19th *ALLIANCE AGAINST TRAFFICKING IN PERSONS* Conference

Using Technology to Combat Trafficking in Human Beings: Turning a Liability into an Asset

8-9 April, 2019

Panel 4 – Changing the policy landscape: current and future strategic approaches to technology and human trafficking

David Mancini

Mr. Secretary General,
Mr. Special Representative and Coordinator for combating trafficking of human beings,
Excellencies,
Distinguished Guests

I am very proud and grateful to be back at the Alliance sharing this experience.

New technologies are a common language in the most serious forms of organized crime.
The immediacy of communication allows criminal groups to be effective, rapid, interconnected with each other and with the victims. ICT are a big challenge for all, also for anti-trafficking stakeholders.
Criminal networks use the internet and social networking tools to recruit victims to be exploited, as a marketing platform for prostitution, labour exploitation, including domestic servitude. Pornography, misuse of live web cameras, live distant child sexual abuse and many other services are online[1]. The use of encryption technologies raises difficulties for investigative authorities.

Research and studies on the ongoing phenomena in Italy[2] shows that in mixed migration flows the line between smuggling and trafficking is even more blurred if we look through the lens of ICT.
The web is used by smugglers and migrants to search for smuggling services.

[1] see the second report from the EU Commission to the European parliament and the Council on the progress made in the fight against trafficking in human beings (2018).

[2] Surf and Sound. The role of the Internet in people smuggling and human trafficking, eCrime – ICT, Law & Criminology
Department, Faculty of Law, University of Trento (2017).

Instagram and Twitter offer images and text contents; on Facebook there are pages, groups and profiles dedicated to the advertisement of illegal migration and to purchase every service and ID documents.

Some of these pages count hundreds or thousands of members/followers.

Some of these groups and profiles are public. Others are “closed” or “private”, meaning that any users must obtain an approval from the administrator (‘friendship’ or ‘membership’) to access the content.

The same is for human trafficking, with many pages on social media websites offering jobs, contracts, visas, and residences in Europe, travels and documents which are necessary to move to and within Europe. That can be found on the visible web but especially on the *Darkweb*.

Private groups system on Telegram are even more encrypted and hidden (particularly used also by terrorist groups).

The use of ICT tools is more and more common among minors. Their high vulnerability and heedless use of ICT expose them to potential abuses and exploitation starting online. Besides human trafficking, this vulnerability can involve them in online pornography and child pornography.

Many websites and posts offers sex-related services – presumably provided by exploited persons. In some cases, these sexual services are hidden behind other activities, apparently legal. It is a huge flow of online offers and it is hard to certify in each case who is administering the uploaded content.

This use of the web fits into the folds of national policies regarding prostitution, making free prostitution (which in Italy is not illegal) appears what in reality hides a situation of exploitation.

A national and international policy effort is required to reduce this grey area.

In terms of contrast the Postal and Communication police service in Italy, plays an effective role monitoring and detecting the web according to undercover investigations in order to penetrate networks online recruitment of children for child pornography and sexual exploitation through existing legislative tools, but there is a need to strengthen international cooperation. Often the different internal policies hinder cooperation despite the existence of valid conventions (e.g. 2001 COE Budapest Convention on cybercrime).

In Italy identification, assistance and protection of trafficked victims is a priority.

The italian national action plan remarked the need to a multi-agency and victims centred approach in combating trafficking of human beings. However the increasing number of vulnerable persons within mixed migration flows makes it difficult to cope with the various needs effectively. The proactive use of new technologies at a social and investigative level allows obtaining a multiplier of results, if everything is organized with a multi-professional method.

There are different levels of intervention that correspond to different levels of effectiveness.

At the lower scale there is the self-regulation; A detailed provision at a national level should be a goal to be achieved by each State. These will be an explicit achievement the new action plan 2019-2021 should try to improve.

From the social sector, italian NGOs have been using ICT to facilitate contacts with people at risk of trafficking. By Facebook (mostly in private groups) or whatsapp that can be used wherever there is a public network (so without costs) and allows the geolocation useful both for scheduling "appointments" (for visits, interviews, etc.), and in case of emergency.

A fundamental tool is *the anti-trafficking toll-free number* set up by the Department for Equal Opportunities as part of action in favour of victims of trafficking provided for in art. 18 of Legislative Decree 286/98.

Anybody can turn to it: potential victims, private citizens, law enforcement agencies, public or private bodies, members of professional associations.

Apart of its own pages in all social networks, an APP has been created to be published in the Play Store catalog of Android devices. Android platform is the one used mostly by trafficked or exploited persons.

The APP will provide information on the *Anti-trafficking toll-free number* and on the main measures envisaged by the identification, assistance and social inclusion programs in at least ten languages. That tool allows victims to contact directly the hotline with the additional functionality to send the georeferencing of the place where the person is located. This is very useful if the person is kept segregated and does not know the exact place where he/she is.

In addition, the APP provides the opportunity for people who come into contact with potential trafficked persons to fill out a report form, even anonymously.

This can help also to figure out the problems with some mobile phone operators who prevents to make phone calls to hotlines or with cost to the recipient. For example, *Lyca Mobile* who is widely used by foreigners and many victims of trafficking because of low costs and the fact that it is sold in “less formal shops” (African Shop, Asian Market etc) or that SIM are delivered without presentation of valid ID documents.

The use of ICT to improve victims' identification can bring added value if stakeholders are connected in networks and operate within a multi-agency approach, sharing information with the same speed of traffickers.

A National Referral Mechanism technologically implemented is an urgent need for each Member State. And in the NRM should be attracted as external cooperative partners all the main Internet and social network Providers.

In the digital age a new investigative horizon is represented by the computer intrusion, or by interceptions through an internet device.

ICT is a covered working tool to recruit, transfer, manage, exploit victims and to exchange money. Then it is more powerful as the criminal capacity of the organizations grows and get the typical structure of mafia organized crime.

Digital investigations have become a need to keep pace with traffickers.

A computer spyware is a software inserted inside the operating system of any ditigal device, able to take possession of that system, to control the audio, thus making a classic wiretapping, but also being able to localize, therefore, tracking the person or collecting any type of information related, emails or private social network messages.

The installation of the spy software can take place on site or remotely.

To install the sensor locally (on site) it is first necessary to know the access code, if enabled.

Remote installation needs a self-installing virus on any device, by forwarding a text message, an email or an update of an application on the target device.

Computer wiretapping can take place according to the following phases:

- getting the imei code of the device;
- analyzing the target and checking the feasibility of infection, installation and data collection;
- getting by the "profiling" that allows to collect data and information on the user's online activity (e.g. which sites to visit, the most frequently visited web pages, what to buy online, etc.) intercepting the flow of electronic data.

After that the wiretapping starts exploiting the system vulnerabilities:

The active wiretapping system with malware/spyware/trojan horse is composed of two separate parts:

- the agent; it is the software installed on the device and ensuring the basic functions of: backdoor, malware and trojan. It receives commands from the operator, intercepts data, hides it on the operating system of the device and transmits all to the remote control center;
- the server for collecting, reconstructing and storing data received from the agent, must be located in the Public Prosecutor's Office.

The features are:

- **wiretapping and call recording**: it allows calls to be heard and recorded in real time (whether they are made via traditional telephone line or through applications such as Facebook, Skype, Viber, WhatsApp etc.).
- **Environmental recording**: through the activation of the internal microphone.
- **Remote Camera and Remote Video**: this particular feature of the spy software allows to control the camera remotely to take pictures and shoot videos.
- **Access to data**: it is possible to access the contents of the directory, the calls register and e-mails, as well as the SMS, MMS and chat archives (Facebook Messenger, Whatsapp, Instagram, Telegram, Tinder, LINE, Hangouts, etc. .).
- **Playback and viewing of images, videos and audio**: using the spy software it is possible to access the multimedia contents saved on the computer device.
- **Localization**: this allows the identification of the position of the device using the GPS.
- **Information about the applications**: the spy software allows to view all the information such as the date of installation, the update version, the size, if the application was used or if it was closed .
- **Internet history**: it is possible to consult the entire browser history of the monitored device, also viewing the websites saved in Favorites;
- **Keylogger**: that of keylogger is a particular feature of the spy software that allows the recording of the entire chronology of the keys operated on specific applications.
- **Program activities**: allows you to view all the programs installed and their activities.
- **File activity**: allows the display of file characteristics and transfers of the latter.
- **Login / logout activity**: the spy software keeps track of the login and logout activities of users on the PC, with the possibility of detecting, for example, when users block the screen.
- **Resource monitoring**: thanks to a spy software it is possible to detect printed pages, network connections and connected USB devices.
- **Access to application content**: allows interception of communications via the Internet via clients such as Skype, LINE, QQ, Hangouts and Webmail.

- **Remote control** : a spy software allows to change the software functions from a distance, deactivate its use and uninstall it.

As the amount of screenshots, snapshots, keyloggers and various data would absorb memory and gigabytes, the bundle capacity can be increased for the purpose when it's limited, just to avoid exhaustion.

Specialized Italian law enforcement agencies use hacking tools in the process of criminal investigations. It is a modern way to face traffickers in a comprehensive approach. Hacking investigations are part of a proactive approach, for example directly linked to financial investigations to get codes, bank account, home banking operations or other encrypted information on money transfer and laundering.

It is something to be handled with care. The Constitution protect fundamental rights such as privacy (Article 2, Italian Constitution and Article 8 of the European Convention on Human Rights) Inviolability of the domicile (Article 14, Italian Constitution) and freedom and confidentiality of communications (Article 15, Italian Constitution).

To deal with these fundamental rights the Higher Chamber of the Italian Supreme Court established that the use of hacking tools is permitted for wiretapping but, when it is not possible for the location to be identified individually and when criminal activities have not been committed, the use of hacking tools is permitted only for criminal proceedings on organised crime and terrorism. Furthermore, the decision separated the operational modes of hacking tools into two categories: "*online surveillance*" and "*online search*". The first category relates to the interception of an information flow between devices (e.g. microphone, video, keyboard etc.) and the microprocessor of the target device. "Online search" relates to copying the memory units of a computer system.

These decision aims to strike a balance between the significant benefits brought by those tools, in terms of investigative efficiency, and their increased invasiveness.

A law was approved in Italy in 2017. By regulating hacking investigations it introduced specific rules within the criminal procedure code.

Some cautions:

- Trojans must be directly operated by law enforcement agencies (not by private contractors);

- Every operation that uses a trojan must be duly logged and documented in a tamperproof, for all the following controls by the defendant
- Once installed, a trojan shall not reduce a device's security level.
- Once an investigation has finished, the trojan must be safely removed from the target device(s) – either by law enforcement or through detailed instructions.

You know, it's not only an italian practice. Many other Countries are working on that. Germany, Netherlands, France, UK, each one with peculiarities and different approaches according to their national legislation and Constitution.

But it is not possible to proceed in random order because investigations against traffickers are often transnational and require cooperation. International harmonization is needed, also in view of the efficiency and functionality of judicial cooperation.
The effectiveness of the Mutual Legal Assistance, the efficiency of the Joint Investigation Teams must be guaranteed through a modern legal framework on ICT investigations, related to the types of investigations available and to the rules to get evidences valid for the trials. States must seek common solutions, including those in balancing with the fundamental rules of the European Charter of Fundamental Rights and with the ECHR.
This necessity is a real priority with reference to the EIO which expressly regulates the relations between the judicial authorities of the Member States in case of wiretapping involving targets and operators located in the territories of more than one State and which provides for specific obligations of mutual communication and authorization.

In conclusion, regardind human resources, professionals must be trained on these new frontiers, always with a multiagency and human rigths centred approach. That why ICT investigations have been included in the live simulation trainings held in last three years and still ongoing, under the direction of the OSR for CHTB.