

The challenges of countering human trafficking in the digital era

Modern communication technologies – namely the internet, social media and mobile applications – have significantly impacted the way in which organised crime groups involved in international trafficking in human beings (THB) operate. Technology has **broadened criminals' ability** to traffic human beings for different types of exploitation (including sexual and labour exploitation, the removal of organs, illegal adoption of children and forced marriages).

The **advantages of technology** for traffickers include increased anonymity, the ability to take part in real-time yet encrypted communications, the possibility of reaching a broader audience (in terms of victims and clients), geographical mobility, and the ability to control victims from a distance. Criminals also capitalised on the boom of e-commerce culture and on legislative discrepancies in regulating and providing data. Today technology is exploited by traffickers during **every phase of sexual exploitation**, from the recruitment and advertisement of victims, to blackmailing them with photos and videos and controlling their movements. The financial management of the criminal business is also often done online.

Technology affords traffickers the ability to recruit victims without face-to-face interaction, thereby reducing the risk of being detected by law enforcement agencies. Social media platforms in particular are used as virtual catalogues by traffickers to identify new victims and develop grooming strategies, since a significant amount of information on the psychological and personal background of users (e.g. level of education, family ties, economic status, place of residence, network of friends, etc.) is frequently displayed (often with pictures included). Social media is also used as a **psychological weapon**, with traffickers threatening to upload compromising pictures of their victims if the latter fail to comply with their demands.

In terms of **targeted groups**, the majority of identified victims in THB cases which involved an online component were adult females being exploited in EU Member States. However, minors are also a particularly vulnerable target group due to their poor digital hygiene. Online grooming is particularly concerning, as a wealth of information on potentially vulnerable children is accessible on the internet, allowing offenders to socially engineer their tactics.

Traffickers are now able to shape their recruitment strategy based on the **online profiling** of their victims. Two different forms of online recruitment strategies can be identified in this context: active and passive recruitment. Active recruitment resembles the 'hook fishing' technique and involves criminals posting false job advertisements on trusted job portals and social media marketplaces. Criminal networks also set up full-fledged websites of fake employment agencies, often promoted on social media to make them easily accessible to a larger number of potential viewers. Sometimes these websites include live chats, ostensibly allowing immediate contact with the alleged hiring managers.

The internet also affords human traffickers opportunities for a more passive recruitment, which is far less detectable by law enforcement. Passive recruitment resembles 'net fishing' in that criminal recruiters scout the internet and social media and reply to announcements posted by job seekers looking for jobs abroad. After initiating a brief conversation, recruiters will request a fee from the victims in return for securing the job abroad and helping with travel arrangements. It is not until victims arrive in the new country that they discover the scam.

Importantly, modern technology means that human traffickers no longer need to be in close proximity to their victims in order to control them. Traditionally, **control**

over victims involved violence and physical restriction of movement. Today, control can be exerted via various forms of **blackmail** (e.g. by threatening to share photos and videos of sex acts online) as well as via virtual forms of **movement restriction** and real-time monitoring (e.g. GPS and built-in video cameras in smartphones, and location-sharing applications).

Much in the same way, victims are no longer required to have a fixed physical location, where they may be more easily identified by police. The internet allows clients to locate victims online and have them delivered directly to them. As a result, victims are often moved, between cities but also countries, as exploiters are able to transfer their activity simply by modifying the details in online ads. In addition, short-term stays in different countries enhance the feelings of confusion among victims and their dependency on exploiters, as well as making it more challenging for law enforcement to detect and safeguard victims.

Human traffickers are using increasingly modern communication technologies to exploit their victims multiple times over: from advertising and recruiting victims, to blackmailing them with photos and videos to control their movements. To counter this threat, we have to use the great advantage of shared intelligence and collect more digital evidence.

Catherine de Bolle - Europol Executive Director

Technology also acts as a force multiplier for trafficking activities as it enables the commercialisation and exploitation of victims on a massive scale. Victims are repeatedly exploited as criminals replicate the same advertisement and live-streaming in multiple platforms in order to maximise outreach and profits.

Technology has also served to lower the entry barrier for human traffickers: while historically, organised crime groups would have needed to exercise physical control and monopoly over specific city neighbourhoods and would generally consist of a large network of members, newcomers to THB can now efficiently manage an online business without the need for a physical criminal infrastructure and with a reduced workforce. As a result, a mastering of technology can make a criminal group more threatening yet less identifiable by law enforcement agencies.

However, while the procurement and delivery of sexual services has largely shifted to the online arena, the criminal proceeds are still predominantly collected in cash. A few, more technologically savvy criminal networks are using more innovative methods to conceal their earnings. These methods include digital wallets and Fintech, which offer virtual banking services and quick access to virtual currencies. To date, very few criminal networks have been found operating with cryptocurrencies. Nevertheless, the introduction into THB groups of 'crypto-profiles' such as traders, mixers, and exchangers, points to an emerging crime-as-a-service business model.

The use of modern technology has also influenced the traditional structure and division of tasks within trafficking networks. Female offenders have taken on central roles in the era of internet-enabled THB, particularly in trafficking networks involved in sexual exploitation. They are often victims themselves, sometimes in a romantic relationship with another member. In the majority of cases of THB for sexual exploitation reported to Europol, female suspects were in charge of the more essential roles. These included recruitment (e.g. posting enticing job advertisements); grooming the victims and presenting themselves as examples of success stories; receiving the victims upon arrival, and introducing the rules of the prostitution services to them; managing the victims' online advertisements and communicating with customers; administering the regular payments of subscription fees for the upload and maintenance of online advertisements; setting the tariffs for sexual services and keeping accounts of the victims' earnings; and transferring proceeds from the victims to the ring leaders.

In contrast, male members of the networks prefer to remain more distant, dealing with such tasks as the transportation of victims, moving the criminal earnings across countries, and money laundering. Nevertheless, despite the growing role of women in the exploitation process, the top tiers of the criminal network hierarchy are mainly made up of male associates.

Harnessing technology to prosecute criminals

Trafficking in human beings has transformed into a new business model, in which the online component is an essential part of criminals' modus operandi. However,

while on the one hand, technology offers criminals a virtual shield behind which they feel able to operate with near impunity; on the other, criminal moves online leave digital footprints and allow law enforcement to find leads.

Fighting human trafficking is one of the EU and Europol's top priorities. Europol has a team of experts fighting human trafficking at the disposal of our Member States and partners. We analyse criminal information and can connect the dots between national and international investigations.

Catherine de Bolle - Europol Executive Director

While there is still much to be developed in this field, investigators are finding ways to trace criminals' digital footprints for use in judicial proceedings. Investigators are able to discover information on identities, roles, structures, locations and criminal assets from the online activity of suspects. Another valuable source of digital evidence is the financial transactions made by criminal members to upload online advertisements.

A major challenge to law enforcement engaged in proactive THB investigations is the ability to spot exploitation signs among the magnitude of online advertisements. Reactive investigations are simpler, as they offer a starting point, such as the testimony of an identified victim and/or the account or webpage that was used for recruitment or exploitation purposes.

While law enforcement agencies are becoming more skilled in the use of digital technologies and forensics to combat THB crimes, the constant development of new technologies and change in business models used by traffickers keeps the race going between traffickers and law enforcement.

Law enforcement authorities dedicated to fighting human traffickers must be empowered to face these technological challenges. Empowerment needs to happen through an increase in capabilities, both in terms of technical knowledge and dedicated human resources, as well as through an improvement of the legislative tools that can support judicial proceedings and prosecution of traffickers.

The use of what social media and the internet can provide in terms of digital evidence is crucial, as victims of exploitation are particularly reticent due to the

psychological threats and blackmail they are subjected to and to the public shaming that can derive from the disclosure of their exploitation. Thus, an update of the current legal system should be implemented to allow the use of digital footprints in investigations and prosecutions, in terms of easier access to available datasets and faster responses.

Information and communication technology have rapidly changed the criminal landscape with traffickers adopting new modi operandi to recruit, control and exploit victims. To address these challenges, we need to increase capabilities of law enforcement ranging from data processing to decryption capabilities and develop a broad cooperation framework amongst authorities, internet companies and civil society fit for the digital era.

Olivier Onidi – European Commission – EU Anti-Trafficking Coordinator

Investment in equipment and training (including in terms of data privacy, ethics and informed consent) is key for the development of investigative tools. Furthermore, there is a need to amend the existing legislative and policy framework to promote information exchange and cooperation between law enforcement and the private sector (internet service providers and social media companies). In particular, policies are needed to raise awareness among online service providers and coerce them into implementing measures to ensure their platforms are not being abused.

There is also a clear need to develop international investigations as the perpetrators, victims and online platforms involved in the same THB case are often based in different countries. This geographical displacement generates additional challenges with regard to jurisdiction, evidence collection, extradition, and mutual legal assistance. Similarly, training needs for investigators should be addressed at international level, in order to ensure standardised approaches and transnational interoperability.

Last but not least, the COVID-19 pandemic – in which more time is spent online by the public at large – is likely to result in further advantages for traffickers: current victims risk remaining confined to the digital environment, with fewer chances of been detected by law enforcement, while vulnerable individuals (including minors) are increasingly exposed to the risk of being contacted and groomed by recruiters.

The prolonged closure of sex establishments has increased the vulnerability of those victims who were providing services in window prostitution, sex clubs, nightclubs, massage parlours, etc. Their services remain on offer but have largely gone under the radar, putting victims in a much weaker position.

An economic recession in the wake of the COVID-19 crisis could also result in dangerous consequences in the THB landscape. Criminals could have access to a wider pool of individuals in economic distress, and potentially increasingly prone to accept any kind of job opportunity. At the same time, an increased demand for cheap labour may work as a pull factor, provoking a potential rise in trafficking within the EU.

Finally, as the development of digital communication technologies continues, this area will continue to be important for the investigation and prosecution of human trafficking. The next few years will be critical in terms of identifying and agreeing on the legal and technical frameworks that can be implemented to act effectively against trafficking in human beings in the digital age.