Fondation Scelles, Charpenel Y. (under the direction),
Prostitution: Exploitation, Persecution, Repression,
Ed. Economica, Paris, 2016.

Cyber-Vulnerability amongst Social Media Users

The explosion of the Internet has revolutionized human relations, most notably with the increasing use of social media sites, and these virtual communities have taken up an important place in the daily life of almost all web users. The term social media network can be applied to all platforms of online communication that allow users to create networks predicated upon common interests. There are currently over 700 of these networks around the world[1].

These networks ask users to supply personal information, which allows the users to create an online "profile". They also provide tools that allow users to upload their own content and a list of contacts, with whom they can interact (*AJ Pénal*, May 2012).

These social media networks allow free interaction between their users and the possibility to create new and positive links; however this liberty of interaction also creates conditions for abuse. Due to our current addiction to oversharing everything about our private lives online, the vulnerabilities arising from the use of social media networks are increasing. Thus, it suits every person to measure the risks well, which is far from being evident, if we consider the numerous affairs in which users become cybervictims (*Quemener*, 2013). In this free space, one meets not only friends, but also people who can belong to organized networks searching for vulnerable targets – and in particular children.

Indisputably, the idea of Internet freedom, or at least the illusion of it, creates the ideal environment for organizations offering prostitution on web sites, which puts vulnerable users at risk. Social media networks have done nothing but increase the frequency of this phenomenon, as they are the perfect platforms to seek out future victims by making them feel at ease by fostering their trust over time.

The Internet's assurance of relative anonymity, its ephemeral exchanges and its global character have encouraged procurers and various criminal networks to resort to the most discrete means of developing their illegal activities.

In addition, users can perceive their online relations to these criminals as harmless or completely safe, and then be tricked by the seductive criminal tactic of contacting the victims over a long period of time. The criminal is a friend before he becomes an enemy.

The active participation of cyber-procuring victims - their role in speaking to the criminal, exchanging with them and building a relationship - has led some to question if they are in fact culpable, and in some ways, responsible for the inevitable situations in which they find themselves. This raises questions about the complexity of online relationships for fragile

[1] Avis 512009 on the online social network, adopted on June 12th 2009, Workgroup on "article 29 sur la protection des données".

and vulnerable users. So as to understand the nature of these threats, we should present the exploiters' operating modes of targeting the victims of prostitution, and present the legislative responses at both the national and international level.

Cyber Threats to Individual Freedom and Private Life

Firstly, it must be noted that online social networking is the most practical method of communicating for many Internet users, supplying the user with several ways of communicating.

Users often have a tendency to communicate using games and other entertainment based platforms. This leads to intimacy issues (*Adolescence*, 2013) for users who often struggle to figure out who they are, which can lead to a very real maladjustment issue in adolescents.

The wide exposure of private life is equally considered to be another vulnerability arising from frequent social media usage. In this context, users demand that services provide a maximum confidentiality. The giants of this industry (software providers like Google, Twitter and Facebook or hardware providers like Blackberry, Samsung and Apple) creatively compete to seduce new users. All guarantee the most advanced encryption services, whose infallibility is supposed to keep the correspondence of its users safe from privacy invasions. Due to this situation, education and awareness are essential.

Cyber Threats to Identity: Identity Theft and Cyberstalking

The vulnerability of social media users is especially noticeable when their identity is exposed. It is not only the name of the victim which is targeted, but their identity and, more broadly, any "information which makes them identifiable in real life". Data which allow an individual to be identified are numerous and varied: first and last name, pseudonym, photo, marital status, company name, website domain name, IP address, e-mail address…

French Homeland Security law no.2011-267 of 14 March 2011 (called the LOPPSI II law) introduced a specific offense of identity theft which incorporates those perpetrated on digital networks to the French Penal Code. Thus, article 226-4-1 of the French Penal Code punishes 'the act of impersonating a third party or making use of one or more data of any kind that can be identified as those of the third party, in order to disturb the tranquility of the third party or others, or damage his name or social standing'. This new rule filled a hole in the law, allowing the authorities to respond to acts which previously would not have been considered criminal offences. Some previous judicial acts had actually sanctioned acts of identity theft on social media networks on the basis of Article 9 of the French Penal Code which regards respect for private life.

There is also another method of harassment online particular to social networks. The victim receives repeated messages, containing threats, insults, or blackmail. In order for the messages to stop, the senders of these messages may also demand money, a sexual meeting or personal information. This type of harassment is most commonly found on social networks with an absence of identity authentication where anonymity allows the perpetrators to operate with impunity.

Article 222-33-2-2 of the French Penal Code[2] states that 'the legal consequences of harassing an individual by repetitive behavior or words leading to impacts on the physical or mental health of the victim amount to a one year prison sentence and a 16,520 US$ (15,000 €) fine when the harassment has impacted the victims' ability to work, resulting in the loss of eight or less working days or no inability to work. The facts mentioned in the first paragraph are punished with a two year prison sentence and a 33,735 US$ (30,000 €) fine. However the lawmaker has provided, in that matter, for an aggravated circumstance because of the use os online communication with the public, which is then punished with a 3 year prison sentence and 49,560 US$ (45,000 €) fine. Victims have consequently much greater power of prosecution than before and their cases should be processed more rapidly by relevant police services.

Cyber Victims of Prostitution and Human Trafficking

Most organized prostitution and human trafficking networks today use the Internet to develop their business – and they particularly make use of social media (*Fondation Scelles*, 2013). Sexual criminals are generally, just as present on social media as on the Internet, with underage pornography being the most odious example (*Robert*, February 2014), which is sometimes accompanied by links to sites where one can find organized prostitution networks.

The apparent distance between Internet users results in seduction behaviors, drawing new victims into negotiations orchestrated by predators who desire the sexual services of their victims. Sexual negotiations take on a banal and ordinary appearance, seeming to be simply another form of e-commerce (*Fondation Scelles Infos*, April 2014). A recent case has led to the arrest of several people, who had got acquainted through social media, to an indictment for illegal procuring work.

The Legislative Response

Article 6.I.–1 of the Law for Digital Economy (LCEN, no. 2004-575 of June 21st, 2004) states that 'Internet service providers (ISPs) must inform their customers of the existence of technical means to restrict access to certain types of services; they must also provide their customers with at least one of these technical means.' Simply put, service providers must inform their customers of the existence of parental controls and make them easily available to the customer. Furthermore, the same law states that ISPs are not required to monitor the information they transmit or store, nor are they under any obligation to search for illegal activity. However, they must contribute to the fight against the spread of criminal activity, given the general interest attached to the repression of such acts as advocating crimes against humanity, incitement of racial hatred, child pornography, incitement of violence – including incitement to violence against women - and violations of human dignity.

[2] Law no.2014-873 (August 4th, 2014) concerning real equality between women and men.

Specific Protections for Minor Cyber Victims

The growing importance of social networks in everyday life feeds into another phenomenon – the online solicitation of children for sexual purposes (grooming). At the heart of this activity is manipulation. An adult will take advantage of a child's vulnerabilities to propose, via electronic means of communication, a meeting – using it as an opportunity to commit sexual abuse. Grooming is a progressive activity, designed to gradually build a relationship of trust with the victim, who is then prompted to send intimate photos. The child is then blackmailed by the adult, who threatens to send the photos to their parents, their school or their friends. This grants the abuser control, allowing him to continue the abuse without discovery. A recent survey reveals that one in a hundred children has been asked during the previous year for photos or videos showing sexual acts, or has been asked to speak about sexual acts.

French law specifically refers to grooming as 'when an adult makes sexual proposals to a minor – under the age of 15, or a person posing as such – using electronic communication'. Grooming is punished by two years' imprisonment and a 33,000 US$ (30,000 €) fine. This punishment is increased to five years' imprisonment and a 82,552 US$ (75,000 €) fine if the grooming activity culminated in physical contact (article 227-22-1 of the French Penal Code). This law - by its provision for adults posing as minors - allows the authorities to more effectively track down online predators.

Law No. 2007-297 of 5 March 2007, on the prevention of delinquency, is fully applicable when the acts were committed through social media networks – it contains provisions designed to suppress certain deviant behavior in the use of the internet which particularly affects minors (*AJ Pénal*, March 2009).

Thus, infractions against sexual harassment of a minor (Penal Court, art. 227-22-1) prohibit "adults from making sexual propositions to a 15 year old minor, or to a person who presents themselves as this age, through using electronic communication, also known as 'grooming' ". This infraction, which specifically prohibits the targeting of minors via the Internet or by SMS, is punishable by up to two years imprisonment and a 33,000 US$ (30,000 €) fine. The penalties are increased to five years imprisonment and a 82,552 US$ (75,000 €) fine when online sexual exploitation led to a meeting in person. This infraction aims to track adult predators who approach minors via social media networks, by pretending to be minors themselves.

The Aggravated Circumstances of Using a Social Network

Human trafficking is a crime punishable by seven years in prison and a fine of up to 165,105 US$ (150,000 €) (article 225-4-1 of the French Penal Code). However, aggravated punishments are provided for by articles 225-4-2 and the following articles of the French Penal Code. Article 225-4-2 provides for a sentence of 10 years imprisonment and a 1.65 million US$ (1.5 million €) fine when the offence is committed in two circumstances referred to in parts one to four of Section 1 of Article 225-4-1 of the French Penal Code. The same penalties are provided when the criminal act is performed with any of the following circumstances:

- The act involves several people
- An act taking place outside the territory of the Republic or at the time of their arrival on the territory
- When the perpetrator has been in contact with the victim using electronic communication for the express purpose of subsequent public dissemination

Prevention and awareness: indispensable tools

While the average Internet user is rarely a victim of crime, they are often the unintended facilitators. This is particularly true for those who reveal very personal information online without being aware that it may one day be turned against them, and we know that this risk concerns minors in particular.

More than any other type of user, minors must be made aware of the numerous risks posed by their Internet use, and they must equally be made aware of the protective measures that they can take to counteract this risk. The French National Consultative Commission on Human Rights advises this as necessary for a 'culture of caution and security'. The specificity of these issues, as suggested by the number of concerned organizations, has led the French Children's Ombudsman to suggest the creation of a specific platform for reflection, public proposals and intervention; bringing together all public and private actors in order to establish a uniform digital policy regarding minor internet users in France.

This call for a more unified approach joins the call of many other concerned bodies, who would like more impetus put on the coordination and intervention on the part of public bodies, real media training for professionals working with young people, changes in the classification of web content, better consideration of European Charters, and research incentives made available (*Robert*, February 2014). This finding emphasizes the importance of teaching our children about appropriate internet usage, whilst offering a reminder concerning the common values of freedom of expression, which the penal law could limit in its efforts to fight cyber criminality.

The third recommendation of the inter-ministerial report (*Robert*, February 2014) on the fight against cyber criminality emphasizes the following suggestions:

1. A higher level of state involvement in terms of momentum, goal setting and long-term control over the policies designed to prevent cybercrime by:
- Public awareness campaigns on personal data protection and vigilance against scams
- More audience-specific campaigns and help centers
- The creation of 17 online platforms whereby anyone can report online criminal activity occurring on social media networking sites
- Systematically carrying out risk assessments before opening any new services in a regulated domain

2. Making the Internet user its own moderator, and the leading party in the fight for security for users and the fight against inappropriate images or text and illegal activity by:
- Educating young people about the Internet in schools and mobilizing trainers already established in the 5,000 public Internet access centers across France, whilst also assuring the continued availability of high levels training
- The development of information centers with online or telephone accessibility

- Homogenizing the materials which advertise prevention in public settings
- The creation of a search engine to facilitate the detection of sites, companies or spam e-mail addresses associated with illegal online activity
- Streamlining the ways users can flag up illegal activity to authorities
- Improving the coordination and involvement of the various victim support organizations

3. Mobilize the various involved professionals and assure the best awareness raising and advocacy (…)

Stricter Sentencing Guidelines

A recent government flyer circulated with the aim of defining criminal policy directions to strengthen the fight against cybercrime. For the first time, the term cyber prostitution was used in this type of document (*Official Bulletin of the Ministry of Justice*, January 22nd, 2015). Trafficking in human beings for sexual exploitation is the oldest form of human trafficking and the most widespread. In France today foreign trafficking networks mainly do this form of trafficking. Using experienced management and operational logistics, international prostitution networks move their victims swiftly through any given territory, and use the Internet and social media networks to provide logistical support and coordination. This assures a constant replenishment of sex workers coming into France from Romania, Bulgaria, Africa and China, whose activities are often hidden behind legal establishments such as massage parlors. This type of activity is growing, and its discretion, scale and operation outside of spheres accessible to the law make detection and investigation more complex and difficult to achieve.

Due to these circumstances, it must be stressed that the fight against this phenomenon should be a governmental priority[3]. To this end the National Consultative Commission on Human Rights (CNCDH), has launched a widespread consultation process to define the priorities of their new mandate as National Reporter on Trafficking in Human Beings. This consultation should, of course, focus on current trends in the methods employed by human trafficking organizations, and their use of the internet organizations will be subject to investigation in this study.

Sources

- Bailly E., Daoud E., « Cybercriminalité et réseaux sociaux, la réponse pénale », *AJ Pénal*, no. 5, May 2012.
- Charpenel Y., « La prostitution sur internet, au cœur de l'actualité », *Fondation Scelles Infos*, no.28, April 2014.
- "Circulaire du 22 janvier 2015 de politique pénale en matière de lutte contre la traite des êtres humains", *Official Bulletin of the Ministry of Justice*, NOR : JUSD1501974C, January 22nd, 2015.
- CRIDES/Fondation Scelles, *Revue de l'actualité internationale de la prostitution*, 2013.

[3] The National Action Plan against the trafficking of human beings, adopted by the Counselors of Ministers may 14th, 2015, aims to put in place orders 2011/36/EU from the European parliament and the council on April 5th, 2011. This plan was announced by the President of the French Republic.

- CRIDES/Fondation Scelles, *Revue de l'actualité internationale de la prostitution*, 2014.
- Fondation Scelles, Charpenel Y. (under the direction of), *Sexual Exploitation – A growing menace*, Economica Ed., 2013.
- Gozlan A., Masson C., « Le théâtre de Facebook : réflexion autour des enjeux psychiques pour l'adolescent », *Adolescence*, 2/2013 (T.31 no.2), 2013.
- Quemener M., « Réponses pénales face à la cyberpédopornographie », *AJ Pénal*, no.3, March 2009.
- Quemener M., *Cybersociété - Entre espoirs et risques*, L'Harmattan Ed., Coll. « Justice et Démocratie », 2013.
- Robert M., ministère de la Justice, ministère de l'Economie et des Finances, ministère de l'intérieur, ministère des petites et moyennes entreprises, de l'innovation et de l'économie numérique, *Protéger les internautes - Rapport sur la cybercriminalité*, Groupe de travail interministériel sur la lutte contre la cybercriminalité, February 2014.

