19th Alliance against trafficking in Persons Conference, Vienna, 8-9 April 2019

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

Presentation by Petya Nestorova, Executive Secretary of the Council of Europe Convention on Action against Trafficking in Human Beings

I am delighted and honoured to be invited to speak at today's conference dedicated to one of the most topical issues in the fight against human trafficking: how to turn the use of technology from a liability into an asset.

The organisation that I represent, the Council of Europe, has been actively engaged in combating human trafficking in its 47 member States and beyond, in partnership with other international organisations, notably the OSCE. The Council of Europe Convention on Action against Trafficking in Human Beings, opened for signature in 2005, is currently in force in 47 countries (46 of the member States as well as Belarus). The Convention provides a comprehensive, multidisciplinary framework for tackling human trafficking, encompassing prevention, protection of victims, prosecution of traffickers, and the promotion of partnerships through international co-operation and co-operation with civil society.

In my presentation, I will first provide an overview of the work of the CoE around the intersection of information and communication technologies (ICT) and trafficking, with examples of approaches to targeting ICT facilitated/enabled human trafficking. Secondly, I will introduce recent policy developments in the CoE relevant to the topic of the conference. Finally, I will draw some recommendations on developing policies addressing ICT facilitated or enabled human trafficking.

1. Relevant CoE work

Back in 2007, the CoE commissioned a study on the misuse of the Internet for the recruitment of victims. Since then, the rapidly increasing availability of technology and generalised access to the Internet have significantly changed the landscape: perpetrators of human trafficking offences can work from home and reach out to potential victims in many countries, taking advantage of ICT for recruitment of victims, grooming, financial transactions, advertisement of services, sexual exploitation via live streaming, and to control and monitor the victims. Cyber-trafficking (to use the buzzword in scientific and policy discussions related to human trafficking) is posing new challenges to law enforcement as digital traces are difficult to track because users are anonymous or a series of different providers located in different countries are used. There are additional challenges posed by the protection of personal data and the confidentiality of information. At the same time, ICT create new opportunities for the investigation and offer an important medium for prevention, while also serving as a tool to assist victims, by breaking the social isolation, and providing a way to report abuse.

The drafters of the CoE Anti-Trafficking Convention foresaw the use of new information technologies by traffickers and decided that the Convention's definition of trafficking in human beings covered trafficking involving use of those technologies. For instance, the definition's reference to recruitment covers recruitment by any means (personal, through the press or via

the Internet), regardless of the mode employed (threat, force, etc.). It was therefore not considered unnecessary to add a further provision making the CoE Cybercrime Convention's applicable to trafficking in human beings.

The CoE Convention on Cybercrime, known as the Budapest Convention, which entered into force in 2004, and is the first and so far only binding international instrument on crimes committed via the Internet and other computer networks. The Budapest Convention deals particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. While it does not refer specifically to trafficking in human beings, it comprises a series of procedural powers and tools which should be regarded as covering all crimes committed on or via the Internet, such as the search of computer networks and interception and seizure of computer-stored data, as well as international co-operation provisions related to any criminal offence, including aspects of human trafficking where evidence is available on computer systems. This can be anything from mobile phone location data of victims or suspects, email traffic, websites to recruit or groom victims, and so on. The Cybercrime Convention covers both public and private networks and communication systems – which is of considerable importance, since many seemingly public networks may be fakes, or imitations of actual public networks or services. The Budapest Convention has 63 States Parties (almost all CoE member states, expect for Ireland, Russia and Sweden, as well as 19 other countries across the world).

The interaction between the two Council of Europe conventions can be used to crack down on cyber-trafficking. Law enforcement agencies can use the "production orders" under Article 18 of the Cybercrime Convention to compel suspects to release specified computer-stored data in their possession or under their control. The same goes for the "expedited preservation of stored computer data" (Article 17), "search and seizure of stored computer data" (Article 19), and "real-time collection of traffic data" (Article 20).

In the absence of a global agreement on cybercrime, the CoE Cybercrime Convention and the work related to it, such as the Octopus Community, which is a platform for information sharing and co-operation on cybercrime and electronic evidence, and the GLACY project on Global Action on Cybercrime, provide avenues for closer international co-operation in a world connected by global computer networks. The Cybercrime Programme Office of the Council of Europe in Bucharest is expanding its programmes to strengthen the criminal justice capacities of some 120 countries worldwide to investigate, prosecute and adjudicate offences involving electronic evidence.

In July 2018, the Cybercrime Convention Committee published a mapping study on cyber-violence. The study highlights amongst the challenges to the investigation and prosecution of cyber-violence, the fact that victims have no information on available remedies and receive limited help by law enforcement. It also notes that children might be better protected than adults because child exploitation statutes may be usable to cover cyber-violence against children. Further, it notes that Internet/social media platforms can play a role in cyber-violence. The study refers, *inter alia*, to a decision by the Regional Trial Court of Quezon City dated 29 May 2017, by which a 44-year-old man was sent to a lifetime in prison for multiple counts of human trafficking, cybercrime and rape. He hired the complainant to be his domestic helper at his residence. The man would wake up his housemaid early in the morning for a live sex show, where he would force her to have sex with him in front of a computer. Along with her sister and

six other children, the housemaid would also be taken to different hotels and forced to have sex with foreign clients. The court ordered the perpetrator to pay the victim a total of P1.8 million in exemplary and moral damages. However, the study stops short of making recommendations concerning the linkages between cybercrime and human trafficking.

The Council of Europe Group of Experts on Action against Human Trafficking, GRETA, which monitors the implementation of the CoE Anti-Trafficking Convention, has included in its country evaluation reports information on investigation of human trafficking offences committed through the Internet, including the possibility of blocking websites which are used to facilitate the recruitment of trafficking victims. Practically all countries monitored by GRETA have reported an increased use of the Internet and mobile phones for recruiting and/or controlling victims of trafficking. Despite the challenges of investigating online offences, there are examples from Norway, where the District Court in Bergen convicted in 2016 a Norwegian man of THB in the form of on-line abuse of children. The man had used recruiters in the Philippines to find vulnerable children who were instructed to engage in sexual acts with other children, which the offender watched in live-streaming.

At the same time, there are significant variations between countries as regards the national legislation in the area of telecommunications and the Internet, as well as the capacity detect and respond rapidly to computer-related crimes.

A CoE commissioned "Study on Blocking, Filtering and Take-down of Illegal Internet Content in the 47 Member States of the Council of Europe", prepared by the Swiss Institute of Comparative Law in 2016, established that there were, in general, two national regulatory models. The first model, applied in countries such as Germany, Austria, the Netherlands, Poland and Switzerland, relied on an existing legal framework that is not specific to the Internet to conduct limited blocking or takedown of unlawful online material. Some jurisdictions have chosen to combine approaches, maintaining a largely unregulated framework, but with legislative or political intervention in specific areas. In the UK and Albania, self-regulation has been adopted by the private sector to supplement the void left by the legislator's choice not to intervene in the area at stake. Other countries, such as the Netherlands and Germany, rely on the domestic courts to ensure that the necessary balance between freedom of expression, on the one hand, and safety of the Internet and the protection of other fundamental rights, on the other, is preserved to the greatest extent possible. The second group of countries (including Finland, France, Hungary, Portugal, the Russian Federation, Spain and Turkey) have adopted legislation specifically aimed at regulation of the internet and other digital media. Such legislation typically provides for the legal grounds on which blocking or removal may be warranted, the administrative or judicial authority which has competence to take appropriate action, and the procedures to be followed.

When it comes to the procedure, many of the States with legal rules targeted at the removal of Internet content provide for the urgent blocking of material related to child abuse, terrorism, criminality (in particular, hate crimes) and national security without the need for a court order. Administrative authorities, police authorities or public prosecutors are given specific powers to order Internet access providers to block access, usually within 24 hours. In other countries, such as Finland, hosting providers who have knowledge of illegal material may be expected to remove it voluntarily without judicial authority and to provide the content provider with due notice, which permits them to challenge the action through the courts.

2. Recent policy developments in the CoE

On 30 March 2016, the CoE Europe adopted the Internet Governance Strategy 2016-2019, which stresses that Internet companies play a critical role in dealing with online issues such as extremism and violence, abuse and intolerance, crime and insecurity, and calls for dialogue and co-operation with Internet companies and their representative associations. The strategy is a multi-disciplinary tool which covers issues concerning content, services and devices connected to the internet, including relevant aspects of its infrastructure and functioning which can affect human rights and fundamental freedoms. The CoE is currently working on a new Digital Governance Strategy 2020-2023, which is an opportunity to address the intersection between ICT and human trafficking.

The Council of Europe has been developing co-operation with the private sector in order to promote an open and safe Internet, where human rights, democracy, and the rule of law are respected in the online environment. Following multi-lateral consultations, the Council of Europe Secretary General signed an agreement (in the form of an exchange of letters) with representatives of leading technology firms and associations. It gives Internet companies a recognised status in the Council of Europe which, in turn, enables them to sit side-by-side with governments in the shaping of Internet policy. This means that they can participate in an array of intergovernmental activities and related work of the Council of Europe. The companies and associations include Apple, Deutsche Telekom, Facebook, Google, Microsoft, Orange, Computer & Communications Industry Association (CCIA), DIGITALEUROPE, the European Digital SME Alliance, the European Telecommunications Network Operators' Association (ETNO), GSMA and the Global Network Initiative (GNI). Additional agreements can be signed in the future.

Further, in 2018 the Committee of Ministers of the Council of Europe adopted Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries, which provides guidelines to member States when devising and implementing legislative frameworks relating to internet intermediaries, in line with relevant CoE conventions. Particularly relevant are the following obligations of States and responsibilities of Internet intermediaries:

> "1.3.8. In order to ensure that illegal content – as determined either by law or by a judicial authority or other independent administrative authority whose decisions are subject to judicial review – is effectively prevented from being accessed, States should co-operate closely with intermediaries to secure the restriction of such content in line with the principles of legality, necessity and proportionality. They should also take into account the fact that automated means, which may be used to identify illegal content, currently have a limited ability to assess context. Such restrictions should not prevent the legitimate use of identical or similar content in other contexts."
>
> "2.3.6. (content moderation) In cases where content is restricted by intermediaries in line with their own content-restriction policies because it contains an indication of a serious crime, restriction should be accompanied by adequate measures to ensure that evidence is retained for effective criminal law investigations. If intermediaries have specific knowledge of such restricted content, they should report this to a law-enforcement authority without undue delay."

3. Recommendations on developing policies addressing ICT facilitated or enabled human trafficking

The advantages of the use of ICT by traffickers – such as anonymity of users, risks of deletion of evidence, and use of different providers in different countries - create challenges for criminal justice in the cyberspace, but there are means to turn the liability into an asset.

At national level, the lack of appropriate legislation and State policies creates problems in prosecution and jurisdiction. At international level, other than the CoE Cybercrime Convention and the EU legislation on electronic communications and the responsibility of Internet service providers, there are no international instruments on the use of Internet or Internet-related crimes.

According to Europol, the rapid evolution of cyber threats has led to a situation in which certain conduct is criminalised in some countries, but not in others. An example is the live-streaming of child sexual abuse. Within the EU, there are countries where the act of live-streaming is not separately criminalised, while at the same time it cannot be captured under «possession». Similarly, wilful facilitation of the hosting of illicit content is not criminalized in a number of countries, effectively creating a safe haven for bulletproof hosters.

It is essential to harmonise legislation related to cyber-trafficking, such as on blocking, filtering and take-down of illegal internet content, including the possibility of withdrawal of data protection in the case of human trafficking investigations.

At the same time, there is lack of knowledge and experience amongst law enforcement officials, prosecutors and judges, and sometimes limited resources, to address cyber-trafficking. Capacity building on cybercrime and e-evidence - ranging from strengthening domestic legislation, training of judges, prosecutors and investigators, setting up of specialised institutions, and enabling cooperation at all levels - is a crucial part of the response to cyber-trafficking.

Regular monitoring and analysis of reported cases can help develop preventive action to alert potential victims and clients.

It is also necessary to make mutual legal assistance more efficient and to address the problem of evidence in the "cloud", that is, in foreign, multiple or unknown locations, and the related issues of jurisdiction and loss of knowledge of location. Concepts of jurisdiction are evolving, and increasingly the location of the person in possession or control of data is considered more relevant than the location of data.

It is also increasingly important for governments and companies to work together to respect and protect human rights and the rule of law on the Internet. Further steps should be taken to establish a framework for partnership with Internet companies on issues related to the exercise and enjoyment of human rights online.

At the same time, self-regulation is inefficient by itself, as there is little oversight over enforcement of self-commitments and insufficient predictability. The CoE is therefore increasingly calling for clear regulatory frameworks (particularly where law enforcement is

concerned), where States do not "oblige platforms to co-operate voluntarily", but set clear boundaries.

Finally, and on a positive note, I would like to mention a new method using bank data to identify human trafficking developed in the Netherlands, which is said to have "enormous potential". ABN Amro, the University of Amsterdam and the Inspectorate for Social Affairs and Employment have conducted a pilot to explore how abuses such as labour exploitation can be recognised from the financial data possessed by a bank, such as money transfers. In the initial pilot project, ABN Amro discovered and reported 'dozens' of unusual situations. In this new method the bank searches transactions in the computer system without any specific evidence, on the basis of an algorithm containing variables or indicators of labour exploitation. An example is a bank account in which the salary has been deposited and then immediately withdrawn in its entirety. The Dutch Financial Intelligence Unit analysed the transactions, described a number of them as suspicious and reported them to the investigations division of the Inspectorate of Social Affairs and Employment. From 1 March other Dutch banks were planning to take part in this project.