition to India that has a whole body of laws on the matter. The main consequence is that several crimes don't have a specific definition when committed in cyberspace. This lack of definition is essentially found in laws protecting individuals such as cyber harassment, cyber bullying, cyber stalking etc. Although section 66 A of the IT Act defines several cybercrimes, there is no provision regarding cyber stalking and sexual harassment on cyberspace as sexual harassment is only prohibited in the workplace (Protection of Women against Sexual Harassment at the Workplace Act 2013). As these offenses take different forms in cyberspace, there is a need both in France and in India of legal clauses defining and punishing them in cyberspace. We are aware of the difficulties of such definitions but penal code's provisions are not enough to protect individuals against new forms of harassment facilitated by new technologies. Currently, the Equality between Women and Men Bill is pending in the French Parliament introducing the offence of "cyber harassment" defined as "the fact of using the new technologies of information and communication to humiliate or intimidate a person repeatedly over time".[30] It "may take several forms such as intimidation, insults, mockery or online threats, spreading rumors, hacking accounts and digital identity theft, creating a topic, group or a page on a social network against a person, or the publication of photos or videos of the victim so as to impair its dignity".

4.4 Liability of Internet Service Providers

The question of whether or not internet service providers should be liable for hosting illegal contents and their ability to withdraw them are still debated worldwide. France and India have contrasting views on the matter. On the one hand, ISPs are not judge or representatives of the State, therefore France objects to their empowerment which would consist of a restriction on users' freedom of speech and expression. On the other hand, the way ISPs are given guidelines to observe due diligence in order to prevent and avoid the cases of many instances (for instance of hate speech, obscenities, harassment) happening in India show that Indian stance on the topic is giving ISPs more responsibilities and limitations helps to fight cybercrimes, especially those violating the right to dignity, to be protected against discrimination and defamation as well as privacy.

Hence, in France ISPs don't have the duty to look for illegal data. According to Art. 6 of the Law on Trust in Digital Economy, ISPs cannot be held liable if they do not have actual knowledge of the illicit nature

[30]Parliamentary Assembly, Commission on Equality and Non-Discrimination, REPORT ON HARASSMENT, October 15, 2013 *available at* http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=20036&lang=fr(Last visited January 17, 2014)

of data except if said data is clearly illegal. However, neither the law nor judgments have defined what constitutes a "clearly illegal" offense. Hence, we argue that the expression "clearly illegal" should be legally defined in order to prevent ISPs that didn't react when such acts came to their knowledge to pretend that they weren't aware. Moreover, ISPs can only engage their civil liability which has been strongly criticized by Human Rights activists. Hence, we also argue that the French Law on Trust in Digital Economy should be amended to engage the criminal liability of ISP in case of violation of the Law.

By contrast in India, if ISPs do not have to filter contents of what they host, they have much clearer indications on what they have to forbid when what is considered illegal comes to their attention. As opposed to the French "clearly illegal" which indeed needs a definition, the rather exhaustive list of what is not to be allowed shall the ISP know of it is long and may even give place to some doubts as to whether such an extensive clause wouldn't impair on the freedom of speech by itself.

4.5 Increasing penalties to better protect children

In France, penalties are systematically modulated and more specifically effectively increased in case of aggravating circumstances, which include the situation of a minor being victim, included in case of cybercrimes[31].

Such a measure in India would possibly be effective against such crimes like as letting children access to pornography online, cyber pedophilia and other offenses, characterizing the even graver and more dramatic aspect of the crime when committed against a child, who is more vulnerable and hence exploitable than an adult with average cyberspace knowledge.

4.6 Promoting awareness

The French Ministry of Education in collaboration with E-enfance Association and supported by the European Commission has established a national campaign against child cyber-harassment. Cyber harassment is defined as "an aggressive act, committed intentionally by an individual or a group of individuals using electronic forms of communication, the way repeatedly against a victim who cannot easily defend it."[32] In school, children can be victim of harassment by other children. As children possess younger and younger phones and access to instant messaging, forums and social network, school harassment has taken a new form and develops itself outside school through cyberspace. Moreover, children victim of bullying or harassment in school are easier target for cyber predators. Actually, a study shows that 40% of pupils are subject to cyber harassment.[33] Hence, the campaign aims to raise awareness of children and parents and actively combat cyber harassment and cyber bullying.

---

[31]Les Circonstances Aggravantes en Droit Pénal - Notions, *available at*http://www.droit-cours.fr/circonstances-aggravantes-droit-penal/ (Last visited on January 7, 2014)

[32] "Cyber Harassment", Ministère de l'Education Nationale, *available at* *http://www.agircontreleharcelementalecole.gouv.fr/quest-ce-que-le-harcelement/le-cyberharcelement/#titre6)* (Last visited 11th December, 2013)

[33] C. Blaya, LES ADOS DANS LE CYBERESPACE, PRISE DE RISQUE ET CYBER VIOLENCE, 2013

There are also cybercrimes awareness campaigns in India but they are mostly happening locally (February 2013 in New Delhi by ND Police cybercrime cell targeting teenagers[34], a five day cyber safe campaign by Gurgaon police happening in schools[35]). Hence this type of campaigns should be spread and intensified in order to be more effective. Launching a national campaign would ensure a level awareness especially amongst youngsters nation-wide. Our argument is to use this tool of campaigning in a more spread and regular manner so that it can prove more effective.

4.7 Toward international cooperation

A major legal concern in the combat of cybercrimes is that they upset the national boundaries of criminal law: offenses and applicable laws differ from one State to another. In response, the Budapest Convention or Convention on Cybercrimes created by Council of Europe is the first international instrument to address cybercrimes. Open to signature in November 2001, it entered in force on 1st July 2004. The Convention deals specifically with offenses relating to copyright, fraud, computer-related, child pornography and offenses related to network security. It also contains a series of procedural skills, such as the search of computer networks and interception.

It aims to pursue "a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation.[36]It was supplemented by an additional protocol to criminalize the dissemination of racist and xenophobic propaganda via computer networks in March 2006.

The Convention has a larger scope than the Council of Europe any country can ratify it. Even if Canada, China and Japan helped in the redaction of the Convention, the United States is the first non-European country to ratify it in 2006 (and entered into force on 1st January 2007). France ratified it in 2005 as well as the additional protocol. It has already been ratified by forty one countries, while eleven countries have signed it.[37] As cybercrimes are in nature transnational, this Convention is a huge step in the criminalization and prevention of such crimes through a worldwide cooperation and unification of national legislations. During his 2009 visit to New Delhi, the head of Economic Crime Division of the Council of Europe publicly asked the Indian Government to join the Convention. The signature process has not started yet even though India has collaborated with the Council of Europe on the matter, a major event being the Cybercrimes & Network Security Conference that took place in New Delhi in May 2012. Signing and ratifying the Convention may be

[34]Delhi Police launches cyber awareness campaign, TIMES OF INDIA, February 20, 2013, *available at*http://articles.timesofindia.indiatimes.com/2013-02-20/internet/37199132_1_cyber-crime-cyber-laws-internet-safety (Last visited on January 7, 2014)

[35]Anchal Dar, Cybercrime awareness campaign begins in Gurgaon, THE INDIAN EXPRESS, April 30, 2013, *available at*http://archive.indianexpress.com/news/cyber-crime-awareness-campaign-begins-in-gurgaon/1109516/1 (Last visited on January 7, 2014)

[36] Preambule, Convention on Cybercrime, 2001

[37] Situation on 11th December 2013, data *available at* *http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=FRE* (Last visited 11th December, 2013)

a great step for India to combat cybercrimes and efficiently guarantee human rights of cyberspace users. Hopefully, it will launch dynamism through Asian countries and enhance their collaboration.

CONCLUSION

Cyberspace legislations in India and in France, and more generally around the world do not essentially focus on human rights protection, they are laws or bodies of clauses that provide for specific cyberspace issues such as data protection, ISP reliability etc. but never solely for human rights protection and free exercise promotion online. Hence, there is a need to reinforce existing clauses to effectively protect people from human rights violations in both countries.

There have been some private human rights activists' initiatives – Bill of rights in cyberspace or Declaration- written, but they seem idealistic and unlikely to be implemented, especially as some clauses would be virtually impossible to realize; however, the idea in itself shows the fact that legislations are partially lacking as far as human rights on cyberspace are concerned which is why these activists feel the need to propose such projects. In such a context, the best enforceable solution would be enhanced international cooperation, which would be binding on ratifying countries and which would make them coordinate their policies more than just regionally.

Hence, our hypothesis is confirmed by this paper and suggestions were proposed that would possibly increase the concern for human rights on cyberspace and their need for special focus.

TABLE OF AUTHORITIES

Cases

France:

- Constitutional Council, Decision n°94-343/344 DC, 27th July 1994

European Court on Human Rights

- *Söderman* v. *Sweden*, 2013

Books

- Professor VimlenduTayal, CYBER LAW, CYBER CRIME, INTERNET AND E-COMMERCE, Bharat Law publications
- S.T. Vishwanathan - INDIAN CYBER LAW AND CYBER GLOSSARY –
- Dr. R.K. Chaubey, AN INTRODUCTION TO CYBER CRIME AND CYBER LAW, 2009
- K. Jaishankar, CYBER CRIMINOLOGY, CRC Press

Legislative material

In France

- French Constitution, 1948

- Declaration of Rights of Men and Citizens
- Penal Code and Penal Procedure Code
- Law on Information Technology, Data Files and Civil Liberties, 1978
- Law on the Press, 1981
- Godfrain law on Computer Frauds, 1988
- Law relative to the secrecy of correspondences sent via telecommunications, 1991
- Equality between Women and Men Bill, 2012

In India

- Constitution of India, 1950
- Indian Penal Code, 1860
- IndianContractAct, 1872
- Indian Telegraph Act, 1885
- Public Financial Institutions Act, 1993
- Credit information Companies Act, 2005
- Information TechnologyAct, 2000 & 2008 Amendement
- Protection of Women against Sexual Harassment at the Workplace Act, 2013
- Privacy Bill, 2013

Reports

- The internet and Human Rights: Building a free, open and secure Internet - Messages from Berlin, Chaipersons' Summary of the 2nd berlin Cyber Conference, September 13 & 14, 2012
- Human Rights in a Wired World - How Information & Communications Technology impacts human Rights, A special BSR Series, BSR, June 2009
- First Analysis of the Personal Data protection Law in India - Final Report, CRID - University of Namur available at http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_india_en.pdf
- Toby Mendel & Al., Unesco Publishing, Global Survey on Internet Privacy and Freedom of Expression, Unesco Series on internet Freedom
- Parliamentary Assembly, Commission on Equality and Non-Discrimination, REPORT ON HARASSMENT, October 15, 2013 *available at* http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=20036&lang=frF
- La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Report to the Human Rights Council, 17th session, UN Doc A/HRC/17/27 (2011), p 19, *available at* http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx

- "UN Treaty Collection : International Covenant on Civil and Political Rights", United Nations, updated data on 11th December 2013 *available at* http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en

Articles

- http://www.pcinpact.com/news/82356-le-cyber-harcelement-bientot-infraction-a-part-entiere.htm
- Anchal Dar, Cybercrime awareness campaign begins in Gurgaon, THE INDIAN EXPRESS, April 30, 2013, *available at*http://archive.indianexpress.com/news/cyber-crime-awareness-campaign-begins-in-gurgaon/1109516/1
- Delhi Police launches cyber awareness campaign, TIMES OF INDIA, February 20, 2013, *available at*http://articles.timesofindia.indiatimes.com/2013-02-20/internet/37199132_1_cyber-crime-cyber-laws-internet-safety

Conventions

- Universal Declaration of human Rights, 1948
- European Convention on Human Rights, 1950
- International Covenant on Civil and Political Rights, 1966
- Convention on the Rights of Children, 1990
- Convention on Cybercrime, 2001

Websites

- Le service public de la diffusion du droit, *available at* http://legifrance.gouv.fr/
- Les Circonstances Aggravantes en Droit Pénal - Notions, *available at*http://www.droit-cours.fr/circonstances-aggravantes-droit-penal/

Miscellaneous

- Data Security Council of Indian, Memorandum on Cyber Security and Right to Privacy, submitted to Standing Committee on Information Technology, July 9, 2010