# Cyber Crimes against Women: Qualification and Means

**Nadjiba Badi Boukemidja**

PhD, Lecturer at Algiers University -1- , Faculty of law, Algeria.

**Abstract**

Crimes against women are constantly changing, especially with the emergence of electronic means to express them. Thus, violence against women using electronic means, has become a phenomenon with multifaceted manifestations and causes also multiple, it must be measured in all its aspects to combat it effectively. Of course, violence also takes place in the context of a relationship of power and domination, which explains why electronic violence predominates over female violence, which remains largely contained. This violence can be psychological, it consists in denigrating, humiliating, degrading the woman in her human value. It is manifested by verbal attacks, insults, threats, pressure, blackmail, control of activities, isolation of relatives, friends and the outside world. Also, verbal abuse in electronic form, which is the constant repetition of insulting words or insults to a woman. In mistreating the woman, the person behind the screen hurts her as much as if she hit her, because the woman in this case loses self-esteem. Verbal abuse can lead to a range of behavioral, emotional and physical problems. Violence in this context results in the use of hurtful or humiliating words, such as naming a person who is ridiculous, insulting the woman, making racist comments or incessant teasing. In addition to general harassment and sexual harassment more specifically, who may be subject to violence against women, by electronic means. The problem concerns the legal qualification of this kind of violence, what the old texts are enough, then they apply automatically; or the new texts are needed.

**Keywords:** women, violence, harassment, problems, electronic, legal

## Introduction

The mobilization of women against violence against women increased in the early 1980s, and the third World Conference on Women held in Nairobi in 1985 made the issue more prominent. The Nairobi Forward-looking Strategies for the Advancement of Women took into account the prevalence of violence against women, "in various forms, everywhere, in everyday life", and identified the various manifestations of violence against women. This violence by drawing attention to the situation of women who are victims of domestic abuse or trafficking and forced prostitution, as well as the situation of women suffering from armed conflict and women prisoners.

The link between violence against women and other issues on the United Nations agenda was started when this violence emerged as a major impediment to achieving the goals of the United Nations. United Nations Decade for Women: Equality, Development and Peace. Forward-looking Strategies have advocated for preventive policies, legal measures, a country-specific approach and comprehensive assistance to women victims of violence. In addition, these Strategies confirm the need to raise public awareness of violence against women as a social problem.

The emergence of international definitions of gender-based violence and violence against women dates back to the early 1990s. Thus, in 1992, the General Recommendation of the UN Committee on the Elimination of Discrimination Against Women [1] defines gender-based violence as "violence directed against a woman because she is a woman or especially affects women" [2].The 1993 United Nations Declaration on the Elimination of Violence against Women [3] proposes the first internationally agreed definition of violence against women, namely: all acts of violence directed against and causing or

[1] -C.E.D.A.W.
[2] - Article 6
[3] - Article 1

causing to women physical, sexual or psychological harm or suffering, including the threat of such acts, coercion or arbitrary deprivation of liberty, whether in public life or private life.

Other agreements and reports of the United Nations, the Council of Europe, the Fundamental Rights Agency of the European Union and the European Institute for Gender Equality (EIGE) align themselves largely to these initial definitions (FRA 2014). In 2011, the Convention on Preventing and Combating Violence against Women and Domestic Violence [1] was adopted by the Council of Europe and signed by France. The Istanbul Convention marks a major turning point for the following reasons: it is legally binding; it has a monitoring mechanism, G.R.E.V.I.O.[2] to monitor compliance by the parties; it defines violence against women as both a cause and a consequence of gender-based power struggles. It advocates an integrated approach that incorporates the achievement of gender equality to eliminate violence against women.

The Istanbul Convention defines violence against women as both a cause and a consequence of gender-based power struggles. It recognizes that violence against women is a manifestation of historically unequal power relations between women and men; that it is one of the crucial social mechanisms by which women are kept in a position of subordination to men; and that the achievement of equality between women and men is a key element in the prevention of violence against women. It also recognizes that women and girls are at greater risk of gender-based violence than men, and that domestic violence disproportionately affects women [3].

But the problem that arises is the specificity of cyber crimes against women, is this type of delict is subject to traditional rules in the context of adaptation or new rules is imposed in relation to the nature of the offenses.

For this, we answer the problem according to the following axes :

**1- Adaptation of traditional rules in cyber crimes against women**

**2- Imposition of new rules in cyber crimes against women**

**3-The specificity of the evidence in relation to cyber crimes against women .**

**1- Adaptation of traditional rules in cyber crimes against women**

The increasing spread of the internet, the rapidity of information dissemination through mobile devices and the widespread use of social networks, coupled with the existing pandemic of violence against women and girls, have created a global problem that is growing: cyber violence against women and girls, a phenomenon that can have major economic and societal consequences.

According to research in this area, one in three women will experience a form of violence in their lives, and although the development of the internet is a relatively new and growing phenomenon, an estimated one in ten women already been a victim of a form of cyber violence at the age of 15 years. Access to the internet is rapidly becoming a necessity for economic well-being and is increasingly seen as a fundamental human right. It is therefore crucial to ensure that this digital public space is a safe environment and a source of increased autonomy for all, including women and girls " [4].

According to the declarations of the UN In the last ten years, some American and European pornography producers have moved to places such as Budapest, Hungary because of the availability of cheap actors from Eastern and Central Europe. Budapest is also a destination and transit city for women trafficked from Ukraine, Moldova, Russia, Romania, and countries of the former Yugoslavia. The city is also now the biggest center for pornography production in Europe, eclipsing traditional centres such as in Amsterdam and Copenhagen.

[1] - The so-called Istanbul Convention

[2] - The Group of Experts on Combating Violence against Women and Domestic Violence

[3] - Gill Allwood , la violence à l'égard des femmes fondée sur le genre dans la France contemporaine ; Modern & Contemporary France, DOI. http://dx.doi.org/10.1080/09639489.2017.1340003.

[4] - Cyber violence à l'encontre des femmes et des filles , Institut européen pour l'égalité entre les hommes et les femmes (EIGE) , 2017.

In 2014 a virtual market was uncovered involving four websites, online forums and some 30 groups on a popular Chinese messaging platform, connecting traffickers with potential buyers. Some 200,000 persons are kidnapped in China every year and sold online [1].

When women and girls do have access to and use the Internet, they face online forms and manifestations of violence that are part of the continuum multiple, recurring and interrelated forms of gender-based violence against women.

Despite the benefits and empowering potential of the Internet and ICT[2], women and girls across the word have increasingly voiced their concern at harmful, sexist, misogynistic and violent content and behaviour online. It is therefore important to acknowledge that the Internet is being used in a broader environment of widespread and systemic structural discrimination and gender-based violence against women and girls, which frame their access to and use of the Internet and other ICT.

Emerging forms of ICT have facilitated new types of gender-based violence and gender inequality in access to technologies, which hinder women's and girls' full enjoyment of their human rights and their ability to achieve gender equality .

Terminology in this area is still developing and not univocal. In several official United Nations documents, and in particular the 2030 Agenda for Sustainable Development, reference is made to the general and inclusive term "information and communications technology" , while in other reports "online violence", "digital violence" or "cyber violence" are used. In the present report, the Special Rapporteur refers to "ICT-facilitated violence against women" as the most inclusive term, but mainly uses "online violence against women" as a more user-friendly expression.

Where appropriate, she uses both and terms, as well as the terms "cyber violence" and "technology-facilitated violence" as alternatives. Mindful that many forms of online violence covered in the report are perpetrated against both women and girls, she uses the term "women" in a hasty manner, which includes girls whenever applicable, while recognizing that girls are a frequent target of this form of violence [3].

The "violence" that comes from the Latin "vis" designating the force, is the fact of using force, to exert the domination and the physical or moral constraint on a person, to reach it in its physical or psychic integrity . It is found in the public sphere or in the private sphere, within the family and especially within the couple.

Concerning psychological violence, it consists in denigrating, humiliating, degrading the woman in her human value. It is manifested by verbal attacks, insults, scenes of jealousy, threats, pressure, blackmail, control of activities, isolation of relatives, friends, and the outside world.

Verbal abuse is the constant repetition of insulting words or insults to a woman. By mistreating the woman, the man hurts her as much as if he hit her, because she loses self-esteem. Women living in such situations come to believe that they are worthless and think that it is useless to try to be something else. Verbal abuse can lead to a range of behavioral, emotional and physical problems.

Verbal abuse in this context results in the use of hurtful or humiliating words, such as giving a ridiculous nickname, insulting the woman, making racist comments or incessant teasing.

Firstly , stealth tracking online is a hunt done through email, text messages (or online) or the Internet. It consists of repetitive incidents that can be individually harmless or not, but which, accumulated, can generate in the victim a sense of insecurity, cause him a certain distress, frighten him or alarm him. Stealth tracking online may include: sending emails, text messages (SMS) or offensive or threatening instant messages; Publication on the Internet of comments offensive to the person; Sharing of photos or intimate videos of the person, on the internet or by means of a mobile phone. In order to be considered a stealth hunt online, these acts must be done in a hasty manner and committed by the same person.

For exemple Cyber Stalking can take many forms, but for the purposes of this document, we will cite the following behaviors: electronic mail and text (or online) messages that are sexually explicit and unsolicited s; Av Offended and offensive

[1] - Cyber violence against women and girls a world –wide wake –up call a report by the UN broadband commission for digital development working group on broadband and gender ,2015.
[2] - Information and communications technology
[3] - Report of the Special Rapporteur on violence against women, its causes and consequences of online violence against women and girls from a human rights perspective, Human Rights Council, Thirty-eighth session , 18 June–6 July 2018, A/HRC/38/47.

advances on social networking websites or on online chat sites; Threats of physical and / or sexual violence by electronic mail or text message (or online); Hateful speech, offensive, insulting, threatening, or self-targeting individuals motivated by their identity (gender) or other characteristics (ex : sexual orientation or disability) [1].

Cyber Stalking is one of the most widespread net crimes in the modern world. The word “stalking” means "pursuing stealthily". Cyber stalking can be used interchangeably with online harassment and online abuse (Muthukumaran 2008). It is the use of the Internet or other electronic means to stalk or harass a GJRIM Vol 4, No 1, June 2014 40 person(Kumar 2010). The utilization of technology allows stalkers to harass their target from oceans away (Cyber Stalking 2011) .It involves invading the privacy by following a person's movements across the Internet by posting messages on the bulletin boards, entering the chat-rooms frequented by the victim, constantly bombarding the victim with messages and emails with obscene language. While Cyber Stalking affects both men and women, women are disproportionately targets, especially of age group of 16-35, who are stalked by men.

It is believed that Over 75% of the victims are female. More than one million women and 370,000 men are stalked annually in the United States. An astonishing one in twelve women and one in forty-five men will be stalked in their lifetimes (Moore 2009) .

In Cyber Stalking, stalker access the victim’s personal information like name, family background, telephone numbers and daily routine of the victim and post them on the websites related to dating services with the name of victim [2].

Efforts to categorize online sexually violent threats and nonconsensual sharing of intimate photos, for example, as sexual violence are working against a strong social current of resistance [3] . This reluctance reveals important social attitudes, and in fact tells us a great deal about how well equipped we feel as a society to deal with the complications that arise from taking online sexual violence seriously. In this context, two questions are important to keep in mind.

First, what other forms of violence were once considered inevitable (and even acceptable) for many women? Marital rape, domestic violence, and the sexual harassment of women and girls in the workplace and in schools were all once socially acceptable, and attitude changes took time (and are still underway). Second, whose interests lie in maintaining the status quo, where online sexual violence is often trivialized? Defining something as violence is a call to action, a way to explicitly convey that certain behaviours are an abuse of power; harmful; and unacceptable.

**«** *Just ignore the trolls. Don’t share personal information. Go offline. »* These mantras pervade discussions of digital communication and the abuse and harassment that occur online. Although often well meaning, these statements contain problematic assumptions about whose responsibility it is to prevent harassment and how seriously we take certain forms of abuse. These statements also contain insights into how we relate the online interactions to the physical world, or what is often referred to as “in real life.” However, this is changing.

Like sexual harassment and domestic violence in previous decades, advocates and activists are rejecting the notion that online abuse and harassment is an unfortunate but inevitable feature of girls’ and women’s existence. This notion is being replaced by a growing understanding that much abuse and harassment online is a manifestation of broader social ills such as misogyny, racism, and homophobia, and should therefore be taken seriously [4].

The attack, which is close to the previous form, is the revenge porn,it is generally described as the practice of someone (usually a man) sharing intimate photos in order to humiliate an ex-partner (usually a woman). The photos are often thought to have been taken consensually initially (though this is often not the case), but are then used by the “spurned lover” for revenge when the relationship ends.

Revenge porn, as a social phenomenon, came into the spotlight during 2012 and 2013 primarily through the identification and arrest of an American man named Hunter Moore. Moore created and ran the site isanyoneup.com, where he encouraged men to share naked photos of women, along with their names, age, location, and links to their various social

[1] - Cyberviolence à l’encontre des femmes et des filles , Institut européen pour l’égalité entre les hommes et les femmes (EIGE) , 2017
[2] - Nidhi AGARWAL & Neeraj KASUHIK, Cyber crimes against ,The Times of India, 2013. GJRIM VOL. 4, NO. 1, June 2014 SRIMCA 37
[3] - Ex., “But he wasn’t actually going to rape her”
[4] - *Jordan FAIRBAIN ,* Rape Threats and Revenge Porn: Defining Sexual Violence in the Digital Age. University of Ottawa Press.2017.p. 229-251.

media profiles. Although he was previously immune to criminal charges because he was said to be only sharing third-party material, in 2012 Moore was charged for his role in hacking into people's email accounts to steal photos. In December 2013 Moore was indicted on felony charges that included identity theft and conspiracy [1] .

In recent years, the media has reported in the EU and US many cases of women victims of pornography against their will, many of whom committed suicide. Research shows that up to 90% of pornographic revenge victims are women and the number of cases is increasing. There are also more and more websites dedicated to the sharing of pornographic acts of revenge, where users can upload images as well as personal information about victims: their address, their employer and links to their profile online.

Another trend with equally devastating consequences for victims is the live broadcast of sexual assault and rape on social networks. So far, in 2017, two cases have had a strong impact: one in Sweden and the other in the United States, where rapes were broadcast live online via the "Facebook Live" feature. [2]

Based on the original definition of harassment, it is an easy anonymity. It has always existed, but it is all the more easy that the aggressor can take a pseudonym, impersonate another person and not reveal his own. Less easily identifiable, he perceives a feeling of impunity and a lack of empathy, encouraged by what is called "the cockpit effect", namely the distance between the attacker and his victim. The aggressor does not see the effects of his actions on his victim.

Another characteristic of this cyber violence is the high power of dissemination. In one click, the message or the photograph can be distributed to millions of people, and circulate twenty-four hours a day, seven days a week, offering no respite for the victims. It should be noted that half of victims of cyberviolence also experience face-to-face violence . It constitutes a violence of distance, but especially of proximity. The abuser (s) know the victim and have regular contact with her most of the time, even if the victim does not know who the perpetrator is.

In addition, cyber violence is facilitated by opportunities for less control of online youth behavior by adults. The author himself no longer controls what he has broadcast in cyberspace, others can seize and disseminate it.

There are several types of online violence. The one that interests us today is related to sexist and sexual harassment, derogatory comments about the gender, image and appearance of the victim, as well as sexually motivated messages. The cyber space facilitates online prostitution, especially among very young girls, the most vulnerable to this type of message, because very sensitive to their appearance. [3]

Also , we have insult , wich can be defined as a term involving a negative value judgment, a metaphorical, metonymic, or even hyperbolic term, which associates a person with animals or objects that are negatively connoted or perceived as disgusting. It is a social act with consequences, an intentional act done to injure. Ethnotypes, sexotypes and ontotypes occupy an important place in cyber violence, especially in cyber violence between adolescents.

Generally, cyber defamation is cyber tort including libel and defamation is another common crime against women in the net. Although this can happen to both genders, but women are more vulnerable. This occurs when defamation takes place with the help of computers and/or the Internet when someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

The term defamation is used to define the injury that is caused to the reputation of a person in the eyes of a third person Cyber defamation is publishing of defamatory material against another person with the help of computers or internet. You build a great brand over 20 years and all it takes is 2 days to destroy it, on the Net (The Times of India 2010).

Unfortunately cyber defamation is not defined by the different IT Act and it is treated by the criminal justice system under the same provisions of publication of obscene materials in the internet. With the exponential increase in the use of the

[1] - Danielle Keats CITRON & Mary Anne FRANKS , "Criminalizing Revenge Porn ," *Wake Forest Law Review* 49 (2014): 345.
[2] - Cyberviolence à l'encontre des femmes et des filles , op.cit , 2017.
[3] - Catherine BLAYA , Les ados dans le cyberespace : prises de risque et cyberviolence , Les cyber violences sexistes et sexuelles : Mieux les connaitre , mieux les prévenir .Colloque, Paris , 25 novembre 2014 .

internet as a medium of communication and sharing of information, chances of use of the web for publication of defamatory content has increased multi-fold and there is a coherent need for a clear law in this area [1].

**2- Imposition of new rules in cybercrimes against women**

Other forms of crime are of a relatively new nature, so it is prerequisite not to move towards adaptation in the qualification, but rather to move towards new special texts for this kind of situation. As flaming , roasting , and digital self-harm.

Incidences of online violation against women are quite high and these are believed to be on the increase. Cyber violence in his strict approach , is a new form of violence against women which is facilitated by internet and information technology. Women are more prone to victimization than men in cyber space and most of them receive mails from unknown men with disturbing contents or texts, friend requests etc. which may be the result of data mining [2].

To start , the flaming is a practice of sending a series of insulting or even hateful messages to a discussion forum or comment area of a blog or site for the sole purpose of provoking open conflict.

This is reminiscent of trolling, the only difference being that the latter is intended to create an endless controversy to the point where discussion is impossible and the words may be provocative without necessarily being insulting or hateful. But, in everyday language, flamers are often called trolls.

Flaming can target a group or a category of people or fall on the same person. The wave of insulting, misogynistic and hateful comments prompted by the release of a video titled "#HasHarcelée How did you see how you were dressed? "Posted by YouTuber Marion Seclin on the webzine Madmoizelle in July 2016 illustrates quite well the phenomenon. Just like the hundreds of insults and threats of rape and death received by journalist Nadia Daam in the fall of 2017, following her acidic chronicle against members of the forum « Jeuxvideo.com. » Two of his cyber harceleurs have also been sentenced to six months suspended sentence and 2,000 euros in damages [3].

The ease with which users of online groups get rid of inhibitions that characterize social life is usually linked to the absence of social cues and internet culture. When the person composes his message, she can easily forget the norms that are imposed on everyone because she does not have the person in front of her. Because proxy-based exchanges obscure some aspects of communication or make them less salient, actors would tend to be more aggressive because they feel less compelled by social control.

In this same context, flaming is the manifestation of a toxic disinhibition. However, several authors have found that the incidence of flaming is often exaggerated. Because flaming is therefore far from systematic since it concerns only between 3% and 5% of messages. This therefore qualifies the hypothesis that flaming would be the consequence of online deindividuation.

Indeed, everyone is being subject to the same communication constraints, the same causes should produce the same effects. Since this is not the case, this means that online aggression depends less on the media than on the culture of the groups. In this context, conflicts are not caused by the absence of a rule, but by the respect of a rule assumed by the group. Some authors have proposed identification as an explanatory mechanism: social influence requires first and foremost that we identify ourselves with a given social group and this social identity is "in our head" even if we are not physically present in the group [4].

Also , roasting is from the English roast ("mocking", "ridiculing"), the term roasting is now used to describe a new practice that appeared some time ago in social networks and consisting of asking to be ridiculed publicly.

[1] - Nidhi AGARWAL & Neeraj KASUHIK , op.cit .
[2] - Jaspreet SINGH , Violence against women in cyber world : A special reference to INDIA , International Journal of Advanced Research in Management and Social Sciences , Vol. 4 | No. 1 | January 2015 , p60.
[3] -By the court of Paris .
Cyberviolence & Cyberharcèlement, FR analyse, Bérengère STASSIN , 09/10/2018.
[4] - Yann LEROUX , Adolescence et réseaux sociaux ,Un point de vue psychodynamique , Janvier 2015.
https://www.researchgate.net/publication/320357369_Adolescence_et_reseaux_sociaux_Un_point_de_vue_psychodynamique.

This practice seems to aim above all to make people laugh. For some, it is to emulate the American TV roasts in which a comedian openly mocks a celebrity on the set, which must submit to the game and cash the "shots" without saying anything.

In addition to the digital self-harm , wich was revealed in 2013 following the suicide of the young Hannah Smith, initially attributed to a cyberstalking of which she would have been victim. But the investigation revealed that the insults and suicides that she received online came mainly from herself. The girl posted questions on the social network Ask.fm (ex: "What do you think of me?") And answered it herself via an anonymous account she had opened: "Go die," "catch a cancer "," bleach wood "... A study conducted in 2017 with 6,000 US students aged 12 to 17 found that 6% of them had already anonymously posted offensive comments online. Among these 360 students who have practiced this practice, 51% said they did it only once, 36% said they did it several times and 13% said they did it regularly [1].

Finally, some authors consider self-mutilation from a little known but certainly heuristic angle: it would be an adaptation mechanism .[2] The existence of a real or imagined problem would indeed cause the establishment of an answer to face this stressful event. During a difficult situation, some people would self-injury to face this test. Self-injurious actions would release feelings, find an avoidance solution, feel better, or simply forget what happened. For some people, self-mutilation would even be a means of expression and a substitute for speech and language to the extent that another person would be able to understand that message. Self-injury would then provide some control over both the intensity of the pain that the person feels inevitably has, and the timing of the pain [3]. It would be a means of survival against uncontrollable emotions: rejection, abandonment, fear or anger.

Some women claimed to have negative feelings before committing their self-injurious actions: guilt, anger and frustration. Respondents do not dare to discuss their behavior with those around them. They are therefore aware that self-harm is a taboo subject. This makes them feel social isolation. They know that their self-injurious gestures are not well seen and ashamed of not being able to solve their problems otherwise. This corresponds to Le Breton's (2003) observation that self-mutilation is often experienced in solitude and gives the feeling of being apart and not being completely normal. Four respondents say they have a small social network. They therefore do not have the privilege of being listened to by their relatives, which leads them to be marginalized [4].

New technologies enable a transgression of the boundaries of “physical” or “real” identities, and in these fluid spaces, individuals forge new relationships and networks, navigating new, and often times, multiple identities. These identities become essential to understand social relationships in cyberspace, and consequently, the relationships that can become abusive and violent. The anonymity and forays into new self-expression and selfhood inherent in new ICTs comprise new spaces for information access, empowerment, and solidarity. At the same time, these very characteristics associated with online spaces allow perpetrators of violence against women to get away. Since cyber identities and physical identities may not necessarily overlap, the former are not necessarily bound to the same social context or rules that the latter might operate under.

The protection of women’s rights to information and communication emphasises the need to balance concerns of self expression with concerns of protection from exploitation. While there is no doubt that policies are needed to address online violence, the boundaries of state involvement in effecting such protection becomes critical. While the government should be able to prosecute those engaged in violence against women, a right to surveillance in general, without adequate basis is likely to infringe on women’s privacy. The state's duty to intervene and prosecute violence when it happens online should not become an excuse for surveillance over the Internet. Thus, policy approaches need to recognise both women's “public”, political rights as well as “private”, individual rights, especially in the context of violence against women [5].

**3-The specificity of the evidence in relation to cyber crimes against women .**

[1] - Cyberviolence & Cyberharcèlement, op.cit , 09/10/2018.
[2] - Wegscheider, 1999
[3] - Correctional Service of Canada, 1999
[4] - Isabelle FORTIER ,L’automutilation, une stratégie d’adaptation ? Étude exploratoire auprès de femmes . Cahiers de l’ORÉGAND : série Recherche- No. R-9 - ORÉGAND, 2008 Gatineau, Qc. – Canada.
[5] - Anita GURUMURTHY, Niveditha MENON,Violence against women via cyberspace Economic & Political Weekly EPW October 3, 2009 vol xliv no 40 , p19.

One of the obstacles to the effectiveness of the fight against violence against women and couples is the fact that it is difficult to prove it .

I note that the family can become the place of brutality, vexation, psychological pressure . Cases of flagrant offenses are rare, witnesses are few; Psychological disorders are by definition invisible and often remain so until their destructive effects on the person can be medically observed, which sometimes happens too late.

For the litigant who is in the practical incapacity to establish the proof of the violence of which he is victim, the adoption of penal qualifications can be a decoy. The private family circle quickly transforms the requirement of testimony into evidence impossible to provide "diabolica probatio".

My personal vision is that in general, abused women appeal to others to temporarily stop a situation of aggression which they do not know how to dispose of. However, they do not necessarily wait for legal action in return. This social role is taken up by judges who, despite their primary function of repressing offenses by applying the law, advocate a social approach to cases perceived as "different" from "classic" criminal cases.

An identifiable person must always have the physical custody of a piece of evidence. In law enforcement, this means that a police offi cer or detective will take charge of a piece of evidence, document its collection, and hand it over to an evidence clerk for storage in a secure place. In the corporate world, a similar responsible individual will need to be identifi ed and will be required to assume similar responsibilities as his or her law enforcement counterpart. It will become imperative that the corporate cyber forensic investigator maintain and adhere to the same stringent rules of collecting, preserving, handling, and storing evidence as followed by law enforcement professionals.

This is especially true if the corporation wishes to ultimately use the collected evidence in the legal pursuit of wrongdoing by an employee, contractor, trading partner or other third party. Th ese transactions, and every succeeding transaction between the collection of the evidence and its appearance in court, should be completely documented chronologically to withstand legal challenges to the authenticity of the evidence.

Documentation should include the conditions under which the evidence is gathered, the identity of all evidence handlers, duration of evidence custody, security conditions while handling or storing the evidence, and the manner in which evidence is transferred to subsequent custodians each time such a transfer occurs. Ultimately, rules of evidence must be established and maintained and the chain of custody must be preserved for all evidence that may be potentially or eventually used in court. Th is chain in part insures the integrity of the evidence. In practice, the person responsible for maintaining custody of the evidence can testify that the evidence was not altered (or if it was how it was altered) [1].

Criminals look for easy prey and they include women. The general public, especially women, need to be properly educated on the incapacitating effect of cyber crimes and improper computer ethics. They need to be more aware of the dangers of cyber crime and at the same time should be educated on becoming ethical users of computers and information systems. The public should understand its role in the country's cyber security .

The public may be educated using the five main categories of particular interest to technologists , privacy, ownership, control, accuracy, and security . How much information should one divulge in public so as not to have problems in personal security? Information such as compensation, background data, personal identification information such as social security number and account identifiers should not be easily accessible to the public and should not be entered in computers accessed by the public. Personal outputs, pictures, and videos are matters of ownership. To protect them from abuse, individuals should learn not to make them accessible to everyone [2].

We notice that The law and its officers are stuck in the 'physical', and the instinct in cases of violence is to focus on identifying physical injury. However, the logic of cyberspace is different from the real world, and hence, laws of the cyber world must be different from the real world. The cyber world can be oppressive and exclusionary. The digital is intimidating, but it is so entrenched in our lives that we can not abandon it.

[1] - Albert J. MARCELLA , Jr. Doug MENENDEZ , cyber forensics , a field manual for collecting, examining, and preserving evidence of computer crimes second edition, Auerbach Pubications , 2010, p42.
[2] - Lizel Rose Q. Natividad, MA San Beda , cyber crime safety of women and children: A matter of cyberspace stakeholders' ethics and responsibility ,College , /2017/07/Vol.-4.1-L-R-Q-Natividad

Essentializing violence as a problem of urban, educated women is a convenient reductionism by officials to evade responsibility for providing effective redress to gender-based cyber violence. Most laws focus on punishment or protection but not prevention. However, it is 'prevention' that is the crux of state recognition of rights. When a woman makes a complaint of violence, it is a violation of her right that is being reported. And so the law must use language that forces officers of the law to acknowledge the inviolability of the right to dignity. Harm must be understood as an affront to dignity [1].

The existing policies here indicate that there is an awareness of the potential harm – and perhaps even a partial willingness – to act in order to tackle issues of harassment and violence against women online. There are number of sporadic and piecemeal mechanisms that have been implemented by the social media platforms in order to offer so-called solutions.

These existing policies span a number of different approaches but have, to date, failed to engage or interact or complement the disparate legislative measures used to address some – limited – incidences of online violence against women.

Whilst it is apparent that there can be a willingness to discuss potential policies and measures, the lack of any substantive policies addressing online violence against women, particularly text-based abuses, speaks volumes – especially when compared to the action taken in respect of image-based abuses and extremist content. This is, therefore, indicative of a lack of commitment to implementing effective mechanisms to tackle abusive behaviours online. Similar to the lack of legislative action on misogynistic text-based abuses, there has been little real impetus given to service provider or platform provider policies – evidence of a further systemic failure in tackling harmful behaviour [2] .

Cyber security has quickly risen to the forefront of concern for both nations and private firms and collaboration between them, despite their often-competing interests, will be of increasing importance. Due to the high frequency of cyber-attacks today, there has been an increasing call for greater collaboration between policy makers, businesses and experts. There is thus a need for a macro-level design on policies that will shape the internet.

One area of interest is the question of efficacy of deterrence policies and whether domestic policies alone can be effective. International legislation too needs to be examined for efficiency. It is also necessary to decide which actors and actions should be targeted with the greatest focus to ensure the most efficient results in deterring cyber crime.

Key areas of interest include legislation for international collaboration, the criminalisation of possession, distribution and production of computer misuse tools, as well as the creation of legal obligations on the part of private firms to report cyber crimes.

Since the turn of the century, many countries have introduced legislation to enhance cybercrime enforcement. From 2002 to 2015, 56 countries have signed cyber crime conventions, with 52 having entered these conventions into force.

Research has shown that international conventions and legislation on cyber crime can reduce international attack rates. Countries that fully embrace these conventions, allowing for greater collaboration and the sharing of information have shown the greatest reductions in attack rates. Criminalisation of production, possession and distribution of computer misuse tools helps to deter information sharing on hacker techniques and tools on hacker forums, resulting in a reduction in cyber-attacks. However, this might also have the sideeffect of driving hacker collaboration further underground, making them harder to track and investigate.

Expecting different states and commercial firms to cooperate, many of whom are competitors on different levels, is a huge challenge that will require developing effective mechanisms that do not advantage any one group over the other [3].

So, a good model of cyber crime investigations is important, because it provides an abstract reference framework, independent of any particular technology or organisational environment, for the discussion of techniques and technology

[1] -Prabha Sridevan, Gender-based cyber violence as real violence,report of the national dialogue on gender-based cyber violence , 1-2 February, 2018 TATA Institut of social sciences, MUMBAI.
[2] -Dubravka ˇSimonovi´c , Submission of Evidence on Online Violence Against Women to the UN Special Rapporteur on Violence Against Women, its Causes and Consequences, November 2017.
[3] -Report on the Workshop organised by: Centre of Excellence for National Security (CENS) S. Rajaratnam School of International Studies (RSIS) Nanyang Technological University, Singapore, 13-14 November 2017.

for supporting the work of investigators. It can provide a basis for common terminology to support discussion and sharing of expertise.

The model can be used to help develop and apply methodologies to new technologies as they emerge and become the subject of investigations. Furthermore, the model can be used in a proactive way to identify opportunities for the development and deployment of technology to support the work of investigators, and to provide a framework for the capture and analysis of requirements for investigative tools, particularly for advanced automated analytical tools.

At present, there is a lack of general models specifically directed at cyber crime investigations. The available models concentrate on part of the investigative process (dealing with gathering, analysing and presenting evidence) but a fully general model must incorporate other aspects if it is to be comprehensive. Such a model is useful not just for law enforcement. It can also benefit IT managers, security practitioners, and auditors. These people are increasingly in the position of having to carry out investigations because of the increasing incidence not only of cybercrime, but of breaches of company policies and guidelines [1].

**Conclusion :** It is clear that this form of violence, which leads us to the electonic form of crimes , is very often directed against women of all backgrounds, including the most intellectually privileged. They are victims of men who display immaturity, egocentrism, machismo or serious personality disorders.

Beyond the possible lines of action to be put in place, should we not recontextualize the violence and the cyber crimes , to understand its roots. How, when one influences the mind of all generations by concepts like "power", "virility", "patriarchal authority", to think that boy or girl, man or woman, will escape to engage in conflicts, violence and inequalities.

In the face of cyber crimes , women use different strategies to defend themselves.

But alas, in other cases the woman is encouraged to submit, some people, in the entourage of the abused woman, do not deny this form of violence but unfortunately accept it as a fatality or make "the woman indirectly responsible" .

**References**

[1] The UN Committee on the Elimination of Discrimination Against Women : C.E.D.A.W.
The Convention on Preventing and Combating Violence against Women and Domestic Violence : Istanbul Convention.
[2] Gill ALLWOOD , la violence à l'égard des femmes fondée sur le genre dans la France contemporaine ; Modern &
[3] Contemporary France, DOI. http://dx.doi.org/10.1080/09639489.2017.1340003.
[4] Nidhi AGARWAL & Neeraj KASUHIK, Cyber crimes against ,The Times of India, 2013. GJRIM VOL. 4, NO. 1, June 2014 SRIMCA 37
[5] Danielle Keats CITRON & Mary Anne FRANKS , "Criminalizing Revenge Porn ," *Wake Forest Law Review* 49 (2014): 345.
[6] Catherine BLAYA , Les ados dans le cyberespace : prises de risque et cyberviolence , Les cyber violences sexistes et sexuelles : Mieux les connaitre , mieux les prévenir .Colloque, Paris , 25 novembre 2014 .
[7] Jaspreet SINGH , Violence against women in cyber world : A special reference to INDIA , International Journal of Advanced
[8] Research in Management and Social Sciences , Vol. 4 | No. 1 | January 2015 .
[9] Bérengère STASSIN , Cyberviolence & Cyberharcèlement, FR analyse, 09/10/2018.
[10] Yann LEROUX , Adolescence et réseaux sociaux ,Un point de vue psychodynamique , Janvier 2015. https://www.researchgate.net/publication/320357369_Adolescence_et_reseaux_sociaux_Un_point_de_vue_psychodynamique.
[11] Isabelle FORTIER ,L'automutilation, une stratégie d'adaptation ? Étude exploratoire auprès de femmes . Cahiers de
[12] l'ORÉGAND : série Recherche- No. R-9 - ORÉGAND, 2008 Gatineau, Qc. – Canada.

[1] - Séamus Ó Ciardhuáin , An Extended Model of Cybercrime Investigations , International Journal of Digital Evidence Summer 2004, Volume 3, Issue 1, p 01.

[13] Anita GURUMURTHY, Niveditha MENON,Violence against women via cyberspace Economic & Political Weekly EPW October 3, 2009 vol xliv no 40 .
[14] Albert J. MARCELLA, Jr. Doug MENENDEZ , cyber forensics , a field manual for collecting, examining, and preserving evidence of computer crimes second edition, Auerbach Pubications , 2010 .
[15] Lizel Rose Q. Natividad, MA San Beda , cyber crime safety of women and children: A matter of cyberspace stakeholders' ethics and responsibility ,College , /2017/07/Vol.-4.1-L-R-Q-Natividad
[16] Prabha SRIDEVAN , Gender-based cyber violence as real violence,report of the national dialogue on gender-based cyber violence , 1-2 February, 2018 TATA Institut of social sciences, MUMBAI.
[17] Dubravka ˇSimonovi´c , Submission of Evidence on Online Violence Against Women to the UN Special Rapporteur on Violence Against Women, its Causes and Consequences, November 2017.
[18] Séamus Ó Ciardhuáin , An Extended Model of Cybercrime Investigations , International Journal of Digital Evidence Summer 2004, Volume 3, Issue 1 .
[19] Cyber violence against women and girls a world –wide wake –up call a report by the UN broadband commission for digital development working group on broadband and gender ,2015.
[20] Report on the Workshop organised by: Centre of Excellence for National Security (CENS) S. Rajaratnam School of International Studies (RSIS) Nanyang Technological University, Singapore, 13-14 November 2017. Cyber violence à l'encontre des femmes et des filles , Institut européen pour l'égalité entre les hommes et les femmes (EIGE) , 2017.
[21] Rape Threats and Revenge Porn: Defining Sexual Violence in the Digital Age.*Jordan Fairbairn* University of Ottawa Press.2017.
[22] Report of the Special Rapporteur on violence against women, its causes and consequences of online violence against women and girls from a human rights perspective, Human Rights Council, Thirty-eighth session , 18 June–6 July 2018, A/HRC/38/47.