



Part 2: Focus

The role of social media and the internet in human trafficking and smuggling

Social media and the internet are increasingly used by human traffickers and smugglers in their recruitment processes, for criminal purposes, but also for marketing their services and managing their criminal activities. At the same time, the internet and social media are also used to facilitate the fight against human trafficking and smuggling.

This focus will first give an overview of the phenomenon of the role of social media and the internet in human trafficking and smuggling, before examining how the internet and social media function as a method of investigation. We will also briefly address the new challenges facing policy, the police and the judiciary in this respect.

This section also includes contributions from external authors:

- The head of the internet investigation service of the Directorate for the fight against serious and organised crime of the Federal Police sheds light on his support role in investigations on the internet and social media;
- The Head of the UNHCR's 'Communicating with Communities' team makes a number of observations on the existing grey area between human trafficking and smuggling, based in particular on a study carried out by her department.

Introduction



This section analyses the use of the internet and social media in human trafficking and smuggling, at the various levels. The internet has permeated all facets of society over the last 10 years. In many countries, it has become an important part of the formal education system, meaning that children come into contact with it at a younger age. We live in a world which is in thrall to technology, which continues to evolve. This development brings with it a myriad of possibilities and opportunities. This is a positive development. In addition to its barrier-reducing effect on education, it provides people with numerous platforms for communicating and being part of groups that promote social cohesion. Unfortunately, digital media is also used for less wholesome purposes. Among other things, this medium facilitates human trafficking and smuggling. Social networking sites and classified websites are increasingly used by traffickers and smugglers in their recruitment process for criminal ends, and in trafficking and exploiting people. At the same time, the internet and social media, as a method of investigation, facilitate the fight against human trafficking and smuggling.

Internet and social media allow users to connect and communicate with individuals and reach a wider audience remotely. Human trafficking and smugglers are also able to reach and exploit a greater number of victims across national borders.¹¹ The internet also has a barrier-reducing effect.¹² The anonymity of the platform enables people to be whoever they want to be via a simple click of the mouse. Moreover, the internet makes it more difficult to establish the burden of proof of criminal offences.

As an introduction to this chapter, it is important to clarify certain concepts.

Digital human trafficking and smuggling falls under the category of cybercrime. Cybercrime is a very broad concept pertaining to unlawful acts committed using computers, computer networks, the internet and web-based information and communication technology.¹³ On 23 November 2001, the Council of Europe signed the Convention on Cybercrime, also referred to as the Budapest Convention. It was signed by 38 countries and encompasses the investigation and punishment of computer-related crime.¹⁴ This legislation covers computer fraud, hacking, and the possession and distribution of child pornography, etc. The countries that signed the Convention have a cooperation agreement to detect cybercrime, given that these offences are often cross-border in nature.

The term internet also includes the term **dark web**. The dark web literally refers to the dark side of the internet. It is an encrypted world of hidden and anonymous services or exchanges which are proposed or consumed, whereby users cannot be traced or identified. It is not a separate physical network, but a part of the World Wide Web. It is a part of the internet which cannot be indexed by search engines such as Google, Bing, Yahoo, etc.¹⁵ The dark web is a collection of networks and technologies which are used to share digital content. It is used for the sale of drugs, weapons and child pornography. The magistrates and policemen we interviewed have not seen much activity here on the part of traffickers, and this view is shared by the EU's Surf and Sound¹⁶ project, so we will not cover this phenomenon any further. However, for the sake of completeness, we refer to the European project Trace¹⁷ (Trafficking as a criminal enterprise) which refers to

11 M. LATONERO, *Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds*, 2011, p. 12. Consulted at <https://ssrn.com/abstract=2045851>.

12 D. MUIR, *Violence against Children in Cyberspace*, ECPAT International, 2005, pp. 25-29. Consulted at www.ecpat.net/ei/Publications/ICT/Cyberspace_ENG.pdf.

13 E. MCLAUGHLIN & J. MUNCIE, *The sage dictionary of criminology* (3rd ed.), London, United Kingdom: Sage, 2013, pp. 112-114.

14 Jura, België ratificeert Cybercrimeverdrag (Belgium ratifies the Convention on Cybercrime), 2012. Consulted at www.legalworld.be/legalworld/content.aspx?id=57284&LangType=2067.

15 P. BIDDLE, P. ENGLAND, M. PEINADO & B. WILLMAN, *The Darknet and the Future. Lecture Notes in Computer Science*, 2002, 155-176. Consulted at www.researchgate.net/profile/Reihaneh_Safavi-Naini/publication/221609583_Traitor_Tracing_for_Shortened_and_Corrupted_Fingerprints/links/5466dc1c0cf2f5eb18017b40.pdf.

16 www.surfandsound.eu, *Improving and sharing knowledge on the Internet role in the processes of human trafficking and smuggling*, ISEC 2013 Action Grants (HOME\2013\ISEC\AG\THB) \ 24 months (02.11.2014 - 01.11.2016), 2017.

17 http://data.trilateralresearch.com/wp-content/uploads/2015/11/TRACE-D4.1_Role-of-technologies-in-human-trafficking_FINAL.-1.pdf.

articles¹⁸ which identify websites trafficking in women within the dark web.¹⁹

Social networking sites are platforms and services that



allow users to build up a network or make connections. This can be done by sharing messages and content with fellow users. The use of social media has increased exponentially in recent years, both among young people and adults.²⁰ Online communities are created where people around the world can network with all kinds of organisations and individuals, for specific purposes. These sites are very popular due to the benefits they offer, such as the ability to make quick and easy contact. The downside of this system is the dissemination of false data, such as fake identities, online intimidation and stalking, etc.²¹

Finally, the source material for this focus is based on case analyses, informal interviews with magistrates and police officers, and literature reviews. It successively presents an overview of the role of social media and the internet in human trafficking and smuggling (Chapter 1), the internet and social media as a method of investigation (Chapter 2) and, finally, the new challenges for policy, police and the judiciary in this area (Chapter 3).

18 J. COX, "My Brief Encounter With a Dark Web 'Human Trafficking' Site", *Motherboard*, 27 July 2015.

<http://motherboard.vice.com/read/my-brief-encounter-with-a-dark-web-human-trafficking-site>; See e.g. GREENEMEIER, 2015; R. SIEGEL, *Investigators use New tool To Comb Deep Web For Human Traffickers*, nr special series, 6 July 2015; "The Dark Net and Human Trafficking: Is There a Connection?", *A21 Blog*, no date. www.a21.org/content/the-dark-net-and-human-trafficking-is-there-a-connection/gjdplv?permcode=gjdplv; "Human Trafficking on the Darknet", *Darknet Injustice* blog, 4 May 2015. <http://darknetinjustice.tumblr.com>.

19 Ulster University, *TRACE WP4 validation workshop on the role of technologies in human trafficking*, TRACE project, Tilburg, the Netherlands, 29 September 2015.

20 M. LATONERO, *op. cit.* p. 12.

21 A. ABHYANKAR, *Social Networking Sites*, SAMVAD, 0 (2), 2011, pp. 18-21. Consulted at www.sibm.edu/assets/pdf/samvad2.pdf#page=18.

Chapter 1

The phenomenon

In its 2016 Situation Report, Europol states: "The global development of online infrastructures has made the Internet a crucial tool for human traffickers, and it is likely to become more significant in the future. Online interaction facilitates several aspects of human trafficking and exploitation: targeting of potential victims; access to personal data; arrangement of logistics and transportation; recruitment through social media, chat forums and other websites; advertisement of victims; their exploitation and surveillance."²²

In this outline of the phenomenon, the first of such, we will only discuss the impact of the internet and social media on human trafficking and smuggling to a limited extent. We will mainly focus on the way in which human trafficking and smuggling networks use social media and the internet as a tool. Due to their different dynamics, we will address human trafficking and human smuggling separately.

The internet and social media are an efficient recruitment channel through which traffickers can reach their potential victims anonymously and on a larger scale.

1. THE ROLE OF SOCIAL MEDIA AND THE INTERNET IN HUMAN TRAFFICKING

Human traffickers use social media and the internet to recruit victims, market their prostitution services and manage their criminal activities.²³ At present, this is particularly true of sexual exploitation. We will also investigate how the victims deal with social media.

We find in the cases that the most important tools are Facebook, the chat forums of sex dating sites, Viber, Whatsapp, Skype, and other internet platforms.

1.1. | Recruitment by human trafficking networks

The internet and social media are an efficient recruitment channel through which human traffickers can reach their potential victims anonymously and on a larger scale.

Europol states: "The recruitment of victims increasingly takes place online. Traffickers lure victims with promising advertisements for jobs or travel placed on general advertisement sites or distributed through au pair agencies, international marriage agencies or dating sites".²⁴

²² EUROPOL, *Trafficking in human beings in the EU*, Situation report, The Hague, February 2016, Document Ref No: 7651, www.europol.europa.eu/publications-documents/trafficking-in-human-beings-in-eu.

²³ Report of the Meeting of the Informal EU Network of National Rapporteurs or Equivalent Mechanisms on Trafficking in Human Beings, 6-7 May 2014.

²⁴ EUROPOL, *Intelligence Notification 15/2014*, The Hague, October 2014: www.europol.europa.eu/publications-documents/trafficking-in-human-beings-and-internet.

In several cases in which Myria initiated civil proceedings, it was able to observe how victims are recruited via a job offer or prostitution work, or via the *lover boy* method. This can take place in the country of origin, a transit country or the destination country. It is usually done via Facebook or other internet platforms. According to some magistrates, Snapchat can also be used during the recruitment phase. In addition, a compromising screenshot is taken during a video conversation or chat or voluntarily supplied photographs are used as a means of blackmail.

1.1.1. | Jobs

In the past, many victims were recruited via a job offer, including vacancies for dancers, waitresses, hostesses, housekeepers, cleaning ladies, childminders or household help, etc. and were subsequently forced into prostitution. This is still the case, but social media and the internet are also being used for this purpose.

In its external contribution on human trafficking and the internet, the federal police wrote in our own 2010 annual report: "Recruitment for the purposes of sexual exploitation does not necessarily take place through sexually explicit websites, but rather through sites recruiting for jobs, through classified ads. Communication thus takes place, amongst others, through chat forums where it is possible to post messages and exchange information without knowing who is on the other side of the screen."²⁵

Internet

Bogus modelling agencies recruit victims through their websites. An ongoing judicial investigation has revealed that young girls, including minors, had reacted to so-called internet advertisements for modelling work in their countries of origin, and were ultimately forced into prostitution in Belgium. As a recruiter, the modelling agency in the country of origin was an important part of the international prostitution network that exploited its victims in Western European countries, including Belgium.

In an Antwerp-Latvian case²⁶ from 2010-2011, a bogus modelling agency recruited Belgian girls online, in addition to Latvian girls. The website stated (translation): "The most beautiful models in the Benelux for your catwalk fashion

shows and the promotion of your products. Our models are available for €200 per working hour for catwalk shows, photo shoots, hostess work, model presence, guidance tasks, etc.". Immediately after replying to the offer, and at their first interview, the girls were given a proposition to work as escorts with the promise to earn between €4,000 and €6,000 per month, for which they would have to work two days a week. A Belgian girl testified to the police: "I'm 18 years old and my friend 17, she's foreign and doesn't speak our language. I'm of Belgian origin. A few weeks ago, we met a man on the internet. He offered us a job as private escorts in the centre of Antwerp. After we met him, we began work immediately as escort girls. We want to stop as soon as possible but we can't stop or leave just like that. He threatens us in all sorts of ways, he blackmails us with photos of us naked or in underwear".

A Latvian victim in this case was contacted after placing her own internet advertisement looking for work. She said: "In Latvia I lived with my parents. I had studied, looked for work, and placed a job advertisement on the internet for work in the hotel and catering industry. I was contacted by the defendant X, the wife of the main defendant, who promised me work in a restaurant. A few days later she phoned, and apologised since I was not going to work in a restaurant but in an escort agency, as company. I only had to keep the customers company in a restaurant, theatre, etc., and did not have to provide sex services. This would earn me a few thousand euros per month. I agreed and left."

Facebook

Human traffickers also use Facebook to recruit their victims via job offers. In a Liège case²⁷ from 2012, a Belgian victim testified that she was approached via a fake Facebook profile for a job as hostess. One of the male defendants had created a fake profile for the recruitment of victims, in which he had pretended to be a woman with a fake profile picture. The man recruited young girls online or approached them on the street. He generally targeted young girls with no experience in the prostitution milieu, and recruited them based on their looks. In addition to this male recruiter, there was also a female defendant who was engaged in recruiting. She made the initial contact with the young girls via social media such as Facebook. They proposed a job for them in the events business or as an escort, in which they would earn a lot of money, and then referred the girls to the main defendant. During the first interview, he organised a photo shoot and manipulated the girls, until they were prepared to

²⁵ MYRIA, 2010 Annual Report on Human Trafficking and Smuggling, *Combating social fraud to prevent trafficking in human beings*, p. 128.

²⁶ MYRIA, 2015 Annual Report of Trafficking and Smuggling of Human beings, *Tightening the Links*, case study, pp. 69-71.

²⁷ MYRIA, 2015 Annual Report on Trafficking and Smuggling of Human Beings, *Tightening the Links*, p. 108.

have sex. In addition, the main defendant and his escort agency also ran an internet site through which he recruited victims, and immediately after the photo shoot for their first interview, subjected them to a 'test' for his website as a kind of selection procedure.

Economic exploitation

Human traffickers also use Facebook to recruit their victims via job offers.

Victims of economic exploitation can also be recruited via advertisements on the internet, but this can also be done via social media.²⁸ According to a HEUNI report²⁹, internet adverts, and to a certain extent Facebook, are increasingly taking the place of newspaper adverts, and applicants themselves are actively soliciting via the internet.³⁰ A study as part of a European project on the role of social media and the internet in human trafficking (Surf and Sound) refers to online advertisements in Romania for jobs in the hotel and catering industry by bogus companies, or in the agricultural sector in another EU country such as Spain, which result in exploitation.³¹

In Belgium, in a Bulgarian case³² from the transport sector, workers were lured to Belgium by advertisements in newspapers or on the internet, where they were supposed to work for a Bulgarian transport company. They were to earn a lot of money, but this promise was not kept.

In a Chinese case³³ from the hotel and catering sector, a Chinese victim responded to a Belgian internet advertisement from a company run by the Chinese main defendant. His Chinese contacts in Belgium had alerted him to this internet advertisement via Facebook.

In a case from a riding school³⁴, an illegally-resident Moroccan was hired as a stable hand after responding to an internet advertisement for this job in Belgium. The contact address for this internet advertisement was the email address of the main defendant.

In cases from the construction sector, victims were recruited as construction workers via internet advertisements. In a case from the construction sector involving bogus self-employment³⁵, the victims were recruited in Bulgaria and Bosnia. In a case from the construction sector involving posted workers³⁶, the Polish and Ukrainian victims were recruited in Poland, where the so-called construction company was active.

1.1.2. | Prostitution

Some young women also seek voluntary employment in the prostitution sector and may find themselves in a situation of exploitation. They contact the internet sites of escort agencies themselves or leave their telephone number on a Facebook address of a contact they know from the prostitution sector. They sometimes already have experience, but are looking for a better working area where they can earn more money.

Facebook

Social media can be a relevant tool for contacting young women with a proposal for prostitution work. According to Europol, women in chat rooms are also approached by traffickers.³⁷

In a Ghent case³⁸ from 2013-2014, a Hungarian victim explained how she was recruited in Hungary: "I got acquainted with a man called X. via Facebook, who I got to know as P. We wrote to each other several times. He learned from me that we were living in poverty. It was mentioned that I wanted to work as a prostitute. He told me that he could help, he would give me money for the trip, he would organise the work there. He told me that in Belgium, in Ghent, women need to stand in the window

28 EUROPOL, *Trafficking in human beings in the EU*, Situation report, The Hague, February 2016, Document Ref No: 7651, www.europol.europa.eu/publications-documents/trafficking-in-human-beings-in-eu.

29 HEUNI is the European regional institute within the network of the United Nations drugs and crime agency (UNODC). HEUNI operates under the auspices of the Finnish Ministry of Justice as an independent research and policy institute.

30 HEUNI, *Exploitation of migrant workers in Finland, Sweden, Estonia and Lithuania: Uncovering the links between recruitment, irregular employment practices and labour trafficking*, Natalia Ollus, Anniina Jokinen and Matti Joutsen (eds.), Helsinki 2013, www.cbss.org/wp-content/uploads/2012/11/HEUNI-report-75-15102013.pdf.

31 www.surfandsound.eu, *Improving and sharing knowledge on the Internet role in the processes of human trafficking and smuggling*, ISEC 2013 Action Grants (HOME\2013\ISEC\AG\THB) \ 24 months (02.11.2014 - 01.11.2016), Surf and Sound, National Report Romania, 2017. www.crpe.ro/en/wp-content/uploads/2017/04/Improving-and-sharing-knowledge-on-the-role-of-internet-in-the-human-trafficking-process-national-report-Romania.pdf.

32 2016 Annual Report Trafficking and Smuggling of Human Beings: *Beggars in the hands of traffickers* case study, pp. 110-111.

33 2016 Annual Report Trafficking and Smuggling of Human Beings: *Beggars in the hands of traffickers* pp. 158-159.

34 See also Part 3, Chapter 3 (case-law overview): Corr. Court Liege, subsection Liege, 21 November 2016, 18th chamber.

35 See also Part 3, Chapter 3 (case-law overview): Corr. Court Limburg, subsection Tongeren, 9 February 2017, 9th chamber.

36 See also Part 3, Chapter 3 (case-law overview): Corr. Court East Flanders, subsection Ghent, 1 February 2017, G29w chamber.

37 EUROPOL, *Intelligence Notification 15/2014*, The Hague, October 2014: www.europol.europa.eu/publications-documents/trafficking-in-human-beings-and-internet.

38 MYRIA, 2015 Annual Report on Trafficking and Smuggling of Human beings, *Tightening the Links*, case study, pp. 69-71.

and lure the men from the street inside, and prostitute themselves. Later investigation of the Facebook profiles revealed that the defendants created fake Facebook accounts using fictive identities, to recruit their victims. The defendants also used Facebook as a selection tool in the recruitment of victims. They placed the photos of the girls who agreed to their proposal on their Facebook profile and forwarded the photos to each other to compare them. The telephone tapping revealed that the suspects regularly consulted their Facebook page to view and rate the photographs of girls.

In a Brussels case³⁹, a Brazilian victim in Italy received a proposal via Facebook from a Portuguese defendant to work in prostitution in Belgium, on the basis of a so-called 50/50 profit distribution. She was photographed naked, and these photos were placed on a Brussels website for sex dates against her explicit will.

Facebook variant

In the Antwerp case (see above) young Latvian women were offered work in prostitution via a social networking site for sex contacts. Draugiem.lv is a Latvian version of Facebook in which interested women click on a friendship request message, and then respond positively. The main defendant had specifically called in a prostitute to approach the girls and convince them to work as escorts in Belgium and the Netherlands. She actively went looking for girls with a draugiem.lv profile and approached them with empty financial promises. In the end, they earned very little because their money was taken from them, and they were severely mistreated.

Dating sites

In Bulgaria, traffickers use the same techniques. In the previously-mentioned EU Surf and Sound project, various magistrates, police, human traffickers, victims and NGOs were questioned. In the Bulgarian country report, the authors refer to an interview with a Bulgarian human trafficker: "According to the interviewed person, now he recruits exclusively girls who independently engage in prostitution, and for this reason checks the dating sites where they could be frequently met: " We regularly follow the dating sites (Elmaz, Twoo, Gepime, etc.). I most frequently seek girls in Elmaz and Facebook I play it a man who needs companion and try to be cautious, but they disclose their selves alone that they seek sex for payment" [sic]. (Sex trafficker)".

The interviewed person shared that the girls recruited from the mentioned sites are used for exploitation and trafficking within the country, while the girls for international trafficking are recruited through Tinder, because those who have registered there speak at least two European languages, and the profits they bring, respectively, are double in comparison with profits made in the home country. Regardless whether Facebook or dating sites are used, in all cases the communication is made through private chats, and then transferred to applications like Skype or Viber, or directly to mobile phones.⁴⁰

1.1.3. | *Loverboys*

The *loverboy* technique focuses on the role of social media as a means of initial contact with the victims. Some internet sites can also play a useful role for *loverboys* in their recruitment.

Facebook

Loverboys make victims of both underage and adult women, but minors in particular are vulnerable prey on social media. Thanks to digitisation, a lot of information is available on Facebook. Minors can easily expose themselves to these websites and share their entire lives there. Using this information, human traffickers can target vulnerable girls. It is a form of social engineering in which traffickers adapt to the needs and wishes of the victim. The role of hobbies will play an important role in this respect. If the girl is a horse enthusiast, the *loverboy* will also present himself as a horse enthusiast. Using a search function on Facebook, for example, they can also specifically target victims from youth institutions. In a subsequent phase, they use mobile apps such as WhatsApp and Viber to make direct contact.⁴¹

39 Corr. Court Brussels, 22 September 2016, 47th chamber (not published).

40 www.surfandsound.eu, *Improving and sharing knowledge on the Internet role in the processes of human trafficking and smuggling*, ISEC 2013 Action Grants (HOME\2013\ISEC\AG\THB) \ 24 months (02.11.2014 - 01.11.2016), Surf and Sound, National report Bulgaria, 2017. www.csd.bg/artShow.php?id=17951.

41 www.surfandsound.eu, *Improving and sharing knowledge on the Internet role in the processes of human trafficking and smuggling*, ISEC 2013 Action Grants (HOME\2013\ISEC\AG\THB) \ 24 months (02.11.2014 - 01.11.2016), Surf and Sound, National Report Romania, 2017. www.crpe.ro/en/wp-content/uploads/2017/04/Improving-and-sharing-knowledge-on-the-role-of-internet-in-the-human-trafficking-process-national-report-Romania.pdf.

Minors in particular are vulnerable prey on social media.

In a Leuven prostitution case⁴², it was found that *loverboys* had made contact with their victims via Facebook in Romania, recruited them and then exploited them in Belgium. In an Antwerp case⁴³ of *loverboys* involving minors from youth institutions, the victims were recruited using Facebook in Belgium. When asked how she had gotten into prostitution, the minor replied during her questioning: "Through an ex-friend I met on Facebook. He put me on the online forum site for sex dates. He drove me to the customers". The *loverboy* also encouraged an underage victim to put some Facebook friends, also underage runaways, into contact with him via Facebook, whom he then sexually exploited.

Internet

Loverboys can also actively look for victims at modelling sites. These are popular websites for young girls who, on their own initiative, apply for modelling work. They must present themselves on the site and post a photo. Some girls think they are more likely to have a better chance by posting a more risqué picture. *Loverboys* target this group to try to seduce them.

Skype

Loverboys also use Skype to search for vulnerable potential victims at random. In concrete terms, a young person can get set up on Skype online with a certain saying or proverb. *Loverboys* respond to this by looking specifically for girls with certain sayings which show that they don't feel good about themselves and are vulnerable. He will then approach them and try to recruit them using the *loverboy* technique. Often the victim thinks that she has met her *loverboy* by chance on Skype.

In another Antwerp case⁴⁴ of *loverboys* involving minors from youth institutions, the victims were recruited using Skype, as well as Facebook. In this case, a 14-year-old girl who had fled from a youth institution explained that she had ended up with *loverboys* after getting to know one of them 'by chance' via Skype. They talked to each other

every day and she fell in love with him, she could not resist. One evening he came to visit her at a café in Verviers and then took her to Antwerp. In her testimony she spoke about the severe acts of violence that she subsequently had to endure.

Instagram

A study as part of the EU Trace project⁴⁵ (Trafficking as a criminal enterprise) on the internet, social media and human trafficking referred to a case in the US where a model was recruited by traffickers through Instagram. The newspaper reported the case under the title 'Florida model allegedly lured to New York on Instagram and forced to be sex slave'⁴⁶ as follows: "She was lured to New York with promises of cash and gifts, but a naive Florida model ended up a sex slave and pimped out to johns by a Brooklyn man who wooed her on Instagram. Cops said the Instagram picture she posted caught Attz's eye, and he began messaging her false promises that he would financially take care of her and her children if she came to New York. She accepted his invitation and \$150 in travel expenses to come north, sources said. The 23-year-old woman's pleasure trip to New York turned into a 12-day tour of hell, in which she was forced to turn tricks in hotel rooms under constant threats of death."

1.2. | Marketing by human trafficking networks

For their marketing activities, traffickers use websites to promote their prostitution services. These days, prostitution is primarily arranged via the internet and social media. Many women who prostitute themselves on display behind windows also prostitute themselves via the internet.

'Window prostitution' suffers from competition from the internet. Twenty years ago, clients had to go looking for prostitutes in newspaper adverts, or visit known red light districts. This is now arranged from behind a computer. It is possible to find all categories of prostitutes on the

42 MYRIA, 2015 Annual Report on Trafficking and Smuggling of Human Beings, *Tightening the Links*, case study, p. 29; 2013 Annual Report on Human Trafficking and Smuggling, *Building Bridges*, pp. 17, 60 and 108; Corr. Leuven, 4 July 2013, 17th k. (available at www.myria.be).

43 2016 Annual Report on Trafficking and Smuggling of Human Beings: *Beggars in the hands of traffickers* case-law overview, p. 134.

44 2016 Annual Report Trafficking and Smuggling of Human Beings: *Beggars in the hands of traffickers* p. 88.

45 Project ID: FP7-SEC-2-13-607669 http://data.trilateralresearch.com/wp-content/uploads/2015/11/TRACE_D4.1_Role-of-technologies-in-human-trafficking_FINAL_-1.pdf.

46 PARASCANDOLA, ROCCO, SANDOVAL, EDGAR, YANIV, OREN, HUTCHINSON, BILL, "Florida model allegedly lured to New York on Instagram and forced to be sex slave", *Daily News*, 16 July 2013. www.nydailynews.com/news/crime/cops-model-lurednyc-forced-hooker-article-1.1399559.

internet, at all prices. Higher-end escorts have individual websites, and do not work via 'sex-dating' websites. These escorts also target a specific kind of client from a certain milieu.

Websites

In the cases mentioned above, the traffickers advertised their victims with their photographs on the website of their escort agency. In the Antwerp modelling case, the defendant responsible for the victims' photo shoots also admitted that he had placed photos of an underage Latvian girl on the internet to advertise for his own escort agency.

In a Nigerian case⁴⁷, the Nigerian defendants worked together with the owners of a prostitution hotel. The Nigerian victim said: "From the research carried out by your services, it appears that there are photos of myself online on the website 'X'. You ask me who took these photos and who put them online? These photos were taken by the owner of the hotel and put online by her"

Thai massage parlours also advertise through their websites and the internet ads of the girls on them.⁴⁸

Online advertising sites

In a Ukrainian case⁴⁹, the victims were recruited and photographed by acquaintances as dancers or servants. Among other things, the exploiters put their sexually-tinged photos on an online advertising site in Brussels where, in addition to renting/rental of real estate, job offers, music lessons, babysitting, holidays, sales computers, etc., a special service for escorts is also offered to customers. The defendants found a USB flash drive with several pictures of victims of which several unidentified people still had to be placed online.⁵⁰ In addition, some of the victims were recruited as masseuses, and ended up on an escort site.

In a Liège escort case⁵¹, several Thai victims were recruited using a 'debt bondage' system and their photos were

placed on a similar online advertising site in Belgium. Two Romanian victims were also placed on similar sites, but also on escort sites.

Online forum sites for sex dating

In a *loverboy* case involving a rapper⁵² and the same Nigerian case, the defendants used online forums for sex dating, on which they advertised the details and photographs of the prostituted victim. One of the Nigerian defendants took erotic photographs of victims and created a personal profile on this site, for the victim's sex dates with clients. According to a Nigerian victim, the defendant sold it to her as follows: "Mama' also told me that she had a new system of work: she would put my photo on the internet, along with a mobile phone number, so that I could arrange my appointments myself". In addition to the Nigerian networks, *loverboys* also use these websites regularly to arrange sex dates with their victims and clients.

For their marketing activities, traffickers use websites to promote their prostitution services.

These are highly interactive internet sites with a wide market offering of sex adverts. Clients can make contact through Facebook, Twitter and email. There is an online forum where clients can leave comments on the prostitutes. At some sites, review forms are available showing rates, and the sexual services offered. Through Twitter, specific questions can be asked separately to prostitutes, and their individual reviews can be monitored.

1.3. | Managing human trafficking networks

"One of the most worrying aspects of human trafficking is its continuous modernisation, to the extent that it has become a veritable industry. Criminals are acquiring more and more know-how, and work ever more professionally. They carry out marketing activities for their 'products' and 'services', and make substantial use of the internet and other communication tools."⁵³

47 See also Part 3, Chapter 3 (case-law overview): Dutch-speaking Corr. Court Brussels, 28 March 2017, 60th Chamber (definitive).

48 See also Part 3, Chapter 3 (case-law overview): Corr. Court West Flanders, subsection Dendermonde, 11 October 2016, chamber. D19D; MYRIA, 2016 Annual Report Trafficking and Smuggling of Human Beings: *Beggars in the hands of traffickers* case-law overview, p. 156; Corr. Court Brussels, 46th Chamber, 27 January 2016.

49 See also Part 3, Chapter 3 (case-law overview): Corr. Court Brussels, 14 July 2016, holiday chamber.

50 See also Chapter 2 of this focus (investigation methods).

51 See also Part 3, Chapter 3 (case-law overview): Corr. Court Liege, subsection Liege, 16 November 2016, 19th chamber (appeal).

52 See also Part 3, Chapter 3 (case-law overview): Corr. Court Antwerp, subsection Antwerp, 21 September 2016, chamber AC8.

53 EUROPOL, *Trafficking in human beings in the EU*, Situation report, The Hague, February 2016, Document RefNo: 7651, www.europol.europa.eu/publications-documents/trafficking-in-human-beings-in-eu.

Logistics

In a Bulgarian case⁵⁴, it was already established a few years ago that an organisation in Germany used the internet to arrange logistics support for prostitution in Germany as subcontractors, and offered the necessary facilities for a fee, based on clear agreements. All the girls were posted on the internet via a website.

In a large-scale prostitution network⁵⁵ offering sexual services via erotic dating sites, the Belgian main defendant ran several websites from Spain as an 'agency' on which the services of the Moroccan, Romanian and Bulgarian girls were advertised. He recruited the girls through his internet platform. This was mostly in Belgium but also in Romania and Germany. When they were recruited, the girls were asked to create a new Facebook profile.

Confidential communication

Human traffickers realise that their phone can be tapped and prefer to conduct their confidential conversations via Viber, WhatsApp and Skype, etc., which are difficult for the police to wiretap. This was observed in a wiretapped conversation of an Albanian mafia case of sexual exploitation. Another technique is to use a single e-mail address for which the password is known by all participants, so that the messages that are drafted, but not sent, are read and deleted on the spot.

In the Hungarian case⁵⁶ of 2013-2014 in Ghent, the police found Facebook messages from the defendants about a number of girls who had been supplied by the defendant, and who were under his control.

Counter-espionage strategy

Human traffickers are starting to realise that the police can now also use Facebook as a tool for gathering evidence. In the Nigerian case, a defendant made this clear to another defendant during a telephone call: "Defendant X says that when someone logs in

on Facebook, the police can see it". In response, the defendants discussed their Facebook actions with each other: "Defendant X asks the main defendant whether

Y wrote on Facebook that he was staying in Belgium. The main defendant says she doesn't know, because she doesn't know anything about Facebook, but she thinks Y would have written that X is staying in London. X says that Y has denied chatting about this. The main defendant asks X if Y told him that Z had read it. X says that Y told her that Z deleted the Facebook page." As was the case for the phone tapping, the defendants had already developed a counter-espionage strategy: "X says, since he (Y) is the one who was contacted, he needs to change his Facebook and mobile phone number".

Threats and blackmail of victims

Europol states: "[Criminal organisations] use the internet to threaten or coerce victims of trafficking in human beings. The internet is used to blackmail victims, by threatening to send compromising pictures to their family or friends or to expose them online."⁵⁷

Especially in *loverboy* cases, and cases in which victims were recruited for a job as a model via photo shoots, the traffickers try to blackmail the victims with naked photographs to force them into prostitution. *Loverboys* sometimes use screenshots taken with Snapchat during the seduction process of the victims.

This is an even greater problem among children. In the Romanian report of the EU project Surf and Sound, a Romanian magistrate stated: "[The trafficker would approach] especially victims that were 11,12, 13 years old, who had little life experience, requesting that they take off their clothes and display pornographic poses. [...] Once the victims sent their first picture, they start being blackmailed. They don't tell their parents and that's where the child pornography really snowballs, through the minor's friends. (Prosecutor)".⁵⁸

Control of victims

As observed in a study of the EU Trace project⁵⁹ (Trafficking as a criminal enterprise), Europol⁶⁰ likewise observed:

54 MYRIA, 2011 Annual Report on Trafficking and Smuggling of Human beings, *The Money that matters*, p. 92.

55 See also Part 3, chapter 3 (case-law overview): Corr. Antwerp, subsection Antwerp, 2 May 2016, chamber AC4. and Antwerp, 24 November 2016, 14th chamber.

56 MYRIA, 2015 Annual Report on Trafficking and Smuggling in Human beings, *Tightening the Links*, case study, pp. 69-71.

57 EUROPOL, *Intelligence Notification 15/2014*, The Hague, October 2014; www.europol.europa.eu/publications-documents/trafficking-in-human-beings-and-internet.

58 www.surfandsound.eu, *Improving and sharing knowledge on the Internet role in the processes of human trafficking and smuggling*, ISEC 2013 Action Grants (HOME\2013\ISEC\AG\THB) \ 24 months (02.11.2014 - 01.11.2016), Surf and Sound, National Report Romania, 2017. www.crpe.ro/en/wp-content/uploads/2017/04/Improving-and-sharing-knowledge-on-the-role-of-internet-in-the-human-trafficking-process-national-report-Romania.pdf.

59 http://data.trilateralresearch.com/wp-content/uploads/2015/11/TRACE-D4.1_Role-of-technologies-in-human-trafficking_FINAL.-1.pdf.

60 EUROPOL, *Intelligence Notification 15/2014*, The Hague, October 2014; www.europol.europa.eu/publications-documents/trafficking-in-human-beings-and-internet.

Human traffickers realise that their phone can be wiretapped and prefer to conduct their confidential conversations via Viber, What's App and Skype.

"Online technologies also enable traffickers to more easily harbour and control victims. [Criminal organisations] maintain close surveillance of their victims, by imposing daily e-mail exchanges or chat sessions to prove their presence".

In one of the Antwerp cases⁶¹ involving minors from youth institutions, the victim made statements about her *loverboy* and how he always managed to find her: "I am afraid of that because he always finds me. I only knew him for two weeks. During those two weeks I ran away twice and each time he found me. He found me via Facebook".

1.4. | Victims and social media

How do victims deal with social media? We have observed that victims use social media to create a certain image for people back home. But social media and the internet can also be a tool to strengthen the resilience of victims.

Creating an image for people back home

A media report by Public Radio International (PRI),⁶² a global not-for-profit media company, revealed that Nigerian victims present an image of their lives which is much more wonderful than the reality. They conceal the fact that they have been raped en route and have ended up in prostitution after they arrive. They have a sense of pride and want to come across well to their friends, and certainly not as victims.

The article 'On Facebook, Nigerian victims of sex trafficking often present their life as far more glamorous than it is' tells the story of some of the victims we have summarized:

"Walking out of church one sunny Sicilian Sunday, Fortune puckers her lips, looks coyly into the camera and snaps a selfie. Like millennials everywhere, Fortune loves social media. She asks her friend to take a few quick pics, striking different poses. She's looking sharp in her matching skirt and suit jacket, red lipstick, and a sleek new blonde wig tied in a knot at the back of her head. She publishes the photo on Facebook, and likes the comments coming in from friends back in Nigeria. "Very fine", types one friend.

According to Fortune's Facebook profile, she is living in Europe — grateful, happy, and devout. "Most of them lie," concludes Peace, another Nigerian woman living in Palermo. To her, the Facebook posts of her Nigerian and African friends who live in Europe make it look like they are "enjoying" Europe, when often the exact opposite is true. "It's a living hell". Publicizing their traumas and problems to their friends back home would be useless. "They won't believe you," Peace explained, saying they might think you were lying, in order to keep all the goods of Europe to yourself.

Social control

The cases show that the Nigerian victims also maintained close contacts between themselves, and kept each other informed via Facebook, which could at least equate to a minimum level of protection. For example, a Nigerian victim in a case⁶³ was able to indicate to the police the place where another victim prostituted herself: 'Regarding X, I can tell you that she is currently also working as a prostitute in a club located in X. She uses the telephone number.... And she also has a Facebook profile. She is a contact of mine on my Facebook profile'. In a case involving the Albanian mafia, the defendants did not take any risks in this respect and forbade their victims from accessing Facebook. Based on a tapped phone call, the police concluded: "The defendant did not allow victim X to have Facebook, so she had to use her sister's Facebook profile". However, the victim found an alternative solution.

Nigerian victims use social media to portray their life as being much more wonderful than it is in reality to family and friends.

Facebook can also be a relevant instrument of social control, whereby the police can be alerted in urgent cases. In a Liège case involving a *loverboy* and adult Belgian victims, a neighbour informed the mother of a disabled victim via a Facebook message that her daughter had been beaten by two men and a woman.

Economic exploitation

Among the victims of economic exploitation, we have observed that they exchange their positive and negative work experiences with each other, for example through a Polish website (Etransport.pl), about companies from the transport sector, in order to inform and protect their compatriots from abuse.

61 MYRIA, 2016 Annual Report Trafficking and Smuggling of Human Beings: *Beggars in the hands of traffickers*, p. 154.

62 www.pri.org/stories/2017-05-19/facebook-nigerian-victims-sex-trafficking-often-present-their-life-far-more?utm_campaign=TheWorld&utm_source=Facebook&utm_medium=SocialFlow.

63 See also Part 3, Chapter 3 (case-law overview): Dutch-speaking Corr. Court Brussels, 28 March 2017, 60th Chamber (definitive).

2. HOW LOVERBOYS MANIPULATE THEIR VICTIMS WITH SOCIAL MEDIA

In this section we will go into more detail on the role of social media among *loverboys*, since this is currently an essential tool for *loverboy* victims, and especially Belgian victims, including many minors.

Various methods are used by human traffickers to manipulate victims. One of these is the *loverboy* method.⁶⁴ In such cases, the perpetrator will ensure that the victim becomes emotionally dependent, often using seduction. The victim is then exploited by human traffickers through coercion and violence.⁶⁵ The *loverboy* technique is a method of human trafficking, and not an isolated phenomenon.⁶⁶

In recent years, the *loverboy* problem has become more widespread. Instead of seducing their victims in public places frequented by many young people, the internet is increasingly used. Research shows that half of victims have been recruited via the internet.⁶⁷ The internet offers a wide range of opportunities for this kind of criminality. Firstly, the internet has a barrier-reducing effect.⁶⁸ The anonymity of the platform allows criminals to adopt a different identity. Perpetrators no longer have to move around physically, meaning that they can reach a larger number of targets in less time and at less cost. Distances become irrelevant. The internet has also made the whole process easier and faster. All of the victim's information is available on the internet, which enables perpetrators to pick up on the victim's personality more quickly. This means that the problem is not shifted,

Loverboys appear to use Facebook most often for starting relationships.

but rather it broadens out. This development has been facilitated by new technologies, including the internet and the social media associated with it. Generally speaking, use of the internet has increased the *loverboy* problem.

In principle, there has been no increase in *loverboys* since the development of the internet. The lack of comparable material means that it is not possible to measure any increase in the phenomenon. Despite the lack of data, many experts believe that the phenomenon has existed for a very long time, even though it has only recently come into the spotlight. A possible increase in the number of cases in recent years can be attributed to the fact that the phenomenon has been given more attention, and people can find the various organisations responsible for combating *loverboys* more easily. A possible change may also be due to trends in the country of origin, which is therefore dependent on time periods. Another possible explanation for an increase in the phenomenon can be attributed to cases which are qualified more precisely. In the past, *loverboy* cases often fell under vice cases rather than human trafficking.

Loverboys appear to use Facebook most often for starting relationships. This is because vulnerable young people who are prone to getting involved in dependency relationships with a *loverboy* have an open profile on this platform. In addition to the open profiles, these young people are often available 24/7 on Facebook, making them easy prey. In addition to the use of Facebook, Skype, Whatsapp, Viber and MSN are also used.

Loverboys usually work according to a three-phase pattern. The first is the grooming phase. This is followed by the habituation phase and finally the exploitation phase.

The grooming phase can be further divided into three stages. The literal meaning of grooming is 'taking care of, or preparing something or someone'.⁶⁹ In the scientific jargon, grooming is described as the process whereby an adult approaches a young person manipulatively and starts to prepare them for abuse, often of a sexual nature.⁷⁰ The internet has influenced individual grooming behaviour in various ways. The aim of traffickers remains

64 EUROPOL, *Trafficking in human beings in the EU*, Situation report, The Hague, February 2016, Document Ref No: 7651, www.europol.europa.eu/publications-documents/trafficking-in-human-beings-in-eu.

65 F. BOVENKERK & M. VAN SAN, "Loverboys in the Amsterdam Red Light District: A realist approach to the study of a moral panic", *Crime Media Culture*, 7(2), 2011, pp. 185-199.

66 R. VERWIJS, A. MEIN, M. GODERIE, C. HARREVELD & A. JANSMA, *Loverboys en hun slachtoffers* (Loverboys and their victims), 2011, p. 20. Consulted at www.verwey-jonker.nl.

67 V. ZANETTI, (2009), "De digitale loverboy", (The digital loverboy), *Proces*, 88 (5), p. 282.

68 D. MUIR, *Violence against Children in Cyberspace*, 2005, pp. 25-29, ECPAT International: www.ecpat.net/ei/Publications/ICT/Cyberspace_ENG.pdf.

69 L. STEVENS, "Grooming en cyberlokking strafbaar (Grooming and cyber-enticelement punishable. Uitbreiding van de strafrechtelijke bescherming van de seksuele integriteit van minderjarigen in cyberspace)" (Extension of criminal law protection of the sexual integrity of minors in cyberspace), *Rechtskundig weekblad*, (Legal Weekly Journal) 78(22), 2015, pp. 844-855.

70 CHILD FOCUS, *Slachtoffers van tienerpooiers in Vlaanderen* (Victims of teenage groomers in Flanders), 2016. Consulted at www.childfocus.be/sites/default/files/rapport_tienerpooiers_1.pdf; H.C. WHITTLE, C. HAMILTON-GIACHRITSIS, A.R. BEECH & G. COLLINGS, "A review of online grooming: Characteristics and concerns". *Aggression and Violent Behavior*, 18, 2013, pp. 62-70.

the same. However, traffickers use other techniques and media to achieve their goal. They see the internet as a safe environment where all forms of behaviour are acceptable and the likelihood of prosecution is low.⁷¹ The only difference between the online grooming phase and offline grooming is the space in which the grooming occurs.⁷² The internet has created a new dimension for grooming, namely the online dimension. The aim of grooming remains the same. The online grooming process can be divided into several phases which the groomer needs to progress through.

First and foremost, the perpetrator must create a profile. Here, a distinction can be made between two approaches. The first involves the perpetrator drawing up a very incomplete, screened profile with little or incorrect information. In the second approach, the perpetrator will portray himself as a 'gangster', hoping to catch the eye of their victim.⁷³ The second phase within the grooming phase is the recruitment phase, during which the perpetrator looks for his victim. He recruits his victim based on gender, age, place of residence, hobbies, educational level, etc.⁷⁴ The recruiting sites are primarily social networking sites, youth sites and chat boxes.⁷⁵ The *loverboy* can approach multiple youngsters at the same time much more easily. In the third phase, the perpetrator will select a potential victim. This is called hawking, in reference to a hawk circling around its prey. This recruiting method can be divided into the direct recruitment of potential victims, and the indirect recruitment. In the case of direct recruitment, the perpetrator will focus on one individual victim. In the case of indirect recruitment, this is done via social media. The perpetrator will then send as many messages as possible, in the hope that someone will take the bait. Once this phase is completed, the perpetrator will start to approach his victim.⁷⁶ This can be done directly or indirectly. The fifth phase of the grooming process involves moving in on the victim.⁷⁷ This process

goes much faster via the internet. This is because people often reveal more information on the internet than in the offline world.⁷⁸ During this phase, sites are used that facilitate communication with the victim. The perpetrator will intentionally gather compromising information about the potential victim, to subsequently use it for blackmailing purposes. During this phase, the perpetrator will put the idea of prostitution into the victim's head.

During the habituation phase, the perpetrator often uses the internet as a means of blackmail. In order to maintain control, the perpetrator will blackmail his victim by threatening to spread sensitive information.

The final phase is the exploitation phase. Here, the perpetrator will primarily use the internet as a means of advertising. He will mainly advertise on large-scale commercial sex advertisement websites.⁷⁹ These websites are a simple way for customers to organise a sex date cheaply, without much control. Victims can take any identity on these websites, which makes it very easy to advertise underage girls. The problem with these websites is that it is prohibited to advertise for prostitution in Belgium, meaning that any dates arranged via these sites are illegal. And if the judiciary were to enact a regulation in this respect, it could itself be accused of breaking the law. Subsequently, the internet is also used to keep a close eye on the victim. Research has shown that the vast majority of prostitution takes place online these days.⁸⁰

The internet is used as a means of blackmail, whereby threats are made to spread sensitive information.

71 J. DAVIDSON, "Internet Child Abuse: Understanding Offender Online Grooming Behaviour", in M. SEIFI (Editor), *Advances in the Analysis of Online Paedophile Activity*, pp. 39-55. Consulted at <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.167.8208&rep=rep1&type=pdf#page=39>.

72 CEOP, *Strategic Overview*, 2006, pp. 25-26. Consulted at www.ceop.gov.uk/pdfs/CEOPStrategicOverview2007.pdf; P. GOTTSCHALK, "A Dark Side of Computing and Information Sciences: Characteristics of Online Groomers", *Journal of Emerging Trends in Computing and Information Sciences*, 9, 2011, pp. 447-448. Consulted at www.cisjournal.org/journalofcomputing/archive/vol2no9/vol2no9_5.pdf.

73 V. ZANETTI, *op. cit.*, p. 286.

74 MOVISIE, (2009), *Meisjesprostitutie: feiten en cijfers* (Prostitution of girls: facts and figures), 2009, p. 6. Consulted at [www.movisie.nl/sites/default/files/alfresco_files/Factsheet%20meisjesprostitutie%20\[MOV-226011-0.5\].pdf](http://www.movisie.nl/sites/default/files/alfresco_files/Factsheet%20meisjesprostitutie%20[MOV-226011-0.5].pdf).

75 MYRIA, 2015 Annual Report on Trafficking and Smuggling of Human Beings, *Tightening the Links*, p. 28.

76 V. ZANETTI, *op. cit.*, p. 287.

77 MYRIA, 2015 Annual Report Human Trafficking and Smuggling, *Tightening the Links*, p. 28.

78 V. ZANETTI, *op. cit.*, p. 288.

79 *Ibid.*, p. 289.

80 M. FARLEY, K. FRANZBLAU, & A.M. KENNEDY, (2014), "Online Prostitution & Trafficking", *Albany Law Review*, 77(3), 2014, pp. 101-102. Consulted at <http://prostitutionresearch.com/wp-content/uploads/2014/09/FarleyFranzblauKennedyOnlineTrafficking-2014.pdf>.

3. THE ROLE OF SOCIAL MEDIA AND THE INTERNET IN HUMAN SMUGGLING

In 2016, the European Migration Network (EMN) investigated the role of social media in human smuggling.

Social media started playing a role in human smuggling around 2013-2014.⁸¹ The EMN report states: "The use of social media in migrant smuggling has witnessed an exponential growth in recent years. Smugglers use social media to: advertise smuggling services; to provide information on migration routes; as well as to facilitate communication. The increasing use of social media can be explained by the fact that it is less costly, safer to use for both the migrant and their smugglers (anonymity/ encryption), whilst more effective in increasing visibility and reaching a wider group of migrants".⁸²

The EMN launched a survey in the EU Member States using a questionnaire. This revealed that 11 EU countries were confronted with this problem.⁸³

3.1. | The smuggling market

In 2016, Europol traced 17,000 smugglers who used Facebook for their smuggling activities into the EU.

In 2016, there was a huge increase in the use of social media by smuggling networks. In 2016, Europol traced 17,000 smugglers

who used Facebook for their smuggling activities into the EU.⁸⁴ In addition, in the same year, Europol was able to trace more than 2,500 counterfeit travel documents on social media.⁸⁵

One smuggler stated to the BBC that between 10 and 20 people are smuggled daily, through his Facebook account.⁸⁶ He had not used social media before 2012. At the time of publication of the BBC article (13/05/2015), Facebook already accounted for between 30% and 40% of his smuggling business.

Advertisement

In its first annual report, Europol's European Migrant Smuggling Centre (EMSC)⁸⁷ stated: "In 2016, the migrant smuggling content in social media facilitated illegal migration and associated content became not only increasingly visible in the online environment, but also significantly increased in quantity and complexity. In 2016, 1150 suspect social media accounts were communicated to the EMSC. This reflects an 87% increase when compared to approximately 148 such accounts in 2015. The social media platform of choice for smugglers remains Facebook; however a very slight movement towards other service providers, such as Telegram, was detected". Frontex also noted that smugglers were very quick and flexible in their handling of social media: "I might have more than 40 to 50 Facebook accounts. I activated them as needed, and when my passengers arrived at their destination, I deactivated them".⁸⁸

Smugglers also use Facebook to advertise their services, including the cost, type of transport, success rate, and, in some cases, information on asylum policies or family reunification processes across the EU, says the International Centre for Migration Policy Development (ICMPD).⁸⁹

81 <https://emnbelgium.be/news/experts-migrant-smuggling-gather-be-emn-ncp-roundtable?q=/news/experts-migrant-s>.

82 European Migrant Network (EMN) Inform, *The Use of Social Media in the Fight Against Migrant Smuggling*, September 2016.

83 Summary of EMN Ad-Hoc Query No. 1055 from 18 April 2016, *Addressing and preventing the use of social media in migrant smuggling*: "Eleven (Member) States (BE, CZ, ES, FI, HU, LT, NL, NO, PL, SK, UK) have confirmed that social media is used to advertise smuggling services, provide information on migration routes and communicate with smugglers using applications such as WhatsApp or Viber. For example Facebook is used to provide information on specific trips (travel packages including price), contact details, live blogs on the progress of other clients across the sea as well as for sharing of stories to tackle safety concerns of potential clients".

84 Europol, *Migrant Smuggling in Europe*, February 2016; www.express.co.uk/news/world/771957/smugglers-mediterranean-traffickers-facebook-europol-report.

85 L. TAYLOR and V. CARDI, *The Smuggling Game Playing with life and death to reach Europe*, 28 March 2017: <http://news.trust.org/shorthand/the-smuggling-game>.

86 D. ADAMSON and M. AKBIEB, *The Facebook smugglers selling the dream of Europe*, BBC World Service, 13 May 2015: www.bbc.com/news/magazine-32707346.

87 European Migrant Smuggling Centre, *Activity Report: First Year*, January 2016 - January 2017, Europol.

88 <http://frontex.europa.eu/pressroom/hot-topics/profitting-from-misery-how-smugglers-bring-people-to-europe-aUY2f>.

89 FRONTEx, *Profiting From Misery - How Smugglers Bring People To Europe*, 18 February 2016 <http://news.trust.org/shorthand/the-smuggling-game>.

The UNHCR has examined the role of social media in smuggling from the perspective of migrants.⁹⁰ It found a whole range of offers on social media tailored to various migrant groups.

For Afghans who receive a total package for a smuggling route from Afghanistan to the destination country via a so-called travel agent (see below): "Smuggling networks are not only responsible for transport, they also arrange the necessary documents. On Facebook, there are always numerous offers, with details of the sellers' contact details. Sometimes potential customers even get information about the expected waiting times and price. Counterfeit visas are also continually for sale. In addition, there are also short-term offers for genuine visas from various embassies/consulates. These include visas for the 'Schengen' area or specific EU Member States, but also for Turkey, Ukraine, Canada and the USA. In some cases, the offers also include details on the type of visa, such as a tourist or student visa, but sometimes bizarre details such as "marriage visas", "visas and place of residence", "investment visas" or "visas to buy property".⁹¹

Arabic speakers, including Syrians and possibly Iraqis, are suspicious of smugglers and try to organise their own journeys in stages, and only contact smugglers in the event of a difficult illicit trafficking route. "Smuggling proposals on Facebook now include illegal international land, air or sea transportation, embassy staff being bribed to deliver visas, passports being stolen in one country to be stolen in another".⁹²

During its survey of EU countries, the EMN also found comments on Facebook advertisements with an offer of sham marriages.⁹³

Public Relations

Various smugglers recruit their customers through word-of-mouth advertising. For them, this is still the most important way to reach migrants. They use Facebook to take care of their public relations, with promotional films for their smuggling trips.

The newspaper *De Morgen* interviewed a smuggler on this subject: (translation) "He claimed to use Facebook as a means of reinforcing his image, so that migrants who had been given his name by others could see that he was the real deal. His Facebook account contains videos of refugees who have arrived at Lesbos in dinghies. They raise their thumbs: 'Let's hear it for X (name of smuggler)!', the migrants call out, relieved that they have made it to the other side".⁹⁴ The UNHCR report also found promotional material from smugglers from the time when they were in a negative light due to the many people who were drowning.⁹⁵

Facebook user groups

Facebook contains various Arabic-speaking user groups for human smuggling". According to the UNHCR report, Syrian and Iraqi migrants are more likely to make use of this for a certain part of their planned smuggling journey.

The role of these Facebook user groups was also covered in the smuggling cases. Analysis of a smuggling case⁹⁶ showed that a Kurdish-Palestinian smuggling network used Facebook to further develop its international network with potential smuggling customers. At the start of its investigation, the police noted in an official report that a Facebook group had been set up for this purpose: "We have also learned that there are various Arabic-speaking user groups on the social media website Facebook. These are intended to bring people who want to come to Europe without having valid documents in contact with each other and people smugglers. People can ask questions within these user groups about the situation in European countries and cities. The aim is to gather information to reach these areas. People also ask for contact details of people who can help them in this regard. These contact details are then sent to the person asking the questions via private messages. Other users are also sometimes informed if the crossing to the UK was successful. We obtain the names of some of these user groups. We add these to the appendix of this official report".

90 UNHCR, *From A Refugee Perspective, Discourse of Arabic speaking and Afghan refugees and migrants on social media from March to December 2016*, April 2017: www.unhcr.org/uk/5909af4d4.pdf. See also the external contribution by M. SUNJIC, "Refugees: when human smuggling becomes human trafficking".

91 *Ibid.*

92 *Ibid.*

93 Summary of EMN Ad-Hoc Query No. 1055 from 18 April 2016, *Addressing and preventing the use of social media in migrant smuggling*: "Other similar activities on social media include advertisements of sham marriages. For example Poland explained that they detected advertisements of such services being provided in the UK in exchange for GBP 6,000".

94 *De Morgen*, 7 November 2015.

95 "Criticism of the dangers of illegal migration on Facebook pages poses a threat to the smuggling business and smugglers react in various ways. When more and more Facebook users started to point out the dangers of the sea crossing, smugglers put beautiful photos of yachts and luxury cruise liners online, to make potential customers believe that this was the kind of ships they were using. In addition, images about safety and persons brought to Europe on the wings of angels also appeared".

96 MYRIA, 2016 Annual Report on Trafficking and Smuggling of Human Beings: *Beggars in the hands of traffickers* pp. 113-114.

Various specific Facebook user groups linking migrants to smugglers have been listed in several study reports⁹⁷: "Smuggling Into the EU", "How to Emigrate to Europe", "Smuggling from Turkey to Europe", "Immigration and Travel to Europe", "Wishing to immigrate to Europe through Libya". Migrants can compare smuggling routes, destination countries and cost prices.

Fake passports can be bought here.⁹⁸ In addition, smugglers also use success stories to promote themselves⁹⁹ and respond to migrants' fears of drowning.¹⁰⁰

Maps with routes via WhatsApp

In Whatsapp, there are chat groups for migrants who wish to travel autonomously as much as possible and who seek contact with smugglers for certain difficult routes. They exchange maps showing routes, major cities, border areas, means of transport, prices and the contact points of smugglers. These maps were discussed in an EU project from 2016-2018 that examines the role of social media among migrants.¹⁰¹

Travel agencies

Travel agencies play a key role in human smuggling through internet advertising. Using pleasant photographs on Instagram, smugglers offer smuggling trips to Western European cities via travel agencies. They promote these using attractive photographs of the cities, and photographs



Facebook group of smugglers

of the necessary false identity documents. Facebook is also used to distribute advertisements, as Frontex identified.¹⁰² Moreover, according to Europol, some of these Facebook accounts look similar to those with the offers from normal travel agencies.¹⁰³ In Thailand, such travel agencies with internet ads are engaged in human smuggling, as well as trafficking.¹⁰⁴

The UNHCR report found many advertisements in Afghanistan from so-called travel agencies dealing in human smuggling.¹⁰⁵

Human smuggling is highly ingrained in Afghan society. This has already been observed in the case study of an Afghan smuggling network.¹⁰⁶ Human smugglers are seen as travel agents there, and they enjoy great prestige. Afghan migrants therefore place their full trust in these smugglers to organise their journey.

97 Danish Refugee Council, *Getting to Europe the 'WhatsApp' way*, June 2016. http://reliefweb.int/sites/reliefweb.int/files/resources/RMMS%20Briefing%20paper%202_Social%20Media%20in%20Mixed%20MigrationUPLOAD.pdf.

98 *Ibid.*: "Smugglers also use social media to offer specific services such as fake passports and other identity documents. The so-called Facebook page in Arabic: 'Issuing and renewing passports, driving licences and educational diplomas' helps Syrians who want to obtain such documents".

99 *Ibid.*: "The 'Asylum and migration to pan-Europe' Facebook group listed below has 23,810 members. There is a testimonial from someone who managed to reach Sweden, and after these comments, smuggler W. posted his number on Viber and WhatsApp to others who may want to use his services.

100 *Smugglers, Migrants connect using Facebook*, The Toronto Star, 10 July 2015: "The smugglers writing in Arabic mention phone numbers, rates, details about routes and means of transport, and even provide their Facebook page walls with a: 'book now' button. In an attempt to dispel the fear of migrants drowning at sea, a Facebook page of smugglers has added the term 'safe travel' to the title, while another page has added the word 'smuggling' and openly mentions the size of the boats and smuggling costs".

101 The Open University and France Médias Monde, 2016. *Mapping Refugee Media Journeys: Smartphone and Social Media Networks*. www.open.ac.uk/research/main/sites/www.open.ac.uk/research/main/files/files/ecms/web-content/Mapping-Refugee-Media-Journeys-16-May-final-V1.pdf. "The maps show in great detail the specific transport options between locations and their cost, the optimal routes and border crossings. Information can also be found about specific cities and places where smugglers or drivers offer their services. Its highly detailed nature indicates a very well-organised partnership".

102 <http://frontex.europa.eu/pressroom/hot-topics/profitting-from-misery-how-smugglers-bring-people-to-europe-aUY92f>: "Some Facebook pages also offer false travel documents for sale and sell themselves as travel agencies which are generally based in Turkey".

103 De Morgen, 7 November 2015.

104 See above point 1 of this focus (the role of social media and the internet in human trafficking) and below, Part 3, Chapter 3 (case-law overview).

105 UNHCR, *From A Refugee Perspective, Discourse of Arabic speaking and Afghan refugees and migrants on social media from March to December 2016*, April 2017. www.unhcr.org/uk/5909af4d4.pdf: "Afghans practically always book all-inclusive trips from country of origin to destination. Among Dari speakers, there are both direct contacts and advertisements on social media. Often travel agencies will operate legitimate as well as illegal businesses. Afghan smugglers sell the 'European Dream' with enticing pictures and promises of a good and safe life.

106 MYRIA, 2015 Annual Report on Trafficking and Smuggling of Human Beings, *Tightening the Links*, case study, p. 82.

The smugglers also use the same marketing strategies as a travel agency. This was identified in an EU project from 2016-2018 that examines the role of social media among migrants.¹⁰⁷

Communication between smuggler and customer

Smugglers mainly communicate with their customers through social media. They operate under a pseudonym. This communication is an extra dimension, especially in the Syrian and Iraqi smuggling cases. According to the UNHCR report, this communication with Syrian and Iraqi migrants is not just to make contact. It is veritable negotiation between smuggler and customer, since these migrants have little trust in smugglers.¹⁰⁸

As observed in numerous cases, smugglers prefer to communicate via Viber, Skype, WhatsApp and Facebook because they realise that their mobile phone can be wiretapped by the police.

In a Syrian smuggling case, the police were able to read the chat conversations from a smuggler's iPhone. This showed that the smuggler in question had communicated with 769 customers via Viber, WhatsApp and Skype. There was also talk of communication via Facebook, but the police had no details in this respect.

In a Kurdish smuggling case¹⁰⁹ the smugglers communicated with their customers via Viber. In a tapped telephone call from a smuggler, customers were referred to Viber: "At 14:17, the smuggler (796) calls the user of the Iraqi phone number 788. He asks after a boy (unknown) who, according to 788, was staying in Bulgaria. The user of 788 was going to send the smuggler's (796) number to the boy so that he could call him. The smuggler explains that he also has a few other numbers and that he will send them all by Viber". A smuggled person who had successfully arrived in the UK reported this to the smuggler

by telephone and was promptly advised to use Viber for this communication.

In another Kurdish smuggling case¹¹⁰, the smugglers were explicitly instructed by their leader to contact the smuggling customers via Viber. The police were able to trace the chat messages between the smugglers and their Iranian customers, which contained the locations of the appointments (hotels in Brussels).

In a Ukrainian smuggling case¹¹¹, the smugglers used various Skype profiles with which they forwarded the smuggled people to Viber: "Hello! How is it going? Will there be something today? How is it with a package for the chicken house (note: safehouse where the smuggled persons are located)? Answer: Hello. There is a boy from Spain. He is arriving. This boy has not called yet. There is no one yet. Add him via Viber. He will be in Brussels this morning".

Using pretty photographs on Instagram, smugglers offer smuggling trips to Western European cities, through travel agencies.

3.2. | Managing smuggling networks

Social media have a strong impact on the dynamics of human smuggling. The EMN concluded: "The use of social media has a significant impact on irregular migration. It helps migrants congregate, producing faster dynamics at the external borders, and, it has also increased the capacity of smugglers to change smuggling routes in response to security situations or law enforcement operations".¹¹² At the same time, they can better protect their smuggling activities through social media. Frontex came to the same conclusion.¹¹³

We have found in the cases that smugglers use the social media in various facets for their confidential conversations to manage their smuggling business internally. This

107 The Open University and France Médias Monde, 2016. *Mapping Refugee Media Journeys: Smartphone and Social Media Networks*. www.open.ac.uk/research/main/sites/www.open.ac.uk.research.main/files/files/ecms/web-content/Mapping-Refugee-Media-Journeys-16-May-final-V1.pdf. "This is why smugglers often use new technologies for marketing purposes, just as travel agencies do. Or, as one of the MEDMIG surveys put it: "In order to win our trust [the smuggler] gave us the telephone numbers of all the people who would travel with us".

108 UNHCR, *From A Refugee Perspective, Discourse of Arabic speaking and Afghan refugees and migrants on social media from March to December 2016*, April 2017. www.unhcr.org/uk/5909af4d4.pdf. "Potential clients ask each other on social media about ways to get to Europe or certain countries. Smugglers monitor Facebook conversations and post their offers. Negotiations are done via private channels (Viber, Imo, WhatsApp,...).

109 MYRIA, 2016 Annual Report on Trafficking and Smuggling of Human Beings: *Beggars in the hands of traffickers* case studies p. 119.

110 See also Part 3, Chapter 2, point 2, (human smuggling case studies).

111 See also Part 3, Chapter 3 (case-law overview): Corr. Court East Flanders, subsection Ghent, 10 January 2017, G28bis chamber.

112 EMN Inform, *The Use of Social Media in the Fight Against Migrant Smuggling*, September 2016.

113 <http://frontex.europa.eu/pressroom/hot-topics/profitting-from-misery-how-smugglers-bring-people-to-europe-aUY2f>: "Persons who advertise their services on social media are aware of the risks and are active on various social media platforms. They usually use Facebook, WhatsApp and Viber to discuss the financial details and logistics of smuggling operations".

relates to the various facilitating aspects of social media: financial management, customer management, internal organisation management, the smuggling network and counter-strategy.

Financial management and discussions

The cases show that human smugglers prefer to conduct their financial conversations via social media. Delicate subjects such as financial discussions could not be discussed over the phone.

By tapping the telephone conversation of a smuggler in a Kurdish case¹¹⁴, the police found that the smugglers agreed by telephone to discuss these matters via Skype or Viber: "Smuggler X reproaches smuggler Y that he is holding back money from 3, which was sent on Thursday 04.12. Smuggler Y is currently in the Netherlands and doesn't want to discuss it over the phone, but over the internet".

Human smugglers prefer to conduct their financial conversations via social media.

The smugglers used Facebook to arrange and manage the payments. In a Kurdish smuggling case¹¹⁵, in connection with a customer's payment, a smuggler referred to an unknown account number during a telephone call for the settlement of his payment, which then had to be reported via Facebook. In the same smuggling case, text messages containing transaction codes of money remittances via money remittance services such as Moneygram, Western Union etc., names and bank details were found when a smuggler's Facebook messages were read.

In another Kurdish smuggling case¹¹⁶, payments from the smugglers within the network were settled via Viber: "On Saturday 24 January 2015 at 11:47, the user of 796 (smuggler) calls the person looking after finances in the Netherlands and explains that he sent her a name the day before. The woman (779) explains that she hasn't received anything. The smuggler tells her that he will send the name by Viber. The person looking after the finances most likely has to pay the smuggler. At 11.56am. the user of 796 will again send the same message with the name of the person involved to the financier in the Netherlands".

According to the UNHCR report¹¹⁷, more than one hundred Afghan freelance bankers are active on Facebook who arrange financial transfers between the smuggler and the customer. The UNHCR found evidence on social media of such contacts in the UK, Hungary, Austria, Germany and Ireland.

Confidential discussions about customer management

Smugglers prefer social media to communicate about their customer management. There are clear examples of this in the cases.

In a Ukrainian smuggling case¹¹⁸, they deliberately switched from a mobile phone conversation to Skype when customers were mentioned: "Smuggler Z. calls smuggler S. and explains the situation. He still has 12 or 13 'candidates' to move. Further communication via Skype'. The police found relevant Skype and Viber messages in a smuggler's smartphone where locations (mainly car parks along motorways) and addresses of safehouses were passed on, as well as a communication about a person arriving from Spain.

In an Iraqi smuggling case in Dendermonde¹¹⁹, a smuggler A. from Belgium had privileged contacts with a Syrian smuggler in London who was known as a supplier of Syrians. These two smugglers were friends via Facebook. Smuggler A. stated during his questioning that all his communications with the Syrian smuggler from London had to go through Viber and Facebook. In a related smuggling case in Brussels¹²⁰, the same Syrian smuggler from London maintained contacts with another smuggler via Skype.

Confidential discussions on internal organisation and cooperation

Smuggling networks arranged their operations via social media. In a Ukrainian smuggling case¹²¹, smugglers arranged their operational smuggling management via Skype. The police analysed the Skype messages of the smugglers and concluded: "We note that in the communication (Skype) between X, Y and Z relatively structured messages are made that can be considered

114 MYRIA, 2016 Annual Report on Trafficking and Smuggling of Human Beings: *Beggars in the hands of traffickers* case study p. 121.

115 See also Part 3, Chapter 2, point 2, (human smuggling case studies).

116 MYRIA, 2016 Annual Report on Trafficking and Smuggling of Human Beings: *Beggars in the hands of traffickers* case studies p. 122.

117 UNHCR, *From A Refugee Perspective, Discourse of Arabic speaking and Afghan refugees and migrants on social media from March to December 2016*, April 2017: www.unhcr.org/uk/5909af4d4.pdf.

118 See also Part 3, Chapter 3 (case-law overview): Corr. Court East Flanders, subsection Ghent, 10 January 2017, G28bis chamber.

119 See also Part 3, Chapter 2, point 2, (human smuggling case studies).

120 Corr. Court Brussels, 13 October 2016, 60th chamber (not published).

121 See also Part 3, Chapter 3 (case-law overview): Corr. Court East Flanders, subsection Ghent, 10 January 2017, G28bis chamber.

relevant for the investigation. The communication mainly covers the following two subjects: a) the forwarding of Polish telephone numbers with an additional amount in euro and a time. These include, with a probability bordering on certainty, numbers of drivers who take "candidates" across the Franco-British border, the amount to be paid to them and the time at which they have to contact the man; b) transfer of Polish names, dates of birth and alphanumeric data from Polish identity cards that are checked for their usefulness (whether or not sealed). These communications transfer data from Polish identity cards which are then returned with or without an OK. The modus operandi shows that [the] organisation uses Polish identity cards bought from their owners".

The smugglers make contact with other smugglers from the countries of origin via social media. In an Afghan smuggling case¹²², the smugglers started talking by telephone about a new Afghan smuggler they wanted to contact. They agreed to continue their conversation later with the help of video chat: "557 asks if 166 has been to Afghanistan. 166 says that he has been in Afghanistan for 51 days and that people smugglers are now asking 17,000 dollars to send people here. 557 asks if he can forward that person's number. 166 says that there is a girl in Kabul doing the work. 557 asks for her number and says that he wants to talk to her. 166 says that she does it in 25 days and then says that he will soon talk to 557 via video chat. The number is (...) and then he says that he will send that number again via Facebook, just to be sure".

In an Albanian smuggling case¹²³, the smugglers exchanged their Skype addresses and directly discussed their smuggling operations and problems through Skype. The police were only aware of this because the smugglers referred to it during their mobile phone conversations.

Counter-espionage strategy

According to the EU countries' survey, the EMN concludes: "Investigations have discovered that smugglers express a preference for communicating over the internet rather than phone. This way of working is more anonymous and reduces the risks of police intervention, while at the same time allowing smugglers to expand their activities."¹²⁴

The smuggling leaders give clear guidelines to communicate not by telephone but by social media. In

an Afghan smuggling case¹²⁵, the smugglers alerted each other to the fact that their phones were being tapped by the police, and said in a tapped phone call: "Go on Skype. Ok, I'll be there in five minutes. There was a similar phone tap in a Kurdish case:¹²⁶ "It is smuggler A who calls a British number, smuggler W asks him to correspond via Viber".

The smugglers regularly changed their mobile phone numbers to make it more difficult and exchanged their new numbers via Facebook. The following is a good example of a telephone wiretap in a Kurdish smuggling case¹²⁷: "Smuggler D asks smuggler S to send his new mobile phone number via Facebook and says that he will also have a new number tomorrow... Both agree to change their number again and forward their new number via Facebook". During his questioning, a smuggler publicly admitted to the police: "We also tried to communicate as much as possible via the internet (Facebook and WhatsApp, but especially Viber) because the police cannot wiretap these calls".

According to an investigative report¹²⁸, such use of social media fits in with a strategy of professionalising smuggling networks.¹²⁹ A smuggler who was interviewed for this study explained: "I have used more than 100 mobile phone SIM cards myself," explains Afghan smuggler J. "I probably have more than 40 or 50 Facebook accounts. I activate them when I need them and as soon as my customers arrive at their destination, I deactivate them".¹³⁰ Such deactivation of a smuggler's Facebook account is seen as a new form of counter-espionage techniques.

We currently see in smuggling cases that smugglers realise that social media chat messages can be read and analysed by the police, as is the case for mobile phones. In a Kurdish smuggling case¹³¹, it appears that smugglers are trying to adapt to this situation and are developing counter-espionage strategies in social media. Following the arrest of several smugglers, four of them managed to flee to France. One of the fugitive smugglers quickly warned the others by telephone to remove the digital traces of the

122 MYRIA, 2016 Annual Report on Trafficking and Smuggling of Human Beings: *Beggars in the hands of traffickers* case studies p. 122.

123 MYRIA, 2015 Annual Report on Trafficking and Smuggling of Human Beings, *Tightening the Links*, case study, p. 73.

124 Summary of EMN Ad-Hoc Query No. 1055 from 18 April 2016, *Addressing and preventing the use of social media in migrant smuggling*.

125 MYRIA, 2015 Annual Report on Trafficking and Smuggling of Human Beings, *Tightening the Links*, case study, p. 82.

126 MYRIA, 2016 Annual Report on Trafficking and Smuggling of Human Beings: *Beggars in the hands of traffickers* pp. 113-114.

127 MYRIA, 2016 Annual Report on Trafficking and Smuggling of Human Beings: *Beggars in the hands of traffickers* case studies p. 122.

128 The Smuggling Game Playing with life and death to reach Europe, by Lin Taylor and Valeria Cardi, 28 March 2017: <http://news.trust.org/shorthand/the-smuggling-game>.

129 "Smugglers are very innovative and they are adjusting their criminal activities very quickly to new obstacles in their way." Through social media platforms like Facebook, or encrypted mobile apps such as WhatsApp, Imo and Viber, smugglers can easily bypass police detection and communicate freely with migrants or their relatives to negotiate payments and logistics.

130 <http://news.trust.org/shorthand/the-smuggling-game>.

131 See also Part 3, Chapter 2, point 2, (human smuggling case studies).

detained smugglers, so that the police could no longer make any connection between them: "On 22/05/2015, Q (fugitive smuggler) contacted P (smuggler) via his French telephone number. Q inquires firstly as to the situation of the suspects arrested on 22/05/2015 (and advises to block their names on Viber), and then indicates that he has lost his smartphone in the car park. He asks P to turn off his Facebook when he finds his smartphone (he transfers PIN code 2101)".

In the same case, a smuggler was in the process of searching for trucks for a smuggling operation. During a phone call, he was asked not to post the photos to Facebook. He knew that these are important operational smuggling data that can be found by the police: "597 calls 782 with the information that he has just taken two photographs, he will send the photos to 782 and asks to see if they are going there or not. (police note: presumably to a given destination in the United Kingdom, presumably photographs of lorries with a given destination, this is removed from the context of the conversation). 782 asks that no photographs are posted to his Facebook account".

3.3. | Social media and the exploitation of smuggling victims

Smugglers also use social media as a tool to assist in the exploitation of victims of smuggling. There are also reports of exploitation on social media.

Social media as a facilitator of sexual exploitation

In an Afghan smuggling case¹³², the smuggling leader, using Skype, arranged a free smuggling trip for a minor to France, where the boy had to pay for it in kind afterwards. An employee phoned the smuggling leader with the message: "There are a few nice-looking boys and I can send them to you if you like". The smuggling leader replied: "Why not, use Skype to show them to me and there's one whose trip to France will be totally paid. Ok, give my number to one of these two minors, the one that looks the most "expensive".

This Afghan smuggling leader operated from a smuggling camp in Calais, where UNHCR also reported sexual abuse of Afghan boys.¹³³

Reports of exploitation on social media and internet

Migrants themselves are also starting to post more situations of abuse on social media, to warn their peers. This can lead to a form of social control at the digital level. For example, stories of rape have already been reported on social media, which have taken place along the way.¹³⁴ Films have also been posted in which smugglers force migrants to cram into an overcrowded boat under the threat of a weapon.¹³⁵

The EU project on the role of social media and migrants mentions an online platform that records violations of the human rights of Mediterranean migrants: Watch The Med¹³⁶ is an online mapping platform that tracks the number of deaths of migrants and human rights violations at sea.¹³⁷ The information on this platform is based on reports and testimonies sent by telephone or internet by migrants, family members, seafarers and other witnesses to violations of migrants' rights at sea.¹³⁸

3.4. | Social media, internet and secure migration routes

Myria has already highlighted the importance of safe migration routes in its previous annual reports. Social media can play a major role in this respect. One study puts

133 UNHCR, *From A Refugee Perspective, Discourse of Arabic speaking and Afghan refugees and migrants on social media from March to December 2016*, April 2017. www.unhcr.org/uk/5909af4d4.pdf: "Individual interviews with our investigator in Calais have shown that a number of very young boys have been sexually abused by smugglers. This is something that young Afghans will not readily talk about due to fears of stigmatisation and/or retaliation... In general, the Afghan travellers are very young and uninformed, and rely entirely on their smuggler, which makes them vulnerable to abuse, including sexual exploitation".

134 *Ibid.*

135 *Ibid.*

136 www.watchthemed.net.

137 www.watchthemed.net/pdf/WTM-flyer-eng.pdf.

138 The Open University and France Médias Monde, 2016. *Mapping Refugee Media Journeys: Smartphone and Social Media Networks*. www.open.ac.uk/research/main/sites/www.open.ac.uk/research/main/files/files/ecms/web-content/Mapping-Refugee-Media-Journeys-16-May-final-V1.pdf.

132 MYRIA, 2015 Annual Report on Trafficking and Smuggling of Human Beings, *Tightening the Links*, case study, p. 82.

it this way: "It is through phones that refugees learn about routes and the cost of transport. It's how they find out which borders are open and which are closed. Even before they make it that far, their phone might have saved their life by informing them about the weather conditions on a sea crossing. The general view is that they have three basic needs: a smartphone, food and water – in that order".¹³⁹

Below are some best practices that have already been developed and show the possibilities of social media.

Safe migration routes

Migrants find their bearings along the way using Google Maps, and exchange safe routes and current changes among each other.¹⁴⁰ In 2015 and 2016, migrants used Google Maps to traverse several countries from Greece along the so-called Balkan route to Western Europe.¹⁴¹ When Hungary closed its borders in 2015 and the migration route shifted to Croatia and Serbia, an application was developed via Facebook with a map of the locations of landmines in these two countries, so that the migrants could travel through safely.¹⁴²

The EU project examining the role of social media for migrants mentions various developed Apps as best practices in its interim report. During the refugee crisis, Google, together with various NGOs, developed the App 'Crisis Info Hub' with up-to-date relevant information on Greece, Macedonia (FYROM), Serbia, Croatia and Slovenia, and their border regions.¹⁴³

Another app is 'Infomobile - Welcome 2 Europe'¹⁴⁴ and was developed by migrants themselves. It provides updated advice on migration policy and contact details of the NGOs of 35 countries.¹⁴⁵

Facebook user groups without smugglers

Facebook groups have been set up for migrants who want to travel to the West without a smuggler. The Facebook page 'Europe without Smugglers' provides information about the routes that were previously only provided by smugglers. One migrant put it as follows to a journalist: "You have an entire network of people at your fingertips. Smugglers via the land-based route are no more than an extra cost. Often it is much more risky to work through them than to rely on other refugees."¹⁴⁶

The Facebook group "Asylum and Immigration without Smugglers" has more than 15,000 members and steers the migrants through Europe individually or in a group without smugglers. One migrant asked the question to join a group: "I am in Turkey and would like to go to Germany or Sweden, is there a group which is ready to leave? One person replied: "My father and brother are also doing the journey and we are just forming a group, call me at this number: xxx".¹⁴⁷

Migrants themselves are also starting to post more situations of abuse on social media, to warn their peers.

139 Babani, 2016. *Phones – crucial to survival for refugees on the perilous route to Europe*. <https://theconversation.com/phonescrucial-to-survival-for-refugees-on-the-perilous-route-to-europe-59428>.

140 J. ZIJLSTRA, IVAN LIEMPT, "Smart(phone) travelling: understanding the use and impact of mobile technology on irregular migration journeys", *International Journal of Migration and Border Studies*, January 2017. www.researchgate.net/publication/312015518_Smartphone_travelling_understanding_the_use_and_impact_of_mobile_technology_on_irregular_migration_journeys.

141 Danish Refugee Council, *Getting to Europe the 'WhatsApp' way*, June 2016. http://reliefweb.int/sites/reliefweb.int/files/resources/RMMS%20Briefing%20paper%202_Social%20Media%20in%20Mixed%20MigrationUPLOAD.pdf.

142 NPR, 2015, A Harrowing Journey Into Europe, Aided By Apps And Internet Access. www.npr.org/2015/09/19/441754735/aharrowing-journey-into-europe-aided-by-apps-and-internet-access.

143 The Open University and France Médias Monde, 2016. *Mapping Refugee Media Journeys: Smartphone and Social Media Networks*. www.open.ac.uk/research/main/sites/www.open.ac.uk.research.main/files/files/ecms/web-content/Mapping-Refugee-Media-Journeys-16-May-final-V1.pdf: "The Google team identified a "lack of timely hyperlocal information for refugees", developing something that would give refugees vital forms of information concerning the particulars of their departure, journey, and arrival, "providing refugees—most of whom carry smartphones—with critical information for their journeys: lodging, transportation, medical facilities, etc.

144 www.facebook.com/w2eu.info/info/?tab=page_info.

145 The Open University and France Médias Monde, 2016. *Mapping Refugee Media Journeys: Smartphone and Social Media Networks*. www.open.ac.uk/research/main/sites/www.open.ac.uk.research.main/files/files/ecms/web-content/Mapping-Refugee-Media-Journeys-16-May-final-V1.pdf: "Refugees are encouraged to navigate across the various links in order to find information concerning issues such as: "safety on the sea", "asylum", "Dublin II", "gender", "minors", "regularization", "detention", "deportation", "living", "family", "medical" and "work".

146 The Financial Times, 2016. *Technology comes to the rescue in migrant crisis*. www.ft.com/cms/s/0/a731a50a-da29-11e5-a72f-1e7744c66818.html#ixzz41ks4s7ZX.

147 Danish Refugee Council, *Getting to Europe the 'WhatsApp' way*, June 2016. http://reliefweb.int/sites/reliefweb.int/files/resources/RMMS%20Briefing%20paper%202_Social%20Media%20in%20Mixed%20MigrationUPLOAD.pdf.

Social media as a lifeline on the move

Migrants use social media as a helpline during their journeys, which can save lives. One migrant testified to a journalist: "At the beginning of his dangerous journey across the Aegean Sea in a rubber boat with 62 other refugees, H. phoned a friend in New York. He wanted to keep her on the line in case something went wrong. And then something did go wrong. The boat started to take in water and sank. When H. fell into the water, he was able to keep his phone above the waves and ask his girlfriend to inform the Turkish coastguard. Through WhatsApp, he was able to give his location. 45 minutes later he was rescued".¹⁴⁸ There was a similar story in which Twitter played a crucial role as an assistance tool which saved many lives.¹⁴⁹

According to the IOM (International Organization for Migration),¹⁵⁰ a total of 7,763 migrants died during their crossing in 2016. Of these, 5,096 people drowned or disappeared in the Mediterranean Sea.¹⁵¹ In 2015, there were 3,771 deaths in the Mediterranean Sea. According to the UNHCR, by 31 July 2017, there had already been 2,409 deaths or missing persons in the Mediterranean Sea.¹⁵²

Migrants use social media as a helpline during their journeys, which can help save lives.

Meanwhile, various applications are being developed that serve as a lifeline. For example, there is a Facebook page with real-time information about missing boats in the Mediterranean Sea.¹⁵³

The EU project on social media and migrants refers to Alarmphone¹⁵⁴ as a hotline for supporting relief operations.¹⁵⁵

148 Wired, 2016, *Refugees are more connected than ever. Rescuers must be too*. www.wired.com/2016/04/humanitarian-aidstartups/?mbid=social_fb.

149 Babani, 2016. *Phones – crucial to survival for refugees on the perilous route to Europe* <https://theconversation.com/phonescrucial-to-survival-for-refugees-on-the-perilous-route-to-europe-59428>: "A Twitter subscriber who received a phone call from someone on a boat with a broken engine on the Mediterranean, used Twitter to get the number of the Italian coastguard, tweeting: "250 Eritreans women and children majority their ship is in distress in Mediterranean. Please help, they asking for help! Motor stop working". This message was retweeted with GPS coordinates to alert the emergency services.

150 <http://migration.iom.int/europe>.

151 See MYRIA, 2017 *Annual Report Migration in Figures and Rights*, p. 103.

152 <http://reliefweb.int/report/italy/mediterranean-dead-and-missing-sea-july-2017>.

153 Danish Refugee Council, *Getting to Europe the 'WhatsApp' way*, June 2016. http://reliefweb.int/sites/reliefweb.int/files/resources/RMMS%20Briefing%20paper%202_Social%20Media%20in%20Mixed%20MigrationUPLOAD.pdf: "More than 58,000 people follow the Facebook page of Lukman Derky, a Syrian in France. He shared information on boats that have gone missing while crossing the Mediterranean Sea. This includes the last known GPS coordinates of the vessels, as well as readings for people in need on dry land, along with a request for the nearest follower to come to their aid.

154 <http://alarmphone.org/en>.

155 The Open University and France Médias Monde, 2016. *Mapping Refugee Media Journeys: Smartphone and Social Media Networks*. www.open.ac.uk/research/main/sites/www.open.ac.uk/research/main/files/files/ecms/web-content/Mapping-Refugee-Media-Journeys-16-May-final-V1.pdf: "The alarm phone was started in October 2014 by activist networks and civil society actors in Europe and Northern Africa. The project set up a self-organized hotline for refugees in distress in the Mediterranean Sea. It offers the affected boat-people a second option to make their SOS noticeable. The alarm phone documents and mobilises in real-time. In this way, pressure to rescue is built-up, wherever possible and push-backs and other forms of human rights violations of refugees and migrants at sea can be opposed. Thus, the Alarm Phone is not a rescue number, but an alarm number to support rescue operations.

Chapter 2

Social media and the internet as a method of investigation

The judiciary and police have also use social media and the internet themselves, as a method of investigation in their work. Despite many new challenges¹⁵⁶, the European Migration Network (EMN) identified, in its survey of EU countries, that most European countries use social media and the internet as an investigation tool to gather evidence in the fight against human smuggling.¹⁵⁷ There is also cooperation in the fight against human trafficking in seven EU countries.¹⁵⁸

In the Belgian human trafficking and smuggling cases in which Myria has initiated civil proceedings, or has taken

The social media and the internet, when used as investigative tools, are much less present in cases of economic exploitation.

note, we have observed that social media and the internet are used in various ways at the different stages of an investigation. The results can be used by the court as objective evidence when justifying their decisions.¹⁵⁹ This is a significant merit of the Belgian judiciary,

which responds to a recommendation from the EMN,¹⁶⁰

not only for the fight against human smuggling, but also human trafficking. However, these details should be shared internationally, as best practice. As such, the EU Trace project recommends introducing this into the Human Trafficking Case Law Database of the United Nations Office on Drugs and Crime (UNODC), which was set up for this purpose.¹⁶¹ It is also desirable and necessary that a similar instrument is established at the EU level.¹⁶²

We have also observed that social media and the internet are much less present as investigative tools in cases of economic exploitation, whereas it could be useful, for example, during the questioning of a victim in identifying a location via Google Maps. The front-line services, including the inspection services, need to be trained in this regard. In addition, a recommendation from the EU's Trace project is worth considering: "To promote the strict control of websites with online job advertisements (either by the police or by civil society organisations), especially in sectors where trafficking in human beings is common".¹⁶³

156 EMN Inform, *The Use of Social Media in the Fight Against Migrant Smuggling*, September 2016: "Social media in migrant smuggling has played a large role in not only increasing the volume but also the effectiveness of smuggling operations, and has made it overall more difficult to investigate and prosecute such crimes. Both Member States as well as EU agencies, however, identified important challenges obstructing their monitoring activities. For example, monitoring is obstructed by the anonymity of users, the use of closed accounts, restricted pages, encryption, the use of the dark net, etc."

157 Summary of EMN Ad-Hoc Query No. 1055 from 18 April 2016, *Addressing and preventing the use of social media in migrant smuggling*: "A majority of Member States (BE, CZ, DE, ES, FR, HR, HU, LT, NL, PL, SE, SI, UK) have reported that they use social media and online platforms to gather evidence against migrant smugglers."

158 *Ibid*: Several Member States (BE, CZ, DE, EE, ES, NL, PL) gave examples of existing cooperation in other crime areas such as human trafficking and sexual exploitation.

159 Myria, 2013 Annual Report on Trafficking and Smuggling of Human Beings, *Building Bridges*, p. 67

160 EMN Inform, *The Use of Social Media in the Fight Against Migrant Smuggling*, September 2016: "Pursuing and further developing the monitoring and analysis of relevant case law on migrant smuggling and the use of e-evidence."

161 http://data.trilateralresearch.com/wp-content/uploads/2015/11/TRACE_D4.1_Role-of-technologies-in-human-trafficking_FINAL_-1.pdf: "In October 2011, the United Nations Office on Drugs and Crime (UNODC) launched the online "Human Trafficking Case Law Database" a publicly available repository of summaries and full 159 court documents of trafficking cases to support successful convictions in trafficking cases. Not only can people search the database, in addition, they can contribute new cases by directly contacting the UNODC, thereby helping to continuously populate the database. At the same time, it is a public space where summaries and complete court documents of human trafficking cases can be viewed, and which can raise awareness about how to reach effective convictions in human trafficking cases".

162 http://data.trilateralresearch.com/wp-content/uploads/2015/11/TRACE_D4.1_Role-of-technologies-in-human-trafficking_FINAL_-1.pdf: Establish national and/or European databases on cases of human trafficking. In principle, such databases do not contain information on the identification of victims or perpetrators, but they do provide for updated statistics, comments on modus operandi, geographical patterns, etc. The information could make future Eurostat reports more reliable and easier to analyse.

163 http://data.trilateralresearch.com/wp-content/uploads/2015/11/TRACE_D4.1_Role-of-technologies-in-human-trafficking_FINAL_-1.pdf.

1. OPEN SOURCE INVESTIGATION

Open source investigation is an important part of police work. It can be provided by a front-line service or by a police support service, if requested.¹⁶⁴

1.1. | Initial phase of an investigation

In cases of human trafficking, a case can be initiated on the basis of an internet investigation into an escort service in which there are indications of sexual exploitation. This is done through internet ads and online forum conversations.

A Nigerian case¹⁶⁵ was initiated in Tongeren following police surveillance of concealed forms of prostitution. The police monitored certain internet websites where African women presented themselves as escorts. After a substantive analysis of the details on the website, the investigators identified possible indications of human trafficking. Using the numerous customer reviews on the publicly accessible forums of certain websites, the police deduced that the accommodation of the African women was precarious, and that they were presumably employed as illegal residents, which is an indication of human trafficking.

In cases of human smuggling, an internet investigation may also lead to the initiation of a smuggling case. As early as 2001, a human smuggling case¹⁶⁶ was started up in Brussels, following a complaint from a victim of smuggling, on the basis of an internet survey of a Russian agency that offered residence documents via an asylum procedure. The judgement¹⁶⁷ in the case was as follows: (translation) "The criminal record starts with an official report of the Ostend Maritime Police (22 January 2001) on a website

that apparently aims to familiarise refugees from Russia with the asylum procedure, and more generally with life in Belgium. On the site "(...)", people can even create their own page. Several newsletters have been published in this way.... The Federal Police - Judicial Department Antwerp (...) knows that Russian nationals offer their services to fellow Russians for payment. A GSM number (...) is indicated on the website. When this number is called, the person is forwarded to the number (...). Police information indicates that the number (...) could be linked to a (...) so-called lawyer, K. D."

1.2. | Detecting victims

The police use social media and the internet to trace victims of human trafficking. In a Hungarian case¹⁶⁸, the police managed to trace an underage victim via Facebook. From the telephone wiretaps, the police identified a conversation in which the minor contacted the accused about prostitution work. She gave him her Facebook profile with her references, so that the police could easily find her.

Facebook can also serve to link victims to a prostitution network. In the same Hungarian case¹⁶⁹, the investigators in the found, in the Facebook profile of the defendant recruiter, 34 Hungarian women among her friends, who worked as 'window' prostitutes in Ghent. The police managed to identify the victims and link them to the prostitution network. In a *loverboy* case¹⁷⁰ involving minors from youth institutions, the police found underage victims on an online forum site for sex dates.

The online forums of clients of prostitutes, where people exchange their experiences, provide important data for the police in determining whether human trafficking is taking place. In these cases, there are then also potential victims of human trafficking. In a Thai case in Leuven¹⁷¹, the police gathered information concerning the prostitution experiences of clients of the massage parlour which were found on the websites where the clients shared

164 See also external contribution: Presentation DJSOC/I2 in the fight against human trafficking: supporting role in investigations on the internet and social media".

165 MYRIA, 2011 Annual Report on Trafficking and Smuggling of Human Beings, *The Money that matters*, p. 90.

166 MYRIA, 2008 Annual Report on Trafficking and Smuggling of Human Beings, *Enlisting people and resources to combat the phenomenon*, p. 73.

167 Correctional Court of Brussels, 22 October 2008, 51st chamber (definitive) (available at www.myria.be).

168 MYRIA, 2015 Annual Report Human Trafficking and Smuggling, *Tightening the Links*, case study, pp. 69-71.

169 *Ibid.* See also Chapter 1, point 1 of this focus (the role of social media and the internet in human trafficking).

170 MYRIA, 2016 Annual Report on Trafficking and Smuggling of Human beings, *Beggars in the hands of traffickers*, case-law overview, p. 154; Corr. Court Antwerp, 22 December 2015, chamber. A4C (definitive).

171 MYRIA, 2011 Annual Report on Trafficking and Smuggling of Human Beings, *The money that matters*, p. 101.

their experiences. This enabled the police to prove that it was a case of human trafficking. In a Thai case in Mechelen¹⁷², the police identified additional victims via

The online forums of prostitution clients, where people exchange their experiences, provide important data for the police.

the online forums of prostitution clients. The comment sections on these websites clearly showed that in addition to the massages, further sexual acts were also performed.

In a 'drink-along' business case¹⁷³, the police could prove via the online forum site that a victim had been exploited for a significant length of time. The police carried out targeted searches on the internet. On an internet site for prostitution clients, a forum post from 2006 caught the attention of the police. The prostitution client had already posted to the forum 47 times about his personal experiences in various bars. In his post about the bar in question, he mentioned a young woman with fake Lithuanian documents. The police conclude from this that she had already been active in this bar in June 2006, more than a year before she was found during the search of the premises in October 2007.

In order to improve victim detection, Trace recommended setting up a kind of hotline via social media: "Work on better tools to facilitate anonymous reporting of suspected human trafficking on websites and social media. An anonymous complaint, for example, via apps / websites / hotlines".¹⁷⁴

1.3. | Identification of suspects

Facebook is a convenient medium for identifying potential perpetrators of human trafficking and smuggling. If Facebook profiles are closed, they fall outside the scope of the open source investigation, and a different procedure applies.¹⁷⁵ These days, the police, and especially the federal judicial police, use this method of investigation in their cases. But the police also check internet data. With Google Image, for example, a personal photo from a surveillance operation can be compared with existing

photos on internet platforms, meaning that the Facebook profile of the person in question can be traced. The result is that the suspect can be identified, as can various other data on his profile.

Identification of main suspects

In various human smuggling cases, the police were able to determine the true identity of a main suspect who operated under a false name, through photographs on Facebook. Through open source investigation, the police were able to find the profile of the smuggler under his false name, and found that the photograph of his profile resembled the photograph of a suspect from their database.

In a Kurdish smuggling case¹⁷⁶ in Bruges, the police established through a telephone wiretap that a main defendant used a false name on social media. When the police checked in the national register, they were unable to find the person in question. However, through an open source investigation on Facebook, the police were able to find the profile of the smuggler under his false name, and found that the photo of his Facebook profile resembled the photograph of the Iraqi M., the true identity of the main defendant, whose data were indeed in the police database.

In an Albanian smuggling case in Ghent, the court, in its judgement,¹⁷⁷ referred to an open source investigation into the Facebook profile of an intercepted person who had been smuggled, in which a link could be made with the Facebook profile of the main suspect.

In a *loverboy* case¹⁷⁸ involving minors from youth institutions, an important suspect was identified by comparing a Facebook profile picture with a photograph from the national register.

In a Thai human trafficking case¹⁷⁹, the perpetrators were identified on the basis of telephone tapping and the internet. When an airline ticket was booked via an airline, the police contacted the airline in question to obtain the full personal details of the person concerned. The police were also able to trace the identity and reference details of other victims and perpetrators, since their airline tickets had been ordered through the internet, and because they had data from wiretapping. The police initially only knew them from their aliases from the telephone conversations

172 MYRIA, 2016 Annual Report on Trafficking and Smuggling of Human Beings, *Beggars in the hands of traffickers*, case study, pp. 87-90.

173 MYRIA, 2010 Annual Report on Trafficking and Smuggling of Human Beings, *Combating social fraud to prevent trafficking in human beings*, p. 53.

174 http://data.trilateralresearch.com/wp-content/uploads/2015/11/TRACE-D4.1_Role-of-technologies-in-human-trafficking_FINAL-1.pdf.

175 See also chapter 3 of this focus (Internet and social media: new challenges for policy, the police and the judiciary).

176 MYRIA, 2011 Annual Report on Trafficking and Smuggling in Human Beings, *Beggars in the hands of traffickers*, case study, pp. 112.

177 Corr. Court East Flanders, subsection Ghent, 23 November 2015, 28th chamber (unpublished).

178 MYRIA, 2016 Annual Report on Trafficking and Smuggling of Human Beings, *Beggars in the hands of trafficker*, case study, pp. 69-71.

179 MYRIA, 2011 Annual Report on Trafficking and Smuggling of Human Beings, *The money that matters*, p. 98.

monitored during the wiretaps, but by linking these data to their bank card payments, their identities could be established.

Switching identity

The police use Facebook to investigate identity switching among suspects. In an Iraqi smuggling case¹⁸⁰ in Dendermonde, the police were able to prove that the smuggler had adopted a different identity when he was arrested, by comparing Facebook profiles.¹⁸¹

Identification of networks

The police can get a better picture of the complete network through a Facebook investigation. As such, it checks the Facebook profiles of the suspects. Links with friends, messages and images can lead investigators to co-suspects, and relevant locations such as safehouses. In this way, the police have detected additional suspects in both human trafficking¹⁸² and human smuggling¹⁸³ cases.

In a case of human trafficking in a Thai escort case¹⁸⁴, the police were able to identify and investigate the internet advert for escort services via Google, based on a telephone wiretap. In its judgement¹⁸⁵, the court explicitly justified the conviction for human trafficking with a reference to the internet investigation of this website. In a Belgian *loverboy* case¹⁸⁶ linked to polycriminality, a video on Facebook in which the victim was humiliated was used as evidence. In an economic exploitation case¹⁸⁷, the police used Google

as a supporting investigative tool to search for information about the defendant's company.

In an Iraqi smuggling case¹⁸⁸ in Dendermonde, the police managed to identify the Syrian smuggler in London (UK) via Facebook, who arranged the supply of Syrian smuggling victims via Belgium from the UK.¹⁸⁹ He was prosecuted and convicted as a co-defendant, and was also the main defendant in a Brussels smuggling case.¹⁹⁰

A Facebook investigation can also provide an additional burden of proof. In a Kurdish smuggling case¹⁹¹ in Ghent, the police were able to find incriminating photographs on the Facebook profile of the main defendant, through an open source investigation. It was ascertained that he had posted four photographs of himself with an alarm gun in his left hand. These photographs were added to the official report as evidence.

The police can get a better picture of the complete network through a Facebook investigation.

180 See also Part 3, Chapter 2, point 2, (human smuggling case studies).

181 An official report states the following (translation): "At the time of his arrest, 'B' was found not to be in possession of any identity document, and was identified as N on the basis of an oral interrogation. Through an open source investigation, we should be able to establish that: the Facebook page of 'B' does not correspond to the identity 'N' which he specified. The same photograph is also found on the Facebook profile 'A.N.'. A check of the latter account (visible section) revealed that this is a different person from 'B'. It is stated on the Facebook page that the user of the profile 'A. N' is someone who lives in S. Both are acquaintances of each other, since the account of 'A. N' has liked various pictures on the Facebook page of 'B'. This all shows that the arrested suspect 'B' had taken a different identity when confronted by the Belgian authorities, which was the identity of an acquaintance of his from his country of origin, Iraq".

182 MYRIA, 2015 Annual Report on Human Trafficking and Smuggling, *Tightening the Links*, case study, pp. 69-71 (Hungarian prostitution case) and p. 29 (Romanian prostitution case); 2013 Annual Report on Human Trafficking and Smuggling, *Building Bridges*, pp. 17, 60 and 108 (Romanian prostitution case); Corr. Court Leuven, 4 July 2013, 17th chamber (available at www.myria.be)

183 See also Part 3, Chapter 2, point 2, (human smuggling case studies).

184 See also Part 3, Chapter 3 (case-law overview): Corr. Court Liege, subsection Liege, 16 November 2016, 19th chamber (appeal).

185 *Ibid.*

186 See also section 3, Chapter 2, point 1.1. (Sexual exploitation case studies).

187 MYRIA, 2016 Annual Report on Trafficking and Smuggling of Human Beings: *Beggars in the hands of traffickers* case-law overview, p. 163.

188 See also Part 3, Chapter 2, point 2, (human smuggling case studies).

189 An official report stated (translation): "On the basis of the aforementioned statement, we carried out a few searches on Facebook in an attempt to identify this Syrian supplier. Searches for the profile X were unsuccessful. However, we did note that some pictures posted to smuggler A's Facebook profile were 'liked' by the holder of the Facebook profile 'M'. Upon checking the public section of the latter's profile, we observe that the holder claims to live in London. There are 5 photographs on the public section, which according to the context presumably depict the profile holder. As regards identification, we have also observed that, according to the General National Database (GND), M is linked to the human trafficking investigation C. Based on the photographs in the GND, we can see that M is linked to the suspect X, who is being traced in the current investigation".

190 See also Part 3, Chapter 2, point 2, (human smuggling case studies).

191 MYRIA, 2011 Annual Report on Trafficking and Smuggling of Human Beings, *Beggars in the hands of traffickers*, case study, pp. 118.

2. HEARINGS

Social media and the internet are useful tools in hearing victims and interrogating suspects. Facebook and Google Maps can provide important added value, as well as additional leads for the investigation.

2.1. | Hearing of victims

When victims are interviewed, the police primarily use Google Maps and Facebook, but the victims themselves can also provide evidence sourced from social media.

Google Maps

Often, victims do not know exactly where they were held captive. In the past, the police drove around the surrounding area with the victims, to try to pinpoint the exact location. The police can now use Google Maps when interviewing victims to find out where they were being held, and they can then find the full address. In addition, when victims make their statements, the police already use the Google Maps web application to find the route to, and the location of the offences, with the victim's help.¹⁹²

Facebook

The police use Facebook profiles when interviewing victims in order to gather as much relevant information as possible for the investigation.

In another *loverboy* case¹⁹³ involving minors from youth institutions, the victim was able to indicate a suspect via his Facebook profile.¹⁹⁴ By comparing the photographs in the profile with police photographs, it was possible to formally identify the defendant.

In a Nigerian case¹⁹⁵ in Brussels, an underage victim was able to identify a co-defendant during her interview, based on his Facebook profile photo. In the same case, the police were able to free another victim as she still had contact with one of the Nigerian victims via Facebook. The victim in question had stated that, through Facebook, she knew which other club she was employed in. The federal judicial police carried out a search of the club and were able to intercept the other girl.

In an Iraqi smuggling case¹⁹⁶ in Dendermonde, following complaints by Iranian smuggling victims in 2014, the Brussels police investigated the Facebook profiles of the suspected smugglers who had been identified by the victims. This enabled the police to identify the smugglers.¹⁹⁷

Evidence from victims

Victims themselves provide evidence to the investigators during their hearings. This may be a Skype call recording or a USB stick containing messages, and images on Facebook.

In a Hungarian human trafficking case¹⁹⁸ in Ghent, a victim was able to prove through Skype that her pimp had made false statements. She contacted a friend who had recorded the oral Skype discussion with the pimp. The police were able to request this Skype interview from her girlfriend and examine the content. This was then included in the judgement¹⁹⁹ as evidence against her pimp.

In a Belgian *loverboy* case²⁰⁰ linked to polycriminality, a victim gave a USB flash drive containing Facebook messages and photographs to the investigators during her second hearing. As such, she could prove that, after having made a complaint, a defendant had threatened her. Based on the photographs and messages, new victims could be detected and identified. One photo depicted a female friend from a refuge who had told her in a Facebook message that the defendant had also wanted to force her into prostitution. The police questioned the female friend as a witness, declaring that the defendant had recruited several victims for prostitution, and was clearly a pimp. In the same case, an underage victim provided the police with a Facebook message during her hearing, which

¹⁹² MYRIA, 2013 Annual Report on Trafficking and Smuggling of Human Beings, *Building Bridges*, pp. 70.

¹⁹³ MYRIA, 2016 Annual Report on Trafficking and Smuggling of Human beings, *Beggars in the hands of traffickers*, case study, p. 87

¹⁹⁴ The official report stated (translation): "Via Facebook, the victim A. indicated the profile of T as the perpetrator; this was presumably B. She also had a suspicion of the suspect's place of residence".

¹⁹⁵ See also Section 3, Chapter 3 (case-law overview).

¹⁹⁶ See also Part 3, Chapter 2, point 2, (human smuggling case studies).

¹⁹⁷ The official report stated: "Based on the content of the hearings, we will proceed to the necessary verifications. With regards to the identified S, we have detected the Facebook profile under the name 'S.N.' and have taken a 'print screen' of the profile page and photos. His GSM number is known in the general national database for the human smuggling case D. and the case 'K'. In this case, the person in question was intercepted, together with our victims, while being transported by truck.

¹⁹⁸ See also Section 3, Chapter 3 (case-law overview).

¹⁹⁹ See also Part 3, Chapter 3 (case-law overview): Corr. Court East Flanders, subsection Ghent, 31 March 2017, Chamber G28m (appeal).

²⁰⁰ See also section 3, Chapter 2, point 1.1. (Sexual exploitation case studies).

showed that the defendant had attempted to contact her via another victim's profile, which is illegal due to possible manipulations.

2.2. | Interrogation of suspects

The police use Facebook and Google Maps as a tool when interrogating defendants.

Google Maps

When interrogating suspects, the police can use Google Maps to trace specific locations linked to smuggling activities, such as safehouses. In a Kurdish smuggling case²⁰¹ in Ghent, the defendant indicated the hotel where he had been lodging with the other smuggler, during his interrogation. The hotel also served as a safehouse for smuggling activities.²⁰²

Facebook

In the same Kurdish smuggling case²⁰³ in Ghent, the defendant voluntarily gave his Facebook password during his interrogation, to demonstrate his full cooperation. The police opened up Facebook in his presence and had him indicate, through the photographs in his profile, which people he referred to in his statement. He also provided further explanation more about other smugglers, using his Facebook photos.²⁰⁴

3. ANALYSIS

Europol highlights the importance of the technical analysis of smartphones, iPads and computers.²⁰⁵ The cases, both relating to human trafficking and human smuggling, show that these analyses provide substantial data which can be used as evidence. In these cases, it relates to analyses of seized equipment which requires a mandate from a magistrate.²⁰⁶

3.1. | Messages and images

Most chat messages and saved images can be traced by technically analysing smartphones, iPads and computers. This has provided decisive evidence in many cases.

In an Iraqi human smuggling case²⁰⁷ in Dendermonde, the police were able to make 9000 messages in a deleted files folder visible again. Most of the files were Skype calls where only the call information was available, but there were also several relevant chat messages with texts about smuggling transportation. In addition, many deleted photograph files were made visible again. In some photographs, the smugglers paraded with firearms. In the case of one defendant, 270 deleted photographs with references to the terrorist group Islamic State were found and made visible again.

In a Kurdish smuggling case²⁰⁸ in Ghent, the retrieved messages provided important data on the main defendant. His smartphone also contained photographs of other smugglers. During the analysis of his computer, it was possible to retrieve Facebook chats about smuggling transport and financial management, and trace the Facebook profiles of the persons involved in the chats. In an Albanian-Czech smuggling case, the judgement²⁰⁹

201 MYRIA, 2016 Annual Report on Trafficking and Smuggling of Human Beings, *Beggars in the hands of traffickers*, case study, p. 116.

202 The official report states (translation): 'A. told me that I could stay with him at hotel X. Together with you I am looking for it via Google Maps and let me take you a print screen from the entrance of the hotel that is named (...)'.
203 MYRIA, 2016 Annual Report on Trafficking and Smuggling of Human Beings, *Beggars in the hands of traffickers*, case study, p. 116.

204 The citations from an official record of the interrogation of the smuggler were as follows: When the police asked him: "Are there still people who you haven't mentioned yet, but who play an important role in the organisation", he replied: "Only D., there are other groups, but the people I have seen in the cafe are those I've already mentioned, I don't have a picture of him on my mobile phone, but I do on Facebook. I will willingly show you the photograph on my Facebook".

205 EUROPOL, *Intelligence Notification 15/2014*, The Hague, October 2014. www.europol.europa.eu/publications-documents/trafficking-in-human-beings-and-internet: "Data found online and on mobile devices can be obtained using forensic examination and used as evidence in cases. Law enforcement specialists require continuous technical training in order to keep up with OCGs' increasing use of countermeasures such as encrypted mail and encrypted mobile devices".

206 See also chapter 3 of this focus (Internet and social media: new challenges for policy, the police and the judiciary).

207 See also Part 3, Chapter 2, point 2, (human smuggling case studies).

208 MYRIA, 2016 Annual Report on Trafficking and Smuggling in Human Beings, *Beggars in the hands of traffickers*, case study, p. 116.

209 See also Part 3, Chapter 3, (case-law overview): Corr. Court East Flanders, subsection Ghent, 2 January 2017, chamber G28m

on the investigation referred, inter alia, to the analysis of Skype messages between the smugglers.

In a Hungarian human trafficking case²¹⁰ in Ghent, a defendant had filmed his victims himself and saved the recordings to his iPhone. The police described this in detail in their technical report. In an economic exploitation case involving Pakistani night shops²¹¹, it was possible to analyse the relevant Skype messages and the defendant's contacts through his smartphone.

Technical analyses are important to substantiate victim statements with objective evidence. In a Belgian *loverboy* case²¹² linked to polycriminality, the images obtained from the computer backed up the statements of the victims and witnesses. This was also the case in several economic exploitation cases. In a case involving a riding school,²¹³ the police determined, following its investigation, that the internet advertisement for the job was connected to the email address of the defendant. In a construction case²¹⁴, the statement by the Pakistani victim substantiated his recruitment in Italy. An investigation of the victim's Facebook profile revealed that he communicated with the Turkish defendant about when he should come to Belgium to work for him.

In another Kurdish smuggling case in Bruges²¹⁷, a technical analysis of the iPhone enabled the police to identify a number of exact locations where the smuggler had visited. The individual in question had clearly gone from the French migrant camp in Calais through Belgian car parks to further abroad (The Netherlands, Barcelona, etc.). These elements of the investigation were included as evidence by the court in its judgement.²¹⁸

In a murder case linked to a Ukrainian smuggling case²¹⁹, the police were able to reconstruct their entire route chronologically, through a GPS tracking system in the truck of the murdered driver/smuggler. This tracking system was connected to a website which offered a wide range of control options: real-time tracking of the vehicle, the journey history of the vehicle, the locations and duration of stops, details regarding the fuel consumed, and instruments such as door opening, engine start-up, etc. The employer provided the password to the police. The places where the driver had stopped were searched by the police with Google Maps and plotted schematically. The technical report served as a basis for the questioning of the defendants.

3.2. | Chronology of the chosen route

Information regarding the chosen routes can provide relevant evidence. This is certainly the case with human smuggling. Trace²¹⁵ indicated geo-mapping²¹⁶ as an instrument in this respect.

210 MYRIA, 2015 Annual Report on Trafficking and Smuggling of Human Beings, *Tightening the Links*, case study, pp. 66-71.

211 Session of the Correctional Court of Ypres scheduled for 9 October 2017.

212 See also Part 3, Chapter 2, point 1.1. (Sexual exploitation case studies).

213 See also Part 3, Chapter 3 (case-law overview): Corr. Court Liege, 21 November 2016, 18th Chamber, and above Chapter 1, point 1 of this focus (the role of social media and the internet in human trafficking).

214 See also Part 3, Chapter 3 (case-law overview): Corr. Court East Flanders, subsection Dendermonde, 20 May 2016, Chamber G29w (definitive), and above Chapter 1, point 1 of this focus (the role of social media and the internet in human trafficking).

215 http://data.trilateralresearch.com/wp-content/uploads/2015/11/TRACE_D4.2_Role-of-Technologies-in-human-trafficking_Briefing-Paper_FINAL.1.pdf.

216 Geo-mapping: "is a visual and geographical representation of data. It resembles a geographical map with symbols containing various information. It may also contain detailed data, representing a sequence of events. The data used to create the map can be collected in various ways, including by applying GPS data to existing data". (Kantin, "Geo-mapping: an attempt at a definition", *Newtactics*, 29 October 2009).

217 MYRIA, 2011 Annual Report on Trafficking and Smuggling of Human Beings, *Beggars in the hands of traffickers*, case study, p. 116.

218 MYRIA, 2015 Annual Report on Trafficking and Smuggling of Human Beings, *Tightening the Links*, case-law overview, pp. 125-126; Corr. Court West Flanders, subsection Bruges, 2 April 2014 (upheld by the Court of Appeal): (see Myria website).

219 See also Part 3, Chapter 3 (case-law overview).

4. FINANCIAL INVESTIGATION

Social media and the internet can be a useful tool for financial investigations, both to track the criminal assets of suspects and to assess their unlawfully acquired assets. The analysis (see point 3. Analysis) already referred to the importance of social media messages regarding financial management on the part of the smugglers.

4.1. | Tracing criminal assets

In a Hungarian human trafficking case²²⁰ in Ghent, the police analysed the smartphone of a pimp and found photos of a house being renovated, on which basis they conducted an internet investigation which led to France.²²¹

The investigation in France led to a construction involving a company, and could not be continued due to the various additional letters rogatory, as this would have delayed the investigation. It is, however, a good example to use as a method of investigation in future cases.

4.2. | Assessing unlawfully acquired assets

In a Syrian human smuggling case²²², the police focused on the number of chat messages in order to assess the unlawfully acquired assets, using the number of persons smuggled by the smuggling organisation. The main defendant communicated with 769 people via Viber, WhatsApp, Skype and Facebook. After analysing

his smartphone, the police were able to trace some of the messages and link them to at least 291 victims of smuggling. Based on the case in question, the police knew that the average smuggling price per person was between €4,000 and €4,500, so a minimum amount could be calculated. The result of this calculation was €1,164,000.

5. COOPERATION WITH SOCIAL MEDIA COMPANIES

Europol²²³ advocates close cooperation between the judiciary and companies including Facebook and Google. The relevant EMN survey²²⁴ shows that various European countries have an informal cooperation agreement with private social media companies.

In Belgium, there are also agreements to cooperate in investigations of human trafficking and smuggling. This is evident from the case studies and our interviews. Template forms have also since been developed for the applications of magistrates, which are mostly filled in and require only certain details to be added. It is however Facebook which determines the opportunity-decision of any cooperation, which was also established by EMN²²⁵ in the fight against human

Informal cooperation agreements with social media companies exist in several EU countries.

²²⁰ MYRIA, 2015 Annual Report Human Trafficking and Smuggling, *Tightening the Links*, case study, pp. 69-71.

²²¹ An official report states (translation): "These last photographs were taken on 22 and 27-03-2013 and 25-04-2013. When we enter the corresponding coordinates (....) via Google Maps we come to a house in France,.... Striking resemblance, also the streetview photos of Google Maps show a house that is being renovated. It would be useful to find out who owns this property in France".

²²² This case was brought before the Correctional Court of Ghent on 4 September 2017.

²²³ EUROPOL, *Intelligence Notification 15/2014*, The Hague, October 2014. www.europol.europa.eu/publications-documents/trafficking-in-human-beings-and-internet: "LEAs (law enforcement agencies) will need to increasingly engage with partners in the private sector in order to improve investigative outcomes and preventative measures. The private sector is a crucial partner as traffickers rely on technologies and service offerings by companies to facilitate their activities. Contacts with social media companies or domain hosts will make investigations more effective."

²²⁴ EMN Inform, *The Use of Social Media in the Fight Against Migrant Smuggling*, September 2016: "As to cooperation with online service providers, only 7 out of 17 responding Member States (CZ, DE, EE, ES, FI, HU, UK) have some form of cooperation with online service providers to prevent and fight migrant smuggling, but in the majority of cases (CZ, DE, EE, ES), these are not formalised".

²²⁵ EMN Inform, *The Use of Social Media in the Fight Against Migrant Smuggling*, September 2016: "Service providers like Facebook, Twitter or Google have their own internal policy about shared content. In the case of Facebook, activities related to human smuggling are not allowed and Facebook has its own team of legal experts and law enforcements officers to make sure the rules of their platform are not breached, they primarily react to referrals from users of content deemed inappropriate, which they subsequently remove. Nevertheless, Facebook also indicated that the monitoring of content related to migrant smuggling is not always prioritised as compared to other crime areas, for example child pornography, and could be further improved".

smuggling. The application is made via a request for legal assistance through a liaison officer who acts as the central contact point for a given country. As such, the relevant Facebook profiles can be temporarily frozen, without the suspect noticing anything. This ensures that the person in question will no longer be able to delete his profile. This also applies to Instagram and WhatsApp, since these two applications are also owned by Facebook.

The Belgian cases show that it has been possible to request data from social media companies for a number of years already. In January 2015, the police involved in the Iraqi human smuggling case in Dendermonde informed the competent magistrate about the possibility of requesting information from Facebook: "*Facebook request order: We refer to the original official report which shows that we requested information about the open Facebook profile X. to be able to determine the possible place of residence of 'S'. They [another police unit] inform us that the following crucial information is visible via the open Facebook profile (...). For the sake of completeness, we inform you that a history of the logins on the relevant Facebook profile can be requested from Facebook within a certain period of time. In addition, you can also request the email address with which the Facebook profile was created. In a second phase, IP identifications can lead to specific addresses/ persons*".

As part of the tracing of telephone communications, the magistrate then served a petition to Facebook to obtain the identification and location of the suspected smuggler.²²⁶ The results of the Facebook investigation yielded important data which made it possible to identify the smuggler.²²⁷

Based on the cases, we find that there is cooperation with social media companies, such as Facebook, but there is still room for improvement. According to the EMN, various

problems arise, relating to the cumbersome procedure.²²⁸ Eurojust needs to try to standardise this.²²⁹

6. INTERNATIONAL COOPERATION

The use of social media and the internet has led to an international increase in the scale of the human smuggling and trafficking phenomenon. According to Europol²³⁰, this needs to result in improved international cooperation. Social media and the internet can be useful tools. Europol's internet referral unit has already proven its usefulness in the fight against human smuggling.²³¹

The EMN recommends that international bodies including Eurojust facilitate international cooperation by exchanging best practice.²³² We can go further here and request that this be structurally embedded in a future forum which stimulates the use of social media in international cooperation, and regularly exchanges best practice.

226 An official report states (translation): "My official is requesting the technical cooperation of Facebook in order to provide my official with the following information: in accordance with article 46bis of the Belgian Code of Criminal Procedure, to provide all available information concerning the person using the following account or pseudonym on the website www.facebook.com with the following two Facebook profiles: (...) the complete identification/registration data (including any linked numbers) of the user of the aforementioned pseudonyms; IP address/date/time/time zone of the creation of the accounts; a list of the available IP addresses with dates, times and time zone, used to consult these pseudonyms".

227 An official report states (translation): "The history data show that Facebook profiles were opened in at least the last 3 months on the Internet Service Providers (ISP) network in Belgium, the Netherlands, Germany, Sweden, Denmark and the United Kingdom.. The history data of both profiles are parallel (= within the same timeframes logged in on the networks of the same ISPs in the same countries), indicating that both profiles are used by the same person. The IP when logging in with the Facebook profile 'A' belongs to the Belgian ISP Skynet/Belgacom, which implies that this Facebook profile was created in Belgium. The GND shows that the number (...) linked to this Facebook profile appears to be linked to the Brussels memo (...) under the name C. This leads to the identification of the suspect 'S'.

228 Summary of EMN Ad-Hoc Query no. 1055 from 18 April 2016, *Addressing and preventing the use of social media in migrant smuggling*: "It is difficult to cooperate in this area due to the national legislation on privacy. Most online service providers have offices abroad which makes cooperation cumbersome. Cooperation is often slow and information can be lost because platforms can change rapidly. The procedures to access data once a request is submitted to providers are long.

229 EMN Inform, *The Use of Social Media in the Fight Against Migrant Smuggling*, September 2016: EMN recommends "Eurojust to help in streamlining legal assistance by facilitating discussions of best practice amongst judicial experts (...) contributing to the further development of streamlined cooperation with private (social media) companies, e.g. contributing to the elaboration of standard request forms, or by helping to streamline the current MLA system through standardised procedures and trainings".

230 EUROPOL, *Intelligence Notification 15/2014*, The Hague, October 2014. www.europol.europa.eu/publications-documents/trafficking-in-human-beings-and-internet: "Internet-facilitated trafficking takes place on a global scale, which complicates investigations. Effective information-sharing across multiple jurisdictions is of utmost importance for law enforcement agencies.

231 Europol, *EU Internet Referral Unit year one report: Highlights*, 22 February 2016: "According to its mandate, the EU IRU expanded its open source and Internet monitoring activities, in order to contribute to the disruption of illegal immigrant smuggling networks. The EU IRU has processed 122 accounts linked to illegal immigration upon request from the European Migrant Smuggling Centre (EMSC)". For more information on the IRU, see external contribution: "Presentation of the DJOC/i2 service in the fight against human trafficking: a supporting role in internet and social media investigations".

232 EMN Inform, *The Use of Social Media in the Fight Against Migrant Smuggling*, September 2016: EMN recommends "Eurojust to help in streamlining legal assistance by facilitating discussions of best practice amongst judicial experts on matters of procedure and international cooperation related to cyber-enabled crime aspects of migrant smuggling, in line with the Budapest Convention on Cybercrime, as well as the European Judicial Cybercrime Network".

In Belgium, some of these best practices have already been identified in the various cases. This was also briefly covered in the financial investigation, although there are other cases.

In a human trafficking case involving a Thai massage parlour, the police were able to ask additional relevant questions for an international rogatory commission, based on an internet investigation. Using this data, it was ruled²³³ that the internet shop of the travel agency in Thailand where the victims were recruited could be traced: (translation) "Using the IP address from which the mails of the travel agency 'T.C' were sent. it could be established through an international rogatory commission in Thailand that the travel agency 'T.C.' was found to be operating from a telephone and internet shop/travel agency in Bangkok, operated by the defendant and her husband".

In an Iraqi smuggling case²³⁴ in Dendermonde, the police traced a smuggler via a rogatory commission to the United Kingdom, and to this end used his Facebook profile in addition to telephone tapping data. Partly thanks to his profile picture, the smuggler in the UK could be clearly identified.²³⁵

233 See also Part 3, Chapter 3 (case-law overview): Corr. Court West Flanders, subsection Dendermonde, 11 October 2016, chamber. D19D.

234 See also Part 3, Chapter 2, point 2, (human smuggling case studies).

235 An official report states (translation): "The suspect under number 13 has not yet been identified. He is addressed with the call sign 'H' and: 'H. B', and has been active as a smuggler for at least 6 years. He is an Iraqi Kurd. He is staying at an unknown location in the United Kingdom. At the least, he has used the telephone numbers (...) and (...). He is a user of the Facebook nickname: H.B. via account (...). He was in contact with both the suspects in Belgium and the United Kingdom. In a short period of time, he has carried out various smuggling-related money transactions for the attention of the user of the number (...) under three different aliases, namely 'A.O', 'A.A', and 'A.M'. A similar investigation at the Home Office (comparable to the Immigration Office in Belgium) produced a positive result. For example, this man was formally identified as A. It was certain that he was the same person as the one on the profile picture of the Facebook account (...) used by: 'H'".

Chapter 3

Internet and social media: new challenges for policy, the police and the judiciary

This focus delves deeper into the various facets of the use of the internet and social media in the context of human trafficking and smuggling. Human traffickers now use the internet and social media constantly for recruiting and controlling victims, and also to manage their affairs. As we have seen, the police and the judiciary also use the internet and social media in their fight against traffickers and smugglers. Yet there is still a long way to go, and many obstacles.

The challenges in this respect should not be underestimated.

1. THE LEGAL FRAMEWORK OF THE METHODS OF INVESTIGATION AVAILABLE TO THE JUDICIAL AUTHORITIES

The first challenge relates to the legal framework of the methods of investigation which are available to the judicial authorities.

The legislative framework is always one step behind the ingenuity of criminals, or worse.

The legislative framework is always one step behind the ingenuity of criminals, or worse. Many of the provisions of our Code of Criminal

Procedure were no longer up to the task, compared with the rapid technological developments of recent years. As a result, the police and judiciary had fewer resources available to collect evidence in IT systems.

In the fight against terrorism, and in order to give magistrates and police investigators the resources appropriate to their time and the reality on the ground, the Minister of Justice presented a draft law to Parliament in July 2016. The draft law aims to complete Belgian law with regards to special investigation methods and certain investigative methods as regards the internet and telecommunications.²³⁶ The aim was to create a legal framework which is better suited for searches in IT systems. The new law was adopted in Parliament on 22 December 2016 and published in the Belgian Official Journal on 17 January 2017.²³⁷ Most of these new provisions entered into force on 27 January 2017.²³⁸

The latest major amendments in the area of investigative measures date back to 2000, with the law on computer crime.²³⁹ For example, this law introduced new investigation possibilities in the Code of Criminal

²³⁶ Draft law of 8 July 2016 on the improvement of special tracing methods and certain methods of investigation relating to the internet and electronic and telecommunications, *Doc. parl.*, Chamber, Session 2015-2016, Doc 54-1966/001.

²³⁷ Law of 25 December 2016 on various amendments to the Code of Criminal Procedure and the Criminal Code, with a view to improving the special tracing methods and certain methods of investigation relating to the internet and electronic and telecommunications, and establishing a database of voice prints, *BOJ*, 17 January 2017.

²³⁸ However, some of these amendments still require the approval of a royal decree before they can enter into force.

²³⁹ Law of 28 November 2000 on computer crime, *BOJ*, 3 February 2001.

Procedure, including the seizure of data in an IT system (Article 39bis)²⁴⁰ and network searches (Article 88ter).²⁴¹

The new law adapts these articles to the changing needs, by incorporating the content of Article 88ter into Article 39bis. This has become the reference article for *non-covert* searches in IT systems (a smartphone for example).²⁴²

As such, an officer of the judicial police (OGP) can now order a search in a confiscated computer system (a smartphone without access code, for example).²⁴³ However, it is up to the Public Prosecutor to order a search in an IT system which has not been confiscated, but which could be (a computer in a cybercafé or a bank for example, in which case the confiscation would be impossible or inappropriate).²⁴⁴ It is also the Public Prosecutor who can decide on a network search²⁴⁵ (for example, a search in the cloud, provided that the data is accessible without a new password).²⁴⁶ In the past, the investigating judge was competent in this respect. Both the search in an IT system and the search in a seizable carrier can only be performed after the external connections have been deactivated beforehand²⁴⁷ (for example, a smartphone must be switched to aeroplane mode). Likewise, the network search ordered by the Public Prosecutor is limited to the accessible parts only.²⁴⁸

Finally, any other non-covert search in an IT system can only be ordered by an investigating judge (for example, when access to the cloud has additional protection).²⁴⁹

For example, when interrogating a suspect in possession of a smartphone²⁵⁰, an immediate check of the device may be necessary. An officer of the judicial police (OGP) can decide in this respect, but only if access to the data does not require a password or a specific technical action, and if the smartphone is put in aeroplane mode. If an unlocking or technical action is required, the Public Prosecutor's approval is compulsory.

If the smartphone provides access to a Gmail or Facebook account and the user has saved his login and password in the device, the Public Prosecutor can order a network search. The external connections can therefore also be activated (i.e. the device is no longer in aeroplane mode) and searches may be made on the accounts that are accessible without a password. If, however, a login and password are not configured in the device, permission from an investigating judge is compulsory. The investigating judge will then be able to order the necessary operations to retrieve the codes, since passwords need to be entered to activate the external connections to search the accessible accounts.

Another situation occurs when access to non-accessible accounts is required. This then becomes a covert search for which the permission of an investigating judge is required (see below, amendments to Article 90ter).

The new law also introduces new methods of investigation into the Code of Criminal Procedure.

Examples include:

- interactions and infiltrations occurring exclusively on the internet ("digital" infiltration or "light" infiltration (new article 46sexies)). In this case, contacts via the internet are maintained with one or more persons, if necessary under a fictive identity. The conditions for such infiltration are more flexible than for 'physical' infiltration. Incidentally, this does not require an order from an investigating judge. Permission from the Public Prosecutor's office is sufficient.
- the surveillance operation (infiltration into an IT system (Article 46quinquies)).

Finally, Article 90ter, which regulates the conditions under which telephone wiretaps may be carried out, has also been radically amended. This article was originally drafted

240 This refers to data seizure, in contrast to the seizure of the IT carrier (a mobile phone or computer, for example). This is then a seizure of movable property within the meaning of Article 35 of the Code of Criminal Procedure. Data seizure refers to the copying of data on ad hoc carriers, if confiscation of the carrier is not desirable.

241 The investigating judge could order a search in an IT system or part of it. Under certain circumstances, this search could also be extended to an IT system or part of it, which is located in a different place from the one where the search is carried out (search within a network).

242 Article 39bis applies in the event that the smartphone holder refuses to give his consent.

243 New §2, paragraph 1, of Article 39bis of the Code of Criminal Procedure. E.g.: After a smartphone is set to aeroplane mode, an email will appear on the screen. The OGP is authorised to take a photo from the screen, but if he wants to click on it, etc., he no longer has the authority to do so.

244 Article 39bis, §2, paragraph 2 Code of Criminal Procedure.

245 Article 39bis, §3 Code of Criminal Procedure.

246 Report of the first reading within the Judiciary Commission of the draft law of 8 July 2016 on the improvement of special tracing methods and certain methods of investigation relating to the internet and electronic and telecommunications, *Doc. parl.*, Chamber, Session 2016-2017, Doc 54-1966/006, p. 5.

247 Article 39bis, §2, paragraph 3 Code of Criminal Procedure.

248 Article 39bis, §3, paragraph 2 Code of Criminal Procedure.

249 Article 39bis, §4. See also the report of the first reading in the Judiciary Commission of the draft law, *op. cit.*, Doc 54-1966/006, p. 5.

250 This example is quoted in the presentation by the specialised Chief Inspector General of the RCCU of Namur, H. COLIN, entitled "La saisie des données informatiques en pratique", during the seminar organised by the 'Centre de recherche information, droit et société' of the University of Namur (CRIDS): "Les méthodes d'enquête pénale dans le domaine des nouvelles technologies", on 12 May 2017.

with conventional telephony in mind, and was only applicable to communications and telecommunications during the transmission. In the internet age, the article therefore needed to be adapted to communications on the information superhighway.²⁵¹ Except on telephones, covert searches and wiretaps may now be carried out on e-mails, Skype, Whatsapp, Facebook, Snapchat, etc. The list of violations for which the measure in Article 90ter can be applied has been extended (wiretap list). Human trafficking and smuggling were already on this list, but the measure has since been extended to 'simple' human trafficking and smuggling, whereas aggravating circumstances were required in the past.²⁵²

This law is undoubtedly a breakthrough in a world in which technology is rapidly evolving, and it clearly offers new opportunities for investigation. However, there are also points of criticism. The amendments made appear to go far beyond mere modernisation.²⁵³ For example, actors from the judicial (investigating judges and lawyers²⁵⁴) and academic worlds²⁵⁵, as well as human rights associations²⁵⁶ and members of parliament²⁵⁷, have made various observations which raise questions. The shift of the powers of the investigating judge, an independent and impartial judge, to the Public Prosecutor's Office, which is party to criminal proceedings, without real judicial control, the higher risks of violating the right to privacy²⁵⁸ and the right to a fair trial²⁵⁹ are the main criticisms of the new law. Moreover, the 'Liga voor de mensenrechten' (League of

Human Rights) and *La Ligue des Droits de l'Homme* have lodged an appeal for annulment with the Constitutional Court.²⁶⁰

2. THE (INTERNATIONAL) COOPERATION WITH OPERATORS AND PROVIDERS

A second challenge is the (international) cooperation with, inter alia, operators and providers.

One of the problems is that communications made in Belgium pass through service providers who are officially established abroad. As the Minister of Justice has pointed out, "The problem of territoriality has become particularly complex with the development of new technologies and social media".²⁶¹ Moreover, the Code of Criminal Procedure only addresses this issue of territoriality to a limited extent when determining the conditions for the application of each investigative measure, since this is in principle governed by international law.²⁶²

In addition, the EU Member States have highlighted various difficulties in their cooperation with social media and internet providers, in particular in the area of preventing and combating human smuggling: difficult cooperation due to national privacy laws; service providers with headquarters abroad, leading to cumbersome and bureaucratic cooperation; slow cooperation and lost information due to platforms which can change rapidly; lengthy procedures to obtain access to the data, once a request has been submitted.²⁶³

251 Explanatory memorandum to the draft law of 8 July 2016 on the improvement of special tracing methods and certain methods of investigation relating to the internet and electronic and telecommunications, Doc. parl., Chamber, Session 2015-2016, Doc 54-1966/001, p.7.

252 This measure is referred to in Article 90ter, §2, 22° (human trafficking) and §2, 37° (human smuggling).

253 M. KEITA, "De wet bijzondere opsporingsmethoden: een delicate evenwicht", (The special tracing methods law: a delicate balance) *TvMR*, (Human Rights Journal) 2017, nr. 1, p. 12.

254 See in this respect the paper by E. BROCKMANS: "Minister wil opsporings- en onderzoeksbeleid op internet versterken" (Minister wishes to strengthen tracing and investigation policy on the internet), *De juristenkrant* (Jurists' Journal), 28 September 2016, no. 334, p.11, and the report of the first reading within the Judiciary Commission of the draft law of 8 July 2016 on the improvement of special tracing methods and certain methods of investigation relating to the internet and electronic and telecommunications, *Doc. parl.*, Chamber, Session 2016-2017, Doc 54-1966/006, pp. 33-34 and 56-57.

255 The risks of possible derailment and lack of sufficient control were already highlighted during the seminar organised by the CRIDS on 12 May 2017, which dealt with the: 'méthodes d'enquête pénale dans le domaine des nouvelles technologies'.

256 See also the hearings with the representatives of the "Liga voor mensenrechten" and the "Ligue des droits de l'homme" during the examination of the draft law in the Chamber (report of the first reading within the Judiciary Commission, *op. cit.*, Doc 54-1966/006, pp. 67-74).

257 See also the report of the first reading in the Judiciary Commission of the draft law, *op. cit.*, Doc 54-1966/006, p. 8-9 and 12-15.

258 It should be borne in mind that this fundamental right is guaranteed by Article 8 of the European Convention on Human Rights (ECHR) and by Article 22 of the Constitution.

259 This right is guaranteed in particular by Article 5 of the ECHR.

260 Docket number 6711.

261 Explanatory memorandum to the draft law of 8 July 2016 on the improvement of special tracing methods and certain methods of investigation relating to the internet and electronic and telecommunications, *op. cit.*, Doc 1966/001, p. 10.

262 *Ibid.* These include the Budapest Convention on Cybercrime of 23 November 2001 of the Council of Europe, and Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 on the European Investigation Order on criminal matters, *OJ.*, L130 of 1 May 2014, p. 1. For example, Article 31 of this Directive provides for a specific system of interception of communications, depending on the location of the person to whom the interception relates, and depending on the State, where the person to whom the interception relates may or may not need technical assistance.

263 European Migration Network, Summary of EMN Ad-Hoc Query n° 1055 from 18 April 2016, point 3.4.

Many of the actors surveyed indicated a positive cooperation with various such operators (such as Facebook), but this is far from being the case for all of them. Moreover, there is no truly formal framework for cooperation in this area.²⁶⁴ In Belgium, for example, the Judiciary needed to intervene on various occasions, in order to oblige certain operators to cooperate. Indeed, in a judgement of 18 January 2011 concerning the company Yahoo, the Court of Cassation ruled that the duty to cooperate applied to 'any person providing electronic communications services, including the transmission of communication data', and that the obligation to cooperate laid down in Article 46*bis* of the Code of Criminal Procedure is not limited to operators of an electronic communications network or providers who provide their electronic communications services only through their own infrastructure.²⁶⁵ As such, a provider of an electronic communications service can also be considered as 'the person offering a service consisting in allowing customers to obtain, receive or disseminate information via an electronic network'.

The new law of 25 December 2016 is a breakthrough in this respect, as it gives effect to this case law in various provisions. For example, companies providing an internet service within Belgian territory must cooperate with the Belgian judicial authorities within the context of the measures, with the aim of identifying a service or subscriber (Article 46*bis*) detecting communications (Article 88*bis*) or intercepting communications or covert searches in an IT system (Article 90*ter*). The obligation of cooperation therefore also applies to operators of electronic communications networks and providers of electronic communications services, in particular "any person who makes or offers a service, in any way whatsoever, within Belgian territory, consisting of transmitting signals via electronic communications networks or allowing users to obtain or receive or disseminate information via an electronic communications network".²⁶⁶

Moreover, during the examination of the draft law in the Chamber, the Minister of Justice pointed out that "any internet service offered within Belgian territory must comply with Belgian law, including the enforcement of judicial decisions regarding access to data".²⁶⁷ However,

he also pointed out that there is a need for comprehensive European regulation in this area.²⁶⁸

The need for more efficient and faster international mutual legal assistance was also highlighted.²⁶⁹

In addition, it is advisable to pursue cooperation with private social media operators, in order to initiate a dialogue on best practice in the fight against, and prevention of, human trafficking.²⁷⁰

The sharing of best practice in the area of cooperation between national bodies, social media and other service providers should also be encouraged.

Finally, the private companies managing social media should recognise (some already do) that perpetrators of human trafficking and smuggling make use of their platforms. These companies should therefore take measures to implement proposals and technologies which tackle human trafficking, including, for example, the online reporting mechanism on Facebook.²⁷¹

3. THE RESOURCES OF FRONT-LINE SERVICES

A third challenge relates to the resources of the front-line services. In the context of cooperation with Europol, the creation of a support service such as the IRU²⁷² is undoubtedly a positive development. However, front-line services are still insufficiently equipped for dealing with the internet and social media: obsolete computers, un-

²⁶⁴ *Ibid.*

²⁶⁵ Cass. Court, 18 January 2011 (Decision available at www.juridat.be): (translation) "This obligation also applies to anyone providing a service consisting wholly or mainly of transmitting signals over electronic communications networks".

²⁶⁶ See article 46*bis*, §1, 2° Code of Criminal Procedure (identification).

²⁶⁷ Report of the first reading within the Judiciary Commission of the draft law of 8 July 2016 on the improvement of special tracing methods and certain methods of investigation relating to the internet and electronic and telecommunications, *op. cit.*, Doc 54-1966/006, p. 4.

²⁶⁸ *Ibid.*

²⁶⁹ Among other people, Professor V. FRANSEN emphasised this point in his speech on 30 October 2015 in the context of the: "Middagen van het recht" (Legal afternoons) organised by the FPS Justice on the theme: "Internet en nieuwe technologieën: welke nieuwe middelen voor de opsporings- en vervolgingsautoriteiten". (The Internet and new technologies: what are the new means for the investigating and prosecuting authorities?).

²⁷⁰ In this sense: H. WATSON and others, *Report on the role of current and emerging technologies in human trafficking*, Deliverable 4.1., TRACE project, p. 79 (available at: <http://data.trilateralresearch.com>).

²⁷¹ *Ibid.*, p. 80.

²⁷² In July 2015, the Justice and Home Affairs (JHA) Council, composed of the Ministers of Justice and Home Affairs of all EU Member States, decided to set up a new unit within Europol: the EU-IRU (Internet Referral Unit). Each country, including Belgium, has set up a national contact point. See *below*, in this respect, the external contribution: "Presentation DJSOC/I2 in the fight against human trafficking: supporting role in internet and social media investigations".

trained police officers, etc. It would certainly be useful and appropriate to invest in information technology, and provide the necessary financial and human resources.

In this context, specific on-the-job training is envisaged.

The front-line services are not yet sufficiently equipped to deal with the internet and social media.

Moreover, the departments involved in economic exploitation should also be better trained on internet monitoring (as regards online job advertisements, for example).²⁷³

4. SCIENTIFIC INVESTIGATION

A final challenge relates to scientific investigation.

It should be possible to fund internet and social media-related investigations, when these are used for human trafficking and smuggling. In the context of the fight against human trafficking, it is important to continue gaining insight into the role of the internet and new technologies, and their use. However, little in the way of scientific information is available at the present time. For example, a comparative scientific study on the role and impact of social media and the internet could be carried out, as a source of objective evidence for the judiciary.

²⁷³ In this sense, see H. WATSON and others, *op. cit.*, p. 80.



External contribution: Presentation DJSOC/i2 in the fight against human trafficking: supporting role in internet and social media investigations

Alain Luypaert
Police Commissioner
Head of Department

The Internet Investigation Unit of the Directorate of Serious and Organised Crime - **DJSOC/i2** was set up as part of the optimisation of the services of the Federal Police (2014) and was extended with the 'Kanaalplan' (Canal Plan).²⁷⁴

In July 2015, the Justice and Home Affairs (JHA) Council, composed of the Ministers of Justice and Home Affairs of all EU Member States, decided to set up a new unit within Europol: the EU-IRU (*Internet Referral Unit*). The activities of this unit are as follows:

- The coordination of searches on the internet for content related to terrorism, violent radicalism and human trafficking and smuggling, and the coordination of its removal.
- Operational support to national units;
- Strategic analysis and assistance in prevention;
- Coordination and awareness-raising in the area of R&D (Research and Development);

Since January 2016, on the initiative of the Minister for Home Affairs, the BE-IRU unit has been part of DJSOC/i2, which is now called **DJSOC/i2-IRU**. As part of the operationalisation of the 'Canal Plan', the Minister for

Home Affairs decided to increase staff within the service in February 2016.

In November 2016, the Ministries of Justice and Home Affairs officially designated the **i2/BE-IRU** service as the Reference Unit and single national and international contact point for the removal of hate content - 'Hate Speech - Hate Crime' - on the internet, but also other illegal content, covering all phenomena, including human trafficking.

The service currently consists of 21 persons: A Commissioner - Head of Department, Chief Inspector and 19 inspectors. Via Mobility, new staff will shortly reinforce the team. The aim is to recruit 33 members of staff in total.

The responsibilities of the **DJSOC/i2-IRU** unit in the area of terrorism are to search the internet, transmit reports to the relevant units, submit proposals for the removal of content to Europol, which along with the OTT Providers, acts as a contact point. These tasks are carried out on the basis of cumulative criteria defined by the Plan R - Radicalism:

- The entity minimises and/or justifies the use of coercion or force;
- The entity disseminates its own objectives to third parties through specific operations or channels (propaganda).
- The entity poses a threat to democracy and/or seeks to destroy or dismantle the democratic system.

For all kinds of hate messages (racist, homophobic, xenophobic, religious or sexual remarks) the **IRU** either searches the internet autonomously, or receives elements from various sources (integrated police services, the magistrates, UNIA, national or international partners, etc.). The investigative work focuses mainly on content related to Belgium.

Once the evidence has been established and recorded, the unit identifies the author - if necessary, the magistrates are called upon - and draws up an official report against him. As a reference unit, it also requests the providers directly to remove the content, based on non-compliance with the Code of Conduct.

When searching the Internet, the **i2/BE-IRU** unit also provides support to the investigation units in the context of judicial orders, in particular to the entities responsible for the cases falling under the National Security Plan (NSP), including human trafficking and smuggling, to carry out investigative work for online and freely-available content.

²⁷⁴ The 'Canal Plan' is the action plan against: "radicalisation, violent extremism and terrorism in the canal zone" and comprises seven municipalities in Brussels, the territory of Laeken (the Brussels-City entity), Sint-Gillis, Anderlecht, Molenbeek, Koekelberg, Sint-Joost and Schaerbeek, and Vilvoorde in the outskirts. Among other things, this plan envisages the strengthening of the police forces in this area, and includes a section for the investigation and identification of associations through which propaganda is disseminated and/or which are responsible for the recruitment and shadow financing of these associations and of hate preachers.

The **i2/BE-IRU** unit does not operate autonomously and only operates when requested. In this context, the unit actively participated in the investigation following the attacks in Zaventem and Brussels.

With regards to human trafficking, the unit has already been called upon to investigate possible instances of sexual exploitation. Our services do not always have to intervene in critical situations, in which a person may be exploited. Sometimes the investigative work carried out can help resolve certain cases. A concrete example where the service has provided assistance is the following:

The service was called in for the case of a minor from an EU country who was suspected of having travelled through Belgium before being forced into the Belgian prostitution milieu. We were asked to find traces of her stay in Belgium, to check whether the person in question had stayed in Belgium voluntarily and what she had done here. As such, we were able to identify two men, and move the investigation forward.

The open source investigation consisted of analysing the data available on various social media: Facebook, Instagram and Twitter.

In the case of minors, the investigation revealed the following elements:

a) Facebook

- She has a public Facebook account in her name, and has 1,781 friends;
- In Belgium there was a link, with the Facebook page of a nightclub which she had 'liked';
- The photos, likes and comments on her Facebook account were investigated, but nothing alarming was found;
- Via Facebook, no link could be established between this minor and the two men.

b) Instagram

- Her Facebook account showed that she also had an Instagram account;
- After a check, we were able to establish that she did indeed have an Instagram account, which was also public;
- She has 12 photos and 744 followers on this account. She follows 1,272 other Instagram accounts herself;
- One of her followers is one of the two men (P.) involved, who also has an Instagram account himself;
- However, no link could be established between his Instagram account and that of the other man (V.).

As regards the first man (P.), the investigation revealed the following elements:

a) Facebook

- He has a public Facebook account in his name, and has 152 friends;
- He has many contacts with the other man (V.);
- After examining the photos and pages which he "liked", two nightclubs of a sexual nature were identified.

b) Instagram

- Via the minor's Instagram account, 'P' could be identified as one of her followers. He himself has an Instagram account in his name;
- He has 346 photos and 334 followers on this account. He follows 281 other Instagram accounts himself;
- His account contains a link to one of the nightclubs with a sexual nature on his Facebook page. Given the number of hashtags, he appears to be very active in terms of this nightclub, which is located in an EU country. Moreover, it appears that he has recently been in the country in question;
- His account also contains various photos showing him with large sums of money and drugs, as well as confirmation that he purchased two new mobile phones for an amount of €2,258.

As regards the second man (V.), the investigation revealed the following elements:

a) Facebook

- He has a Facebook account in his name, and has 110 friends, including the other man (P.);
- He is not friends with the underage girl;
- He is often tagged on the photographs of a Belgian company specialising in graphic design;
- He is tagged on a photo of the first man (P.): it is the same photo as the one which appears on the Instagram account of P., during the purchase of the two mobile phones;
- The investigation into this man's profile did not reveal anything suspicious.

b) Instagram

- He has an Instagram account. However, it is apparently a private account;
- Nonetheless, we can see that he has placed 60 posts/photographs on it, that he has 38 followers and that he

follows 688 people.

c) Twitter

- He has a Twitter account, but his last tweet dates from 2014.

d) LinkedIn

- Subsequent investigation shows that this man also has a LinkedIn profile, in which he presents himself as a businessman.

The results of these analyses have been passed on to the relevant departments for further investigation.

In the area of human trafficking, our service therefore supports the services that call on us for a particular aspect of an investigation, namely investigative work and analysis on the internet.



External contribution: Refugees: When human smuggling becomes human trafficking

Melita H. Sunjic.

*Head of the "Communicating with
Communities" team*

UNHCR²⁷⁵

Law books make a clear distinction between the definition of human smuggling and human trafficking, the former being a voluntary transaction between the provider of an (illegal) service and a paying client, while the latter involves deception and violence, and pertains to the transport or detention of persons against their will by criminals. If we look at mixed migration flows towards Europe in practice, however, it quickly becomes apparent that there is no binary distinction between the two phenomena but a continuum which always involves elements of both. There is no smuggling without moments of coercion, and conversely, elements of voluntary cooperation can be found between traffickers and victims. The smuggling industry, once established on a certain route, is hungry for profits and will resort to trafficking methods to secure them.

The observations described in the text are based on the following:

- Interviews and discussions within focus groups with hundreds of asylum seekers and refugees, conducted by the author and her team over the past four years, in the countries of origin, transit and destination;
- Systematic assessment of the interviews between asylum seekers and refugees on open social media platforms;²⁷⁶
- Briefings by UNHCR colleagues in the field and journalistic sources.

Key terms and definitions

There are a number of key definitions explaining the terms "Trafficking in Human Beings" and "Smuggling of Migrants":

The Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children (UNTOC) supplementing the United Nations Convention Against Transnational Organised Crime (UNTOC)²⁷⁷ specifies that "'Trafficking in persons' shall mean the recruitment, transportation, transfer, harbouring or receipt of persons, 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 or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs".

According to the Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the UNTOC ('Protocol against the Smuggling of Migrants'), "Smuggling of migrants" shall mean the procurement, in order to obtain, directly or indirectly, a financial or other material benefit, of the illegal entry of a person into a State Party of which the person is not a national or a permanent resident.

Migrant smuggling affects almost every country in the world. It undermines the integrity of countries and communities, and claims the lives of thousands of people every year.

Obviously, there are overlaps between the two forms of organised criminal activities related to migration. According to UNTOC, there are three main differences between human trafficking and the smuggling of migrants²⁷⁸:

²⁷⁵ The author is an employee of the UNHCR. The views expressed here are those of the author and not necessarily those of the United Nations.

²⁷⁶ www.unhcr.org/publications/brochures/5909af4d4/from-a-refugee-perspective.html.

²⁷⁷ www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCbook-e.pdf.

²⁷⁸ www.unodc.org/lpo-brazil/en/trafico-de-pessoas/index.html.

Consent

The smuggling of migrants, while often undertaken in dangerous or degrading conditions, involves migrants who have consented to the smuggling. Trafficking victims, on the other hand, have either never consented or, if they initially consented, that consent has been rendered meaningless by the coercive, deceptive or abusive actions of the traffickers.

Exploitation

Smuggling ends with the migrants' arrival at their destination, whereas trafficking involves the ongoing exploitation of the victim in some manner to generate illicit profits for the traffickers. From a practical standpoint, victims of trafficking also tend to be affected more severely and to be in greater need of protection from re-victimization and other forms of further abuse than are smuggled migrants.

Transnationality

Human smuggling is always transnational, whereas trafficking may not be. Trafficking can occur regardless of whether victims are taken to another State or only moved from one place to another within the same State.

How does trafficking and smuggling relate to asylum seekers and refugees?

Even though "Everyone has the right to seek and to enjoy in other countries asylum from persecution" (Article 14: Universal Declaration of Human Rights), in practice tight visa regimes, restrictive asylum policies and strict border controls make it nearly impossible for refugees to access the territory of the EU without using the services of smugglers.

Whether a person is in need of international protection is unrelated to the way s/he entered the country of asylum. Smuggled as well as trafficked persons must have access to fair and efficient asylum procedures, in order to establish if the claimant has a well-founded fear of persecution linked to one or more of the 1951 Convention grounds: for reasons of race, religion, nationality, membership of a particular social group or political opinion. Having been trafficked does not constitute a claim to asylum per se, but victims

of trafficking may qualify for international protection if their country of origin is unable or unwilling to provide protection against further re-trafficking or serious harm as a result of traffickers' potential retaliation.²⁷⁹

With 65.6 million people forcibly displaced people worldwide²⁸⁰, the largest number in the history of humankind, it is hardly surprising that a minority of them is trying to come to Europe. (Currently, 84% of all refugees and internally displaced persons remain in the developing world, and only 16% move to industrialized countries.) Consequently, international criminal networks see lucrative business opportunities and move in, adapting their modus operandi. As a result, the common definitions are not up-to-date, as they do not fully reflect today's realities and newly emerged phenomena:

- Very present in today's mixed migration movements is the repeated alteration between smuggling services and trafficking methods during the same journey.
- Unsuspecting clients of a smuggler might find themselves taken hostage by the smugglers themselves or be kidnapped by various militias who prey on people along smuggling routes. They would then be subject to torture and mistreatment for the purpose of extorting a ransom from relatives at home. Sometimes, victims are even traded between different trafficking groups.
- Smugglers who do not get paid as much as they ask for or who increase the price during the journey, might kidnap the client or a family member at home in order to get the requested amount.
- The smugglers are interested in getting their clients to their destination quickly, as they will only get fully paid upon completion of the journey. They will therefore use violence against clients who have a change of heart and want to return home, or who refuse to put themselves in danger by mounting an overcrowded boat or squeezing into suffocating spaces in vehicles.

²⁷⁹ www.fmreview.org/peopletrafficking/floor.html.

²⁸⁰ www.unhcr.org/fr/apercu-statistique.html.

Case study: A smuggling industry emerges

UNHCR's case study (*From a Refugee Perspective*²⁸¹) clearly demonstrates through social media sources that the smuggling industry is a demand-driven business. If there are potential clients, it emerges at breathtaking speed. And, more importantly, once a major smuggling network with its considerable infrastructure is in place, it expects profits from paying clients. When client numbers dwindle, this is initially compensated by "special offers" and low prices to entice potential customers. In such cases, we can still talk of **smuggling** networks. However, when marketing becomes more aggressive and smugglers start luring clients with false promises, deceit and coercion, it morphs into **trafficking**.

When analysing the social media discourse on asylum and migration related issues in Arabic between March and December 2016, UNHCR could demonstrate how the smuggling industry developed and professionalized within months after legal possibilities for refugees to reach Europe via the Western Balkans route had been closed. The level of sophistication and complexity of smuggling offers found on Facebook in Arabic language dramatically increased between March and July 2016, indicating that experienced cartels moved in and took over the business.

In early 2016, our researchers found posts on Facebook indicating the presence of opportunistic local money making schemes. Offers were put forward by individuals who would sometimes identify themselves as Syrians, Moroccans and Pakistanis, as well as Turkish citizens. Most of them operated from Izmir, more precisely around Basmane Square. Potential clients in search of smugglers informed each other on Facebook that smuggling agents could be found in streets and cafés of certain Turkish cities. Apparently, local criminals and businessmen seized the opportunity to make money by offering life vests and accommodation in coastal cities, as well as boat rides to Greece on cheap dinghies, and sometimes on their private yachts or fishing boats.

Smuggling offers during that time seemed amateurish and experimental. For example: on Sunday, 27 March 2016, there were several Facebook announcements of direct ship connections on commercial cargo vessels from Turkey to Italy, but on Monday they were all cancelled. Short-lived, bizarre offers of transfer appear and disappear: by Jet Ski or in plastic containers which would be towed behind

boats submerged under water. Impracticable routes for Europe were being promoted, e.g. from hard to reach Albania to Italy, others even via Latin America and the Caribbean.

In spring 2016, access to Europe became difficult for refugees and migrants. The humanitarian corridor which, in preceding months, allowed refugees and migrant easy access via Greece, Serbia, Hungary (later Croatia and Slovenia) to Austria and Germany was shut down. On 9 March, the President of the European Council, Donald Tusk, declared the Western Balkans route closed. On 18 March, the EU concluded a deal with Turkey to stop the influx to Europe across the Aegean Sea, boosting the demand for more sophisticated smuggling services.

Already in April 2016, professionals started moving in. The number of smugglers' accounts on Facebook increased every day. Their pages were mostly set up as closed groups, requiring interested clients to identify themselves before seeing the content. By the end of April, regular tourist and student visas from various European consulates were on offer, indicating that criminal networks had established links to corrupt officials.

In the beginning of May 2016, a vast number of smugglers posted offers for various routes to Europe on Facebook, mostly departing from Turkey. Such offers comprised flights, boat rides, road trips and guided treks on foot or combinations thereof. This implied that a growing number of persons worked in the smuggling business and that the networks had at their disposal collaborators at ports, airports, borders crossings, etc.

Smuggling advertisements usually included the names (or aliases) and full telephone numbers of contact persons. Detailed negotiations between smuggler and client were not openly conducted on Facebook but through private communication channels. Enquiries by clients were removed quickly from Facebook pages, so as not to leave too much of an electronic trail.

Over the following months, European politicians and media kept debating whether all borders would remain closed, whether the EU-Turkey deal would collapse or not. Meanwhile, smugglers tried to calm down fears of refugees and migrants that they might get stuck in Turkey and/or Greece. On Facebook, they encouraged potential customers to keep coming as they have ways to get people to Europe. One smuggler even had the audacity to post the slogan "Keep coming. Only legal borders are closed".

By the end of May 2016, Facebook was full of visa offers for numerous Schengen and non-Schengen countries in Europe. Tourist visas, student visas and fake marriages

281 www.unhcr.org/publications/brochures/5909af4d4/from-a-refugee-perspective.html.

could be bought. Tourist visas, student visas and marriages of convenience were offered for sale.

The first stolen passports were on sale in June 2016, showing the existence of international cooperation between persons who steal ID documents in various countries and those who sell them, mostly in Turkey.

As of July 2016, forged passports, diplomas, driving and marriage licenses could be bought from providers on Facebook. A full-fledged transnational criminal network was at work.

Apparently, competition was high and profits were dwindling by August 2016: for the first time, smugglers on Facebook named and shamed rivals who had allegedly cheated clients out of their money. At the same time, they downplayed the dangers of irregular movement. They called their trips “safe” and “100% guaranteed” while people kept losing their lives drowning at sea or suffocating hidden in tiny spaces in vehicles.

Different routes - Different dangers

The way to Europe is becoming increasingly difficult as a general rule, but there are major differences as to the level of danger travellers are exposed to. Each route has characteristic moments where smuggling degenerates into trafficking and smugglers endanger the lives of their clients in their greed for profit.

Afghans

Afghan refugees and migrants usually book an “all-inclusive” trip from a major city in Afghanistan or Iran all the way to a destination country in Europe. They travel in groups of mostly young and minor males and are accompanied by handlers called “uncles”. Travellers completely rely on the instructions and guidance provided by these “uncles” as they often have no notion of the geographical, cultural or political circumstances on route or at the destination, and they rarely speak any foreign language.

The local smuggling agent normally changes from country to country. The young Afghans are dependent on their services regarding food, water, accommodation and transportation and, thus, vulnerable to mistreatment and exploitation, including sexual abuse.

The most dangerous stretches of the journey are the Afghan-Iranian border areas, where border guards shoot to kill, as they do not distinguish between drug traffickers and people being smuggled. In order to avoid contact with the authorities, smugglers load their clients on pickup trucks and drive by night, off-road, without lights and at neck-breaking speed. If accidents occur, injured people are left behind.

The next critical leg of the journey is the crossing of the Van mountain range between Iran and Turkey that the migrant groups and their guides normally pass on foot, by night, without the necessary gear and in all weather conditions. Here, too, if someone is injured or too exhausted to move on, they will be left behind.

The most dreaded stretch is the Aegean Sea. Although it is a relatively short trip, Afghans, coming from a landlocked country and mostly unable to swim, are terrified. As such, it is quite common that they refuse to board overcrowded dinghies to cross to a Greek island. Such last-minute debates are dangerous for the smuggling agent.

To maximize their profits, smugglers push far too many persons on the boats and do not care much about weather conditions. They are interested in sending off the vessels as quickly as possible in order to avoid being detected by police, and they only get paid when the customers arrive. As such, they often threaten people with knives or fire arms.

In interviews, UNHCR heard of cases where the travellers or their families could not pay the full amount asked by the smuggler. In such incidents, it is not uncommon that either the traveller or a family member at home in Afghanistan is taken hostage until the smuggler is fully compensated.

Syrians and Iraqis

Both on the Western and Central Mediterranean routes, smugglers use force during embarkation. They need as many people as possible to enter the boats as quickly as possible and do not allow them to change their minds at the last minute (see above). They do not refrain from using violence to make this happen. Delays in departure decrease the profit rate and increase the danger of detection by law enforcement.

Eritreans and Somalis

Eritreans and Somalis are two groups that run the highest risk of becoming Victims of Trafficking (VOTs) during their attempts to reach Europe. Trafficking agents prey on young people in Somalia, Ethiopia and Sudan, looking for potential clients at typical youth congregation points such as schools. They promise gullible teenagers that they will take them to Europe for little or no money and paint a rosy picture of the riches and comforts awaiting them there. Most young people leave in a clandestine manner without informing their parents.

Once they cross into another country, the traffickers show their true colours. They start brutally torturing and abusing their victims and send proof of their suffering to the families back home in order to extort a ransom. Sometimes they threaten to remove the victims' organs if the money is not paid in time. These threats are underpinned by phone calls during which the victim is being tortured and screams for help or their ordeal is recorded on sound files and videos posted on social media. Prices range from a few thousand dollars up to a few tens of thousands of dollars.

When hostages get traded between different criminal networks, prices go up. It might also happen that during a journey a person is taken hostage multiple times in succession, especially in Libya where many armed groups operate. During incarceration, victims are regularly tortured and raped by their captors, receive little food and water and live under incredibly unhygienic conditions.

Those whose families cannot pay are sold into slavery and forced prostitution.

There are luckier travellers who deal with smugglers rather than outright traffickers. The dangers they are exposed to are of a different nature: travellers are transported across the desert on the backs of trucks. During the trip, they might fall off the truck, get sunstroke, be dehydrated, or fall ill. In these cases, the smuggler leaves them behind in the desert. The testimonials UNHCR collects²⁸² show that women regularly get raped.

Once they arrive at the coast, they often have to wait many days, even weeks for their departure. During this time, they are kept locked in remote industrial buildings, with little food and water and under deplorable hygienic circumstances. Again, sometimes the guards turn violent and abuse their hostages physically and sexually. Embarkation onto vessels follows the same patterns of violent smuggler behaviour as described above.

West Africans

Migrants and refugees from West Africa can move freely within the ECOWAS area, using public transport to get to the city of Agadez in Niger, where the Sahara Desert begins. In order to cross this stretch and get to the Libyan coast they need to commission the services of smugglers who are easily contacted in the streets.

Bringing people and goods across the Sahara has been the main source of income for some of the local families for hundreds of years. Currently, they offer such services to migrants and refugees heading for Europe. Danger is mostly looming on the Libyan side, where armed groups can take the travellers hostage to extort ransom and the same pattern emerges as described for Somalis and Eritreans in the previous paragraph.

Nigerian women

There is one particular group that stands out however, these are Nigerian women, mostly from Edo State and its capital city Benin, who are trafficked to become sex workers in Europe. In their case, it is not smuggling that turns bad, but it is trafficking from the start.

The women know from the beginning that they will be forced to do sex work in European brothels for several years in order to "pay back" the transportation costs incurred by the trafficker. These young women are not forced to come along but conclude an agreement with their traffickers that is often reinforced by religious ceremonies. After that the agreement becomes binding and the women have to follow the orders of their traffickers. Sex work sometimes already starts on route. ID papers are taken from the women and they cannot leave or breach the contract without serious repercussions for themselves and their families at home. This is how ordeals start that may last for many years in a spiral of violence, exploitation and dangerous work.

Few women find the strength to break out. They lack experience, means of sustenance and they believe breaching the contract will endanger themselves and the lives of their families at home. Also, their legal status and right to residency in Europe is uncertain.

282 www.tellingtherealstory.org.

Interaction between smugglers and clients on social media

Target audience	Somalis and Eritreans	Syrians and Iraqis	Afghans	West Africans
Social media use pre-departure	some	yes	no	some
Social media use en route	yes	yes	some	too expensive, rather text messages
Social media use upon arrival	yes	yes	yes	yes

Syrians and Iraqis are most active: Smugglers offer their services on social media (Instagram and Facebook), but business deals are negotiated on closed channels.

Afghan smugglers offer their services directly and on social media. Often travel agencies have a legitimate business and some illegal offers on the side. No negotiations are done on social media.

Smugglers get in touch directly with Somalis and Eritreans to recruit clients. However, when they are taken hostage, the trafficker's sometimes use social media, sometimes mobile phones to get in touch with the families. Families sometimes use social media to raise funds for paying the ransom.

Smugglers for the West African route rarely use social media at this point in time, but this might change soon as the use of mobile phones and smart phones is growing fast in the region.

Solutions must be global and comprehensive

In the past years, Europe has tried to stem the influx of asylum seekers by closing its borders, tightening border controls and making regular access to EU territory nearly impossible. Such measures proved to be short-sighted. Tackling refugee flows at their tail end rather increases the dependency of refugees on ever-growing international smuggling cartels.

Europe needs to understand and address the root causes of forced displacement and the drivers of onward movement. In December 2016, UNHCR presented a paper to the European Union calling for a far-reaching reform of Europe's global engagement with refugees.²⁸³

Asylum policy should not start at European borders but should engage with countries of origin in order to prevent and resolve conflict. In countries of first asylum and transit the EU should support measures to stabilize refugee populations and offer them protection closer to home. In addition, UNHCR is calling for a more efficient asylum system within Europe, and for legal pathways for refugees to enter EU territory.

When presenting this paper in Brussels, UN High Commissioner for Refugees Filippo Grandi stressed that Europe can develop comprehensive solutions, drawing "on its history of tolerance, openness and protection principles".

²⁸³ Better Protecting Refugees in the EU and Globally: www.refworld.org/pdfid/58385d4e4.pdf.