Panel 3 – The power of technology to assist in the identification of victims, investigation of cases, and prosecution of perpetrators of human trafficking

Technology is both a blessing and a curse for officials fighting against human trafficking. 90% of all crimes today have a technological or a digital component, whether it is planning, commission or after-crime. Tech-savvy perpetrators use technology to facilitate the crimes - for grooming, recruitment, logistics, planning and advertising of the victims, but also to take advantage of the anonymization and encryption tools to cover their actions. The perceived anonymity and mass audience of online services increases both discretion as well as profitability of these services, making it challenging to identify criminals by using traditional police techniques. Moreover, everything that has been disclosed online can be changed and deleted fast.

On the other hand, we know that enforcement operations are usually reactive, not proactive. Therefore, it is evident that in order to be successful in these criminal investigations, law enforcement has to be creative and to combine and adapt 'classical' investigation techniques. In Estonia, a special unit was formed in the criminal police in 2003, to fight against prostitution in a targeted way. Since 2005, the main focus went from the streets to the World Wide Web. The idea was and is still today that technology can also be used as an asset - to identify more victims and perpetrators and to turn conspiracy methods and tactics that criminals use - against them, by collecting even better evidence to represent in the court via information and communication technologies. As a result, most of the criminal cases are pro-active today and initiated by the police based on the information that has been collected by themselves with operative monitoring of the Internet.

So how does it work in practice? For us, virtual presence of the authorities means that there are several investigators whose daily job is to analyse the information. Criminals, who are engaged in trafficking of human beings, are driven by the financial gain, so they need a place to sell, a marketplace. In Estonia, we have identified the main channels where this is taking place. Usually, these are the web pages dedicated to offer sexual services or employment mediation. What our law enforcement has been initiating is to have conversation and mutual understanding with the owners of those web pages – to raise the awareness of the problem they might be part of and to steer them to cooperation and gradually, there has been a success, as they are providing us with an information that is vital for detecting the victims and perpetrators, like IP and DNS addresses and mobile phone numbers used to activate the account and add the advertisement. Therefore, from the webpage itself we are able to see a little more, than it would be possible with open source intelligence tools, but it is also important to stress out, that in this phase, none of the information is identifiable with an actual person. So, what happens next, is that we are using Linkcluster analysis programme to convert those non-personalized ads into the basic Microsoft Excel file. What we are looking for here, are the patterns, for example, we can sort the worksheet by the telephone numbers used to activate the ad, but this itself does not give us enough information about possible human

trafficking case. So, the next step would be to link this data together with the help of IBM i2 Analyst's Notebook programme, which enables us to get a more comprehensive overview. We call this graph a 'dragon' and what interests us the most in here is its head, where connections between data provided and analysed are the densest. So from here we can see that several ads have been added from the same IP-address or mobile phone number and can by the metadata be linked to each other. It is like a small ecosystem where you can identify by the connections who is probably who – the mediator, dispatcher and the victim. After this process, the official will check the advertisements to seek confirmation for the suspicion. For example, were the advertisements uploaded at the same time? Are there similarities in the pictures or linguistics? What kind of feedback do the clients provide? Do they mark that the possible victim is someone from a different ethnic or race group, is speaking foreign or only limited sexual local language? Or did they seem to be abused substances or have any health issues? Then finally, only if the impression provided by the analysis is confirmed, personification of the particular subjects will be initiated and of course, starting from this investigation phase, motivated order of the prosecutor is mandatory to gain information from the telecommunication companies. Undoubtedly, this method helps us to target our resources better and guarantee that we are addressing the root of the possible trafficking crime, not only single actors.

Another topic where the online presence of the law enforcement is inevitable is grooming of children for the sexual exploitation. As *modi operandi* of those criminals is usually unique - for example, the victim selection, trust development, establishing a relationship and maintaining control is predominantly made via social media - our investigation methods are also different. Usually, we obtain the court order to carry out a sting operation on a specific website, but due to the strict legal framework and court practice, the general rule is that the police agent never initiates the contact first or directs the conversation, to avoid the provocation. After the conversation constitutes enough evidence about the crime, non-content data is requested from the webpage to identify the criminal. Although we have never had any trouble while obtaining the information asked, due to the internal regulations of the companies, they are closing the accounts of the perpetrators immediately, which means that identifying of their real victims of is burdensome and from the legal perspective, we can only prosecute them for the impossible attempt of the crime. Moreover, as at one point, most of the perpetrators are interested of the photos or video calls, the commission of this technique raises both ethical and legal questions, as we cannot and should not reproduce the content. So in the future, we might need a computer-generated child to catch online predators.

The Estonian law enforcement is keeping an eye on a Darkweb also, but fortunately, none of the human trafficking investigations has been carried out so far. The idea that we have been trying to practice in relation to this platform, is that whenever we detain criminals having committed a crime in the Darkweb, we try to confiscate their account(s), to use it/these in other investigations. The value of this step lies in the fact that law enforcement also needs to have a profile which seems trustworthy for

the criminals, so possibility to use an account which has been activated long time ago, has its order history and feedback can be exceptionally beneficial.

The power of technology is also topical after the victims have been identified and perpetrators being caught. Mobile devices like smartphones and tablets contain personal information, such as call history, text messages, e-mails, digital photographs, videos, address books, calendars, web browser artefacts, passwords and sometimes even credit card numbers, making some experts to refer to these even as a new kind of eye-witnesses, as these can be useful as a source of digital evidence to be examined. Although we usually involve digital forensics to guarantee the integrity of the valuable evidence and to document the chain of custody, to make sure that evidence would be admissible in the court, most of the devices and applications support encryption or biometric lock that could make data inaccessible to the law enforcement. In addition, from the legal standpoint, there is a delicate line between an inspection and a search of the device and for example, in a situation where some of the information is located on a cloud service, evidence can be spread around the world, which requires the ability to justify the extraterritorial search and jurisdiction from the prosecution. This means essentially that both law enforcement capacity and methods, and our national and international legal frameworks need constant development to be able to fight the phenomena of modern slavery in a digital age comprehensively.

I would like to finish my presentation with a thought that me and my colleague shared last week, and what we can see is something that is trending - that human trafficking does not mean these days at all, that someone is abused in a physical or even emotional sense, that the victim does not have documents or does not get any salary. It might also appear that the criminals are just using legal loopholes, while formally everything is correct and legal, but then again, if we compare the situation of the victim to the person who is carrying out the same activities without being a victim, then we can see a grave injustice. Therefore, it is important to see a 'bigger picture', but to look at the same time at every case individually.