Cyber trafficking: recruiting victims of human trafficking through the net

ATHANASSIA P. SYKIOTOU
Dr. jur., Assistant Professor, Criminological Sciences,
Democritus University of Thrace, Law School (GR);
International consultant of the UN, OSCE, and the Council of Europe

Abstract

Many forms of trafficking appear to be using the cyberspace as means of victims' recruitment or for advertising trafficking "services and products". Up to now sex- and labour trafficking, child pornography, selling of babies, trafficking of organs and mail order brides are some of the forms of cyber-trafficking. Traffickers, clients, service providers and various stakeholders facilitate the trafficking process through the Internet. From the moment traffickers use cyberspace as a tool, trafficking is considered as cybercrime. The problem is that there are no international texts on cybercrime except at regional level the Council of Europe Cybercrime Convention.

Prevention is crucial to cyber-trafficking, however it generally depends on the importance given to international, regional and local cooperation and between various entities responsible for combating trafficking, as well as to specialized capacity development programmes. There are many challenges for national governments, police and judiciary in the fight against human trafficking. An effective strategy against cyber-trafficking would demand together with a universal legislation on cybercrime a uniform technological infrastructure that would allow the rapid intervention of the prosecuting authorities on the location and identification of the perpetrators and the preservation of evidence as well as a strong international cooperation.

Keywords: human trafficking; cybercrime; Internet related crimes;

victimisation.

Introduction

In relation to traditional means of crime, Internet is a means that provides only benefits to perpetrators and that facilitates organised criminal groups operating at transnational level. However, the majority of Internet related crimes remains dark, since there are very few cases reported internationally and, depending on the type of crime, there is even more "darkness" added.[1]

More and more forms of trafficking appear every day and more of them are using the cyberspace as means of recruitment or for the advertisement of trafficking "services and products". Up to now besides sex-trafficking, child pornography and labour trafficking there is also information about the use of Internet for the selling of babies, trafficking of organs and mail order brides.[2]

---

[1] Steven Branigan (2005), *High-tech Crimes Revealed: Cyber war stories from the digital front*, Boston, MA: Addison-Wesley; Europol, 'High tech crimes with in the EU: old crimes new tools, new crimes new tools', Threat Assessment 2007, High Tech Crime Centre: http://www.europol.europa.eu/publications/Serious_Crime_Overviews/HTCThreatAssessment2007.pdf; Council of Europe, Organised Crime in Europe: the Threat of Cybercrime – Situation Report for 2004, Octopus Programme, 2005.

[2] A couple of years ago, according to undocumented sources another form of cyber-trafficking was added to the already existing list. It concerned the market of certain pills advertised and sold via Internet (for 27 euros), allegedly having 'medicinal' benefits, which were found to be made out of powdered human flesh. Actually, these pills were made out of dead fetuses, babies and placenta chopped up, dried and reduced to powder. The *San Francisco Times* reported that tests discovered 99.7% human flesh in the tablets and that more than 17,000 tablets had been intercepted until May 2012 by the customs authority in South Korea. Such tablets were produced in many Chinese cities, but up to now there is no information as to where the supply of dead babies came from. Even if trafficking of babies does exist in China, it is not easy to assume that this commerce was based on such trafficking, http://edition.cnn.com/2015/01/14/china/china-child-trafficking-bust/http:// sanfrancisco.ibtimes.com/articles/193371/20110805/china-dead-baby-pill-stamina-booster-cannibal-placenta.htm. See also, *Mail On Line*, 7.5.2012, http://www.

Relation of Human Trafficking to Cyber Crime

Cyber-crime is called the crime committed in Internet environment[3]. There are crimes committed in cyberspace and cyberspace related crimes that use Internet as means to their commission, such as trafficking in persons. Cyberspace related crimes can also be committed with the traditional way. In trafficking, perpetrators use all kind of means to recruit victims from traditional to more modern ones. When trafficking is committed with the use of Internet it is called "cyber-trafficking". However, there is no official definition of cyber-trafficking, because there are no texts relating cybercrime with trafficking. The only text at international level that relates cyberspace to trafficking (however through child pornography) is the 2001 Council of Europe Convention on Cybercrime (ETS No 185). The Convention does not give any definition on cyber-trafficking.

Cyber-trafficking refers to the use of cyber-space for:

- the recruitment of victims;
- advertisement of victims,
- advertisement of victims' services or victims' organs; and for
- attracting clients.

Very often the term of "virtual trafficking" is used instead of "cyber-trafficking". I believe that the use of the term "virtual trafficking"

---

dailymail.co.uk/news/article-2140702/South-Korea-customs-officials-thousands-pills-filled-powdered-human-baby-flesh.html. Also, Charles Custer, "Missing, Kidnapped, Trafficked: China has a problem with its children", The Guardian, 12.3.2015: http://www.theguardian.com/commentisfree/2015/mar/12/ missing-kidnapped-trafficked-china-children; BBC news 11.3.2015: http://www.bbc.com/news/magazine-31814295; 'Something horrible is happening in China', All Girls allowed: http://allgirlsallowed.org/statistics; Bureau of Democracy, Human Rights, and Labor. 2011. 2010 Human Rights Report: China. Washington, DC: U.S. Government Printing Office. http://www.state.gov/g/drl/rls/hrrpt/2010/eap/154382 .htm

[3] For bibliographical sources on cybercrime, see Library of Congress – Federal Research Division(Nov.2009), *Cybercrime: An annotated bibliography of select foreign-language academic literature*, WashingtonDC:https://www.ncjrs.gov/pdffiles1/nij/231832.pdf

is wrong. "Virtual trafficking" can only produce "virtual" victims. Real persons do not deserve to be treated as virtual victims. The term "virtual" "softens" the substance of the crime. It refers to something that is not real. However, when Internet is used people become real victims; so it is real trafficking, not virtual.[4]

I prefer the term cyber-trafficking instead of "virtual trafficking", because it refers to the use of cyberspace as a means to commit trafficking and not to something that is not real. However, I can understand how the confusion of those who use the term "virtual trafficking" started. Actually, it starts with the term "virtual sex". When we use the term "virtual sex" as a synonym of "cyber-sex" it is because we refer to –normally– consenting adults who under other circumstances (: if they were not using cyberspace) would have had real sex. So, the term "virtual" comes here to emphasise the contrast with the "real" sex. However, in trafficking not only there is no consent, but there is also no need to consume the sexual act to call it trafficking.[5] So, when a person is coerced to have sex on line, this is neither "virtual sex" –as something that is not real sex– nor "virtual trafficking".[6] It is trafficking

[4] A good example is the Greek law against child pornography. Art.348A of Criminal Code punishes not only the person who detains pornographic material with images of real children, but also the person who detains pornographic material with *virtual representation* of children, meaning images not of real children, but designs of children or cartoons instead. Even if in this situation there is no real victim, nevertheless the legislator punishes the detainer of such material, because he believes that a person who likes virtual representation of children expresses a stage of *pre-criminal dangerousness.* Thus, he needs to be punished before he attempts to commit the crime to a real child. So, in this case we may speak about *virtual trafficking* and *virtual child pornography,* since there is no real victim implicated.

[5] See explanatory report of the Council of Europe Convention on Action against Trafficking in Human Beings. According to point 87 of the above Explanatory Report: "Under the definition, it is not necessary that someone have been exploited for there to be trafficking in human beings. It is enough that they have been subjected to one of the actions referred to in the definition and by one of the means specified 'for the purpose of' exploitation. Trafficking in human beings is consequently present before the victim's actual exploitation."

[6] According to BBC News a 10-year-old deaf orphan girl from Pakistan was

through cyberspace, thus cyber-trafficking!

In some forms the term 'cyber-trafficking' refers also to the space of commission of the crime (e.g. if the exploitation is on line by cyber-sex or of by procuring material of child pornography).

Advantages of the use of the Internet for the traffickers

Internet offers enormous advantages to criminals since it knows no borders and enables offenders to act from a country distant from the victim's, which may be located on the other side of the globe. The increase in the use of new technologies by perpetrators has been generally attributed to:

i) More generalised access to the Internet;
ii) Increased affordability of technology and services (low cost);
iii) Anonymity and/or disguise of users which allow traffickers to commit their crimes at a reduced risk;
iv) Speed – as it is fast (leaving only digital traces);
v) Ease of use;
vi) Criminals ability to work from home and operate in many countries reaching an indefinite number of victims;
vii) Difficulty in tracing (since criminals can operate in many countries and digital traces are difficult to track);
viii) Inability of victims to denounce the perpetrators because their identity might be unknown to them;
ix) High profitability of crime in relation to the investment required;
x) Lack of appropriate State policies and legislation and lack of uniform international legislation on trafficking and cyber-crimes that creates problems not only in prosecution but in jurisdiction in general.

---

trafficked into the UK and kept in a cellar as a virtual slave for almost a decade. The child was forced to work for no pay and was sexually assaulted; *BBC News*,9 February 2012, http://www.bbc.co.uk/news/uk-england-manchester-16974149. UN. GIFT has launched a virtual human trafficking knowledge hub on 2010, http://www.ungift.org/knowledgehub/en/stories/un.gift-launches-new-virtual-human-trafficking-knowledge-hub.html

In addition, Internet addresses to a broad audience thus, it gives the opportunity for more victims and more options for recruitment to traffickers and it offers also more targeted virtual spaces where individuals can be recruited, such as social networking sites and Internet dating. The evolution of wireless and broadband networks offered even greater opportunities for actors, since there are more rapid and economical.

The Prevalence of Sexual Exploitation in Cyber-trafficking and the Increasing Appearance of Other Forms of Trafficking in Cyberspace

According to the UNODC/UN.GIFT Global Report on Trafficking in Persons,[7] sexual exploitation appears to be by far the most commonly identified form of human trafficking (79%), followed by forced labour[8] (18%). Of all the previously mentioned forms, women and girls are most frequently identified as victims.[9] The same report shows that 66% of women and 13% of girls are identified as trafficked victims against 12% of men and 9% of boys. It needs to be noted that a disproportionate number of women are identified as being involved in human trafficking, not only as victims, but also as traffickers.

---

[7] UNODC/UN.GIFT (2009), *Global Report on Trafficking in Persons*, Febr. 2009, p. 11.

[8] A survey carried out by the Human Rights Centre of Berkeley University, California shows that between 1998 and 2003 more than 500 people from 18 countries were ensnared in 57 forced labour operations in almost a dozen cities throughout the state. There were a large number of cases concerning prostitution, which accounted for 47.4 percent of the cases. Domestic service cases comprised 33.3 percent. Sweatshop work accounted for only three cases (5.3 percent) but involved 143 victims (25.8 percent of the victims). The survey data for California included only one case of agricultural labour involving two individuals. See, 'Freedom denied. forced labour in California', Human Rights Centre, Berkeley University, California, Febr. 2005, p. 9.

[9] As mentioned in the UNODC report, it is important to note also that these numbers may be the result of trafficking legislation being in many countries focused on trafficking in women and children and also that the public opinion and law enforcement is more aware of that type of trafficking.

To date, the following forms of exploitation have been linked[10] to the use of Internet by traffickers besides the child pornography that is considered the oldest form related to Internet:

i) Sexual exploitation;[11]
ii) Labour exploitation;
iii) Mail order brides (mainly for advertising).

Up to now there are forms of exploitation that have not been documented as related to Internet. For instance, the recruitment of children for their involvement in armed conflicts has been reported as located in specific countries – mainly in Africa and has therefore not been known to be linked to the use of the Internet for the recruitment of victims. In addition, the recruitment of persons especially children with any kind of infirmity for begging, despite its growth mainly in the Balkan region,[12] does not seem to be connected to the use of Internet either; nor has the recruitment of children in order to be used in thefts.

However, as mentioned above, more and more forms of human trafficking seem to "evolve" through the possibilities offered by new technologies.[13] Cases have been reported linking the use of the Internet to:

(a) trafficking for illegal adoptions (including babies and surrogate mothers);
(b) trafficking for the purpose of the removal of organs.[14]

With respect to trafficking in babies[15] and mothers for the purpose

[10] A. Sykiotou, 'Trafficking in human beings: internet recruitment. Misuse of the internet for the recruitment of victims of trafficking in human beings'. Directorate General of Human Rights and Legal Affairs of the Council of Europe, Strasbourg, 2007.

[11] A. Sykiotou (2003), *Trafficking in Human Beings in the Balkans*, Athens, Ant. Sakkoulas Publs, p. 60.

[12] *Ibid*.

[13] A. Sykiotou (2010), 'The impact of the internet on trafficking in persons', Concept Paper prepared for UN.GIFT.

[14] Council of Europe/United Nations (joint study) (2009), 'Trafficking in organs, tissues and cells and trafficking in human beings for the purpose of the removal of organs', Joint Council of Europe/United Nations Study: www.coe.int/trafficking

of illegal adoptions it appears that traffickers use the Internet mainly as an advertising tool to reach desperate childless parents. In European countries with low birth rates, trafficking in babies is becoming an increasingly prevalent form of trafficking.[16]

Sites for the advertisement of illegal adoptions of babies are flourishing in the Internet.[17] It is reported that in China there was a site called 'Eachnet' (until October 2005) which was actually selling, through auctions, boys for an amount of 3,450 Euros and girls for 1,603 Euros. The sites offering babies for adoptions gave not only the description of the babies, but also the price for what is called: "adoption expenses", which are essentially the purchase price of the child.[18] The advertisement for the sale of a baby by his/her own parents on the auction site eBay[19] has also been reported, with a starting price of one euro.[20]

Regarding trafficking in organs it has to be pointed out, that there might be a relation between the increase in deceased donation activities of organs and tissues and trafficking in persons as the valid con-

[15] The first cases of trafficking of babies and children have been located in Africa in the 1980s with illegal adoptions of children going to USA and Europe.

[16] In Greece an illegal adoption is priced around 20,000 euros, while the mother (if consenting) takes ¼ of the amount. The price varies according to the preferences of the parents in gender or country of origin of the baby. In the Balkans Bulgaria, Romania and Albania are considered the main 'markets' for illegal adoptions. However, worldwide the main country of destination of babies for illegal adoptions is considered to be USA and as main country of origin China.

[17] Jewkes Yvonne (ed.), *Dot.cons: Crime, deviance and identity on the internet*, Willan Publishing 2002; Letherby Gayle and Marchbank Jen (2003), 'Cyber-chattels: buying brides and babies on the net', in: *Dot. Cons: Crime, deviance and identity on the internet*, p. 68.

[18] Article in Greek news paper 'Kathimerini' of 30.7.2006: http://www.kathimerini.gr/

[19] It is interesting to note that eBay is a minority shareholder of Craigslist. *New York Times*, April 25, 2010: http://www.nytimes.com/2010/04/26/technology/26craigslist.html?hpw. See, below for further information on Craigslist.

[20] Article of 26-5-2008 under the title 'Baby for sale in eBay' in: http://www. foreignpress-gr.com/

sent of the deceased cannot be established in many countries. According to a study,[21] such activities increased within one year (from 2005 to 2006) by as much as 60% in Colombia, 30% in Cuba, 27% in Venezuela, 22% in Chile, 20% in Uruguay and 11% in Argentina.

On a global level, it is estimated[22] that up to 5%-10% of kidney transplants performed annually around the world are the result of trafficking. Given the Global Observatory on Donation and Transplantation's estimate of overall activity of about 68,000 kidney transplants a year, this would mean that 3,400-6,800 kidney transplants are being carried out on the basis of these forms of trafficking.[23] However, the link between trafficking in organs, tissues and cells (OTC) and trafficking in human beings for the purpose of organ removal has not been clearly established.[24]

---

[21] Council of Europe/United Nations joint study, *op.cit*., p.52.

[22] *Ibid*., p.5 8.

[23] The 2008 *Declaration of Istanbul* defines trafficking in organs, tissues and cells (OTC) as: "the recruitment, transport, transfer, harbouring or receipt of living or deceased persons or their organs by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability, or of the giving to, or the receiving by, a third party of payments or benefits to achieve the transfer of control over the potential donor, for the purpose of exploitation by the removal of organs for transplantation."

[24] The fundamental difference between the two cases lies in the fact that trafficking in organs is a crime where the organ and the use of it are the central elements; it does not matter whether the organ has been removed from a living or a deceased donor. In contrast, trafficking in human beings is a crime where the exploitation of an individual is the central aspect and where a combination of three elements (action, means and purpose) has to apply in order for the crime to be constituted. Therefore, trafficking in human beings for the purpose of organ removal can only be committed if organs are removed from living donors. As the exploitation of the victim results in the removal and further use of an organ, a case of trafficking in organs (and thereby both offences) also applies. However, as the aim of the two crimes is not the same, they overlap but differ in scope. Trafficking in organs can be committed separately from trafficking in human beings, e.g. if organs are removed from deceased donors or if no illegal activities or means have been used with respect to a living donor but, e.g., if the requirements for legal interven-

The form described most frequently occurs in the context of what has been called "transplant tourism".[25] Recently, many of these "services" have been offered openly through dedicated web sites in the form of "packages" including the travel and the transplantation procedure itself. The price of "kidney packages", for example, may range from US$70,000 to US$160,000. These web sites are easily found on the Internet.[26] On the other hand, "donors" are usually, but not always, recruited in their countries of origin. There have been cases reported in which donors are recruited and transferred to other countries, where the organ extraction and the transplantation procedure takes place.

Even if the recruitment of victims via the Internet cannot be proved in this case, this is however a strong indication of the on-going use of the Internet connected to trafficking in organs, as an advertising tool and as a tool for attracting potential buyers of organs that have obviously been removed illegally[27] (since the legal process of organ transplantation does not involve such methods as auctions of organs via the Internet).

Yet, in order to measure correctly the impact of Internet to the victimisation[28] of a person we should be in a position to reply to the fol-

---

tions. *Ibid*., p. 55.

[25] *Ibid*., p. 58.

[26] Even if there are no documented cases for recruitment of victims via Internet for this form of trafficking, there has been documentation on advertisements of sales of organs through Internet, in particular of kidneys. There are reported cases for (attempted) auctions of kidneys through in the above mentioned site "eBay".

[27] On the organ markets see, Council of Europe/United Nations (joint study), (2009), 'Trafficking in organs, tissues and cells and trafficking in human beings for the purpose of the removal of organs', Joint Council of Europe/United Nations Study, p. 31. According to the above mentioned study, as the term is described generally, recruitment by one of the means for the purpose of organ removal is regarded as trafficking in human beings for the purpose of organ removal regardless of how the recruitment is performed – whether through personal contact or contact through third persons, newspapers, advertisements or the Internet, p. 78.

[28] Athanassia Sykiotou (2007),'Trafficking in human beings: misuse of Internet for the recruitment of victims', *op.cit*; Athanassia Sykiotou (2009), *The Internet as*

lowing questions:

1. How many persons use the Internet in a specific place?
2. What kind of use they make of it?
3. What is the frequency of the use?
4. What is the structure of telecommunications in the specific country?
5. What kind of preventive measures (if any) are taken at personal and governmental level to prevent victimisation and revictimisation through Internet?
6. Does the victim (or his/her environment if the victim is e.g. a child) understand that s/he is being victimised?

Socio-economic Background of Victims

The socio-economic background of victims is not quite uniform in all forms of cyber-trafficking. So, in trafficking for labour exploitation many of the victims are workers who seek a job. In trafficking for sexual exploitation we find several forms: for instance, in child pornography there are children of all back-grounds. From street-children that never use Internet or children that are kidnapped and then their photos are uploaded to several Internet sites, to children that are very well placed in a family environment, but who are lured through a chat-room. There are also young women who seek work abroad and who are lured through fraudulent advertisements, or through social networking sites, such as face book. However, the socio-economic background of victims is in a large majority that of persons that seek work (men and women) or company or marriage (mainly women) and who may be deceived through marriage and dating agencies.

The Process of Recruitment of Potential Victims through the Internet

The links between the Internet and recruitment of victims for trafficking can take several forms:

a) Victims may fall prey to traffickers via web sites and other Internet

Means of Victimisation, Ant. Sakkoulas Publ., Athens.

services. Victims are deceived by fake advertisements such as for domestic work; waitress/bartender; au pair/care; modelling, etc. or forced to produce pornographic material (the Internet is mainly used for the dissemination of the pornographic material, but it can also contribute to the production of material if a web camera is used. For instance, a child or a young woman can be lured through a chat-room and then forced to pose naked on-line or be exploited sexually on line e.g. for peepers);

b) Victims recruited in traditional ways may be forced to contact clients online. Hence, some victims contribute to their own further victimisation;[29]

c) Trafficked victims may be traded or their services advertised to clients via the Internet.

The two *methods* mainly identified as used by traffickers to recruit victims via the Internet are: (a) spurious advertisements for employment, dating agencies,[30] marriage agencies (that could act as mail-order-bride agencies and/or as façade to dating clubs) and (b) social networking web sites such as 'Facebook'[31] and 'Craiglist' (considered

[29] US classifieds website *Backpage.com* has become one of the primary destinations on the Internet to buy sex. Hundreds of advertisements are posted each day by both pimps and prostitutes.In the past several years, the newspaper company that owns *Backpage*, 'Village Voice Media', has faced a string of protests from activists, as well as lawsuits from victims of sexual exploitation who allege that the site aids and abets forced prostitution.

[30] See A. Sykiotou, 'Misuse of the internet for the recruitment of victims', *op.cit*. Victims are normally (but not always) recruited in their own countries. In such cases, a recruiter from an "employment agency" persuades them to sign an incomplete or incomprehensible job contract. The necessary documents (visa, work permit, etc) are then procured by the agency, which normally charges a fee or gives the victims a "loan" to cover the costs. Persons recruited are often assisted by "agency representatives" and, on reaching their destination, are taken over by a local contact.

[31] Anti-trafficking campaigns have been created in Facebook such as the Blue Heart Campaign against human trafficking which is considered one of the larger anti-human trafficking groups on Facebook and one of the larger social cause groups on this issue. UNODC launched the Blue Heart Campaign in March 2009 to

as the biggest online hub for offering sexual services of women against their will).[32]

Online employment agencies and in particular model and marriage agencies can all be ploys to lure potential victims. Internet chat web sites are often used to befriend potential victims with the risks for young people to fall into the traffickers' net.

The Procedure of the "Trade"

When referring to "trade" we focus of course only to the forms of trafficking that have the aspect of "trade" and mainly to sexual and labour trafficking and to mail-order brides that are the main forms using Internet as a means of recruitment.

There are several possibilities of "trade" implicating the Internet:

1. the victim may be recruited via the Internet, but the trade may take place traditionally (transfer of the victim to the exploitation place);
2. the victim may be recruited via Internet and may also be used to attract clients through the Internet (advertising its services in sexual exploitation), but the trade may take place traditionally (with the

raise awareness of the crime of human trafficking and its impact on society. It is a campaign that is open to all those who want to participate and wear the Blue Heart as a symbol of their support for this campaign and solidarity with victims of trafficking; http://www.unodc.org/unodc/en/frontpage/2010/January/blue-heart-campaign-against-human-trafficking -reaches-10000-members.html

[32] Craigslist is a centralized network of online communities, featuring free online classified advertisements with sections devoted to jobs, housing, personals for sale, services, community, résumés, and discussion forums. However, it has been implicated to networks of child prostitution through its ads. On May 13, 2009, Craigslist announced that it will close the 'Erotic services' section, replacing it with an 'adult services' section where the postings will be reviewed by Craigslist employees. This decision comes after allegations by several US states that the erotic services ads were being used for prostitution. However, according to a *New York Times* article, Craigslist has increased its revenue 22 percent in 2010, largely from its controversial sex advertisements. That financial success is reviving scrutiny from law-enforcement officials who say the ads are still being used for illegal ends. See *New York Times*, April 25, 2010, http://www.nytimes.com/2010/04/26/technology/26craigslist.html?hpw

possibility for the client to pay by credit card and book the services on-line);

3. the victim may be recruited either traditionally or via Internet and may be forced to expose in Internet (child pornography) or forced to make virtual sex with a client paid through credit cards;
4. in the case of mail order brides, the trade often occurs when the client pays by credit card and the "package" is delivered to him at home. The victim in such cases is often a girl child who may have been sold by her parents or abducted.

According to a study commissioned by the Council of Europe,[33] police operations in several Member States and by Europol suggest that the Internet and mobile phones are more widely used to recruit victims of trafficking in human beings than was originally thought. Traffickers point to the Internet for the recruitment for purposes of labour exploitation and also sexual exploitation, via bogus escort services, marriage agencies, job advertisements, chat-rooms, among others.

In Canada, the Canadian National Threat Assessment[34] shows that most of the victims of human trafficking were recruited for sexual exploitation through the Internet or an acquaintance and that Internet is also used to advertise their services. Ads were posted in ethnic newspapers and an Internet classifieds website to solicit clients. Alberta & BC investigators have seen the girls move from one city to another on Craigslist.The ad is placed in one city for a period of time and then it's removed and the same female is placed in an ad in a different city (e.g. "Apple is in Edmonton now"). Advertisements of under aged girls have been placed in Craigslist. Law enforcement in Canada has contacted Craigslist to have ads removed when they know that a victim is under the age of 18 years.

It is rather common in sexual trafficking that the traffickers place

[33] A. Sykiotou (2007), 'Misuse of the internet for the recruitment of victims', *op.cit*.

[34] Material provided by Cpl. Nillu Singh (Human Trafficking National Coordination Centre, RCMP HQ, Ottawa, Canada) during the UN World Congress ancillary meeting organised by UN.GIFT on 17.4.10 in Salvador, Brazil.

their victims in apartments or hotels in various cities. They have strict rules, forbidding their victims to leave their place of work, visit restaurants or receive visitors without their permission. Clients are charged expanding the "services" and the "product" from €70-€80 up to €3,000. The victims pay normally a weekly fee of €500-€2,000, which go to traffickers based in another country. In addition to this weekly fee, they are forced to hand over at least 50% of the money they receive from clients. A separate arrangement is made with each victim.

Traffickers often post nude photographs of all the recruited victims on the Internet, advertising sexual services. Traffickers use also concealed surveillance cameras and computers to control the prostituting victims, in apartments.

The trade is rather obvious in several sites that offer e.g. escort or "personal" services. However, what is not obvious is if that "trade" is legal or not and -if not legal- what type of crime this may constitute. If it concerns children it is obvious that it is trafficking. But if it concerns adult persons there may be either legal activities (in countries where prostitution is legal) or illegal (if prostitution is prohibited), but it is difficult to conclude if this constitutes trafficking or facilitation of prostitution unless there is more prove that these persons have been coerced or deceived.

Description of the Role of Traders and Consumers

1.*The role of consumers*

Consumers or clients (in sexual exploitation) are the second type of Internet users. They should be distinguished from traffickers, although – in the field of pornography – many pedophiles create their own sites, exploiting their victims directly. In such cases, they can be considered as traffickers and consumers.

It is obvious that consumers contribute to trafficking in human beings, since it would not exist without them. The Internet allows them to stay safely in their homes and preserve their anonymity, giving them the feeling that they can wallow in any perversion online without fear of detection.

Most of the men who use the Internet to find women trafficked for purposes of sexual exploitation (and to share their experiences) seem to be travelling businessmen, people reporting on local prostitution, and students.

Under Article 19 of the Council of Europe Convention on action against trafficking in persons, using the services of a trafficked victim is a criminal offence. It must be emphasised that the fact of its possibly being hard to prove makes no difference.[35]

At this point, we should note that some of the fraudulent advertisements posted on the Internet are aimed, not just at potential victims, but also at consumers (but in a different way). For instance, Web sites which include nude photographs of women (some of whom may not even know that their pictures have been posted) can affect both in the following way:

a) Women who never intended to let themselves be advertised as prostitutes are stigmatised as such. In this case, the only exploitation they suffer is exploitation of their image.
b) Clients may be deceived as well, since they may pay for sexual services which are never provided. In such cases, the client is the direct victim, and the woman whose picture has been published is the indirect victim.[36]

2. *The role and identification of traffickers*

Traffickers need either a minimum knowledge of the use of Internet

[35] See point 234 of the 'Explanatory Report of the European Convention on Action against Trafficking in Human Beings: "Proving knowledge may be a difficult matter for the prosecution authorities. Similar difficulty arises with various other types of criminal law provision requiring evidence of some nonmaterial ingredient of an offence. However, the difficulty of finding evidence is not necessarily a conclusive argument for not treating a given type of conduct as a criminal offence."

[36] In 2006-2007, a three-country study (Greece, Cyprus, Germany) on the demand side of trafficking was carried out as part of the European project AGIS run by the University of Thrace. The conclusions showed that most clients were unaware that trafficking in human beings is a crime, while a large percentage did not care about the girls, but only wanted to get the services they had paid for.

or accomplices that have the knowledge to recruit their victims through this means.

Additionally, traffickers who have the knowledge might create sites themselves or rely on existing ones.[37] Exploitative sites, such as those that recruit and exploit (mainly) women from abroad differ from pornographic sites in being harder to manage and by exposing traffickers to greater risks, e.g. the risk that the victim will be stopped at the border, and that border officials may need bribing. This partly explains why this type of trafficking seems mainly to attract organised criminal groups. However, there are other problems, e.g. when criminals use proxy servers, usually based in countries with no proper legislation – which makes it increasingly difficult to identify the persons behind the web sites. These sites (especially pornographic sites) can also use payment methods such as e-gold and Web money – virtual charge cards, which make it hard for the police to follow the money trail.

Trying to establish a typology of traffickers in order to easily identify them is not easy. Several categories of traffickers might often be applicable to the same person:

– Traffickers that use the form of spams[38] to lure their victims or

[37] It appears that 70% of Internet sites are invisible (sites which have a reference, but are not pointed to by others and cannot be located by traditional search methods). This applies to many illegal image sites, whose life is very limited.

[38] It is reported that only in the second half of 2009 there was an overall increase in the levels of malicious spam to 3 billion messages per day, compared with 600 million messages per day in the first half of the year. Social networks such as Twitter are reported as being used to spread malicious spams. See M86 Security, 'Security Labs Report', Jul 2009-Dec 2009 Recap; www.m86security.com Victims of labour exploitation have been reported as being lured by spam mail or by fraudulent job offers online. A. Sykiotou, 'Misuse of internet for the recruitment of victims of trafficking', *op.cit*., p.83. At the European Union level, the European Commission acknowledged, in a Communication on spam, that laws to combat these threats are already in the making – particularly the European Union-wide "ban on spam", adopted under the ePrivacy Directive in 2002. However, enforcing them is still a problem in most European Union countries. Spam was reduced in the Netherlands with the help of prosecutions brought by OPTA, an anti-spam agency with just 5

- Traffickers who lure their victims through chat-rooms, instant messaging, or social networks, and
- Traffickers who use traditional methods of recruiting them, but who use the Internet to advertise and sell their 'products' and who often belong to transnational organized criminal networks.

The various typologies of traffickers vary according to:

i) The method of recruiting their victims;
i) Whether they choose to transfer their victims abroad or not for exploitation;
ii) How they use the Internet and their involvement in the creation of sites;
iii) Their personal involvement in the exploitation of the victims (e.g. exploitation for personal use and not necessarily for economic profit;[39]
iv) Their level of association with transnational/national organized criminal networks.

Depending on their contribution to the production of sites and the use they make of them, traffickers can be grouped in three categories. It should be noted that these three categories are often connected with the organised transnational form of trafficking in human beings and that traffickers can figure in all three categories simultaneously:

i) Traffickers often set up sites in the countries of origin and in the languages of potential victims. These sites then spawn others, often

full-time staff and 570,000 euros' worth of equipment. *Ibid*., p.28. On 27 November 2006, the Commission called on all the regulatory authorities and stakeholders in Europe to step up the fight against spam, spyware and malicious software. It insisted that, although Internet safety had been on the political agenda for some time, national authorities must do more to prosecute illegal online activities. *Ibid*., p. 51. See also the malware targeting Macs discovered during 2009 that included Trojans posing as ActiveX components required to view pornographic videos. http://www.sophos.com/security/topic/security-report-2010.html; and also http://www.sophos.com/blogs/gc/g/2009/06/10/mac-malware-adopts-porn-video-disguise/

[39] The concept of profit does not necessarily entail economic profit. See A. Sykiotou (2006), 'The concept of victim in human trafficking', Review: *Poinika Chronika*, pp. 684-693.

building up to form national recruitment networks. They are also tailored to the market the traffickers are targeting;

ii) The material collected via a first site is then used on a second, aimed at attracting users. Information on the recruited victims is translated into English and the languages of other sex or labour markets where the traffickers wish to operate.[40] Traffickers in these two groups may be identical (the same person) or, more often, the second may act as accomplice to the first;

iii) The third type is the trafficker who recruits victims and exploits them directly (without middlemen) via online booking with users (clients, employers, etc.).

A distinction should obviously be made between traffickers who set up sites themselves and then exploit the victims recruited, and the operators who are paid by traffickers to set up sites and, thus, becoming their accomplices. These people play a key role in trafficking in persons via the Internet, since they have the technical know how needed to create sites and hide electronic traces from the police. However, innocent IP addresses can also be stolen by traffickers and used to hide their true addresses.

3. *Problems regarding the identification of traffickers*

There are several difficulties in identifying traffickers through the above mentioned sites. Criminals may use proxy servers, usually based in countries with no proper legislation, making it increasingly difficult to identify the persons behind the web sites.

[40] At this stage, sites aiming at sexual exploitation offering mainly "escort services" start seeking subscriptions from members (clients), who are given the option of paying online to visit the girls in their own countries or, alternatively, "import" them (availability in terms of place and time is specified). If a client wants to bring a girl to his/her own country, a local go-between makes sure that /he/she gets in and out "safely". The same process may apply if a local trafficker wants to bring in victims advertised on the Internet and exploit them in his/her own business. Often, this involves contacting a "middleman", which can be the case with most forms of trafficking in human beings, from domestic slavery to sexual exploitation.

Problems regarding identification by the police and consequently prosecution of cyber-traffickers mainly relate to (lack of) evidence. In particular:

i) Timely location of perpetrators and preservation of digital evidence is an important issue for consideration due to the inability of many countries to store big quantities of data and also the lack of obligation for Internet Service Providers to store data (in EU there is such legislation since Directive 24/2006[41] obliges ISPs to store data for a minimum of 6 months);
ii) There is an important degree of volatility of digital evidence (it is as easy to create many copies, but it is to destroy evidence instantly);
iii) It is essential to display objectivity in court, as well as the continuity and integrity of evidence. It is also necessary to demonstrate how evidence has been recovered, demonstrating the process through which evidence has been obtained.[42] Evidence should be preserved to such an extent that a third party is able to repeat the same process and arrive at the same result as the one presented in court;
iv) Digital evidence is only part of the evidential material which can support charges against traffickers.

4. *The role of service providers in trafficking*

Apart from the *traffickers, the victims and the clients,* there are also *service providers* and various stakeholders that facilitate the trafficking process through the Internet such as financial institutions that allow payment by credit cards and also the press and/or the media that might host deceptive advertisements[43]. All the above can play a key

[41] Modifying the Directive 58/2002 of the European Parliament and of the Council of the European Union.

[42] ACPO e-crime Strategy, 2009 Report.

[43] Newspapers and magazines as well as the media have a part of responsibility in publishing through their sites advertisements that manifestly offer exploitative services e.g. 'slaves for all tastes').

role to Internet-related cases of trafficking. Their role in such cases is not documented and needs to be more thoroughly researched.[44] In addition, the role of legal entities that seek cheap labour worldwide needs also to be further researched.

Human Trafficking and Anti-cyber Crime Legislation

From the moment traffickers use cyberspace as a tool, trafficking is considered as cybercrime and normally it falls under the scope of legal texts addressing to cybercrimes. However, as said above the only text on cybercrime at international level is the Council of Europe Cyber Crime Convention[45] and it took more than 10 years for the member States to ratify it[46]. Other texts at EU level regulate mainly the issue of safety in the use of Internet, but do not refer expressly to cyber-

[44] The distinction between voluntary and forced prostitution might be difficult, but when it comes to other forms of THB such as forced labour, slavery or practices similar to slavery it becomes obvious that the behaviour of individuals actively seeking the services of trafficked victims (or even accepting such services) needs to be criminalised and punished. Up to now transnational researches on the demand side of trafficking have been realised by: Anderson, B. & O'Connell-Davidson, J. (2003), *Is Trafficking in Human Beings Demand Driven? A multi-country pilot study*, Geneva: IOM: http://www.iom.int//DOCUMENTS/PUBLICATION/EN/ mrs_15_ 2003.pdfand in the framework of the European program AGIS between four countries of the EU: Greece, Germany, Cyprus and Belgium: 'DeStoLi. Demand of stolen lives. Researching the demand side of trafficking in human beings', 2005-2007; ILO (2005), 'The Mekong challenge. human trafficking: redefining demand'; ILO (2006) 'Combating child trafficking. Demand side of human trafficking in Asia: empirical findings'; USAID (Auf. 2011), 'Tackling the demand that fosters human trafficking – final report'.

[45]Council of Europe/Octopus Programme (2008): 'Guidelines for the cooperation between law enforcement and internet service providers against cybercrime', http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/ LEA_ISP/default_en.asp ; Council of Europe/Global Project on Cybercrime & the Lisbon Network (2009), 'Cybercrime training for judges and prosecutors: a concept'.

[46] Status as of 29.4.2015. Total number of ratifications/accessions: 45. Total number of signatures not followed by ratifications: 8.

trafficking; only to the issue of storing data for eventual prosecution if there any criminal activity.[47]

The European Convention on Trafficking on Action against Trafficking in Human Beings of 16.5.2005 [ETS 197] is considered as covering also the use of Internet. The drafters looked at use of new information technologies in trafficking and they decided that the Convention's definition of trafficking in human beings covered trafficking involving use of new information technologies.[48] For instance, the definition's reference to recruitment covers recruitment by whatever means (oral, through the press or via the Internet). It was therefore felt to be unnecessary to include a further provision making the international-cooperation arrangements in the *Convention on Cybercrime* [ETS No.185] applicable to trafficking in human beings.

Art. 9 of the Cybercrime Convention refers to child pornography, but it is considered that any crime of common criminal law that is committed with the help of cyberspace can be prosecuted under this Convention. The legal basis for this argument is given by Art. 19 allowing the prosecuting authorities to access, research and seizure data stored in any computer system or portable media. In addition, the prosecuting authorities may impose an individual who possesses special knowledge for the preservation of data in PCs to provide law enforcement authorities with all necessary information. Furthermore, there is provision on the obligation upon order of the prosecuting authorities to maintain the data that is stored on an individual's computer for as long as required (up to 90 days) in order to help the investigation. The convention is the first text at international level required to preserve data.

The reason why trafficking is not embedded as such in the Cyber Crime Convention is because the Convention is a general tool aiming to cover four large categories of cybercrimes:
a) against confidentiality, integrity and availability of data, such as il-

[47] Directive 24/2006[47] obliges ISPs to store data for a minimum of 6 months.
[48] See point 79 of the Explanatory Report to the Convention [ETS no 197].

legal access, illegal trapping-interception, data interference, or system;

b) relating to computers such as forgery and fraud associated with PCs;

c) crimes relating to the infringement of copyright and related rights; and

d) content related crimes, such as trafficking where the Convention gives the example of child pornography as a form of trafficking which is considered to be more related to cyber-space (at least at the time of drafting the Convention).

It is rather strange that in 2010 Russia's proposal for the adoption of a Convention on Cybercrime at international level has been rejected by the UN, despite broad agreement that closer international cooperation is vital in a world more closely connected by global computer networks.[49]

The Declaration Salvador[50] in 2010 had left a window open for a global agreement (paragraphs 39-42 of the Declaration). A UN Advisory Committee was supposed to draw up a study on legislation and law enforcement strategies for Cybercrime. The process was intended to bring the opposing countries closer and lead to suggestions that could open a path for preparatory talks for a global agreement on cybercrime. Such discussions can last for years.[51]

Unlike UN, the Council of Europe seems more active and has already established a Special Committee within the framework of the Octopus.[52] On December 2014 (23.12.2014) the Commission has pub-

[49] http://www.computerweekly.com/news/1280092617/UN-rejects-international-cybercrime-treaty

[50] Declaration of the UN 12th World Congress for crime prevention, Salvador, Brazil, 12-19.4.2010.

[51] The negotiations for the Council of Europe Convention on Cybercrime lasted 12 years.

[52] Council of Europe, Zahid Jamil, Cybercrime model Laws, 'Discussion paper prepared for the Cybercrime Convention Committee (T-CY)', 23.12.2014, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/3021_model_law_study_v15.pdf

lished a model for the creation of model laws on the basis of the sole supranational text: the Convention on Cybercrime (Convention of Budapest).

Obstacles Regarding the Implementation of Transnational Conventions

Horizontal action taken through conventional cooperation of States makes the implementation of texts depending on the one hand by the political will and on the other from the existence of financial resources suitable for the realization of its implementation. It is known that traffickers are often located in a country that has not ratified the convention or in a country known for its unwillingness to cooperate with the rest of community despite the fact that it may have ratified the specific convention.

Further, among the countries that have ratified the Convention (total 37) there is great variation in relation to the telecommunications infrastructure and the corresponding Internet penetration. In addition, conventions leave room of implementation in every national legislature which results to emerging in practice various problems related to the qualification of acts, but also issues of jurisdiction.

What is more, transnational conventions are texts of regional character having reduced field of application and this is not enough for an effective implementation, in the sense of effectively fighting the crime, since many providers are established outside the region. They also offer only partial regulation of the subject since up to now existing texts attempt to either cover the issue of safety in Internet or the issue of trafficking.

The legal framework that regulates cybercrimes is not enough since cyberspace is a field that advances with an extreme rapidity.

Preventive Measures

Web pages of police departments, social organisations, Ministries, Embassies, Banks and other public or private entities can all provide advice to increase public awareness, avert and protect persons against the dangers inherent in the new technologies. They can also offer ad-

vice on safe Web surfing and on how users can be protected from being implicated either as potential victim or as client[53] when using the Internet. Programs that detect pedophile activities could be also adapted to prevent forms of trafficking related to the Internet.

However, prevention generally depends on the importance given to international, regional and local cooperation and the co-ordination between the various entities responsible for combating trafficking, as well as to specialized capacity development programmes; especially in information, communication and technologies, since this is a field that evolves rapidly and has an impact on the new modus operandi of the traffickers.

For prevention efforts to be effective, it has to be understood that trafficking is not only a problem of the State(s), but it concerns societies and citizens worldwide. Only with a collective confrontation of the problem this phenomenon can be prevented. For this reason, raise awareness of the media and the civil society is an important tool to prevent Internet related trafficking (in countries of origin and in countries of destination so as to reduce the demand that fosters exploitation). Also cooperation can be an effective tool from government and non-governmental organizations as well as the private sector for the prevention of persons at risk; and for the prevention of re-trafficking and re-victimisation.

Prevention is also directly linked to the assistance and protection for potential victims of trafficking and to the demand that fosters all forms of exploitation. The involvement of the private sector in preventing Internet-related crimes applies in particular to Internet service providers and financial institutions that have a role in detecting and investigating suspicious financial transactions.

Up to now there are several preventive measures implemented either by governments or by private organizations both at national and international levels.

---

[53] Persons wishing to use (adult) sexual services online should be averted for avoiding services of trafficked victims.

It needs to be underlined that according to the case-law of ECTHR, governments have an *obligation* to take appropriate preventive measures for their nationals. The first time that the Court of Human Rights highlighted the obligation to cooperation between States, as well as the obligation to take immediate action on the training of authorities for the proper and timely identification of victims of trafficking in human beings was in 2010 with the case *Rantsev v. Russia and Cyprus*[54]. In its judgment, the ECTHR accepts openly that, trafficking in human beings is identical with the meaning of slavery of art. 4 of the Convention and as such constitutes a serious violation of human rights. In other words, Member States have a clear obligation to take positive measures to prevent trafficking and protect victims, or else they violate the fundamental rights protected by the provisions of the ECHR.

1. *Measures at international level*

INTERNATIONAL PARTNERSHIPS

Virtual Global Taskforce[55] (VGT) is an international partnership of law enforcement agencies, which was established in 2003 to fight online child abuse It comprises the Australian High Tech Crime Centre, the United Kingdom's Child Exploitation and Online Protection Centre (CEOP), the Royal Canadian Mounted Police, the United States Immigration and Customs Enforcement authorities, the Italian law-enforcement authorities, the New Zealand Police, the Ministry of Interior of the United Arab Emirates, Europol and Interpol. VGT could expand its mandate to serve for combating the recruitment of victims for all forms of trafficking in persons.

[54] Decision of ECHR of 7.1.2010 (Application no.25965/04). This is the first decision that condemns Member States of the Council of Europe in the case of trafficking in human beings for lack of victim protection measures, effective prevention and suppression of crime. Decision commented by A. Sykiotou (2010) in: Efarmoges Dimosiou Dikaiou no 3, pp. 656-678.

[55] http://www.virtualglobaltaskforce.com/

2. *Preventive measures of the European Union*

One example of preventive measures taken at international level is the forum created by the European Union on organised crime prevention[56], comprising national law enforcement authorities, business and professional groups, academic researchers, non-governmental organizations and civil society in general. This forum was set up in 2001 to discuss new approaches to preventing organised crime and it has also included trafficking in human beings.

In the framework of Europol the Analytical Work File (AWF) has been set up in 2001 to help participating member states to prevent and combat the activities of criminal networks involved in the production, sale or distribution of child pornography, and associated types of crime within Europol's mandate, e.g. sexual exploitation of children. So far, it has been immensely, and increasingly, successful.

PREVENTIVE MEASURES TAKEN BY GOVERNMENTS

Many governments have taken preventive measures at national level. For instance, in Greece there have been installed help-lines for victims in 2006 by the National Centre for Social Solidarity (EKKA) with multilingual staff. In June 2007, the Ministry of Finance has set up a new body, the DART (Digital Awareness and Response to Threats) in order to increase public awareness, avert and protect against the dangers inherent in the new technologies, and provide advice on safe Web surfing, particularly for children and parents.

In Belgium the -eCops system was created mainly to fight child pornography, but it also addresses other Internet-related crimes, and can be used to report offences committed via or against the Internet.

---

[56] Athanassia Sykiotou (2009), 'The European Convention against Trafficking of Human Beings in Relation to the Case-law of the European Court for Human Rights on Art.4 of the ECHR and the Case-law of the International Criminal Tribunal for the Former Yugoslavia on Enslavement' (in English), in: M. Kranidiotis, (ed.), *Volume in honor of Prof. Aglaia Tsitsoura*, Sakkoulas Publs., pp. 103-140.

PREVENTIVE MEASURES TAKEN BY PRIVATE ORGANISATIONS

a. Public awareness tools

Up to now several interesting preventive initiatives have been taken by organisations:

- In Poland the NGO 'La Strada' has developed Internet web site to provide advice for people going abroad to work. They also monitor Internet forums containing suspect job offers.[57]
- In the United Kingdom the NGO "Safe Modelling" has set up such a site, which gives detailed advice on avoiding fake agencies.
- In the USA the Polaris Project[58] has launched several programmes against trafficking such as the "Public Outreach and Communications Programme" aiming to increase public awareness about the realities of human trafficking in the United States and build local capacity to combat human trafficking by engaging media, community members, and key stakeholders in anti-trafficking activities at local and national levels. In an effort to develop the grassroots movement against trafficking and enable individuals, communities, and organizations to make an impact, the Polaris Project also launched the Polaris Project Action Centre[59], which is a site that provides individuals and groups with the information and tools they need to take action. The site includes basic facts about human trafficking and information on recent trafficking cases, testimonies of survivors, daily news, and concrete ways to take action.

b. Filtering systems

Filtering systems and programs that detect pedophile activities have been created to prevent children from being lured by pedophiles while

[57] A. Sykiotou, 'Misuse of internet', *op. cit*., p.102.

[58] http://www.polarisproject.org/content/view/53/72/

[59] "Believing that widespread public awareness, community involvement, and local ownership are essential to bringing about sustainable social change, Polaris Project's public outreach efforts are an integral component of our holistic approach to combat modern-day slavery", http://actioncentre.polarisproject.org/

in Internet. Such systems can be at the same time considered as contributing to both prevention and to disrupting trafficking activities. Some examples include:

i) Cyber Tipline: AOL (America on Line) in collaboration with the National Centre for Missing and Exploited Children (NCMEC) has created a filtering, monitoring and reporting system for the domain names of chat rooms. The idea is to capture using the name of the domain what is the creators' potential objective (for instance: from the chat room listings a chat topic such as: "new born 'secks'" refers to 'sex'; or "raype abduct" can refer to 'rape abduction'). Consequently, if the user gives the name of a chat room which sounds suspicious AOL can either block it (not allow its creation) or close it down. AOL also publishes all the cases that result to arrests to increase awareness-raising on the issue.[60] This system was created mainly to combat child pornography and child exploitation and it applies for domestic cases (in USA & Canada, each system is independent). As a consequence, it presents a deficiency when a case is of an international character.

The Greatest Challenges for National Governments, Police and Judiciary in the Fight against Human Trafficking through Cyberspace

The difficulty in monitoring information networks, especially the Internet, the anonymity of users and the risk for the disappearance of traces of the crime through the deletion of evidence or using a series of different providers that are located in different continents create constantly the need for new legal instruments in such crimes. The latter poses a problem regarding the confidentiality of communication and protection of personal data, while there is the evident risk of ending up

[60] For instance in 2007 there was a case of a man in Oklahoma who attempted to sell his children over the Internet for sex. He had a conversation in an Internet chat room where he allegedly promised to procure a 5-year old and a 1-year old for sex to a New York man for 5,000$. The National Centre for Missing and Exploited Children picked up on the possible transaction and alerted New York State Police. Following up on information the Oklahoma Police arrested the perpetrator.

in a generalized surveillance. The transnational character of cybercrimes imposes the need for police and judicial cooperation between Member States in order to prosecute and convict the offenders. The absence of a uniform legal framework creates problems both in terms of the definition of the crime, as well as in the investigation and collection of evidence.

1. *Challenges for the governments*

The major difficulties in the fight against human trafficking through cyberspace lie first of all in two types of shortcomings:

1) Shortcomings in legislation, since the related legislation on Internet remains chaotic and regional. There are not internationally agreed instruments on the use of Internet or on Internet related crimes (including cybercrime). Only regional instruments exist for the moment: In the framework of the Council of Europe the Cybercrime Convention,[61] and in the framework of the European Union, the legislation on electronic communications and the responsibility for Internet service providers of 2006.[62]
2) Shortcomings in technical means and infrastructure, mainly concerning telecommunications that impede the collaboration between law enforcement authorities and implementation of adequate measures in all countries. Success in fighting Internet-related trafficking relies at the same time on the *technical know-how* and in the quick response of law enforcement authorities as well as on the co-

[61] Council of Europe Convention of 23.11.2001 (ETS 185); in force since 1.7.2004. See Sylvia Mercado Kierkegaard (2005), 'Cracking down on cybercrime global response: the Cybercrime Convention', *IIMA* 2005 5(1), Article 7, pp. 59-66.

[62] There is also the legislation on Internet such as the 2005 EU Framework Decision on attacks against information systems which provides for the criminalisation of instigation, aiding and abetting and attempt to commit certain cyber offences, such as illegal system interference and illegal data interference, but it is not related to trafficking. It provides for aggravating circumstances (at least between two and five years of maximum imprisonment) for offences committed within the framework of a criminal organization or offences that caused serious damages or has affected essential interests.

operation and coordination of authorities at national and international levels.

Governments should take the following steps in the fight of cyber-trafficking:

1) Harmonisation of Internet legislation aiming at the retention of data by Internet Service Providers, including the possibility of withdrawal of any prohibition related to data protection for any action related to human trafficking investigations, while ensuring the protection of bona fide users;
2) Compliance of national provisions on trafficking in persons with the international texts;
3) Standards setting(preferably harmonised at the international level) for various types of web sites and services offered through the Internet, e.g. employment or marriage agency sites;
4) Institutionalisation of capacity development measures to increase the capacity of law enforcement authorities to investigate Internet-related trafficking cases;
5) Regular monitoring[63] and investigation through innovative and specialised investigative methods and techniques by law enforcement authorities, combined with preventive action to alert potential victims and clients;
6) Regular analysis of reported cases to help create profiling systems for sites and tools used to recruit victims via the Internet, by:
   (i) Gathering all information on Internet-related cases of human trafficking using existing systems (such as Interpol, Europol, Eurojust) to which only authorised persons would have access;
   (ii) Gathering tactical intelligence about the methods of recruit-

[63] There are however some concerns on the safeguard of privacy. Recently in Algeria, a government proposal to filter Algeria's Internet traffic to beat cybercrime and online pornography is opposed by those who worry about privacy and connection speeds. It is sustained that the government's desire to crack down on questionable sites would be better served by passing an "ethics code for cybercafes and Internet stores" specifying their duties and rights. http://www.maghrebia.com/cocoon/awi/xhtml1/en_GB/features/awi/features/2009/12/15/feature-02

ment;

(iii) Refining methods for analysing patterns and sharing information on trafficking in persons' cases carried out through the use of the Internet;

(iv) Developing specific indicators to detect different forms of trafficking in persons through the Internet.

2. *Challenges for the police*

Unfortunately in most cases the perpetrators are faster than the authorities and especially able to have technology on their side.

Very often the certification of victimisation is not possible, unless the police find the digital traces that prove the offence. However, the geographic location of the server that the offenders choose to locate in countries with weak legal framework is possible to neutralize the prosecution. So, for example, if the perpetrator uses one or more hyperlinks his tracing is not easy.

In addition to that, the location of the victims may be impossible only by using the Internet.

According to Europol,[64] organised crime groups are difficult to trace over the Internet. This is because there are deficiencies in a number of key areas, such as:

i) Global information about the Internet itself;
ii) A common reporting system;
iii) Reporting systems for the victims;
iv) Dissemination of information;
v) Data retained by Internet Service Providers (ISP) and Telecoms companies;
vi) A common strategy at international level.

An effective prosecution of Internet related cases of trafficking would benefit from the existence of a global database, which could include organisations and institutions working on anti-human traffick-

[64] 'High tech crimes within the EU: old crimes new tools, new crimes new tools'; Threat Assessment 2007, High Tech Crime Centre.

ing, intended to:

i) Facilitate rapid identification of, and contact between, institutions and organisations active in the anti-trafficking sector in different countries (NGOs, local authorities, government bodies, universities, etc.); working on different forms of trafficking (sexual exploitation, forced labour, organ trafficking, illegal international adoptions, mail-order brides, etc.);
ii) Address different target groups (children, men, women, transgender people, communities, social and health workers, educators, teachers, law enforcement officers, judicial personnel, etc.);
iii) Support different types of action (detection of cases; reporting; disruption of trafficking activities and assistance directly aimed at trafficked persons);
iv) Facilitate the exchange of up-to-date information on organisations, projects, activities and services concerned with trafficking; and of professionals in this field who need to contact their counterparts in other countries.

Given that many consumers are able to use traditional online payment tools, such as their credit cards, as well as new, alternative payment schemes,[65] to purchase activities related to trafficking (from child pornography on the Internet to various sexual services and mail order brides) a *financial coalition* is crucial to stop the online transactions related to human trafficking (this could work in conjunction with the online reporting system described previously).

Such a system exists already in USA in the framework of ICMEC/NCMEC (expanding its Cyber Tipline to include measures

[65] There is a trend toward these web sites directing buyers away from traditional payment tools and methods, such as credit cards, and toward multilayered, alternative payment schemes. For example, a website may purport to offer the traditional credit card payment methods on a webpage, but after attempting to use a credit card, a purchaser is instructed to send an email to a specified email account. The sellers will then reply with instructions on how to send money through alternative payment (noncredit card) mechanisms.

from financial companies). The financial coalition (FCACP)[66] has been created in 2006 and is an alliance between private industry and the public sector in the battle against commercial child pornography and is managed by ICMEC/NCMEC. The mission of the FCACP is to follow the flow of funds and shut down the payment accounts used by these illicit enterprises. Up to now thirty-two financial institutions (banks, credit-card companies, third-party payment companies) and Internet-service companies have joined the alliance[67]. The Financial Coalition, covering 90 per cent of the U.S. credit card industry, aims to eradicate child pornography by following the flow of funds and shutting down the payment accounts being used by those illegal enterprises.

Likewise, in Brazil a financial coalition has been established to fight child pornography between the entities associated with ABECS (Brazilian Association of Credit Card Companies and. Related Services) in cooperation with Safer Net Brazil, the Federal Public Prosecutors' Office, the Federal Police Department and the Ministry of Justice. Since the creation of the coalition the amount reports of ISPs showed a decrease of 90% in 6 months.

3. *Challenges for the judiciary*

The global character of cyber-crime and the lack of uniform legislation in some countries (in some there is almost nonexistent regulation of Internet issues) is impeding the prosecution. From one hand there are emerging problems of terminology and convergence of legislation, and from the other, there are many accomplices in the committing of such crimes (Web developers, service providers, users, etc.) with the

[66] In 2007 the FCACP developed and published a best-practices guide for financial institutions, titled 'Internet merchant acquisition and monitoring best practices for prevention and detection of commercial child pornography'; http://www. missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=373

[67] The European Financial Coalition was launched on 3 March 2009, and is being supported by the European Commission. Asia Pacific Financial Coalition against Child Pornography has also been formed.

aid and abetting of natural and legal persons on a global scale. This complicates matters of participation in crime, jurisdiction and cooperation between prosecuting authorities, and also of determination of the place of the crime.

The difficulty is that given the legal and technical shortcomings perpetrators avoid often prosecution and conviction.

There are countries that have a legislative framework that punishes severely cyber-trafficking, but they do not have the adequate technological means required to allow a rapid intervention of law enforcement authorities for the identification of perpetrators and the protection of data and countries that may lack from both.

Some of the major difficulties for the judiciary are:

- Establish the location of the commission of the crime. Very often there are more persons involved in the commission of the crime, or the act of the offender/s generates its results in more than one places, and even the flow of information via the Internet may pass through different providers, or it has to do with creating different links and, in short, the crime produces effects in different States and in innumerable victims and at different times. It should be more correct to use the concept of 'space' (digital) and not that of the 'place' in the commission of crime, since cyber-space is much broader place where an Internet crime can be committed.
- Establish the accomplishes and prosecute the entire chain going up to the head of organized network;
- Establish a judicial cooperation with countries that are known for their unwillingness to collaborate with international community;
- Have enough evidence and witnesses for the case. It is often that the victims prefer to return home instead of staying throughout the procedure. Sometimes there are no adequate protection measures for the victims and other witnesses and this undermines the completion of the prosecution.
- In many cases the legal defense of the traffickers is better than the victims (that may be inexistent if there is no legal aid) which results in turning the crime of trafficking in a crime that is punished less

severely (such as solicitation of prostitution), or even in the acquittal of the offender(s). The judge should thus have a strong knowledge on the subject in order not to be carried away by masteries of the offender's attorneys.

More particularly, there are three types of problems for the judiciary related to:

- the evidence;
- the transnational dimension of cyber-crimes and
- the failure of removing measures for the protection of personal data, such as secrecy in some legislations.

CHALLENGES RELATED TO EVIDENCE

1. There is great difficulty in handling digital evidence[68] due to the large amounts of data stored;
2. Digital proofs are part of an event only e.g. when an email is sent we know only the external elements of communication;
3. There is a large degree of variability of digital evidence because there is easy to produce true copies, but it's also easy to delete; and
4. Digital evidence is only part of the evidential material to an investigating process, not enough to support the entire case in any cyber-crime.

CONCERNING THE TRANSNATIONAL DIMENSION OF CYBER-CRIMES

1. Most of the time these cases usually involve more countries that are not EU Member States or Council of Europe members and as a consequence, they do not have a uniform legislative framework that would allow the prosecution or the effective punishment of perpetrators.
2. As mentioned above, some of the States in which the providers op-

[68] Eoghan Casey (2001), *Digital Evidence and Computer Crime: Forensic science, computers, and the Internet*, San Diego, CA, Academic Press; of the same author (ed.) 2002;Chris Proside (2001), *Incident Response: Investigating Computer Crime*, Kevin Mandia, New York: McGraw-Hill; Ernesto Savona (2004), *Crime and Technology: New frontiers for regulation law enforcement and research*, Springer, Dordrecht.

erate may not be willing to cooperate.

3. Often there are problems connected to the conflict of jurisdiction when more Prosecutors are appointed (both inside and outside the country) to deal with the case, in particular when there is criminal activity in more than one places. Of course, the creation and expansion of the role of Eurojust has contributed to resolve this issue.
4. The success of the prosecution relies on the know-how and the quick reaction of the authorities and this, because it takes a minute to erase all the incriminating evidence from the Internet.

FAILURE TO REMOVING PROTECTIVE MEASURES SUCH AS SECRECY IN SOME LEGISLATIONS

In some European legislations such as Greece, in order to request removal of confidentiality of Internet providers, the law requires that there should be prosecution of a crime in the degree of a felony and of a particularly serious felony such as murder, terrorism, extortion, etc., or risk to public safety. In such cases the withdrawal of confidentiality is possible only if it is a matter of national security or for the verification of serious felonies (e.g. high treason, criminal organization, etc.). This may create a problem in cases of p.ex. child pornography which is considered only as misdemeanor.

Conclusion

The use of Internet has transformed (or rather: mutated) the victim-offender relationship. This is said, because in Internet the traditional (person-to-person) confrontation between offender-victim does not exist, since very often the offender is 'invisible' and the victim is unaware of his identity. Consequently, the victimisation has become more 'insidious' and the victim cannot directly help the prosecution authorities (with the description of offender, etc.)

However, this "invisible threat" is nevertheless able to create countless victims, like an atomic bomb. This should be taken into account by the legislator as an aggravating circumstance. I believe that this is necessary, since the Internet allows the offender a rapid spread of his criminal results in many and various locations and also a simultaneous

creation of unspecified number of victims, offering the perpetrator the possibility to act in such way without even moving from his chair.

In the globalization era it is not enough to move only at a level of horizontal action to tackle crime, because it is unrealistic. It is not enough to have a uniform legal framework at a regional level (as the Council of Europe cyber-crime Convention) when States outside this region do not have corresponding provisions. The challenge we face today is that we should respond to the globalised crime with a universal legislation, otherwise all attempts will stay fragmentary and we will not be able to escape from this huge spider's Web that generates daily more and more victims. However, together with a universal legislation we need a uniform technological infrastructure at global level that would allow a joint system of communications setting for the rapid intervention of the prosecuting authorities on location and identification of the perpetrators and the preservation of evidence, as well as a strong international cooperation.-

Sources

Anderson, B. & O'Connell-Davidson, J. (2003), *Is Trafficking in Human Beings Demand Driven? A Multi-Country Pilot Study*, Geneva: IOM: http://www.iom.int//DOCUMENTS/PUBLICATION/EN/mrs_15_2003.pdf

ACPO E-crime Strategy, 2009 Report.

Branigan, Steven (2005), High-tech Crimes Revealed: Cyberwar Stories from the Digital Front, Boston: Addison-Wesley.

Casey, Eoghan (ed.) (2002), *Handbook of Computer Crime Investigation: Forensic tools and technology*, San Diego, CA, Academic Press.

Center for Democracy and Technology(2000),'Bridging the digital divide: internet access in Central and Eastern Europe': http://www.cdt.org/international/ceeaccess/countrydetail

Charles Custer, 'Missing, kidnapped, trafficked: China has a problem with its children', *The Guardian*, 12.3.2015: http://www.theguardian.com/commentisfree/2015/mar/12/missing-kidnapped-trafficked-china-children

Council of Europe (2005), 'Organised crime in Europe: the threat of cybercrime – Situation Report for 2004', Octopus Programme.

Council of Europe/Octopus Programme (2008): 'Guidelines for the cooperation between law enforcement and internet service providers against cybercrime', http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime /Documents/LEA_ISP/default_en.asp

Council of Europe, (2014) 'Zahid Jamil, cybercrime model laws', Discussion paper prepared for the Cybercrime Convention Committee (T-CY), 23.12.2014, http://www.coe.int/t/dghl/cooperation/economic-crime/Source/Cybercrime/TCY/2014/3021_model_law_study_v15.pdf

Council of Europe/Global Project on Cybercrime & the Lisbon Network (2009), 'Cybercrime training for judges and prosecutors: a concept'.

Council of Europe/United Nations(joint study), (2009), 'Trafficking in organs, tissues and cells and trafficking in human beings for the purpose of the removal of organs', Joint Council of Europe/United Nations Study: http://www.coe.int/trafficking.

High Tech Crime Centre (2007), 'High tech crimes within the EU: old crimes new tools, new crimes new tools'; Threat Assessment.

ILO (2005), 'The Mekong challenge. Human trafficking: redefining demand'.

ILO (2006), 'Combating child trafficking. Demand side of human trafficking in Asia': Empirical Findings.

ITU Telecommunication Development Sector (April 2009), 'Understanding cybercrime: a guide for developing countries', ICT Applications and Cyber security Division Policies and Strategies Department; http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf

Jewkes, Yvonne (ed.) (2002), *Dot. coms: Crime, deviance and identity on the internet*, Cullompton, Devon, UK: Willan.

Letherby, Gayle and Marchbank, Jen(2003), 'Cyber-chattels: buying brides and babies on the net', in: Yvonne Jewkes (ed.) (2002), *Dot. coms: Crime, deviance and identity on the internet*, p. 68.

Livingstone, Carol/ECPAT International(2002),*Protecting Children Online: An ECPAT guide*, Bangkok, ECPAT International.

Llyod Kathryn A. (2000),'Wives for sale: the modern international mail-order bride industry', *Journal of International Law & Business*, 20, 341-367.

Lomas, John W. Jr. (2005),'New Jersey's adult internet luring statute: an appropriate next step?', *Duke Law & Technology Review*: http://www.law.duke.edu/journals/dltr/articles/2005dltr0016.html

Muir, Deborah(2005),*Violence against Children in Cyberspace*, Bangkok, ECPAT International.

Goodman, Marc D. and Brenner, Susan W. (2002), 'The emerging Consensus on criminal conduct in cyberspace', http://law.scu.edu/international/File/goodmanbrenner.pdf

Proside, Chris (2001), *Incident Response: Investigating computer crime*, Kevin Mandia, New York: McGraw-Hill.

Save the Children(2004),'Position paper on child pornography and internet-related sexual exploitation of children, London, Save the Children.

Savona Ernesto (2004), *Crime and Technology: New frontiers for regulation law enforcement and research*, Springer, Dordrecht.

Surtees, Rebecca & Stojkovic, Slavica (2004), *Annotated Guide to Internet-Based Counter Trafficking Resources*, International Organisation for Migration (IOM).

Sykiotou, Athanassia (2010), 'Comments on the Decision of ECHR of 7.1.2010 (Application no.25965/04) Rantsev v. Cyprus and Russia', in: *Efarmoges Dimosiou Dikaiou*, 2010 no 3, pp. 656-678.

Sykiotou, Athanassia (2010), 'The impact of the internet on trafficking in persons', Concept Paper prepared for UN.GIFT.

Sykiotou, Athanassia (2009), *The Internet as Means of Victimisation*, Athens, Ant. Sakkoulas Publs.

Sykiotou, Athanassia (2009), 'The European Convention against trafficking of human beings in relation to the case-law of the European Court for Human Rights on Art.4 of the ECHR and the case-law of the International Criminal Tribunal for the Former Yugoslavia on

enslavement' (in English), in: M. Kranidiotis, (ed.), *Volume in honor of Prof. Aglaia Tsitsoura*, Sakkoulas Publs., pp.103-140.

Sykiotou, Athanassia (2007), *Trafficking in Human Beings: Internet recruitment. Misuse of the Internet for the recruitment of victims of trafficking in human beings*. Directorate General of Human Rights and Legal Affairs of the Council of Europe, Strasbourg.

Sykiotou, Athanassia (2006), 'The concept of victim in human trafficking', Review: *Poinika Chronika*, p. 684-693.

Sykiotou, Athanassia(2003), *Trafficking in Human Beings in the Balkans*, Athens, Ant. Sakkoulas Publs.

Treatment of Offenders (UNAFEI) (2000), *Crimes Related to the Computer Network: Challenges of the twenty first century*, UNAFEI, Tokyo.

UNODC/UN.GIFT (2009), 'Global report on trafficking in persons', February 2009.

USAID (Auf. 2011), 'Tackling the demand that fosters human trafficking – final report'.

Wolak, Janis, Mitchell, Kimberly & Finkelhor, David (Nov. 2003), 'Internet sex crimes against minors: the response of law enforcement', Crimes against Children Research Center University of New Hampshire, National Center for Missing & Exploited Children.