

Deel 2: Focus

De rol van sociale media en internet bij mensenhandel en mensensmokkel

Sociale media en het internet worden steeds meer gebruikt door mensenhandelaars en smokkelaars in hun wervingsproces voor criminele doeleinden, maar ook voor de marketing van hun aanbod en het beheer van hun criminele activiteiten. Aan de andere kant worden het internet en sociale media ook gebruikt om de strijd tegen mensenhandel en mensensmokkel te vergemakkelijken.

Deze focus geeft eerst een overzicht van het fenomeen van de rol van sociale media en het internet in mensenhandel en -smokkel, alvorens te onderzoeken hoe internet en sociale media fungeren als onderzoeksmethode. We gaan ook kort in op de nieuwe uitdagingen waar beleid, politie en justitie op dit gebied voor staan.

Dit deel bevat ook bijdragen van externe auteurs:

- Het hoofd van de dienst internetonderzoek van de Directie van de bestrijding van zware en georganiseerde criminaliteit van de federale politie werpt zijn licht op zijn ondersteunende rol in het onderzoek op het internet en sociale media;
- Het hoofd van het team "Communicating with Communities" van UNHCR maakt een aantal observaties over de bestaande grijze zone tussen mensenhandel en mensensmokkel, met name gebaseerd op een studie uitgevoerd door haar afdeling.

Inleiding



Dit deel analyseert het gebruik van internet en sociale media bij mensenhandel en -smokkel op de verschillende niveaus. Het internet is de laatste 10 jaar in alle facetten van de maatschappij doorgedrongen. In vele landen is het een belangrijk onderdeel van het formele onderwijsstelsel geworden, waardoor kinderen er vroeger mee in contact komen. We leven in een wereld die door technologie bepaald wordt en die blijft evolueren. Deze ontwikkeling brengt een myriade aan mogelijkheden en opportuniteiten met zich mee. Dat moeten we toejuichen. Naast het drempelverlagend effect voor onderwijs, biedt het mensen tal van platformen om te communiceren en deel uit te maken van groepen die de sociale cohesie bevorderen. Helaas worden digitale media ook gebruikt voor mindere fraaie doeleinden. Het medium vergemakkelijkt o.a. mensenhandel en -smokkel. Sociale netwerksites en geclassificeerde websites worden steeds vaker gebruikt door mensenhandelaars en -smokkelaars in hun wervingsproces voor criminele doeleinden, en in de handel en uitbuiting van mensen. Aan de andere kant vergemakkelijkt internet en sociale media als onderzoeksmethode de bestrijding van mensenhandel en mensensmokkel.

Internet en sociale media geven gebruikers de mogelijkheid om contacten te leggen en te communiceren met individuen, en een groter publiek van op afstand te bereiken. Mensenhandelaars en mensensmokkelaars zijn op deze manier ook in staat om een groter aantal slachtoffers over nationale grenzen heen te bereiken en uit te buiten.¹¹ Het internet heeft ook een drempelverlagend effect.¹² De anonimiteit van het platform stelt mensen in staat om via een simpele muisklik te zijn wie ze willen zijn. Daarbij komt dat het internet de bewijslast van criminele feiten moeilijker vast te stellen maakt.

11 M. LATONERO, *Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds*, 2011, p. 12. Geraadpleegd van <https://ssrn.com/abstract=2045851>.
12 D. MUIR, *Violence against Children in Cyberspace*, ECPAT International, 2005, pp. 25-29. Geraadpleegd van www.ecpat.net/ei/Publications/ICT/Cyberspace_ENG.pdf.

Als inleiding tot dit hoofdstuk is het belangrijk enkele begrippen te verduidelijken.

Digitale mensenhandel en -smokkel valt onder de noemer cybercriminaliteit. Cybercriminaliteit is een zeer breed concept met betrekking tot onwettige handelingen gepleegd met behulp van, of door middel van computers, computernetwerken, het internet en op het web gebaseerde informatie en communicatietechnologie.¹³ Op 23 november 2001 werd door de Raad van Europa het cybercriminaliteit verdrag (verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Engels: Convention on Cybercrime), ook wel het cybercrimeverdrag of verdrag van Boedapest genoemd), ondertekend. Het werd door 38 landen ondertekend en omvat het opsporen en bestraffen van computercriminaliteit.¹⁴ Deze wetgeving heeft betrekking op computerfraude, hacking, en het bezitten en verspreiden van kinderpornografie etc. De landen die het verdrag hebben ondertekend hebben een samenwerkingsovereenkomst om cybercriminaliteit op te sporen, gezien de handelingen vaak grensoverschrijdend zijn.

Onder de term internet valt eveneens het begrip **darknet**. Het darknet verwijst letterlijk naar de duistere kant van het internet. Het is een gecodeerde wereld van verborgen en anoniem aangeboden en genoten diensten of uitwisselingen, waarbij dus gebruikers niet kunnen worden opgespoord of geïdentificeerd. Het is geen apart fysiek netwerk, maar een onderdeel van het World Wide Web. Het is een onderdeel van het internet dat door zoekmachines zoals Google, Bing, Yahoo etc. niet geïndexeerd kan worden.¹⁵ Het darknet is een verzameling van netwerken en technologieën die worden gebruikt om digitale inhoud te delen. Het wordt gebruikt voor de verkoop van drugs, wapens en kinderpornografie. Magistraten en politiemensen die we interviewden zien hier weinig activiteit van mensenhandelaars, zoals het EU-project Surf and Sound¹⁶ ook vaststelde, zodat we hier niet verder op ingaan. Volledigheidshalve verwijzen we wel naar het Europees project Trace¹⁷ (Trafficking as

13 E. MCLAUGHLIN & J. MUNCIE, *The sage dictionary of criminology* (3^e ed.), Londen, Verenigd Koninkrijk: Sage, 2013, pp. 112-114.

14 Jura, België ratificeert Cybercrimeverdrag, 2012. Geraadpleegd van 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. Geraadpleegd van 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 maanden (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.

a criminal enterprise) dat refereert naar artikels¹⁸ die melding maken van websites van vrouwenhandel binnen het darkweb.¹⁹



Sociale netwerksites zijn platformen en diensten die gebruikers de mogelijkheid bieden om een netwerk op te bouwen of connecties te maken. Dit kan aan de hand van het delen van berichten en inhoud met medegebruikers. Het gebruik van sociale media is de laatste jaren exponentieel toegenomen, zowel bij jongeren als bij volwassenen.²⁰ Men creëert een onlinegemeenschap waar mensen over de hele wereld kunnen netwerken met allerhande organisaties en individuen met specifieke doeleinden. Deze sites zijn zeer populair door de voordelen die ze bieden, zoals het snel en eenvoudig leggen van contacten. Keerzijde van die faciliteit is het verspreiden van valse gegevens zoals valse identiteit, de online intimidatie en stalking etc.²¹

Tenslotte is het bronnenmateriaal voor deze focus gebaseerd op dossieranalyses, informele interviews met magistraten en politiemensen, en literatuurstudie. Het behandelt achtereenvolgens een overzicht van de rol van sociale media en internet in mensenhandel en mensensmokkel (hoofdstuk 1), internet en sociale media als onderzoeksmethode (hoofdstuk 2) en ten slotte, de nieuwe uitdagingen voor het beleid, politie en justitie op dit gebied (hoofdstuk 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>; Zie bv. 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/gjdply?permcode=gjdply; "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. Geraadpleegd van www.sibm.edu/assets/pdf/samvad2.pdf#page=18.

Hoofdstuk 1

Fenomeenschets

In haar situatierapport van 2016 schrijft Europol: “Door de globale ontwikkeling van online infrastructuren is internet voor mensenhandelaars cruciaal geworden en het belang van dit instrument zal in de toekomst enkel maar toenemen. Online interactie vergemakkelijkt bepaalde aspecten van mensenhandel en uitbuiting: het identificeren van potentiële slachtoffers, toegang tot persoonsgegevens, de organisatie van de logistiek en het transport, het ronselen via sociale media, discussiefora en andere websites, advertenties van slachtoffers, de uitbuiting en de controle ervan.”²²

In deze fenomeenschets, een eerste aanzet, gaan we slechts in beperkte mate in op de impact van internet en sociale media op mensenhandel en mensensmokkel. We focussen ons vooral op de wijze waarop mensenhandel-

en mensensmokkelnetwerken sociale media en internet als instrument inzetten. Omwille van hun verschillende dynamiek behandelen we mensenhandel en mensensmokkel apart.

Internet en sociale media zijn een efficiënt rekruteringskanaal waarmee mensenhandelaars op anonieme wijze en op een grotere schaal hun mogelijke slachtoffers kunnen bereiken

1. DE ROL VAN SOCIALE MEDIA EN INTERNET BIJ MENSENHANDEL

Mensenhandelaars gebruiken sociale media en internet voor de rekrutering van slachtoffers, de marketing van hun prostitutieaanbod en het management van hun criminele activiteiten.²³ Momenteel wordt dit vooral bij seksuele uitbuiting vastgesteld. Daarnaast onderzoeken we hoe de slachtoffers omgaan met sociale media.

In de dossiers stellen we vast dat de belangrijkste instrumenten Facebook, chat forums van seksdatingsites, Viber, Whatsapp, Skype en andere internetplatformen zijn.

1.1. | Rekrutering van mensenhandelnetwerken

Internet en sociale media zijn een efficiënt rekruteringskanaal waarmee mensenhandelaars op anonieme wijze en op een grotere schaal hun mogelijke slachtoffers kunnen bereiken.

Europol stelt: “Het ronselen van slachtoffers gebeurt steeds vaker online. Mensenhandelaar lokken slachtoffers met veelbelovende advertenties voor jobs of reizen die op algemene advertentiesites verschijnen of die via au

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 mei 2014.

pair-bureaus, internationale huwelijksbureaus of dating sites worden verspreid.”²⁴

In verschillende dossiers waarin Myria zich burgerlijke partij stelde, kon Myria constateren hoe slachtoffers gerekruteerd worden via een aanbod voor een job of prostitutiewerk of via de *loverboymethode*. Dit kan zich afspelen in het herkomstland, een transitland of het bestemmingsland. Meestal verloopt dit via Facebook of andere internetplatformen. Volgens sommige magistraten kan tijdens het verloop van de rekruteringsfase ook Snapchat gebruikt worden. Daarbij wordt een compromitterende screenshot genomen tijdens een video-gesprek of chat of vrijwillig doorgestuurde foto's als chantagemiddel ingezet worden.

1.1.1. | Jobs

In het verleden werden verschillende slachtoffers gerekruteerd via een jobaanbod als danseres, serveerster, hostess, schoonmaakster, kinderoppas of als huishoudhulp, enz. en werden ze nadien tot prostitutie gedwongen. Dit is nog steeds het geval, maar hiervoor worden nu ook sociale media en internet ingezet.

De federale politie schreef reeds in haar externe bijdrage over mensenhandel en internet in ons jaarrapport 2010: “Rekrutering met het oog op seksuele uitbuiting gebeurt niet noodzakelijk via expliciete sites, maar eerder via sites met zoekertjes voor jobs. Communicatie verloopt onder andere via discussiefora waar berichten kunnen worden gepost en informatie uitgewisseld zonder daarom te weten wie aan de andere kant van het scherm zit.”²⁵

Internet

Malafide modellenagentschappen rekruteren slachtoffers via hun internetsites. In een nog lopend gerechtelijk onderzoek kon vastgesteld worden dat jonge meisjes, waaronder minderjarigen, in hun herkomstland hadden gereageerd op zogenaamde internetadvertenties voor modellenwerk, en uiteindelijk in België tot prostitutie aangezet werden. Het modellenbureau van het herkomstland maakte als ronselaar een belangrijk onderdeel uit van het internationale prostitutienetwerk

dat haar slachtoffers uitbuitte in West-Europese landen, waaronder België.

In een Antwerps-Lets dossier²⁶ van 2010-2011 rekruteerde een malafide modellenbureau online naast Letse ook Belgische meisjes. Op de website stond vermeld: “De mooiste modellen van de Benelux voor uw catwalk modeshows en de promotie van uw producten. Onze modellen zijn beschikbaar aan € 200 per werkuur voor catwalk, fotoshoots, hostessenwerk, model presence, begeleidingsopdrachten,...” De meisjes kregen onmiddellijk na hun reactie en bij hun eerste gesprek een voorstel om als escorte te werken met de belofte maandelijks tussen de € 4.000 en € 6.000 te verdienen waarvoor ze twee dagen per week moesten werken. Een Belgisch meisje getuigde aan de politie: “Ik ben een meisje van 18 jaar en mijn vriendin is 17 jaar van buitenlandse afkomst die de taal niet beheerst. Zelf ben ik van Belgische afkomst. Wij hebben enkele weken geleden een man leren kennen op het internet. Hij heeft ons een job aangeboden als privé-escorte in Antwerpen centrum. Nadat we hem hebben ontmoet zijn we direct aan de slag gegaan als escorte. Wij willen zo snel mogelijk stoppen, maar kunnen hier niet zomaar stoppen of weggaan. We worden namelijk op alle mogelijke manieren bedreigd door hem en gechanteerd met onze naaktfoto's en in lingerie en dergelijke.”

Een Lets slachtoffer in dit dossier werd zelf gecontacteerd na een eigen internetadvertentie voor werk. Ze verklaarde: “In Letland woonde ik bij mijn ouders, had gestudeerd, zocht werk en plaatste zelf een jobadvertentie op het internet voor werk in de horeca. Ik werd gecontacteerd door beklagde X, de echtgenote van de hoofdbeklaagde, die me werk beloofde in een restaurant. Enkele dagen later telefoneerde ze, en excuseerde zich dat ik niet in een restaurant maar wel in een escortbureau moest gaan werken als gezelschap. Ik moest de klanten enkel gezelschap houden in een restaurant, theater, enz., en hoefde geen seksdiensten te leveren. Dit zou me maandelijks een paar duizend euro opbrengen. Ik stemde toe en vertrok.”

Facebook

Mensenhandelaars gebruiken daarnaast Facebook om hun slachtoffers te rekruteren via jobaanbiedingen. In een Luiks dossier²⁷ van 2012 getuigde een Belgisch slachtoffer dat ze via een vals Facebook profiel benaderd werd voor een job als hostess. Een van de mannelijke beklagden

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

25 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2010, *Sociale fraude bestrijden is mensenhandel voorkomen*, p. 115.

26 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2015, *Schakels verbinden*, dossieranalyse, pp. 73-75.

27 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2015, *Schakels verbinden, rechtspraak*, pp. 110-111.

had voor de rekrutering van slachtoffers speciaal een vals profiel opgesteld waarbij hij zich had voorgedaan als een vrouw met een valse profielfoto. De man ronselde online jonge meisjes of sprak ze aan op straat. Meestal richtte hij zich tot jonge meisjes zonder ervaring in het prostitutiemilieu, die hij rekruteerde op basis van hun uiterlijk. Naast deze mannelijke ronselaar was er ook nog een vrouwelijke beklagde die zich bezighield met het ronselen. Ze legde via sociale media zoals Facebook

de eerste contacten met de jonge meisjes. Ze stelden hen een job voor in de evenementen business of als escorte, waarmee ze veel geld zouden verdienen, en stuurde de meisjes dan door naar de hoofdbeklaagde. Deze organiseerde

Mensenhandelaars gebruiken daarnaast Facebook om hun slachtoffers te rekruteren via jobaanbiedingen.

bij het eerste gesprek een fotoshoot en manipuleerde hierbij de meisjes tot ze bereid waren tot seks. Daarnaast had de hoofdbeklaagde met zijn escortbureau ook een internetsite waarmee hij slachtoffers rekruteerde, en hen onmiddellijk bij hun eerste gesprek na de fotoshoot voor zijn website als een soort van selectieprocedure aan een 'test' onderwierp.

Economische uitbuiting

Slachtoffers van economische uitbuiting kunnen ook gerekruteerd worden via advertenties op het internet maar dit kan ook via sociale media.²⁸ Volgens een rapport van HEUNI²⁹ nemen internetadvertenties en daarnaast gedeeltelijk ook Facebook meer en meer de plaats in van de krantenadvertenties en gaan de sollicitanten zelf actief op zoek op het internet.³⁰ Een studie van een Europees project over de rol van sociale media en internet bij mensenhandel (Surf and Sound) verwijst naar online advertenties in Roemenië voor jobs in de horeca door spookfirma's of in de landbouwsector in een ander EU-land zoals Spanje die tot uitbuiting leiden.³¹

In België werden in een Bulgaars dossier³² uit de transportsector de arbeiders door advertenties in de krant of op internet naar België gelokt, waar zij voor een Bulgaarse transportfirma zouden werken. Ze zouden veel geld verdienen maar deze belofte werd niet nagekomen.

In een Chinees dossier³³ uit de horecasector reageerde een Chinees slachtoffer op een Belgische internetadvertentie van een firma van de Chinese hoofdbeklaagde. Zijn Chinese kennissen in België hadden hem via Facebook attent gemaakt op deze internetadvertentie.

In een dossier van maneges³⁴ werd een Marokkaan in onwettig verblijf als stalknecht aangeworven nadat deze gereageerd had op een internetadvertentie voor deze job in België. Het contactadres voor deze internetadvertentie was het emailadres van de hoofdbeklaagde.

In bouwdoosiers werden de slachtoffers via internetadvertenties voor bouwvakkers gerekruteerd. In een bouwdoosier met schijnzelfstandigen³⁵ werden de slachtoffers geronseld in Bulgarije en Bosnië. In een bouwdoosier met gedetacheerden³⁶ werden de Poolse en Oekraïense slachtoffers geronseld in Polen waar de zogenaamde bouwfirma actief was.

1.1.2. | Prostitutie

Sommige jonge vrouwen zoeken ook zelf vrijwillig werk in de prostitutiesector en kunnen in een uitbuitingssituatie terecht komen. Ze contacteren zelf internetwebsites van escortbureaus of laten hun telefoonnummer achter op een Facebookadres van een contact dat ze kennen uit de prostitutiesector. Ze hebben soms reeds ervaring maar zoeken een betere werkplek waar ze meer geld kunnen verdienen.

Facebook

Sociale media kunnen een relevant instrument zijn om jonge vrouwen te contacteren met een voorstel voor

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

29 HEUNI is het Europese regionale instituut binnen het netwerk van het drugs- en misdaadagentschap van de Verenigde Naties (UNODC). HEUNI functioneert onder de auspiciën van het Finse Ministerie van Justitie als een onafhankelijk onderzoeks- en beleidsinstituut.

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 maanden (02.11.2014 - 01.11.2016), Surf and Sound, Nationaal verslag Roemenië, 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 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, dossieranalyse, pp. 92-95.

33 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, dossieranalyse, pp. 98-100.

34 Zie verder deel 3, hoofdstuk 3 (rechtspraak): Corr. Luik, afdeling Luik, 21 november 2016, 18^{de} k.

35 Zie verder deel 3, hoofdstuk 3 (rechtspraak): Corr. Limburg, afdeling Tongeren, 9 februari 2017, 9^e k.

36 Zie verder deel 3, hoofdstuk 3 (rechtspraak): Corr. Oost-Vlaanderen, afdeling Gent, 1 februari 2017, k.G29w.

prostitutiewerk. Volgens Europol worden ook vrouwen in chatrooms benaderd door mensenhandelaars.³⁷

In een Gents dossier³⁸ van 2013-2014 legde een Hongaars slachtoffer uit hoe ze in Hongarije gerekruteerd werd: “Ik maakte kennis via Facebook met een man, X. genaamd, die ik als P. leerde kennen. We schreven meermaals naar elkaar. Hij kwam van mij te weten dat wij in armoedige omstandigheden leefden. Het kwam ter sprake dat ik als prostituee wou werken. Hij vertelde dat hij daarbij kon helpen, hij zou mij geld geven voor de reis, hij zou het werk daar organiseren. Hij vertelde dat ze in België, in Gent in de vitrine zou moeten staan, en de mannen van de straat naar binnenlokken en zich prostitueren.” Uit later onderzoek van de Facebook profielen bleek dat de beklaagden op basis van een fictieve identiteit valse Facebook accounts aanmaakten om hun slachtoffer te rekruteren. De beklaagden gebruikten Facebook ook als selectiemiddel bij de rekrutering van de slachtoffers. Ze plaatsten de foto's van de meisjes die met hun voorstel instemden op hun Facebook profiel en stuurden de foto's naar mekaar door om ze te vergelijken. Uit de telefoontap bleek dat de verdachten regelmatig hun Facebook pagina raadpleegden om de geplaatste foto' van meisjes te bekijken en te beoordelen.

In een Brussels dossier³⁹ kreeg een Braziliaans slachtoffer in Italië via Facebook het voorstel van een Portugese beklagde om in België in de prostitutie te werken op basis van een zogenaamde helft/helft winstverdeling. Ze moest zich naakt laten fotograferen en deze foto's werden tegen haar expliciete wil op een Brusselse website voor seksdates geplaatst.

Facebookvariant

In het Antwerpse dossier (zie boven) kregen Letse jonge vrouwen via een socialenewebsite voor sekscontacten het voorstel om in de prostitutie te werken. Draugiem.lv is een Letse variant van Facebook waarbij de geïnteresseerde vrouw klikt op een boodschap van vriendschapsverzoek en dan positief reageert. De hoofdbeklaagde had speciaal een prostituee ingeschakeld om de meisjes te benaderen en te overtuigen om als escort in België en Nederland te werken. Ze ging hierbij actief op zoek naar meisjes met een draugiem.lv profiel en benaderde hen met valse financiële beloftes. Uiteindelijk verdienden ze heel weinig

omdat hun geld werd afgenomen, en werden ze zwaar mishandeld.

Datingsites

In Bulgarije gebruiken mensenhandelaars dezelfde technieken. In het reeds geciteerde EU-project Surf and Sound werden verschillende magistraten, politie, mensenhandelaars, slachtoffers en NGO bevestigd. In het Bulgaarse landenrapport verwijzen de auteurs naar een interview met een Bulgaarse mensenhandelaar: “Volgens de bevestigde persoon, ronselt hij voortaan enkel meisjes die zich zelfstandig prostitueren en daarom speurt hij datingsites af waar hij er regelmatig ontmoet: “We bezoeken regelmatig dating sites (Elmaz, Twoo, Gepime, etc.). Ik leg vooral via Elmaz en Facebook contact met meisjes. Ik doe me [sic] voor als een man die op zoek is naar gezelschap en probeer voorzichtig te zijn maar het zijn uiteindelijk zij die duidelijk maken dat ze uit zijn op seks tegen betaling.” (Sekshandelaar)”

De bevestigde persoon liet weten dat de meisjes die via deze sites worden geronseld, voor mensenhandel in het herkomstland worden gebruikt. Meisjes die het slachtoffer zijn van internationale vrouwenhandel worden via Tinder geronseld. Zij die zich daar hebben geregistreerd spreken minstens twee Europese talen en de opbrengsten die zij genereren zijn twee keer zo hoog als die in het land van herkomst. Of ze nu via Facebook, dan wel via datingsites worden gerekruteerd, de communicatie verloopt altijd via private chats, later dan via toepassingen zoals Skype of Viber, of rechtstreeks via gsm's.⁴⁰

1.1.3. | Loverboy

In de *loverboymethodiek* staat de rol van de sociale media centraal als middel van eerste contact met de slachtoffers. Bepaalde internetsites kunnen ook een nuttige rol vervullen bij de rekrutering van de *loverboys*.

Facebook

Loverboys maken zowel minderjarige als meerderjarige slachtoffers maar vooral minderjarigen zijn kwetsbare prooien op de sociale media. Door de digitalisering krijg je zeer veel informatie op Facebook. Minderjarigen geven zich gemakkelijk bloot op deze websites en delen

37 EUROPOL, Intelligence Notification 15/2014, Den Haag, Oktober 2014: www.europol.europa.eu/publications-documents/trafficking-in-human-beings-and-internet.

38 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2015, *Schakels verbinden*, dossieranalyse, pp. 66-70.

39 Corr. Brussel, 22 september 2016, 47^e k. (niet gepubliceerd).

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 maanden (02.11.2014 - 01.11.2016), Surf and Sound, Nationaal verslag Bulgarije, 2017. www.csd.bg/artShow.php?id=17951.

Vooraf minderjarigen zijn kwetsbare prooi op de sociale media.

er hun hele leven. Aan de hand van deze informatie kunnen mensenhandelaars zich richten op kwetsbare meisjes. Het is een vorm van sociale engineering waarbij de mensenhandelaars zich aanpassen op maat van de behoeften en wensen van het slachtoffer. De rol van de hobby's zal hier een belangrijke rol spelen. Wanneer het meisje een paardenliefhebster is zal de *loverboy* zich ook als dusdanig presenteren. Met een zoekfunctie op Facebook kunnen ze bijvoorbeeld zich ook specifiek richten op slachtoffers uit jeugdininstellingen. In de volgende fase gebruiken ze mobiele apps zoals WhatsApp en Viber om rechtstreeks contact te leggen.⁴¹

In een Leuvens prostitutiedossier⁴² werd vastgesteld dat de *loverboys* via Facebook in Roemenië contact hadden gelegd met de slachtoffers, hen gerekruteerd, en nadien in België uitgebuit. In een Antwerps dossier⁴³ van *loverboys* met minderjarigen uit jeugdininstellingen werden de slachtoffers ditmaal in België met Facebook gerekruteerd. Op de vraag hoe ze met prostitutie begonnen was, antwoordde de minderjarige tijdens haar verhoor: "Via een ex-vriendje die ik op Facebook heb leren kennen. Hij is het die me op de online forumsite voor seksdates gezet heeft. Hij heeft me naar de klanten gereden." De *loverboy* zette ook een minderjarig slachtoffer aan om enkele Facebookvriendinnen, eveneens minderjarige weglopers, met hem via Facebook in contact te brengen om ze nadien seksueel uit te buiten.

Internet

Loverboys kunnen ook actief naar slachtoffers op zoek gaan bij de modellensites. Dit zijn populaire websites voor jonge meisjes die op eigen initiatief hun kandidatuur voor modellenwerk stellen. Ze moeten op de site zichzelf presenteren en een foto posten. Sommige meisjes denken dat ze meer kans hebben door een meer uitdagende foto te posten. Op deze laatste doelgroep richten *loverboys* zich om ze trachten te verleiden.

Skype

Loverboys speuren daarnaast via Skype naar willekeurige kwetsbare potentiële slachtoffers. Concreet kan een jongere zich op Skype online zetten met een bepaalde spreuk of gezegde. *Loverboys* spelen hierop in door gericht te zoeken naar meisjes met bepaalde spreuken waaruit blijkt dat ze zich niet goed in hun vel voelen en kwetsbaar zijn. Daarop zal hij ze benaderen en trachten te rekruteren via de *loverboy*methodiek. Dikwijls denkt het slachtoffer dan dat ze haar *loverboy* bij toeval ontmoet heeft op Skype.

In een ander Antwerps dossier⁴⁴ van *loverboys* met minderjarigen uit jeugdininstellingen werden de slachtoffers naast Facebook ook met Skype gerekruteerd. Hier verklaarde een veertienjarig meisje dat ontvlucht was uit een jeugdinstelling, dat ze bij *loverboys* beland was nadat ze een van hen 'per toeval' had leren kennen via Skype. Ze praatten elke dag met elkaar en hij maakte haar verliefd, ze kon er niet aan weerstaan. Hij is haar op een avond in Verviers op café komen bezoeken en heeft haar dan meegenomen naar Antwerpen. In haar getuigenis sprak ze over de zware geweldplegingen die ze nadien moest ondergaan.

Instagram

Een studie van het EU-project Trace⁴⁵ (Trafficking as a criminal enterprise) over internet, sociale media en mensenhandel verwees naar een case in de VS waarbij een model door mensenhandelaars gerekruteerd werd via Instagram. Het krantenbericht meldde onder de titel 'Florida model naar New York gelokt op Instagram en gedwongen seks slaaf te zijn' hierover samengevat als volgt⁴⁶: "Vrouw in Florida, pas begonnen als model, werd gecontacteerd via Instagram. De man complementeerde haar over haar foto's, en nodigde haar met valse beloftes uit naar New York, waar hij op termijn voor haar en haar kinderen zou zorgen. Met de bijkomende belofte haar reisonkosten te vergoeden met 150\$ kwam ze dan inderdaad af. Bij aankomst sloot hij haar zonder eten op in een hotelkamer, waarna een vrouwelijke compagnon haar naar verschillende andere hotels bracht om zich onder doodsb bedreigingen te prostitueren."

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 maanden (02.11.2014 - 01.11.2016), Surf and Sound, Nationaal verslag Roemenië, 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.

42 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2015, *Schakels verbinden*, dossieranalyse, p. 29; Jaarverslag Mensenhandel 2013, *Bruggen slaan*, pp. 17, 60 en 108; Corr. Leuven, 4 juli 2013, 17^{de} k. (beschikbaar op www.myria.be).

43 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, rechtspraak, p. 134.

44 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, pp. 81-83.

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.

1.2. | Marketing van mensenhandelnetwerken

Voor hun marketingactiviteiten maken mensenhandelaars gebruik van websites om hun prostitutiediensten te promoten. Prostitutie verloopt tegenwoordig vooral via het internet en de sociale media. Vele vrouwen die zich achter ramen bevinden, gaan zich ook via het internet prostitueren.

Raamprostitutie lijdt onder de concurrentie van het internet. Twintig jaar geleden moest je op zoek gaan aan de hand van de krantenadvertenties of naar de bekende prostitutiestraten gaan. Nu speelt zich dit af van achter de computer. Op het internet kan je ook alle categorieën van prostituees vinden, aan alle prijzen. De chiquere escortes hebben aparte websites en doen dit niet via 'seksdating' websites. Deze escortes mikken ook op een specifiek soort klanten die in bepaalde milieus vertoeven.

Websites

In de reeds vermelde dossiers adverteerden de mensenhandelaars hun slachtoffers met hun foto op de website van hun escortbureau. In het Antwerpse modellendossier gaf de beklaagde die verantwoordelijk was voor de fotoshoots van de slachtoffers, ook toe dat hij foto's van een Lets minderjarig meisje op het internet had geplaatst om te adverteren voor zijn eigen escortbureau.

In een Nigeriaans dossier⁴⁷ werkten de Nigeriaanse beklaagden samen met de uitbaters van een prostitutiehotel. Het Nigeriaans slachtoffer verklaarde: "Uit het door uw diensten gevoerde onderzoek blijkt dat er foto's van mezelf online staan op de site 'X'. U vraagt mij wie deze foto's genomen heeft en wie deze online gezet heeft? Deze foto's werden genomen door de uitbaatster van het hotel en werden door haar online gezet."

In Thaise massagesalons wordt ook reclame gemaakt via hun websites en de internetadvertenties van de meisjes hierop.⁴⁸

Online advertentiesites

In een Oekraïens dossier⁴⁹ werden de slachtoffers door kennissen als danseres of dienstvergoers en gefotografeerd. Hun seksueel getinte foto's werden door de uitbaters onder meer op een Brusselse online advertentiesite gezet waar naast ver/huur van vastgoed, jobaanbiedingen, muzieklessen, babysit, vakantiehuizen, verkoop computers enz... ook een speciale dienstverlening voor escortes aan klanten aangeboden wordt. Bij de beklaagden werd een USB-stick gevonden met verschillende foto's van slachtoffers waarvan verschillende niet-geïdentificeerde personen nog online moesten geplaatst worden.⁵⁰ Daarnaast werden sommige slachtoffers als masseuse gerekruteerd en kwamen ze op een escortsite terecht.

Voor hun marketingactiviteiten maken mensenhandelaars gebruik van websites om hun prostitutiediensten te promoten.

In een Luiks escortdossier⁵¹ werden verschillende Thaise slachtoffers door middel van schuldbinding gerekruteerd en hun foto's op een gelijkaardige Belgische online advertentiesite geplaatst. Twee Roemeense slachtoffers werden ook op dergelijke sites geplaatst maar ook op escortsites.

Online forumsites voor seksdates

In een *loverboy*dossier met een rapper⁵² en hetzelfde Nigeriaans dossier gebruikten de beklaagden online forumsites voor seksdates waarop ze adverteerden met de gegevens en de foto van het prostitutieslachtoffer. Een van de Nigeriaanse beklaagden nam sexy fotootjes van slachtoffers, maakte een persoonlijk profiel aan op deze site voor de seksafspraken van het slachtoffer met de klanten. Volgens een Nigeriaans slachtoffer had de beklaagde het bij haar als volgend geïntroduceerd: "Mama' zei me ook dat ze een nieuw systeem had om te werken: ze zou mijn foto op het internet zetten, samen met een gsm-nummer, zodat ik zelf mijn afspraken zou kunnen regelen." Naast de Nigeriaanse netwerken gebruiken ook de *loverboys* deze internetsites veel om seksdates te regelen met hun slachtoffers en hun klanten.

Het zijn heel interactieve internetsites met een groot marktaanbod van seksadvertenties. De klanten kunnen contact leggen met Facebook, Twitter en email. Er is

47 Zie verder deel 3, hoofdstuk 3 (rechtspraak): Corr. Brussel Nederlandstalig, 28 maart 2017, 60^{de} kamer (definitief).

48 Zie verder deel 3, hoofdstuk 3 (rechtspraak): Corr. West-Vlaanderen, afdeling Dendermonde, 11 oktober 2016, k. D19D; MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, rechtspraak, p. 136; Corr. Brussel, 46^e Kamer, 27 januari 2016.

49 Zie verder deel 3, hoofdstuk 3 (rechtspraak): Corr. Brussel, 14 juli 2016, vakantiekamer.

50 Zie verder hoofdstuk 2 van dit focus (onderzoeksmethoden).

51 Zie verder deel 3, hoofdstuk 3 (rechtspraak): Corr. Luik, afdeling Luik, 16 november 2016, 19^{de} k. (beroep).

52 Zie verder deel 3, hoofdstuk 3 (rechtspraak): Corr. Antwerpen, afdeling Antwerpen, 21 september 2016, k. AC8.

een online forum waarop de klanten hun commentaren kunnen geven op de prostituees. Bij sommige sites zijn er recensieformulieren ter beschikking met ‘rates’ en welke seksuele diensten ze bieden. Via Twitter kunnen specifieke vragen gesteld worden aan de prostituees apart en kunnen hun individuele recensies opgevolgd worden.

1.3. | Management van mensenhandelsnetwerken

“Een van de meest zorgwekkende aspecten van mensenhandel is de steeds verdere modernisering ervan, in die mate dat het tot een heuse bedrijfstak is uitgegroeid. De criminelen verwerven steeds meer knowhow en gaan alsmat professioneler te werk. Ze voeren marketing rond hun ‘producten’ en ‘diensten’ en maken gretig gebruik van het internet en andere communicatietools.”⁵³

Logistiek

In een Bulgaars dossier⁵⁴ werd reeds enkele jaren geleden vastgesteld dat in Duitsland een organisatie met behulp van het internet als onderaannemer de logistiek voor prostitutie in Duitsland organiseerde en tegen betaling de nodige faciliteiten bood op basis van duidelijke afspraken. Alle meisjes werden op het internet geplaatst via een website.

In een grootschalig prostitutienetwerk⁵⁵ dat seksuele diensten aanbood via erotische datingsites beheerde de Belgische hoofdbeklaagde vanuit Spanje als ‘agentschap’ verschillende websites waarop de diensten van de Marokkaanse, Roemeense en Bulgaarse meisjes werden geadverteerd. Hij ronselde de meisjes via zijn internetplatform. Meestal was dit in België maar ook in Roemenië en Duitsland. Bij hun aanwerving kregen de meisjes de opdracht een nieuw Facebook profiel aan te maken.

Mensenhandelaars beseffen dat hun telefoon kan afgeluisterd worden en verkiezen hun vertrouwelijke gesprekken te voeren via Viber, What's App, Skype.

Vertrouwelijke communicatie

Mensenhandelaars beseffen dat hun telefoon kan afgeluisterd worden en verkiezen hun vertrouwelijke gesprekken te voeren via Viber, WhatsApp, Skype, enz die moeilijk door de politie kunnen afgeluisterd worden. Dit kon vastgesteld worden in een afgeluisterd gesprek van een Albanees maffiadossier van seksuele uitbuiting. Een andere techniek is het gebruiken van één emailadres waarvan alle gesprekspartners het paswoord kennen zodat de opgestelde, maar niet verzonden berichten daar ter plekke gelezen en verwijderd worden.

In het Gentse Hongaarse dossier⁵⁶ van 2013-2014 heeft de politie bij de beklagden Facebookberichten teruggevonden over een aantal meisjes dat een beklagde aangeleverd en onder controle had.

Contrastrategie

Mensenhandelaars beginnen te beseffen dat de politie tegenwoordig Facebook ook als instrument kan gebruiken om bewijsmateriaal te verzamelen. In het Nigeriaans dossier maakte een beklagde dit tijdens een telefoongesprek duidelijk aan een andere beklagde: “Beklaagde X zegt als iemand zich op Facebook aanmeldt, dan ziet de politie het.” Hierop bediscussieerden de beklagden onderling hun Facebook gedrag: “Beklaagde X vraagt aan de hoofdbeklaagde of Y op Facebook geschreven heeft dat hij in België verblijft. Hoofdbeklaagde zegt dat ze het niet weet omdat ze niks over Facebook kent maar ze denkt dat Y zou geschreven hebben dat X in Londen verblijft. X zegt dat Y het ontkend heeft dat die gechat heeft. Hoofdbeklaagde vraagt aan X of Y niet verteld heeft dat Z het gelezen had. X zegt dat Y haar verteld heeft dat Z de Facebook pagina gedelete heeft.” De beklagden hadden net zoals bij de telefoontap voor Facebook ook al een contrastrategie ontwikkeld: “X zegt, gezien hij (Y) degene is die gecontacteerd werd, hij zijn Facebook en gsm-nummer moet veranderen”.

Bedreigen en chanteren van slachtoffers

Europol schrijft: “Criminele organisaties gebruiken het internet om slachtoffers van mensenhandel te bedreigen of onder druk te zetten. Internet wordt gebruikt om slachtoffers te chanteren, door ermee te dreigen compromitterende foto’s op te sturen naar familie of vrienden om hen op die manier online te kijk te zetten.”⁵⁷

53 EUROPOL, *Trafficking in human beings in the EU*, Situatieverslag, Den Haag, februari 2016, Referentienummer van het document: 765: www.europol.europa.eu/publications-documents/trafficking-in-human-beings-in-eu.

54 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2011, *Het geld dat telt*, pp. 84-86.

55 Zie verder deel 3, hoofdstuk 3 (rechtspraak): Corr. Antwerpen, afdeling Antwerpen, 2 mei 2016, k. AC4. en Antwerpen, 24 november 2016, 14° k.

56 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2015, *Schakels verbinden*, dossieranalyse, pp. 66-70.

57 EUROPOL, *Intelligence Notification 15/2014*, Den Haag, oktober 2014 : www.europol.europa.eu/publications-documents/trafficking-in-human-beings-and-internet.

Vooral in *loverboy*dossiers en dossiers waarin slachtoffers via fotoshoots voor een job als model gerekruteerd werden, trachten de mensenhandelaars de slachtoffers te chanteren met naaktfoto's om ze tot prostitutie aan te zetten. *Loverboys* gebruiken hierbij soms screenshots die ze met Snapchat genomen hebben tijdens het verleidingsproces van de slachtoffers.

Bij kinderen is dit nog een groter probleem. In het Roemeense rapport van het EU-project Surf and Sound stelde een Roemeense magistraat: "De mensenhandelaar zou vooral slachtoffers van 11, 12, 13 jaar oud benaderen, met weinig levenservaring, aan wie hij dan vraagt zich uit te kleden en pornografische poses aan te nemen. [...] Zodra de slachtoffers een foto hadden opgestuurd begon de chantage. Hun ouders wisten van niets en via de vrienden van de minderjarige ging de bal pas echt aan het rollen. (procureur)." ⁵⁸

Controle slachtoffer

Europol ⁵⁹ stelde net zoals een studie van het EU-project Trace ⁶⁰ (Trafficking as a criminal enterprise): "Dankzij online technologieën is het voor mensenhandelaars ook makkelijker slachtoffers te huisvesten en te controleren. Criminele organisaties houden hun slachtoffers goed in het oog door hen te verplichten dagelijks contact op te nemen via email of via chat, om zo hun aanwezigheid te bewijzen."

In een van de Antwerpse dossiers ⁶¹ met minderjarigen uit jeugdinstituten legde het slachtoffer verklaringen af over haar *loverboy* en hoe hij haar steeds terugvond: "Ik heb daar schrik van want hij vindt me altijd. Ik kende hem maar twee weken. Tijdens die twee weken ben ik twee keer gaan lopen en hij heeft me telkens teruggevonden. Hij vond me via Facebook."

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 maanden (02.11.2014 - 01.11.2016), Surf and Sound, Nationaal verslag Roemenië, 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 EUROPOL, *Intelligence Notification 15/2014*, Den Haag, oktober 2014 : www.europol.europa.eu/publications-documents/trafficking-in-human-beings-and-internet.

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

61 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, p. 134.

1.4. | Slachtoffers en sociale media

Hoe gaan slachtoffers om met sociale media? We stellen vast dat slachtoffers sociale media gebruiken om een bepaalde beeldvorming te creëren naar het thuisfront toe. Maar sociale media en internet kunnen ook een instrument zijn om de weerbaarheid van de slachtoffers te versterken.

Beeldvorming voor thuisfront

Uit een mediaverslag van Public radio International (PRI), ⁶² een global non-profit mediabedrijf, blijkt dat Nigeriaans slachtoffers via sociale media bij vrienden en familie, hun leven mooier voorstellen dan het is. Ze verhullen het feit dat ze onderweg verkracht werden, en na aankomst in de prostitutie belandden. Ze zijn trots en willen goed overkomen bij hun vrienden, zeker niet als slachtoffers.

Het artikel met de titel 'Op Facebook stellen Nigeriaanse slachtoffers van seksuele uitbuiting hun leven veel glamozeuzer voor dan het is' doet het relaas van enkele slachtoffers dat we samengevat hebben:

"Bij het verlaten van de kerk op een zonnige zondag op Sicilië tuit F. haar lippen, ze kijkt ietwat verlegen in de camera en neemt een selfie. Zoals alle millennials overall ter wereld is F. zot van social media. Ze vraagt haar vriendin een paar kiekjes te nemen, terwijl ze verschillende poses aanneemt. Ze ziet er goed uit in haar mantelpakje en rode lippenstift. Ze zet de foto op Facebook en weet de commentaar van vrienden in Nigeria zeer te appreciëren. "Erg mooi", schrijft een vriend. Als we Fortune's Facebook profiel mogen geloven leeft ze in Europa en is ze dankbaar, gelukkig en vroom. "De meesten onder hen liegen," stelt P., een andere Nigeriaanse vrouw die in Palermo woont. Volgens haar geven de Facebook-posts van haar Nigeriaanse en Afrikaanse vrienden in Europa de indruk dat ze volop genieten van het leven in Europa, terwijl het vaak net andersom is. "Het is de hel op aarde." Het zou totaal nutteloos zijn om de trauma's en problemen die ze doormaken te publiceren voor hun vrienden in hun land van herkomst. "Ze zouden je toch niet geloven," zegt P., ze zouden denken dat je liegt om al het goede hier in Europa voor jezelf te houden."

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.

Sociale controle

Uit de dossiers blijkt dat de Nigeriaanse slachtoffers ook onderling nauwe contacten onderhouden en via Facebook elkaar op de hoogte hielden wat enigszins een minimum aan bescherming kon betekenen. Zo kon een Nigeriaans slachtoffer in een dossier⁶³ de politie de prostitutieplaats van een ander slachtoffer aanduiden: “Omtrent X kan

ik U zeggen dat deze momenteel ook werkzaam is als prostituee in een club gelegen te X. Zij maakt gebruik van het oproepnummer... En heeft eveneens een Facebook profiel. Zij is een contact van mij op mijn Facebook profiel.” In een

Via sociale media stellen de Nigeriaans slachtoffers bij vrienden en familie, hun leven mooier voor dan het is in de realiteit.

Albanees maffiadossier voorzagen de beklaagden hiervan het risico en verboden hun slachtoffers de toegang tot Facebook. Op basis van de telefoontap concludeerde de politie: “Slachtoffer X mocht van beklagde geen Facebook hebben, dus moest ze het Facebook profiel van haar zus gebruiken.” Het slachtoffer had wel een alternatieve oplossing geregeld.

Facebook kan ook een relevant instrument van sociale controle zijn waarmee in geval van nood de politie kan gealarmeerd worden. In een Luiks *loverboy*dossier met Belgische meerderjarige slachtoffers kon een buurvrouw via een Facebookbericht de moeder van een invalide slachtoffer verwittigen dat haar dochter geslagen werd door twee mannen en een vrouw.

Economische uitbuiting

Bij de slachtoffers van economische uitbuiting stellen we vast dat ze bijvoorbeeld via een Poolse website (Etransport.pl) onderling hun goede en slechte werkervaringen uitwisselen over firma's uit de transportsector om hun landgenoten te informeren en te behoeden voor misbruiken.

2. HOE MANIPULEREN LOVERBOYS HUN SLACHTOFFERS MET SOCIALE MEDIA

In dit punt gaan we verder dieper in op de rol van sociale media bij *loverboys*, omdat dit momenteel een cruciaal instrument is bij *loverboys*slachtoffers, en zeker bij Belgische slachtoffers, waaronder veel minderjarigen.

Verscheidene methoden worden gebruikt door mensenhandelaars om slachtoffers te manipuleren. Eén ervan is de *loverboy* methode.⁶⁴ Hier gaat de dader zorgen dat het slachtoffer emotioneel afhankelijk wordt, vaak door middel van verleidingstechnieken. Het slachtoffer wordt vervolgens door mensenhandelaars door middel van dwang en geweld, uitgebuit.⁶⁵ De *loverboy* techniek is een methodiek van mensenhandel en geen alleenstaand fenomeen.⁶⁶

De laatste jaren merkt men een uitbreiding van de *loverboy*problematiek. In plaats van hun slachtoffers te verleiden op openbare plaatsen waar veel jongeren komen ziet men dat steeds vaker het internet wordt gehanteerd. Uit onderzoek blijkt dat vijftig percent van de slachtoffers via het internet geworven werden.⁶⁷ Het internet biedt een heel aantal opportuniteiten voor dit soort criminaliteit. Eerst en vooral zorgt het internet voor een drempelverlagend effect.⁶⁸ Door de anonimiteit van het platform kunnen criminelen een andere identiteit aannemen. De dader moet zich niet meer fysiek verplaatsen, waardoor hij in minder tijd en goedkoper een groter aantal doelwitten kan bereiken. Afstanden worden irrelevant. Het internet heeft er ook voor gezorgd dat het hele proces makkelijker en sneller verloopt. Alle informatie van het slachtoffer staat op het internet, waardoor daders sneller kunnen inpikken op de persoonlijkheid van het slachtoffer. Dit zorgt niet voor een verschuiving van de problematiek, maar een

63 Zie verder deel 3, hoofdstuk 3 (rechtspraak): Corr. Brussel Nederlandstalig, 28 maart 2017, 60^{ste} kamer (definitief).

64 EUROPOL, *Trafficking in human beings in the EU*, Situation report, The Hague, February 2016, Document RefNo: 765, p. 3 : 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*, 2011, p. 20. Geraadpleegd van www.verwey-jonker.nl.

67 V. ZANETTI, (2009), “*De digitale 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.

uitbreiding ervan. Deze ontwikkeling wordt in de hand gewerkt door nieuwe technologieën, zoals het internet en de sociale media die ermee verbonden zijn. Algemeen kan men stellen dat het internetgebruik het probleem van de *loverboys* heeft doen toenemen.

In se is er geen stijging sinds de opkomst van het internet. Het ontbreken van vergelijkbaar materiaal laat niet toe om een mogelijke stijging van het fenomeen te meten. Ondanks het gebrek aan data beweren verschillende experts dat het fenomeen al zeer lang bestaat, terwijl het maar recent in de aandacht is gekomen. Een mogelijke stijging in het aantal casussen van de laatste jaren kan toegeschreven worden aan het feit dat men het fenomeen meer aandacht geeft en weet de bevolking de verschillende organisaties die instaan voor het bestrijden van *loverboys* beter te vinden. Een mogelijke verandering kan ook te wijten zijn aan trends in het land van herkomst en is dus afhankelijk van periodes. Een andere mogelijke verklaring voor een stijging van het fenomeen kan toe te schrijven zijn aan dossiers die beter worden gekwalificeerd. Vroeger vielen dossiers van *loverboy* vaak onder zedenzaken in plaats van onder mensenhandel.

Loverboys blijken het meest vaak Facebook te gebruiken voor het opstarten van een relatie. De reden hiervoor is dat kwetsbare jongeren die gevoelig zijn voor afhankelijkheidsrelaties met de *loverboy* beschikken over een open profiel op dit medium. Naast de open profielen zijn deze jongeren vaak 24/7 beschikbaar op Facebook, waardoor ze een makkelijke prooi zijn. Naast het gebruik van Facebook wordt eveneens Skype, Whatsapp, Viber en MSN gebruikt.

Loverboys gaan meestal tewerk volgens een drie-fasen patroon. De eerst is de groomingfase. Vervolgens is er de inlijvingsfase en ten slotte de uitbuitingsfase.

De groomingfase kan nogmaals opgedeeld worden in drie stadia. De letterlijke betekenis van grooming is 'het verzorgen of het voorbereiden van iets of iemand'.⁶⁹ In het wetenschappelijk jargon wordt grooming beschreven als het proces waarbij een meerderjarige een jongere manipulatief benadert en gaat voorbereiden op misbruik, vaak van seksuele aard.⁷⁰ Het internet heeft de individuele grooming-gedragingen op verschillende manieren

beïnvloed. Het doel van de mensenhandelaar blijft dezelfde. Hij gebruikt echter andere technieken en media om zijn doel te bereiken. Hij ziet het internet als een veilige omgeving waar alle vormen van gedrag aanvaardbaar zijn en de kans op vervolging gering.⁷¹ De groomingfase verschilt slechts van het offline groomen door de ruimte waarin het groomen zich afspeelt.⁷² Het internet heeft voor een nieuwe dimensie van grooming gezorgd, namelijk het online facet. Het doel van groomen blijft hetzelfde. Het online groomingproces kan men indelen in verschillende fasen die de groomer moet doorstaan.

Eerst en vooral moet de dader een profiel aanmaken. Hier kan men een onderscheid maken tussen twee werkwijzen. De eerste waarbij de dader een zeer onvolledig, afgeschermd profiel opstelt met weinig of onjuiste informatie. Bij de tweede werkwijze gaat de dader zich als 'gangster' afbeelden in de hoop zo in het oog te schieten van hun slachtoffer.⁷³ De tweede fase binnen de groomingfase is de rekruteringsfase, waarbij de dader op zoek gaat naar zijn slachtoffer. Hij ronselt zijn slachtoffer op basis van geslacht, leeftijd, woonplaats, hobby's, opleidingsniveau, etc.⁷⁴ De ronselsites zijn voornamelijk sociale netwerksites, jongerensites en chatboxen.⁷⁵ De *loverboy* kan veel makkelijker verschillende jongeren op hetzelfde moment benaderen. In de derde fase gaat de dader een potentieel slachtoffer selecteren. Dit noemt men hawking, deze term verwijst naar het rondcirkelen als een havik rond zijn prooi. Deze wervingsmethode kan men opdelen in rechtstreekse werving van potentiële slachtoffers en onrechtstreekse werving. Bij rechtstreekse werving, gaat de dader zich richten op één slachtoffer. Bij onrechtstreekse werving gebeurt dit via sociale media. De dader gaat dan

Loverboys blijken het meest vaak Facebook te gebruiken voor het opstarten van een relatie.

69 L. STEVENS, "Grooming en cyberlokking strafbaar. Uitbreiding van de strafrechtelijke bescherming van de seksuele integriteit van minderjarigen in cyberspace", *Rechtskundig weekblad*, 78(22), 2015, pp. 844-855.

70 CHILD FOCUS, *Slachtoffers van tienerpooiers in Vlaanderen*, 2016. Geraadpleegd van www.childfocus.be/sites/default/files/rapport_tienerpooiers_en_hun_slachtoffers_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.

71 J. DAVIDSON, "Internet Child Abuse: Understanding Offender Online Grooming Behaviour", dans M. SEIFI (Red.), *Advances in the Analysis of Online Paedophile Activity*, pp. 39-55. Geraadpleegd van <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. Geraadpleegd van 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. Geraadpleegd van www.cisjournal.org/journalofcomputing/archive/vol2no9/vol2no9_5.pdf.

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

74 MOVISIE, (2009), *Meisjesprostitutie: feiten en cijfers*, 2009, p. 6. Geraadpleegd van [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, *Jaarverslag Mensenhandel en mensensmokkel 2015, Schakels verbinden*, p. 33.

zoveel mogelijk berichtjes versturen, in de hoop dat iemand toehapt. Eens deze fase verlopen is begint de dader aan een benadering van zijn slachtoffer.⁷⁶ Dit kan op een directe en op indirecte manier gebeuren. De vijfde fase van het groomingproces is het inpalmen van het slachtoffer.⁷⁷ Dit proces gebeurt veel sneller via het internet. Dit komt omdat men vaak meer onthult via het internet dan in de offlinewereld.⁷⁸ In deze fase worden sites gebruikt die het communiceren met het slachtoffer eenvoudiger maken. De dader zal hier opzettelijk compromitterende informatie verzamelen over het mogelijke slachtoffer om in een later proces deze te gebruiken als chantagemiddel. Tijdens deze fase gaat de dader het idee van prostitutie laten gewennen aan het slachtoffer.

In de inlijvingsfase gaat de dader vaak het internet gebruiken als chantagemiddel. Om de controle over het slachtoffer te behouden zal de dader zijn slachtoffer chanteren door te dreigen met het verspreiden van gevoelige informatie.

De laatste fase is de uitbuitingsfase. Hier gaat de dader voornamelijk het internet gebruiken als advertentiemiddel. Deze adverteert voornamelijk op grote commerciële

seksadvertentie-websites.⁷⁹ Deze websites zijn een eenvoudige manier voor klanten om goedkoop seks te krijgen, zonder veel controle. Op dergelijke websites kan men het slachtoffer eender welke identiteit geven, waardoor

men zeer makkelijk minderjarige meisjes kan adverteren. Het probleem met dergelijke websites is dat het in België verboden is om te adverteren voor prostitutie, waardoor je vanuit justitie geen afspraken kan maken met dergelijke websites aangezien ze in wezen de wet overtreden. En indien justitie hierover wel een regeling zou treffen zou ze zelf kunnen beschuldigd worden dat ze de wet overtreedt. Vervolgens zal het internet eveneens gebruikt worden als controlemiddel over het slachtoffer. Uit onderzoek blijkt dat de overgrote meerderheid van de prostitutie vandaag online plaatsvindt.⁸⁰

Internet wordt gebruikt als chantagemiddel door te dreigen met het verspreiden van gevoelige informatie.

3. DE ROL VAN SOCIALE MEDIA EN INTERNET BIJ MENSENSMOKKEL

Het Europees Migratie Netwerk (EMN) onderzocht in 2016 de rol van sociale media bij mensensmokkel.

Rond 2013-2014 begon sociale media een rol te spelen bij mensensmokkel.⁸¹ Het EMN-rapport stelt: "Het gebruik van sociale media in migrantensmokkel is de afgelopen jaren exponentieel toegenomen. Smokkelaars gebruiken sociale media om publiciteit te maken voor hun diensten, om informatie te verstrekken over de migratieroutes en ook om de communicatie te vergemakkelijken. Dat sociale media steeds vaker wordt gebruikt kan te maken hebben met het feit dat ze goedkoper zijn en zowel voor de migrant als de smokkelaars veiliger zijn in gebruik (anoniem/versleuteld), terwijl de zichtbaarheid veel groter is en op die manier ook meer migranten kunnen worden bereikt."⁸²

EMN lanceerde een enquête in de EU lidstaten met behulp van een vragenlijst. Daaruit bleek dat elf EU-landen met dit probleem geconfronteerd werden.⁸³

3.1. | Smokkelmarkt

In 2016 was er een gigantische stijging in het gebruik van sociale media door smokkelnetwerken. Europol kon 17.000 smokkelaars traceren die Facebook gebruikten

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

77 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2015, *Schakels verbinden*, p. 33.

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. Geraadpleegd van <http://prostitutionresearch.com/wp-content/uploads/2014/09/FarleyFranzblauKennedyOnlineTrafficking-2014.pdf>.

81 www.emnbelgium.be/fr/nouvelles/des-experts-en-traffic-de-migrants-se-reunissent-une-table-ronde-du-rem-belgique?q=/news/experts-migrant-smuggling-gather-be-emn-ncp-roundtable.

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*: "Elf (lid-) staten (BE, CZ, ES, FI, HU, LT, NL, NO, PL, SK, UK) hebben bevestigd dat social media worden gebruikt om publiciteit te maken voor smokkeldiensten, informatie te verstrekken over migratieroutes en om te communiceren met smokkelaars, die gebruik maken van toepassingen zoals WhatsApp of Viber. Facebook bijvoorbeeld wordt gebruikt om informatie te verstrekken over specifieke trips (reisformules, met vermelding van de prijs) contactgegevens, live blogs over de vooruitgang die andere klanten op zee boeken of om verhalen te delen om de angst weg te nemen bij potentiële klanten die vrezden voor hun veiligheid."

voor hun smokkelactiviteiten naar de EU.⁸⁴ Daarnaast kon Europol in 2016 ruim 2.500 valse reisdocumenten traceren op sociale media.⁸⁵

Een smokkelaar verklaarde aan de BBC dat via zijn Facebook account dagelijks tussen de 10 en 20 mensen gesmokkeld worden.⁸⁶ Tot 2012 maakte hij nog geen gebruik van sociale media. Op het moment van de publicatie van het BBC-artikel (13/05/2015) was Facebook al goed voor 30% à 40% van zijn smokkelbusiness.

Advertentie

In haar eerste jaarverslag schrijft het European Migrant Smuggling Centre (EMSC)⁸⁷ van Europol: "In 2016 werd het hele jaar zichtbaar meer online inhoud die met migrantensmokkel te maken had vastgesteld. Dit bleek uit de aanzienlijke stijging van het aantal bijdragen die het EMSC heeft ontvangen, met ruim 1.150 bij het EMSC gemelde sociale media accounts die openlijk publiciteit maakten voor de georganiseerde mensensmokkel, of die ermee geassocieerd waren. Dit is een stijging met 775 % in vergelijking met de 148 gelijkaardige accounts in 2015. Het sociale media platform bij uitstek voor smokkelaars blijft Facebook, ook al werd een lichte verschuiving vastgesteld naar andere service providers zoals Telegram." Frontex stelde ook vast dat de smokkelaars heel snel en flexibel omgaan met sociale media: "Wat opvalt is dat deze pagina's zeer snel verschijnen maar net zo snel weer verdwijnen, waardoor het moeilijk is ze te traceren."⁸⁸

Volgens het International Centre for Migration Policy Development (ICMPD) bevatten de Facebook-advertenties van de smokkelaars informatie over hun diensten, de transportmethode, de smokkelprijs, de succes-rating, en in sommige gevallen info over het asielbeleid en de procedures over gezinshereniging van de EU-landen.⁸⁹

Het UNHCR onderzocht de rol van sociale media bij smokkel vanuit het perspectief van de migrant.⁹⁰ Het vond een hele waaier van aanbiedingen op sociale media op maat van de verschillende migrantengroepen.

Voor Afghanen die een totaalpakket voor een smokkeltraject vanuit Afghanistan naar het bestemmingsland bestellen via een zogenaamde reisagent (zie verder) krijgen: "Smokkelnetwerken staan niet alleen in voor het transport, ze regelen ook de nodige documenten. Op Facebook staan er voortdurend tal van aanbiedingen, met vermelding van de contactgegevens van de verkopers. Soms krijgen potentiële klanten zelfs informatie over de verwachte wachttijden en de prijs. Constant zijn er ook vervalste visa te koop. Bovendien zijn er ook aanbiedingen op korte termijn voor echte visa van verschillende ambassades/consulaten. Daaronder visa voor de "Schengen-" ruimte of specifieke EU-lidstaten, maar ook voor Turkije, Oekraïne, Canada en de VS. In sommige gevallen vermelden de aanbiedingen ook details over het type visum, zoals een toeristen- of studentervisum, maar soms ook bizarre details zoals "visa voor huwelijk", "visa en woonplaats", "visa voor investering" of "visa om eigendom te kopen".⁹¹

In 2016 kon Europol 17.000 smokkelaars traceren die Facebook gebruikten voor hun smokkelactiviteiten naar de EU.

Voor Arabischtaligen zoals Syriërs en eventueel Iraki's die smokkelaars wantrouwen en zelf hun reis stapsgewijs per traject trachten te organiseren en enkel een smokkelaar contacteren bij een moeilijke smokkelroute: "Smokkelaanbiedingen via Facebook omvatten intussen internationaal illegaal vervoer over land, via de lucht of over zee, waarbij ambassadepersoneel wordt omgekocht om visa te bezorgen, paspoorten in een bepaald land worden gestolen om die in een ander te verkopen en tal van documenten worden nagemaakt."⁹²

Het EMN vond tijdens haar bevraging van de EU-landen ook reacties over Facebook-advertenties met een aanbod van schijnhuwelijken.⁹³

84 Europol, *Migrant Smuggling in Europe*, februari 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 maart 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 mei 2015 : www.bbc.com/news/magazine-32707346.

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

88 <http://frontex.europa.eu/pressroom/hot-topics/profitting-from-misery-how-smugglers-bring-people-to-europe-aUYY2f>.

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

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. Zie ook verder de externe bijdrage van M. SUNJIC, "Vluchtelingen: wanneer mensensmokkel mensenhandel wordt".

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*: "Andere gelijkaardige activiteiten op social media zijn bijvoorbeeld publiciteit voor schijnhuwelijken. Polen bijvoorbeeld stelde dat het advertenties voor dat soort diensten in het Verenigd Koninkrijk had ontdekt, in ruil voor GBP 6.000."

Public Relations

Verschillende smokkelaars werven hun klanten via mond aan mond reclame. Voor hen is dit nog steeds de belangrijkste manier om de migranten te bereiken. Ze gebruiken Facebook om hun public relations te verzorgen met promotiefilmpjes voor hun smokkelreizen.

De krant *De Morgen* interviewde hierover een smokkelaar: “Hij beweerde Facebook te gebruiken als middel om zijn imago te bevestigen, zodat migranten die van anderen zijn naam hebben gekregen, kunnen zien dat het bij hem wel goed zit. Op zijn Facebook account staan filmpjes van vluchtelingen die met hun rubberboot zijn aangekomen op Lesbos. Duimen gaan de lucht in. “Allemaal naar X (naam smokkelaar)!”, roepen de migranten, opgelucht dat ze de overkant hebben gehaald.”⁹⁴ Het UNHCR-rapport vond ook promotiemateriaal van smokkelaars in een periode dat ze door de vele dode drenkelingen in een negatief daglicht stonden.⁹⁵

Gebruikersgroepen Facebook

Facebook bevat verschillende Arabischstalige gebruikersgroepen voor mensensmokkel. Volgens het UNHCR-rapport zullen eerder Syrische en Iraakse migranten hiervan gebruik maken voor een bepaald deel van hun geplande smokkelreis.

In de smokkeldossiers kwam de rol van deze Facebook-gebruikersgroepen ook aan bod. Uit de analyse van een smokkeldossier⁹⁶ bleek dat een Koerdisch-Palestijns smokkelnetwerk Facebook gebruikte om hun internationaal netwerk met mogelijke smokkelklanten verder uit te bouwen. De politie stelde bij de opstart van haar onderzoek in een proces-verbaal vast dat de smokkelaars hiervoor een Facebook-groep hadden opgericht: “Ook vernemen wij dat er op de sociale mediawebsite Facebook er verschillende Arabischstalige gebruikersgroepen zouden zijn. Deze hebben als doel personen die naar Europa wensen te komen zonder geldige documenten in contact te brengen met elkaar en mensensmokkelaars. Op deze gebruikersgroepen kan men vragen stellen over de toestand in Europese landen en steden. Dit met oog om informatie te verzamelen om tot deze gebieden te geraken. Men vraagt hier ook naar



Facebook groep van smokkelaars

contactgegevens van personen die hen hier bij kunnen assisteren. Deze contactgegevens worden dan via privéberichten bezorgd aan de vraagsteller. Men laat ook soms weten aan andere gebruikers indien de oversteek naar het Verenigd Koninkrijk succesvol was. Wij krijgen de namen van enkele van deze gebruikersgroepen. Deze voegen wij toe aan de bijlage van dit PV.”

Verschillende concrete Facebook-gebruikersgroepen die migranten koppelen aan smokkelaars werden opgesomd in enkele studierapporten⁹⁷: “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”. De migranten kunnen hier de smokkelroutes, de bestemmingslanden en de kostprijs vergelijken.

Valse paspoorten zijn er te koop.⁹⁸ Daarnaast gebruiken smokkelaars succesverhalen om zich te promoten⁹⁹ en

94 De Morgen, 7 november 2015.

95 “Kritiek op de gevaren van illegale migratie op Facebook pagina's vormt een bedreiging voor de smokkelbusiness en smokkelaars reageren op verschillende manieren. Toen steeds meer Facebook-gebruikers begonnen te wijzen op de gevaren van de oversteek via de zee, zetten smokkelaars prachtige foto's van jachten en luxe cruiseschepen online, om potentiële klanten te doen geloven dat dit het soort schepen was dat ze gebruikten. Daarnaast verschenen ook beelden over veiligheid en van personen die op vleugels van engelen naar Europa werden gebracht”.

96 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, dossieranalyse, pp. 101-103.

97 Danish Refugee Council, *Getting to Europe the 'WhatsApp' way*, June 2016. <http://reliefweb.int/sites/reliefweb.int/files/resources/RMMS%20Briefing%20paper%202020%20Social%20Media%20in%20Mixed%20MigrationUPLOAD.pdf>.

98 *Ibid.*: “Smokkelaars gebruiken ook sociale media om specifieke diensten aan te bieden, zoals valse paspoorten en andere identiteitsdocumenten. De zogenaamde Facebook pagina in het Arabisch: “Uitgifte en vernieuwing van paspoorten, rijbewijzen en onderwijsdiploma's” helpt Syriërs die dat soort documenten wil bemachtigen.”

99 *Ibid.*: “De hieronder vermelde Facebookgroep “Asylum and migration to pan-Europe” telt 23.810 leden. Er staat een getuigenis op van iemand die erin is geslaagd Zweden te bereiken en na die commentaar, heeft smokkelaar W. zijn nummer op Viber en WhatsApp gepost voor anderen die mogelijk van zijn diensten gebruik willen maken.”

speelden ze in op de angstgevoelens van de migranten om te verdrinken.¹⁰⁰

Maps met routes via WhatsApp

In Whatsapp bestaan er chatgroepen voor migranten die zoveel mogelijk autonoom willen reizen en voor bepaalde moeilijke trajecten contact zoeken met een smokkelaar. Ze wisselen maps uit met kaarten van routes, belangrijke steden, grensgebieden, het transportmiddel, de kostprijs en de contactplaatsen van smokkelaars. Deze maps kwamen ter sprake in een EU-project van 2016-2018 dat de rol van sociale media bij de migrant onderzoekt.¹⁰¹

Reisagentschappen

Reisbureaus spelen via internetadvertenties een relevante rol bij mensensmokkel. Op Instagram bieden smokkelaars via reisagentschappen met mooie foto's smokkelreizen aan naar West-Europese steden. Ze promoten dit aan de hand van mooie foto's van de steden en foto's van de nodige valse identiteitsdocumenten. Ook via Facebook worden advertenties verspreid, zoals Frontex vastgesteld heeft.¹⁰² Volgens Europol zien sommige van deze Facebook accounts er trouwens hetzelfde uit als die met de aanbiedingen van normale reisbureaus.¹⁰³ In Thailand zijn dergelijke reisbureaus met internetadvertenties naast mensensmokkel ook met mensenhandel bezig.¹⁰⁴

Het UNHCR-rapport vond in Afghanistan veel advertenties van zogenaamde reisagentschappen die zich inlaten met mensensmokkel.¹⁰⁵

Mensensmokkel is sterk ingebakken in de Afghaanse samenleving. Dit kon reeds vastgesteld worden bij de dossieranalyse van een Afghaans smokkelnetwerk.¹⁰⁶ Mensensmokkelaars worden er als reisagenten beschouwd die veel prestige genieten. De Afghaanse migranten schenken dan ook hun volledige vertrouwen aan deze smokkelaars om hun reis te organiseren.

De smokkelaars gebruiken ook de marketingstrategieën van een reisbureau. Dit kon vastgesteld worden in een EU-project van 2016-2018 dat de rol van sociale media bij migranten onderzoekt.¹⁰⁷

Communicatie tussen smokkelaar en klant

De smokkelaars communiceren vooral via sociale media met hun klanten. Ze opereren onder een schuilnaam. Deze communicaties vormen vooral bij de Syrische en Iraakse smokkeldossiers een extra-dimensie. Volgens het UNHCR-rapport zijn deze communicaties bij de Syrische en Iraakse migranten niet louter contactnames. Het zijn echte onderhandelingen tussen smokkelaar en klant omdat deze migranten weinig vertrouwen hebben in smokkelaars.¹⁰⁸

Op Instagram bieden smokkelaars via reisagentschappen met mooie fotootjes smokkelreizen aan naar West-Europese steden.

100 *Smugglers, Migrants connect using Facebook*, The Toronto Star, 10 juli 2015: "De smokkelaars die in het Arabisch schrijven vermelden er telefoonnummers, tarieven, details over routes en transportmiddelen, en voorzien hun Facebook pagina page walls zelfs van een: "boek nu" knop. In een poging om de angst bij migranten weg te nemen om op zee te verdrinken, heeft een Facebook pagina van smokkelaars de term: "veilig reizen" aan de titel toegevoegd, terwijl een andere pagina er zonder schroom het woord: "smokkel" aan toevoegt en openlijk de grootte van de boten en de smokkelkosten bij vermeldt."

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: "De kaarten vermelden uiterst gedetailleerd de specifieke transportopties tussen locaties en de kost ervan, de optimale routes en ook de grensovergangen. Er is ook informatie op te vinden over specifieke steden en plaatsen waar smokkelaars of chauffeurs hun diensten aanbieden. Het uitermate gedetailleerde karakter ervan wijst op een zeer goed georganiseerd samenwerkingsverband."

102 <http://frontex.europa.eu/pressroom/hot-topics/profitting-from-misery-how-smugglers-bring-people-to-europe-aUY2f>: "Bepaalde Facebook pagina's bieden ook valse reisdocumenten te koop aan en verkopen zichzelf als, meestal in Turkije gevestigde reisagentschappen."

103 De Morgen, 7 november 2015.

104 Zie hierboven punt 1 van dit focus (de rol van sociale media en internet bij mensenhandel) en verder, deel 3, hoofdstuk 3 (rechtspraak).

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: "Afghanen boeken bijna altijd 'all-inclusive' reizen van land van herkomst tot in het bestemmingsland. Mensen die Dari spreken hebben via sociale media rechtstreekse contacten maar ze plaatsen er ook advertenties op. Vaak houden reisagentschappen er zowel legale als illegale activiteiten op na. Afghaanse smokkelaars verkopen de "Europese droom" door aantrekkelijke foto's te plaatsen of een goed en veilig leven te beloven."

106 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2015, *Schakels verbinden*, dossieranalyse, pp. 85-90.

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: "Daarom gebruiken smokkelaars zeer vaak nieuwe technologieën voor marketingdoeleinden, net zoals reisagentschappen dat doen. Of zoals een bevraagde in het kader van het MEDMIG-project het verwoordde: "Om ons vertrouwen te winnen gaf [de smokkelaar] ons de telefoonnummers van alle mensen die met ons zouden reizen."

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: "Potentiële klanten stellen elkaar via sociale media vragen over hoe ze in Europa of andere landen kunnen geraken. Smokkelaars volgen die Facebook gesprekken en posten vervolgens hun aanbiedingen. Onderhandelingen verlopen dan via private kanalen (Viber, Imo, WhatsApp,...)".

Zoals vastgesteld in verschillende dossiers geven smokkelaars er de voorkeur aan te communiceren via Viber, Skype, WhatsApp en Facebook omdat ze beseffen dat hun gsm kan afgeluisterd worden door de politie.

In een Syrisch smokkeldossier kon de politie de chatgesprekken van de iPhone van een smokkelaar inlezen. Hieruit bleek dat deze smokkelaar met 769 klanten gecommuniceerd had via Viber, WhatsApp en Skype. Er was ook sprake van communicatie via Facebook, maar hierover beschikte de politie geen gegevens.

In een Koerdisch smokkeldossier¹⁰⁹ communiceerden de smokkelaars met hun klanten via Viber. In een afgeluisterd telefoongesprek van een smokkelaar werden de klanten doorverwezen naar Viber: “Om 14:17 uur belt smokkelaar (796) naar het Iraakse oproepnummer 788. Hij vraagt naar een jongen (onbekende) die volgens 788 in Bulgarije

Mensensmokkelaars verkiezen om hun financiële gesprekken via sociale media te voeren.

zou verblijven. De gebruiker van 788 zou het nummer van (796) doorgeven aan de jongen zodat die hem kan bellen. 796 vraagt ook naar een paar andere nummers (van klanten) en vraagt ze allemaal

via Viber door te sturen.” Een gesmokkelde die met succes in de UK aangekomen was, meldde dit telefonisch aan de smokkelaar en kreeg prompt het advies om Viber te gebruiken voor deze communicatie.

In een ander Koerdisch smokkeldossier¹¹⁰ kregen de smokkelaars van hun leider expliciet de opdracht om de smokkelklanten via Viber te contacteren. De politie kon de chatberichten tussen de smokkelaars en hun Iraanse klanten traceren waarin de afspraakplaatsen (hotels in Brussel) vermeld stonden.

In een Oekraïens smokkeldossier¹¹¹ gebruikten de smokkelaars meerdere Skype profielen waarmee ze de gesmokkelden naar Viber doorstuurden: “Hallo! Hoe gaat het? Zal er vandaag iets zijn? Hoe is het met een pakket kippenhuisje (noot: safehouse waar de gesmokkelden zitten)? Antwoord: Goedendag. Er is een jongen van Spanje. Hij is aan het aankomen. Die jongen heeft nog niet gebeld. Er is nog niemand voorlopig. Voeg hem toe via Viber. Hij zal vanochtend in Brussel zijn.”

3.2. | Management van smokkelnetwerken

Sociale media hebben een sterke impact op de dynamiek van de mensensmokkel. EMN concludeerde hierover: “Het gebruik van sociale media heeft een enorme impact op illegale migratie. Ze helpen migranten de krachten te bundelen, aan de buitengrenzen een snellere dynamiek op gang te brengen en ze verhogen ook de mate waarin smokkelaars hun routes kunnen aanpassen in functie van veiligheidssituaties.”¹¹² Tegelijkertijd kunnen ze hun smokkelactiviteiten beter afschermen via sociale media. Frontex stelde hetzelfde vast.¹¹³

In de dossiers stellen we vast dat de mensensmokkelaars de sociale media voor hun vertrouwelijke gesprekken in verschillende facetten gebruiken voor het intern beheren van hun smokkelbusiness. De verschillende faciliterende aspecten van de sociale media komen hierbij aan bod: financieel beheer, klantenbeheer, intern organisatiebeheer smokkelnetwerk en contrastrategie.

Financieel beheer en discussies

Uit de dossiers blijkt dat mensensmokkelaars verkiezen om hun financiële gesprekken via sociale media te voeren. Delicate onderwerpen zoals financiële discussies mochten niet via de telefoon besproken worden.

De politie kon in de telefoontap van een Koerdisch smokkeldossier¹¹⁴ vaststellen dat de smokkelaars dan telefonisch afspraken om het via Skype of Viber te bespreken: “Smokkelaar X verwijt smokkelaar Y dat hij geld achterhoudt van 3, die op donderdag 04.12 zijn verstuurd. Smokkelaar Y zit op dat moment in Nederland en wilt het niet bespreken over de telefoon, maar via het internet.”

De smokkelaars gebruikten Facebook om de betalingen te regelen en te beheren. In een Koerdisch smokkeldossier¹¹⁵ verwees een smokkelaar in verband met de betaling van een klant tijdens een telefoongesprek naar een onbekend

109 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, dossieranalyse, pp.103-107.

110 Zie verder deel 3, hoofdstuk 2, punt 2 (dossieranalyse mensensmokkel).

111 Zie verder deel 3, hoofdstuk 3 (rechtspraak): Corr. Oost-Vlaanderen, afdeling Gent, 10 januari 2017, G28bis k.

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-aUYY2f>: “Personen die voor hun diensten publiciteit maken op sociale media zijn zich bewust van de risico's en zijn op verschillende sociale mediaplatforms actief. Meestal gebruiken ze Facebook, WhatsApp en Viber om de financiële details en de logistiek van de smokkeloperaties te bespreken.”

114 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, dossieranalyse, pp.101-103.

115 Zie verder deel 3, hoofdstuk 2, punt 2 (dossieranalyse mensensmokkel).

rekeningnummer voor de regeling van zijn betaling waarvan dan nadien een melding moest gestuurd worden via Facebook. In hetzelfde smokkeldossier werden bij het inlezen van Facebookberichten van een smokkelaar tekstberichten gevonden met transactiecodes van geldtransfers via geldtransferdiensten zoals Moneygram, Western Union e.d., namen en bankgegevens.

In een ander Koerdisch smokkeldossier¹¹⁶ werden de betalingen van de smokkelaars binnen het netwerk geregeld via Viber: “Op zaterdag 24 januari 2015 om 11.47u belt de gebruiker van 796 (smokkelaar) naar de financier in Nederland en zegt dat hij gisteren een naam heeft doorgestuurd. De vrouw (779) zegt dat ze niets ontvangen heeft. De smokkelaar zegt dat hij de naam via Viber zal sturen. Hoogstwaarschijnlijk moet de financier geld overmaken aan de smokkelaar op naam van X. Om 11.56u stuurt de gebruiker van 796 nogmaals hetzelfde bericht met de naam van betrokkene door naar de financier in Nederland.”

Volgens het UNHCR-rapport¹¹⁷ zijn er meer dan honderd Afghaanse freelance bankiers actief op Facebook die de financiële transfers regelen tussen de smokkelaar en de klant. Het UNHCR vond bewijzen op sociale media van dergelijke contacten in het VK, Hongarije, Oostenrijk, Duitsland en Ierland.

Vertrouwelijke discussies klantenbeheer

De smokkelaars verkiezen sociale media om over hun klantenbeheer te communiceren. Hiervan zijn er duidelijke voorbeelden in de dossiers.

In een Oekraïens smokkeldossier¹¹⁸ schakelden ze doelbewust over van een gsm-gesprek naar Skype wanneer klanten ter sprake kwamen: “Smokkelaar Z. belt naar smokkelaar S. en geeft een situatieschets. Hij heeft nu nog 12 of 13 ‘kandidaten’ zitten om te verplaatsen. Verdere communicatie via Skype.” De politie vond in de smartphone van een smokkelaar relevante Skype- en Viber-berichten terug waarbij locaties (vooral parkings langs autosnelwegen) en adressen van safehouses werden doorgegeven en daarnaast een communicatie over een persoon die vanuit Spanje ging aankomen.

In een Iraaks smokkeldossier¹¹⁹ van Dendermonde had een smokkelaar A. vanuit België geprivilegieerde contacten met een Syrische smokkelaar in London die gekend stond als toeleveringskanaal van Syriërs. Deze twee smokkelaars waren vrienden via Facebook. Smokkelaar A. verklaarde tijdens zijn verhoor dat al zijn communicaties met de Syrische smokkelaar uit London via Viber en Facebook moest verlopen. In een verwant smokkeldossier van Brussel¹²⁰ onderhield dezelfde Syrische smokkelaar van London zijn contacten met een andere smokkelaar via Skype.

Vertrouwelijke discussies over interne organisatie en samenwerking

Smokkelnetwerken regelen via sociale media hun operationele werking. In een Oekraïens smokkeldossier¹²¹ regelden de smokkelaars hun operationeel smokkelbeheer via Skype. De politie analyseerde de Skype-berichten van de smokkelaars en concludeerde hierover: “Wij stellen vast dat bij de communicatie (Skype) tussen X, Y en Z relatief gestructureerde mededelingen worden gedaan die als relevant voor het onderzoek kunnen worden bestempeld. De communicatie handelt vooral over de volgende twee onderwerpen: a) doorgave van Poolse telefoonnummers met daarnaast een bedrag in euro en een tijdstip. Het betreft hier met een aan zekerheid grenzende waarschijnlijkheid oproepnummers van chauffeurs die “kandidaten” meenemen over de Frans-Britse grens, het aan hen te betalen bedrag alsook het tijdstip waarop met de man contact moet genomen worden; b) doorgave van Poolse namen, geboortedata en alfanumerieke gegevens zijnde gegevens van Poolse identiteitskaarten die gecheckt worden op hun bruikbaarheid (al dan niet geseind staan); ... In die communicaties worden gegevens van Poolse identiteitskaarten overgemaakt die vervolgens al dan niet met een OK worden teruggestuurd. Uit de modus operandi blijkt dat [de] organisatie gebruik maakt van Poolse identiteitskaarten die gekocht worden van hun eigenaars.”

De smokkelaars leggen via sociale media contact met andere smokkelaars uit de herkomstlanden. In een Afghaans smokkeldossier¹²² vatten de smokkelaars telefonisch een gesprek aan over een nieuwe Afghaanse smokkelaar die ze wilden contacteren. Ze spraken af hun gesprek later met behulp van videochat verder te zetten: “557 vraagt of 166 naar Afghanistan is geweest. 166 zegt dat

116 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, dossieranalyse, pp.103-107.

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 Zie verder deel 3, hoofdstuk 3 (rechtspraak): Corr. Oost-Vlaanderen, afdeling Gent, 10 januari 2017, G28bis k.

119 Zie verder deel 3, hoofdstuk 2, punt 2 (dossieranalyse mensenmokkel).

120 Corr. Brussel, 13 oktober 2016, 60° k. (niet-gepubliceerd).

121 Zie verder deel 3, hoofdstuk 3 (rechtspraak): Corr. Oost-Vlaanderen, afdeling Gent, 10 januari 2017, G28bis k.

122 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, dossieranalyse, pp. 107-109.

hij voor 51 dagen naar Afghanistan is gegaan en zegt dat mensensmokkelaars nu 17.000 dollar vragen om mensen naar hier te sturen. 557 vraagt of hij het nummer van die persoon kan doorsturen. 166 zegt dat er een meisje in Kabul is die het werk doet. 557 vraagt om haar nummer en zegt dat hij met haar wilt praten. 166 zegt dat ze het doet in 25 dagen en dan zegt dat hij straks met 557 met videochat zal praten. het nummer is (...) en dan zegt hij dat hij voor zekerheid nog een keer dat nummer zal sturen via Facebook.”

In een Albanees smokkeldossier¹²³ wisselden de smokkelaars hun Skype-adressen uit en bediscussieerden ze via Skype rechtstreeks hun smokkeloperaties en problemen. De politie was hiervan enkel op de hoogte omdat de smokkelaars tijdens hun gsm-gesprekken hiernaar verwezen hadden.

Contrastrategie

Uit de bevraging van de EU-landen leidt EMN af: “Uit onderzoek is gebleken dat smokkelaars liever via internet dan via telefoon communiceren. Deze manier van werken verloopt anoniemer en beperkt de risico’s op een politie-interventie, en tegelijk kunnen ze er hun activiteiten mee uitbreiden.”¹²⁴

De smokkelleiders geven duidelijke richtlijnen om niet telefonisch maar via sociale media te communiceren. In een Afghaans smokkeldossier¹²⁵ verwittigden de smokkelaars elkaar dat ze door de politie afgeluisterd werden en zeiden in een afgeluisterde telefoontap: “Kom via Skype praten. Ok, ik kom over 5 minuten.” Een vergelijkbare tap in Koerdisch dossier¹²⁶: “Het is smokkelaar A die belt met een Brits nummer, smokkelaar W vraagt hem te corresponderen via Viber.”

De smokkelaars wijzigden regelmatig hun mobiele telefoonnummers om de telefoontap te bemoeilijken en wisselden hun nieuwe nummers via Facebook uit. Een mooi voorbeeld van een telefoontap in een Koerdisch smokkeldossier¹²⁷: “Smokkelaar D vraagt aan smokkelaar S om zijn nieuw gsm-nummer via Facebook te sturen en zegt dat hij ook een nieuw nummer zal hebben morgen... Beiden spreken nogmaals af om hun oproepnummer te

veranderen en hun nieuw nummer door te sturen via Facebook.” Tijdens zijn verhoor gaf een smokkelaar aan de politie openlijk toe: “We probeerden ook zoveel mogelijk te communiceren via het Internet (Facebook en WhatsApp, maar vooral Viber) omdat de politie dit niet kan afluisteren.”

Volgens een onderzoeksrapport¹²⁸ past een dergelijke toepassing van sociale media in een strategie van de professionalisering van smokkelnetwerken.¹²⁹ Een smokkelaar die voor deze studie geïnterviewd werd, legde uit: “Zelf heb ik meer dan 100 Simkaarten voor gsm’s gebruikt,” vertelt de Afghaanse smokkelaar J. “Ik heb misschien wel meer dan 40 of 50 Facebook accounts. Ik activeer ze wanneer ik die nodig heb en zodra mijn klanten op hun bestemming zijn toegekomen, deactiveer ik ze.”¹³⁰ Een dergelijke de-activatie van zijn Facebook account wordt als een nieuwe vorm van contratechniek beschouwd.

Tegenwoordig stellen we in de smokkeldossiers vast dat de smokkelaars beseffen dat chatberichten van sociale media net zoals bij gsm door de politie kunnen gelezen en geanalyseerd worden. In een Koerdisch smokkeldossier¹³¹ blijkt dat de smokkelaars zich hieraan trachten aan te passen en bezig zijn met het ontwikkelen van contratechnieken bij de sociale media. Na de arrestatie van verschillende smokkelaars slaagden vier smokkelaars om te vluchten naar Frankrijk. Een van de gevluchte smokkelaars verwittigde telefonisch snel de anderen om de digitale sporen van de aangehouden smokkelaars te verwijderen zodat de politie geen verband meer tussen hen zou kunnen leggen: “Op 22/05/2015 neemt Q (gevluchte smokkelaar) via zijn Frans telefoonnummer contact op met P (smokkelaar). Q informeert enerzijds naar de toestand van de verdachten die op 22/05/2015 zijn aangehouden (en adviseert om hun namen op Viber te blokkeren), anderzijds geeft hij aan dat hij zijn smartphone heeft verloren op de parking. Hij vraagt aan P om bij aantreffen van zijn smartphone zijn Facebook af te zetten (geeft pincode 2101 door).”

In hetzelfde dossier was een smokkelaar bezig met de prospectie van vrachtwagens voor een smokkeloperatie. Tijdens een telefoongesprek wordt hem gevraagd de foto’s niet naar Facebook te sturen. Hij wist dat deze belangrijke

123 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2015, *Schakels verbinden*, dossieranalyse, pp. 78-80.

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, Jaarverslag Mensenhandel en Mensensmokkel 2015, *Schakels verbinden*, dossieranalyse, pp. 85-90.

126 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, dossieranalyse, pp. 101-103.

127 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, dossieranalyse, pp. 103-107.

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 “Smokkelaars zijn zeer creatief en passen hun criminele activiteiten zeer snel aan de nieuwe obstakels aan. Via sociale mediaplatformen zoals Facebook, of versleutelde mobiele apps zoals WhatsApp, Imo en Viber, kunnen smokkelaars makkelijk politieacties omzeilen.”

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

131 Zie verder deel 3, hoofdstuk 2, punt 2 (dossieranalyse mensensmokkel).

operationele smokkelgegevens zijn die door de politie kunnen teruggevonden worden: “597 belt 782 met de mededeling dat hij juist twee foto’s heeft genomen, hij zal de foto’s naar 782 sturen en vraagt om te kijken om te zien of die wel daar naartoe gaan of niet (noot politie: vermoedelijk naar bepaalde bestemming Verenigd Koninkrijk, vermoedelijk foto’s van vrachtwagens met bepaalde bestemming, dit uit de context van het gesprek gehaald). 782 vraagt om geen foto’s op zijn Facebook te sturen.”

3.3. | Sociale media en uitbuiting van smokkelslachtoffers

De smokkelaars zetten ook sociale media in als hulpinstrument bij de uitbuiting van smokkelslachtoffers. Daarnaast zijn er ook meldingen van uitbuitingen op sociale media.

Sociale media als facilitator van seksuele uitbuiting

In een Afghaans smokkeldossier¹³² regelde de smokkelleider via Skype een gratis smokkelreis voor een minderjarige naar Frankrijk waarbij de jongen deze achteraf in natura moest afbetalen. Een medewerker telefoneerde naar de smokkelleider met de boodschap: “Er zijn een paar mooie jongens en als je wil kan ik ze naar jou sturen. De smokkelleider reageerde: laat maar, eerst eentje via Skype zien en dan zal ik eentje zijn reis helemaal tot Frankrijk vergoeden. Oké, geef mijn nummer aan een van die twee minderjarigen, aan diegene die er heel ‘luxe’ uitziet.”

Deze Afghaanse smokkelleider opereerde vanuit een smokkelkamp in Calais, waar het UNHCR ook melding gemaakt heeft van seksueel misbruik van Afghaanse jongetjes.¹³³

132 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2015, *Schakels verbinden*, dossieranalyse, pp. 85-90.

133 UNHCR, *From A Refugee Perspective, Discourse of Arabic speaking and Afghan refugees and migrants on social media from March to December 2016*, Aril 2017. www.unhcr.org/uk/5909af4d4.pdf: “Uit individuele interviews met onze onderzoeker te Calais is gebleken dat een aantal zeer jonge jongens heeft laten verstaan seksueel te zijn misbruikt door smokkelaars. Dit is iets waar jonge Afghanen niet snel over zullen praten uit vrees voor stigmatisering en/of vergelding... Meestal zijn Afghaanse migranten zeer jong en niet-geïnformeerd, en zijn ze volledig afhankelijk van hun smokkelaar, wat hen kwetsbaar maakt voor misbruik zoals seksuele uitbuiting.”

Meldingen van uitbuiting op sociale media en internet

De migranten beginnen zelf ook meer situaties van misbruiken te posten op sociale media om hun lotgenoten te waarschuwen. Dit kan leiden tot een vorm van sociale controle op digitaal niveau. Zo werden op sociale media reeds getuigenissen van verkrachtingen van vrouwen gerapporteerd die onderweg plaatsvonden.¹³⁴ Er werden ook filmpjes gepost waarin smokkelaars migranten onder dreiging van een wapen dwingen in een overbevolkt bootje te kruipen.¹³⁵

Het EU-project over de rol van sociale media en de migrant, maakt melding van een online platform dat de schendingen registreert van de mensenrechten van de migranten aan de Middellandse Zee: Watch The Med¹³⁶ is een online mapping platform, dat het aantal overlijdens van migranten en schendingen van de mensenrechten op zee bijhoudt.¹³⁷ De informatie op dit platform is gebaseerd op verslagen en getuigenissen die via telefoon of internet door migranten, familieleden, zeelui en andere getuigen van schendingen van rechten van migranten op zee worden verstuurd.¹³⁸

De migranten beginnen zelf ook meer situaties van misbruiken te posten op sociale media om hun lotgenoten te waarschuwen.

3.4. | Sociale media, internet en veilige migratieroutes

In haar vorige jaarrapporten heeft Myria reeds gewezen op het belang van veilige migratieroutes. Sociale media kunnen hierin een grote rol spelen. Een studie formuleert het als volgt: “Vluchtelingen worden via telefoon over routes geïnformeerd. Op die manier komen ze te weten welke grenzen open zijn en welke niet. Maar nog voor ze zover zijn kan hun telefoon al hun leven hebben gered, door hen informatie te geven over de weersomstandigheden tijdens een overtocht op zee. Meestal hebben ze drie

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.

basisbehoeften: een smartphone, eten en water – in die volgorde.”¹³⁹

Hieronder enkele best practices die ondertussen reeds ontwikkeld werden en de mogelijkheden van sociale media tonen.

Veilige migratieroutes

De migranten navigeren onderweg met behulp van Google Maps en wisselen onderling de veilige routes met de actuele wijzigingen uit.¹⁴⁰ In 2015 en 2016 gebruikten ze Google Maps om vanuit Griekenland verschillende landen te doorkruisen langs de zogenaamde Balkan route naar West Europa.¹⁴¹ Toen in 2015 Hongarije de grenzen sloot en de migratieroute naar Kroatië en Servië verschoof, werd via Facebook een applicatie ontwikkeld met een map van de locaties van de landmijnen in deze twee landen zodat de migranten veilig konden doorreizen.¹⁴²

Het EU-project dat de rol van de sociale media voor migranten onderzoekt, vermeldt in haar tussentijds rapport verschillende ontwikkelde Apps als best practices. Google ontwikkelde tijdens de vluchtelingencrisis samen met verschillende NGO's de App 'Crisis Info Hub' met de actuele relevante informatie over Griekenland, Macedonia (FYROM), Servië, Kroatië en Slovenië en hun grensgebieden.¹⁴³

Migranten gebruiken sociale media als hulplijn voor onderweg, wat levens kan redden.

Een andere applicatie is "Infomobile - Welcome 2 Europe"¹⁴⁴ en werd door de migranten zelf ontwikkeld. Het geeft geüpdatete advies over het migratiebeleid en contactgegevens van de NGO's van 35 landen.¹⁴⁵

Facebook-gebruikersgroepen zonder smokkelaars

Er werden Facebook-groepen opgestart voor migranten die zonder smokkelaar naar het Westen willen reizen. De Facebook-pagina 'Europe without Smugglers' geeft informatie over de routes die vroeger enkel door smokkelaars geleverd werd. Een migrant verwoordde het zo aan een journalist: "Je hebt een heel netwerk van mensen binnen handbereik. Smokkelaars via de route over land zijn niet meer dan een extra kost. Vaak is het veel riskanter via hen te werken dan beroep te doen op andere vluchtelingen."¹⁴⁶

De Facebook-groep "Asylum and Immigration without Smugglers" heeft meer dan 15.000 leden en navigeert de migranten zonder smokkelaars individueel of in groep door Europa. Een migrant postte de vraag om zich aan te sluiten bij een groep: "Ik ben in Turkije en zou graag naar Duitsland of Zweden gaan, is er toevallig een groep die klaar staat om te vertrekken?" Een persoon antwoordde daarop: "Mijn vader en broer doen ook de reis en we zijn niet een groep aan het vormen, bel me op dat nummer: xxx".¹⁴⁷

Sociale media als levenslijn voor onderweg

Migranten gebruiken sociale media als hulplijn voor onderweg, wat levens kan redden. Een migrant getuigde hierover aan een journalist: "Aan het begin van zijn gevaarlijke reis over de Egeïsche Zee in een rubber bootje met 62 andere vluchtelingen, belde H. een vriendin in New York. Hij wou haar aan de lijn houden in het geval er iets fout zou lopen. En er liep iets fout. De boot begon water te maken en zonk. Toen H. in het water terecht kwam kon hij zijn telefoon boven de golven houden en

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*, juni 2016. <http://reliefweb.int/sites/reliefweb.int/files/resources/RMMS%20Briefing%20paper%202016%20Social%20Media%20in%20Mixed%20MigrationUPLD.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: "Het Google team wees op een "gebrek aan tijdelijke hyperlokale informatie voor vluchtelingen", en ontwikkelde iets wat vluchtelingen behalve vitale informatie over hun vertrek, reis en aankomst, ook gegevens zou verschaffen die essentieel waren voor hun reis: huisvesting, transport, medische voorzieningen, enz. Er circuleert een lijst van Ngo's die vluchtelingen juridische bijstand en gezondheids- en sociale voorzieningen bieden."

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: "Vluchtelingen worden ertoe aangezet de verschillende links aan te klikken om er informatie te vinden over: "veiligheid op zee", "asiel", "Dublin II", "gender", "minderjarigen", "regularisatie", "detentie", "deportatie", "leven", "gezin", "medische aspecten" en "arbeid."

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*, juni 2016. <http://reliefweb.int/sites/reliefweb.int/files/resources/RMMS%20Briefing%20paper%202016%20Social%20Media%20in%20Mixed%20MigrationUPLD.pdf>.

zijn vriendin vragen de Turkse kustwacht te verwittigen. Via WhatsApp kon hij zijn locatie geven. 45 minuten later werd hij gered.”¹⁴⁸ Een gelijkaardige getuigenis was er ook waarbij Twitter een cruciale rol speelde als hulpinstrument dat vele mensenlevens redde.¹⁴⁹

Volgens het IOM (International Organization for Migration)¹⁵⁰ werden in 2016 in totaal 7763 migranten bij hun overtocht als dood geregistreerd. Hiervan zijn er in 2016 op de Middellandse Zee 5.096 mensen verdrinken of vermist.¹⁵¹ In 2015 waren er dit 3.771 voor de Middellandse Zee. Volgens UNHCR waren er op 31 juli 2017 al 2.409 doden of vermisten op de Middellandse Zee geregistreerd.¹⁵²

Ondertussen worden verschillende applicaties ontwikkeld die als hulplijn dienen. Zo bestaat er een Facebook-pagina met real-time informatie over vermiste bootjes op de Middellandse Zee.¹⁵³

Het EU-project over de sociale en de migrant verwijst naar Alarmphone¹⁵⁴ als een hotline voor de ondersteuning van hulpoperaties.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>: “Een Twittergebruiker, die een telefoontje kreeg van iemand aan boord van een schip met motorpech op de Middellandse Zee, gebruikte Twitter om het nummer van de Italiaanse kustwacht te bemachtigen en tweette: “250 Eritreeërs, vooral vrouwen en kinderen, bevinden zich op een schip in nood op de Middellandse Zee. Help, ze hebben hulp nodig! Motor in panne”. Dit bericht werd getweet met de GPS coördinaten om de aandacht van de hulpdiensten te trekken.

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

151 Zie MYRIA, *Jaarverslag Migratie in Cijfers en Rechten 2017*, 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%202020_Social%20Media%20in%20Mixed%20MigrationUPLOAD.pdf: “Lukman Derky, een Syriër die in Frankrijk woont, heeft meer dan 58.000 volgers op zijn Facebook pagina. Hij deelt informatie over boten die vermist zijn geraakt tijdens de overtocht over de Middellandse Zee. Daarnaast vermelden de gegevens ook de laatst gekende GPS coördinaten van de boten, gegevens voor mensen in nood op het vasteland en een hulpoproep gericht aan de dichtste volger om hen te hulp te komen.”

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: “Alarmphone is een “zichzelf organiserende” noodlijn, die binnen een samenwerkingsproject van een activistennetwerk is ontstaan. Het initiatief richt zich tot vluchtelingen die per boot reizen en die tijdens hun overtocht over de Middellandse Zee in gevaar en in nood verkeren. Het geeft de vluchtelingen op zee een tweede kans om een SOS-bericht de wereld in te sturen. Alarmphone documenteert en mobiliseert in real-time. Op die manier verhoogt de druk om zoveel mogelijk hulp te bieden en worden push-backs en andere vormen van schendingen van de rechten van vluchtelingen en migranten op zee bemoedigd. Alarmphone is dus geen noodnummer maar een alarmnummer ter ondersteuning van hulpoperaties.”

Hoofdstuk 2

Sociale media en internet als onderzoeksmethode

Justitie en politie gebruiken sociale media en internet zelf ook als onderzoeksmethode bij hun speurwerk. Ondanks de vele nieuwe uitdagingen¹⁵⁶ heeft de Europees Migratienetwerk (EMN) in haar bevraging van de EU-landen vastgesteld dat de meeste Europese landen sociale media en internet als onderzoeksinstrument gebruiken om bewijsmateriaal te vergaren in de strijd tegen mensensmokkel.¹⁵⁷ In zeven EU-landen bestaat hierover ook een samenwerking in de strijd tegen mensenhandel.¹⁵⁸

In de Belgische dossiers van mensenhandel en mensensmokkel waarin Myria burgerlijke partij is of kennis van genomen heeft, stellen we vast dat sociale media en internet op diverse wijze in de verschillende fases van het onderzoek gebruikt worden. De resultaten kunnen door de rechtbank bij de motiveringen van hun uitspraken als objectief bewijsmateriaal gebruikt worden.¹⁵⁹ Dit is een belangrijke verdienste van de Belgische justitie die beantwoordt aan een aanbeveling van EMN,¹⁶⁰ niet alleen voor de strijd tegen mensensmokkel

De sociale media en internet, gebruikt als onderzoeksinstrumenten, zijn veel minder aanwezig in dossiers van economische uitbuiting.

maar ook mensenhandel. Deze gegevens moeten wel meer internationaal gedeeld worden als een best practice. Het EU-project *Trace* beveelt daarom aan om dit in te voeren in de “Human Trafficking Case Law Database” van de United Nations Office on Drugs and Crime (UNODC), die hiervoor opgericht werd.¹⁶¹ Het is ook wenselijk en noodzakelijk dat dergelijk instrument ook noodzakelijk op EU-niveau in het leven geroepen wordt.¹⁶²

We stellen wel vast dat de sociale media en internet als onderzoeksinstrumenten veel minder aanwezig zijn in dossiers van economische uitbuiting terwijl dit bijvoorbeeld bij het verhoor van een slachtoffer voor het aanwijzen van een locatie via Google Maps nuttig kan zijn. Hiervoor moeten de eerstelijnsdiensten zoals de inspectiediensten een training krijgen. Daarnaast is ook een aanbeveling van het EU-project *Trace* het overwegen waard: “De strikte controle van websites met online jobadvertenties bevorderen (ofwel door de politiediensten, ofwel door organisaties uit het middenveld), vooral in sectoren waar mensenhandel regelmatig voorkomt.”¹⁶³

156 EMN Inform, *The Use of Social Media in the Fight Against Migrant Smuggling*, September 2016: “Sociale media hebben een belangrijke rol gespeeld in de toename van niet enkel het volume maar ook de efficiëntie van smokkeloperaties, waardoor het speurwerk en de vervolgingen in dat soort dossiers doorgaans moeilijker is. Bovendien wordt de controle nog bemoeilijkt door de anonimiteit van de gebruikers, afgesloten accounts, pagina’s met beperkte toegang, versleuteling, het gebruik van het dark net, moeilijke samenwerking met service providers, enz.”

157 Samenvatting van de EMN ad-hoc vraag nr. 1055 van 18 april 2016, *Addressing and preventing the use of social media in migrant smuggling*: de meeste lidstaten (BE, CZ, DE, ES, FR, HR, HU, LT, NL, PL, SE, SI, UK) lieten weten dat ze sociale media en online platforms gebruiken om informatie tegen smokkelaars te verzamelen.

158 *Ibid.*: verschillende lidstaten (BE, CZ, DE, EE, ES, NL, PL) gaven voorbeelden van bestaande samenwerking bij andere vormen van misdaad, zoals mensenhandel en seksuele uitbuiting.

159 Myria, Jaarverslag Mensenhandel 2013, *Bruggen slaan*, pp. 60-61.

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: “De door het VN-Bureau voor drugs- en misdaadbestrijding (UNODC) opgerichte “Human Trafficking Case Law Database” is een voorbeeld van een platform voor de uitwisseling van informatie. Misdaaddossiers die met mensenhandel te maken hebben kunnen er worden geüpload. Het is tegelijk een publieke ruimte waar samenvattingen en volledige gerechtelijke documenten van mensenhandeldossiers kunnen worden ingekeken, en die kan sensibiliseren over hoe het in mensenhandeldossiers tot effectieve veroordelingen kan komen.”

162 http://data.trilateralresearch.com/wp-content/uploads/2015/11/TRACE_D4.1_Role-of-technologies-in-human-trafficking_FINAL.-1.pdf: Nationale en/of Europese databases oprichten over dossiers van mensenhandel. Dat soort databases bevat in principe geen informatie over de identificatie van slachtoffers of de daders, de databank voorziet wel in geactualiseerde statistieken, commentaar bij de modus operandi, geografische patronen, enz. De informatie zou ervoor kunnen zorgen dat de toekomstige Eurostat verslagen in de toekomst betrouwbaarder en makkelijker te analyseren zijn.

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

1. OPENBRONNEN-ONDERZOEK

Het openbronnenonderzoek is een belangrijk onderdeel van het politiewerk. Het kan geleverd worden door een eerstelijnsdienst of door een steundienst van de politie indien hiertoe een verzoek is aangevraagd.¹⁶⁴

1.1. | Opstartfase onderzoek

Bij mensenhandel kan een dossier opgestart worden op basis van een internetonderzoek naar een escortservice waarbij indicaties van seksuele uitbuiting aangetroffen worden. Dit gebeurt aan de hand van internetadvertenties en online forumgesprekken.

Een Nigeriaans dossier¹⁶⁵ van Tongeren werd opgestart naar aanleiding van een politietoezicht naar verdoken vormen van prostitutie. De politie besteedde hierbij aandacht aan bepaalde internetwebsites waar Afrikaanse vrouwen zich als escorte presenteerden. Na een inhoudelijke analyse van de gegevens van de website stelden de speurders mogelijke indicaties van mensenhandel vast. Uit talrijke klantenrecensies op de publiek toegankelijke forums van bepaalde websites kon de politie afleiden dat de huisvesting van de Afrikaanse vrouwen precair was, en dat ze vermoedelijk in een onwettige verblijfsstatus tewerkgesteld werden, wat op mensenhandel wees.

Bij mensensmokkel kan een internetonderzoek ook aanleiding geven tot de opstart van een smokkeldossier. Reeds in 2001 werd na een klacht van een smokkelslachtoffer een mensensmokkeldossier¹⁶⁶ in Brussel opgestart op basis van een internetonderzoek naar een Russisch agentschap dat verblijfsdocumenten aanbood via een asielpcedure. Het vonnis¹⁶⁷ schrijft hierover: “Het straf dossier start op met een PV van de Scheepvaartpolitie Oostende (22 januari 2001) over

een website die klaarblijkelijk beoogt vluchtelingen uit Rusland wegwijs te maken in de asielpcedure, en meer algemeen in het leven in België. Op de site “(...)” kan men zelf een pagina maken. Op die manier zijn er meerdere nieuwsbrieven op verschenen. (...) De Federale Politie GDA (...) heeft er weet van dat Russische onderdanen hun diensten aanbieden aan landgenoten tegen betaling. Op de website is sprake van een GSM nummer (...). Wanneer men dat nummer contacteert wordt er doorverwezen naar het nummer (...). Politie informatie wijst uit dat het nummer (...) zou kunnen worden gelinkt aan een (...) zogenaamde advocaat, K.D.”

1.2. | Detectie slachtoffers

De politie gebruikt sociale media en internet om slachtoffers van mensenhandel op te sporen. In een Hongaars dossier¹⁶⁸ slaagde de politie erin een minderjarig slachtoffer via Facebook op te sporen. De politie vond in de telefoontap een gesprek terug waarin de minderjarige de beklagde contacteerde voor prostitutiewerk. Hier gaf ze hem haar Facebook profiel met haar referenties zodat de politie haar gemakkelijk kon terugvinden.

Facebook kan ook dienen om slachtoffers te linken aan een prostitutienetwerk. In hetzelfde Hongaarse dossier¹⁶⁹ vonden de speurders in het Facebook profiel van de beklagde ronselaarster onder haar vrienden 34 Hongaarse vrouwen terug die in Gentse vitrinebars zaten. De politie slaagde erin de slachtoffers te identificeren en ze aan het prostitutienetwerk te linken. In een *loverboy*dossier¹⁷⁰ met minderjarigen uit jeugdinstanties kon de politie minderjarige slachtoffers terugvinden op een online forumsite voor seksdates.

De online forumsites van prostitutiekanten waar deze hun ervaringen uitwisselen, leveren belangrijke gegevens op voor de politie om te kunnen bepalen of er sprake is van aanwijzingen van mensenhandel. In dit geval is er dan ook sprake van potentiële slachtoffers van mensenhandel. In een Thais dossier van Leuven¹⁷¹ verzamelde de politie

164 Zie verder de externe bijdrage: “Presentatie DJOC/I2 in de strijd tegen mensenhandel: ondersteunende rol bij het doorzoeken van het internet en de sociale media”.

165 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2011, *Het geld dat telt*, p. 90.

166 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2008, *Bestrijden met mensen en middelen*, p. 73.

167 Correctionele rechtbank Brussel, 22 oktober 2008, 51^{ste} kamer (definitief) (beschikbaar op www.myria.be).

168 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2015, *Schakels verbinden*, dossieranalyse, pp. 66-70.

169 *Ibid.* Zie ook hierboven hoofdstuk 1, punt 1 van dit focus (De rol van sociale media en internet bij mensenhandel).

170 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, rechtspraak, p. 134; Corr. Antwerpen, 22 december 2015, k. A4C (definitief).

171 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2011, *Het geld dat telt*, p. 92.

De online forumsites van prostitutieklienten waar deze hun ervaringen uitwisselen, leveren belangrijke gegevens op voor de politie.

informatie over de prostitutie-ervaringen van de klanten van het massagesalon op de websites waar de klanten hun ervaringen deelden. Hiermee kon de politie aantonen dat het slachtoffers van mensenhandel waren. In een Thais dossier van Mechelen¹⁷² kon de politie nog andere slachtoffers detecteren via de online forumsites van prostitutieklienten. De uittreksels met de commentaren op deze websites toonden duidelijk aan dat buiten de massages ook verdere seksuele handelingen werden verricht.

In een dossier van een meedrinkzaak¹⁷³ kon de politie via de online forumsite aantonen dat een slachtoffer al veel langer uitgebuit werd. De politie voerde gerichte opzoekingen uit op het internet. Op een internetsite van prostitutieklienten trok een forumbericht van 2006 de aandacht van de politie. De prostitutieklient had al 47 berichten op het forum gepost over zijn persoonlijke ervaringen in verschillende bars. In zijn bericht over de geviseerde bar sprak hij over een jonge vrouw met valse Litouwse documenten. Hieruit kon de politie concluderen dat zij al in juni 2006 actief was in deze bar, ruim een jaar voordat ze in oktober 2007 aangetroffen werd bij de huiszoeking.

Om de detectie van slachtoffers te verbeteren beveelt Trace aan om via sociale media een soort hotline op te zetten: "Werk maken van betere instrumenten om makkelijker anoniem melding te kunnen maken van vermoedelijke feiten van mensenhandel op websites en sociale media. Een anonieme klacht bijvoorbeeld, via apps / websites / hotlines."¹⁷⁴

1.3. | Identificatie verdachten

Facebook is een makkelijk medium om mogelijke daders van mensenhandel en mensensmokkel te identificeren. Wanneer de Facebook profielen gesloten zijn, valt het buiten het openbronnenonderzoek en is een andere

procedure van toepassing.¹⁷⁵ Tegenwoordig gebruikt de politie en vooral de FGP deze onderzoeksmethode in hun dossiers. Maar de politie controleert ook de internetgegevens. Met Google Image kan bijvoorbeeld een persoonsfoto van een observatieoperatie vergeleken worden met bestaande foto's op de internetplatformen en op deze wijze het Facebook profiel van de betrokkene opgespoord worden. Het resultaat is de identificatie van de verdachte en veel bijkomende gegevens op zijn profiel.

Identificatie hoofdverdachte

In verschillende mensensmokkeldossiers kon de politie via foto's op Facebook de ware identiteit van een hoofdbeklaagde bepalen die onder een valse naam opereerde. Via openbronnenonderzoek kon de politie het profiel van de smokkelaar onder zijn valse naam terugvinden en vaststellen dat de foto van zijn profiel leek op de foto van een verdachte uit hun databank.

In een Koerdisch smokkeldossier¹⁷⁶ van Brugge had de politie per telefoontap vastgesteld dat een hoofdbeklaagde gebruik maakte van een valse naam op sociale media. Bij nazicht in het rijksregister kon de politie deze persoon niet terugvinden. Via openbronnenonderzoek op Facebook echter kon de politie het profiel van de smokkelaar onder zijn valse naam terugvinden, en vaststellen dat de foto van zijn Facebook profiel leek op de foto van de Irakees M., de ware identiteit van de hoofdbeklaagde wiens gegevens wel in de politionele databank zaten.

In een Albanees smokkeldossier van Gent verwijst de rechtbank in haar vonnis¹⁷⁷ naar een openbronnenonderzoek van het Facebook profiel van een geïntercepteerde gesmokkelde waarbij een verband kon gelegd worden met het Facebook profiel van de hoofdverdachte.

In een *loverboy*dossier¹⁷⁸ met minderjarigen uit jeugdinstantellingen werd een belangrijke verdachte geïdentificeerd door het vergelijken van een Facebook profielfoto met een foto uit het rijksregister.

In een Thais mensenhandeldossier¹⁷⁹ konden de daders op basis van telefoontap en internet geïdentificeerd worden.

172 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, dossieranalyse, pp. 87-90.

173 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2010, *Sociale fraude bestrijden is mensenhandel voorkomen*, p. 43.

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

175 Zie verder hoofdstuk 3 van deze focus (Internet en sociale media: nieuwe uitdagingen voor het beleid, de politie en justitie).

176 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, dossieranalyse, pp. 102.

177 Corr rechtbank Oost-Vlaanderen, afdeling Gent, 23 november 2015, 28° k. (niet gepubliceerd).

178 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, dossieranalyse, pp. 66-70.

179 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2011, *Het geld dat telt*, p. 92.

Op het moment dat een vliegtuigticket geboekt werd via een luchtvaartmaatschappij contacteerde de politie deze maatschappij om de volledige persoonsgegevens van betrokkene te bekomen. Via de internetbestellingen van vliegtuigtickets en de telefoontapegegevens kon de politie ook de identiteit en de referentiegegevens van andere slachtoffers en daders opsporen. Ze kende hen aanvankelijk enkel onder hun schuilnaam uit de gesprekken van de telefoontaps, maar door deze gegevens te koppelen aan hun betalingen met bankkaart kon hun identiteit achterhaald worden.

Identiteitswissel

De politie gebruikt Facebook om identiteitswissels van verdachten te onderzoeken. In een Iraaks smokkeldossier¹⁸⁰ van Dendermonde kon de politie via een vergelijking van de Facebook profielen bewijzen dat de smokkelaar bij zijn aanhouding een andere identiteit had aangenomen.¹⁸¹

Identificatie netwerk

De politie kan via een Facebookonderzoek het volledige netwerk beter in beeld krijgen. Hiervoor controleert ze de Facebook profielen van de verdachten. De link met vrienden, berichten en beeldmateriaal kunnen de speurders op het pad zetten van medeverdachten en relevante plaatsen zoals safehouses. Zowel in mensenhandeldossiers¹⁸² als mensensmokkeldossiers¹⁸³ heeft de politie op deze wijze bijkomende medeverdachten opgespoord.

Bij mensenhandel kon de politie op basis van een telefoontap in een Thais escortdossier¹⁸⁴ via Google de internetadvertentie van de escortservice terugvinden en onderzoeken. De rechtbank motiveerde in haar vonnis¹⁸⁵ de veroordeling voor mensenhandel expliciet met een verwijzing naar het internetonderzoek van deze website. In een Belgisch *loverboy*dossier¹⁸⁶, gelieerd met polycriminaliteit, werd als bewijselement op een Facebook profiel een filmpje gevonden waarop het slachtoffer vernederd werd. In een dossier van economische uitbuiting¹⁸⁷ gebruikte de politie Google als ondersteunend onderzoeksinstrument om gegevens over de firma van de beklagden op te zoeken.

In een Iraaks smokkeldossier¹⁸⁸ van Dendermonde slaagde de politie erin via Facebook de Syrische smokkelaar in Londen (VK) te identificeren die vanuit het VK de toelevering van Syrische smokkelslachtoffers via België regelde.¹⁸⁹ Hij werd als medebeklaagde vervolgd en veroordeeld en was tevens de hoofdbeklaagde in een Brussels smokkeldossier.¹⁹⁰

Een Facebookonderzoek kan ook bijkomende bewijslast opleveren. In een Koerdisch smokkeldossier¹⁹¹ van Gent kon de politie via openbronnenonderzoek belastende foto's vinden op het Facebook profiel van de hoofdbeklaagde. Daaruit bleek dat hij vier foto's had gepost van hemzelf met een alarmwapen in zijn linkerhand. Die foto's werden als bewijsstuk toegevoegd aan het proces-verbaal.

De politie kan via een Facebookonderzoek het volledige netwerk beter in beeld krijgen.

180 Zie verder, deel 3, hoofdstuk 2, punt 2 (dossieranalyse mensensmokkel).

181 Een proces-verbaal luidt als volgt: "Op het ogenblik van zijn arrestatie werd "B" niet in het bezit bevonden van enige identiteitsdocument, en werd hij op basis van mondelinge interpellatie geïdentificeerd als N. Middels het openbronnenonderzoek dienen we vast te stellen dat: "B" zijn Facebook pagina niet verwijst naar de door hem opgegeven identiteit N. Diezelfde foto komt ook voor op het Facebook profiel "A.N.". Uit consultatie van dit laatste account (zichtbare gedeelte) blijkt dit een andere persoon te zijn dan "B". Op de Facebook pagina staat te lezen dat de gebruiker van het profiel "A. N." iemand is die in S. woont. Beiden zijn wel kennissen van elkaar want het account van "A. N." heeft multipele foto's op de Facebook pagina van "B" geliked. Het geheel wijst aan dat de aangehouden in verdenkinggestelde "B" zich voor de Belgische autoriteiten een andere identiteit heeft aangemeten, een identiteit van een kennis van hem uit zijn herkomstland Irak."

182 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2015, *Schakels verbinden*, dossieranalyse, pp. 66-70 (Hongaars prostitutiedossier) en p. 29 (Roemeens prostitutiedossier); Jaarverslag Mensenhandel 2013, *Bruggen slaan*, pp. 17, 60 en 108 (Roemeens prostitutiedossier); Corr. Leuven, 4 juli 2013, 17^{de} k. (beschikbaar op www.myria.be)

183 Zie verder, deel 3, hoofdstuk 2, punt 2 (dossieranalyse mensensmokkel).

184 Zie verder, deel 3, hoofdstuk 3 (rechtspraak): Corr. Luik, afdeling Luik, 16 november 2016, 19^{de} k. (beroep).

185 *Ibid.*

186 Zie verder deel 3, hoofdstuk 2, punt 1.1. (dossieranalyse seksuele uitbuiting).

187 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, rechtspraak, p. 146.

188 Zie verder, deel 3, hoofdstuk 2, punt 2 (dossieranalyse mensensmokkel).

189 Een proces-verbaal luidt als volgt: "Op basis van voornoemde verklaring deden wij navolgend enkele opzoekingen op Facebook in een poging om die Syrische toeleverancier te kunnen identificeren. Opzoekingen naar het profiel X bleven zonder resultaat. Echter stelden we wel vast dat enkele geposte foto's op smokkelaar A zijn Facebook profiel werden 'geliked' door de houder van het Facebook profiel "M". Bij consultatie van het publieke gedeelte van dit laatste profiel stellen we vast dat de houder ervan claimt in Londen te wonen. Er staan 5 foto's op het publieke gedeelte welke volgens de context vermoedelijk de profielhouder afbeelden. Inzake identificatie stellen wij bijkomend vast dat M, volgens de Algemene Nationale Gegevensbank (ANG) staat gekoppeld aan het mensensmokkelonderzoek C. Op basis van de gevatte foto's in de ANG stellen wij vast dat M de binnen huidige onderzoek op te sporen verdachte X betreft."

190 Zie verder, deel 3, hoofdstuk 2, punt 2 (dossieranalyse mensensmokkel).

191 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, dossieranalyse, p. 106.

2. VERHOREN

Sociale media en internet zijn nuttige instrumenten bij de verhoren van de slachtoffers en de verdachten. Facebook en Google Maps kunnen een belangrijke meerwaarde en bijkomende pistes opleveren voor het onderzoek.

2.1. | Verhoor slachtoffers

Bij de verhoren van de slachtoffers gebruikt de politie vooral Google Maps en Facebook maar ook slachtoffers zelf kunnen bewijsmateriaal van sociale media aanbrengen.

Google Maps

Dikwijls weten slachtoffers niet exact waar ze werden vastgehouden. Vroeger reed de politie dan samen met het slachtoffer met de auto in de omgeving rond om de exacte plaats te kunnen lokaliseren. Tegenwoordig gebruikt de politie Google maps bij het verhoor van slachtoffers om na te gaan waar ze gelokaliseerd waren en kunnen ze op deze manier het volledige adres achterhalen. Daarnaast maakt de politie bij een slachtofferverklaring al gebruik van de webapplicatie Google Maps om met de hulp van het slachtoffer de route naar en de plaats van de feiten terug te vinden.¹⁹²

Facebook

De politie gebruikt Facebook profielen bij de verhoren van de slachtoffers om zoveel mogelijk relevante informatie voor het onderzoek te verzamelen.

In een ander *loverboy*dossier¹⁹³ met minderjarigen uit jeugdinstellingen kon het slachtoffer een verdachte aanduiden via zijn Facebook profiel.¹⁹⁴ Via een vergelijking met de foto's van de politie kon de beklaagde formeel geïdentificeerd worden.

In een Nigeriaans dossier¹⁹⁵ van Brussel kon een minderjarig slachtoffer tijdens haar verhoor een medebeklaagde aanduiden op basis van zijn Facebook profiel foto. In hetzelfde dossier kon de politie een ander slachtoffer bevrijden omdat ze via Facebook nog contact had met een van de Nigeriaanse slachtoffers. Dat slachtoffer had verklaard dat ze via Facebook wist in welke andere club ze tewerkgesteld werd. De FGP controleerde de club en kon het andere meisje interceperen.

In een Iraaks smokkeldossier¹⁹⁶ van Dendermonde onderzocht reeds eerder de Brusselse politie na de klacht van Iraanse smokkelslachtoffers in 2014 de Facebook profielen van de verdachte smokkelaars die door de slachtoffers aangeduid werden. Hiermee kon de politie de smokkelaars identificeren.¹⁹⁷

Bewijsmateriaal van slachtoffers

Slachtoffers geven tijdens hun verhoor zelf bewijsmateriaal aan de speurders. Dit kan een opname van een Skypegesprek zijn of een USB-stick met berichten en beeldmateriaal op Facebook.

In een Hongaars mensenhandeldossier¹⁹⁸ van Gent kon een slachtoffer via Skype bewijzen dat haar pooier valse verklaringen had afgelegd. Ze beriep zich op een vriendin die het mondeling Skypegesprek met de pooier had opgenomen. De politie kon dit Skypegesprek bij haar vriendin opvragen en de inhoud ervan toetsen. Dit werd nadien als bewijselement tegen haar pooier in het vonnis¹⁹⁹ opgenomen.

In een Belgisch *loverboy*dossier²⁰⁰, gelieerd met polycriminaliteit, gaf een slachtoffer bij haar herverhoor een USB-stick met Facebook berichten en -foto's aan de speurders. Hiermee kon ze bewijzen dat na haar klacht een beklaagde haar bedreigd had. Op basis van de foto's en berichten konden nieuwe slachtoffers gedetecteerd en geïdentificeerd worden. Op een foto stond een vriendin uit een vluchthuis die haar in een Facebookbericht had verteld dat de beklaagde haar ook in de prostitutie had willen plaatsen. De politie verhoorde de vriendin als getuige,

195 Zie verder, deel 3, hoofdstuk 3 (rechtspraak).

196 Zie verder, deel 3, hoofdstuk 2, punt 2 (dossieranalyse mensensmokkel).

197 Een proces-verbaal luidt als volgt: "Op basis van de inhoud van de verhoren gaan wij over tot de nodige verificaties. Voor wat betreft de genaamde S treffen wij het Facebook profiel onder de naam 'S.N.' aan en nemen hiervan een printscreen van de profielpagina en de foto's. Zijn GSM-nummer is gekend in het ANG voor het dossier mensensmokkel D. en het dossier 'K'. In dit dossier werd betrokkene onderschept samen met onze slachtoffers tijdens een transport op vrachtwagen."

198 Zie verder, deel 3, hoofdstuk 3 (rechtspraak).

199 Zie verder, deel 3, hoofdstuk 3 (rechtspraak): Corr. Oost Vlaanderen, afdeling Gent, 31 maart 2017, k.G28m (beroep).

200 Zie verder deel 3, hoofdstuk 2, punt 1.1. (dossieranalyse seksuele uitbuiting).

192 MYRIA, Jaarverslag Mensenhandel 2013, *Bruggen slaan*, pp. 60-61.

193 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, dossieranalyse, pp. 81-83.

194 En proces-verbaal luidt als volgt: "Via Facebook wees het slachtoffer A. op het profiel van T. als dader; dit betrof vermoedelijk B. Ze had ook een vermoeden van de woonplaats van de verdachten."

waarbij deze verklaarde dat de beklagde verschillende slachtoffers gerekruteerd had voor prostitutie en duidelijk een pooier was. In hetzelfde dossier gaf een minderjarig slachtoffer bij haar verhoor de politie een Facebookbericht dat aantoonde dat de beklagde gepoogd had haar via het profiel van een ander slachtoffer te contacteren, wat omwille van mogelijke manipulaties absoluut verboden is.

2.2. | Verhoor verdachten

De politie gebruikt Facebook en Google Maps als een instrument tijdens het verhoor van beklagden.

Google Maps

Bij de verhoren van verdachten kan de politie met behulp van Google Maps bepaalde belangrijke plaatsen voor de smokkelactiviteiten zoals safehouses traceren. In een Koerdisch smokkeldossier²⁰¹ van Gent toonde de beklagde tijdens zijn verhoor aan de politie het hotel waar hij samen met de andere smokkelaar gelogd had. Het hotel deed ook dienst als safehouse voor de smokkelactiviteiten.²⁰²

Facebook

In hetzelfde Koerdisch smokkeldossier²⁰³ van Gent gaf de beklagde bij zijn verhoor vrijwillig zijn Facebook wachtwoord om zijn volledige medewerking aan te tonen. De politie startte in zijn aanwezigheid Facebook op en liet hem via de foto's van zijn profiel aanwijzen welke mensen hij bedoelde in zijn verklaring. Hij gaf aan de hand van zijn Facebook foto's ook meer uitleg over andere smokkelaars.²⁰⁴

201 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, dossieranalyse, p. 106.

202 Een proces-verbaal luidt als volgt: "A. heeft me gezegd dat ik bij hem kon blijven slapen in het hotel X. Samen met u zoek ik het op via Google Maps en laat ik u een printscreen nemen van de ingang van het hotel die de benaming (...) heeft".

203 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, dossieranalyse, p. 106.

204 De citaten uit een proces-verbaal van het verhoor van de smokkelaar werden de volgende: Toen de politie hem vroeg: "Zijn er nog personen waarover je nog niet verteld hebt, maar die toch een belangrijke rol spelen binnen de organisatie?" antwoordde hij: "Alleen D., er zijn nog andere groepen, maar de mensen die ik in het theehuis heb gezien, zijn diegene waarover ik reeds verteld heb, ik heb geen foto van hem op mijn gsm, maar wel op Facebook. Ik toon je vrijwillig de foto op mijn Facebook."

3. ANALYSE

Europol verwijst naar het belang van technische analyse van smartphones, iPads en computers.²⁰⁵ Uit de dossiers, zowel van mensenhandel als mensensmokkel, blijkt dat deze analyses veel gegevens opleveren die als bewijselement kunnen dienen. In dit geval gaat het over analyses van inbeslaggenomen apparaten en is een mandaat van een magistraat vereist.²⁰⁶

3.1. | Berichten en beeldmateriaal

De meeste chatberichten en het opgeslagen beeldmateriaal kunnen opgespoord worden met behulp van een technische analyse van smartphones, iPads en computers. In veel dossiers heeft dit doorslaggevend bewijsmateriaal opgeleverd.

In een Iraaks mensensmokkeldossier²⁰⁷ van Dendermonde kon de politie 9000 berichten die in de map van de verwijderde bestanden zaten, terug zichtbaar maken. De meeste bestanden waren Skypegesprekken waarvan enkel de oproepinformatie beschikbaar was maar er waren ook verschillende relevante chatberichten met teksten over smokkeltransporten. Daarnaast werden vele verwijderde fotobestanden terug zichtbaar gemaakt. Op sommige foto's paradeerden de smokkelaars met vuurwapens. Bij een beklagde werden zelfs 270 verwijderde foto's met verwijzingen naar de terreurorganisatie Islamitische Staat teruggevonden en zichtbaar gemaakt.

In een Koerdisch smokkeldossier²⁰⁸ van Gent leverde de teruggevonden berichten belangrijke gegevens op over de hoofdbeklaagde. Zijn smartphone bevatte ook foto's van andere smokkelaars. Bij de analyse van zijn computer konden Facebook gesprekken over smokkeltransporten en financieel beheer gerecupereerd en de Facebook profielen van de betrokken gesprekspartners getraceerd worden.

205 EUROPOL, *Intelligence Notification 15/2014*, Den Haag, oktober 2014. www.europol.europa.eu/publications-documents/trafficking-in-human-beings-and-internet: "Online en op mobiele apparaten aangetroffen gegevens kunnen via forensisch onderzoek worden gerecupereerd en als bewijs worden gebruikt in dossiers. Gespecialiseerde speurders hebben continu technische bijscholing nodig om mee te kunnen met OCG's, die steeds vaker tegenmaatregelen nemen zoals versleutelde mails en versleutelde mobiele apparaten".

206 Zie verder hoofdstuk 3 van dit focus (Internet en sociale media: nieuwe uitdagingen voor het beleid, de politie en justitie).

207 Zie verder, deel 3, hoofdstuk 2, punt 2 (dossieranalyse mensensmokkel).

208 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, dossieranalyse, p. 106.

In een Albanees-Tsjechisch smokkeldossier verwees het vonnis²⁰⁹ voor het onderzoek onder meer naar de analyse van Skypeberichten van de smokkelaars.

In een Hongaars mensenhandeldossier²¹⁰ van Gent had een beklaagde zijn slachtoffers zelf gefilmd en de opnames opgeslagen in zijn iPhone. De politie beschreef dit uitvoerig in haar technisch verslag. In een dossier van economische uitbuiting in Pakistaanse nachtwinkels²¹¹ konden de relevante Skypeberichten en de contactpersonen van de beklaagde zijn smartphone geanalyseerd worden.

Technische analyses zijn belangrijk om de slachtofferverklaringen met objectieve bewijselementen te ondersteunen. In een Belgisch *loverboy*dossier²¹², gelieerd met polycriminaliteit, bevestigde het beeldmateriaal uit de computer de verklaringen van de slachtoffers en getuigen. Dit was ook het geval in verschillende dossiers van economische uitbuiting. In een manege-dossier²¹³ stelde de politie na haar onderzoek vast dat de internetadvertentie voor de job verbonden was aan het emailadres van de beklaagde. In een bouwdoos²¹⁴ werd de verklaring van het Pakistaans slachtoffer over zijn rekrutering in Italië bevestigd. Uit onderzoek van het Facebook profiel van het slachtoffer bleek dat deze met de Turkse beklaagde communiceerde over de vraag wanneer hij naar België moest komen om voor hem te werken.

3.2. | Chronologie afgelegde route

Informatie over de afgelegde routes kan relevant bewijsmateriaal opleveren. Dit is zeker het geval

bij mensensmokkel. Trace²¹⁵ vermeldde hiervoor geomapping²¹⁶ als instrument.

In een ander Koerdisch smokkeldossier van Brugge²¹⁷ kon via de technische analyse van de iPhone de politie een aantal exacte locaties van de smokkelaar vaststellen waar hij vertoefd had. Die liepen duidelijk van het Franse smokkelkamp van Calais over de Belgische parkings naar het buitenland (Nederland, Barcelona,...). Die onderzoekselementen werden door de rechtbank als bewijsmateriaal opgenomen in het vonnis.²¹⁸

In een moorddossier dat gelieerd is met een Oekraïens smokkeldossier²¹⁹ kon de politie via een GPS-traceersysteem in de vrachtwagen van de vermoorde chauffeur/smokkelaar zijn volledige afgelegde route chronologisch samenstellen. Dit trackingsysteem was verbonden met een website die heel diverse controle mogelijkheden bood: real-time volgen van het voertuig, de historiek van de ritten, de plaatsen en duur van stilstand, de gegevens van de verbruikte brandstof en de instrumenten zoals openen deur, opstarten motor, enz... De werkgever verschaftte de politie het paswoord. De plaatsen van stilstand van de chauffeur werden door de politie met Google Maps opgezocht en schematisch in beeld gebracht. Het technisch verslag diende als basis voor het verhoor van de beklaagden.

4. FINANCIËEL ONDERZOEK

Sociale media en internet kunnen een interessant hulpmiddel voor financiële onderzoeken zijn, zowel om criminele vermogens van verdachten op te sporen als om

209 Zie verder, deel 3, hoofdstuk 3 (rechtspraak): Corr. Oost-Vlaanderen, afdeling Gent, 2 januari 2017, G28m k.

210 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2015, *Schakels verbinden*, dossieranalyse, pp. 66-70.

211 Zitting correctionele rechtbank Ieper voorzien op 9 oktober 2017.

212 Zie verder deel 3, hoofdstuk 2, punt 1.1. (dossieranalyse seksuele uitbuiting).

213 Zie verder deel 3, hoofdstuk 3 (rechtspraak): Corr. Luik, afdeling Luik, 21 november 2016, 18^{de} k. en boven hoofdstuk 1, punt 1 van dit focus (de rol van sociale media en internet bij mensenhandel).

214 Zie verder deel 3, hoofdstuk 3 (rechtspraak): Corr. Oost-Vlaanderen, afdeling Dendermonde, 20 mei 2016, k.G29w (definitief) en boven hoofdstuk 1, punt 1 van dit focus (de rol van sociale media en internet bij mensenhandel).

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 Geografische kartering of 'Geo-mapping': "is een visuele en geografische weergave van gegevens. Het lijkt op een geografische kaart met symbolen die verschillende informatie bevatten. Soms zijn er ook gedetailleerde gegevens in opgenomen, die een opeenvolging van gebeurtenissen weergeven. De gegevens die worden gebruikt voor de aanmaak van de kaart, kunnen op verschillende manieren worden ingezameld, o.a. door het toepassen van GPS-gegevens op bestaande data." (Kantim, "Geo-mapping: an attempt at a definition", *Newtactics*, 29 oktober 2009).

217 MYRIA, Jaarrapport Mensenhandel en Mensensmokkel 2016, *Bedelaars in handen van mensenhandelaars*, dossieranalyse, pp. 111-112.

218 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2015, *Schakels verbinden*, rechtspraak, pp. 125-126; Corr. West Vlaanderen, afdeling Brugge, 2 april 2014 (bevestigd door hof van beroep): (zie website van Myria).

219 Zie verder, deel 3, hoofdstuk 3 (rechtspraak).

hun wederrechtelijk verkregen vermogens te berekenen. Bij de analyse (zie punt 3. Analyse) werd reeds verwezen naar het belang van de berichten van sociale media over het financieel beheer van de smokkelaars.

4.1. | Crimineel vermogen opsporen

In een Hongaars mensenhandeldossier²²⁰ van Gent vond de politie bij de analyse van de smartphone van een pooier foto's van een huis in renovatie waarop ze een internetonderzoek uitvoerde dat tot Frankrijk leidde.²²¹ Het onderzoek in Frankrijk leidde tot een constructie met een vennootschap en kon omwille van de vele bijkomende rogatoire commissies niet verdergezet worden omdat dit het onderzoek zou vertraagd hebben. Maar uiteindelijk is het wel mooi voorbeeld om als onderzoeksmethode te gebruiken in toekomstige dossiers.

4.2. | Berekenen wederrechtelijk verkregen vermogen

In een Syrisch mensensmokkeldossier²²² baseerde de politie zich op het aantal chatberichten om het wederrechtelijk verkregen vermogen te berekenen aan de hand van het aantal door de smokkelorganisatie gesmokkelde personen. De hoofdbeklaagde communiceerde met 769 personen via Viber, WhatsApp, Skype en Facebook. De politie kon na de analyse van zijn smartphone een deel van de berichten traceren en koppelen aan minimaal 291 smokkelslachtoffers. Op basis van het dossier wist de politie dat de gemiddelde smokkelprijs per persoon tussen € 4.000 en € 4.500 bedroeg

220 MYRIA, Jaarverslag Mensenhandel en Mensensmokkel 2015, *Schakels verbinden*, dossieranalyse, pp. 66-70.

221 Een proces-verbaal luidt als volgt: "Deze laatste foto's werden genomen op 22 en 27-03-2013 en op 25-04-2013. Wanneer wij via Google Maps de bijhorende coördinaten (...) ingeven komen wij uit op een woning te Frankrijk... Opvallende gelijkenis, ook de streetview foto's van Google Maps tonen een woning waaraan wordt gerenoveerd. Wij zouden het nuttig achten in Frankrijk te laten achterhalen wie de eigenaar is van deze woning."

222 Deze zaak komt voor op 4 september 2017 voor de correctionele rechtbank van Gent.

zodat er een mininumberekening kon uitgevoerd worden. Het resultaat van deze berekening was € 1.164.000.

5. SAMENWERKING MET SOCIALE MEDIABEDRIJVEN

Europol²²³ pleit voor een nauwe samenwerking van justitie met o.a. Facebook en Google. Uit de EMN-bevraging²²⁴ hierover blijkt dat verschillende Europese landen een informeel samenwerkingsakkoord hebben met privéfirma's van sociale media.

In België bestaan er ook afspraken tot samenwerking in onderzoeken van mensenhandel en mensensmokkel.

Dit blijkt uit de dossieranalyses en onze interviews. Voor de aanvragen van de magistraten werden er ondertussen zelfs type formulieren ontwikkeld die grotendeel zijn ingevuld en waaraan slechts bepaalde details

in verschillende EU-landen bestaan informele samenwerkingsakkoorden met sociale mediabedrijven

moeten worden toegevoegd. Het is wel Facebook dat de opportuniteitsbeslissing van samenwerking bepaalt, wat ook door EMN²²⁵ in de strijd tegen mensensmokkel vastgesteld werd. De aanvraag verloopt via een

223 EUROPOL, *Intelligence Notification 15/2014*, Den Haag, oktober 2014. www.europol.europa.eu/publications-documents/trafficking-in-human-beings-and-internet: "Wetshandhavinginstanties zullen nauwer moeten samenwerken met partners uit de private sector, om tot betere onderzoeksresultaten en betere preventieve maatregelen te komen. De private sector is een cruciale partner aangezien smokkelaars door bedrijven aangeboden technologieën en diensten gebruiken om hun activiteiten makkelijker te kunnen ontplooiën. Overleg met sociale mediabedrijven of hosting bedrijven moet de onderzoeken er efficiënter op maken."

224 EMN Inform, *The Use of Social Media in the Fight Against Migrant Smuggling*, september 2016: "Wat de samenwerking met online service providers betreft, bleek dat slechts 7 van de 17 lidstaten die geantwoord hebben (CZ, DE, EE, ES, FI, HU, UK) op een of andere manier samenwerken met online service providers om migrantensmokkel te vermijden en te bestrijden, maar in de meeste gevallen (CZ, DE, EE, ES), ging het om niet-georganiseerde samenwerking."

225 EMN Inform, *The Use of Social Media in the Fight Against Migrant Smuggling*, september 2016: "Service providers zoals Facebook, Twitter of Google voeren een eigen intern beleid rond gedeelde inhoud. In het geval van Facebook zijn activiteiten die met mensensmokkel te maken hebben niet toegestaan. Facebook heeft trouwens zijn eigen team van juridische specialisten en compliance medewerkers die erop toezien dat de regels van hun platform niet worden geschonden. Ze reageren in de eerste plaats op inhoud die ongeschikt wordt geacht en die ze vervolgens verwijderen. Facebook liet wel weten dat het toezicht op inhoud dat met migrantensmokkel te maken heeft niet altijd prioritair is, in vergelijking met andere misdrijven zoals kinderpornografie bijvoorbeeld, en dus voor verbetering vatbaar is."

rechtshulpverzoek langs een verbindingsofficier die als centraal contactpunt voor een land optreedt. De relevante Facebook profielen kunnen op deze wijze tijdelijk bevroren worden, zonder dat de verdachte hiervan iets zal opmerken. Dit zorgt ervoor dat de persoon in kwestie niets meer zal kunnen wissen van zijn profiel. Dit geldt ook voor Instagram en WhatsApp aangezien deze twee applicaties ook van Facebook zijn.

Uit de Belgische dossiers blijkt dat er sinds enkele jaren al gegevens kunnen opgevraagd worden bij sociale mediabedrijven. In januari 2015 informeerde de politie in het Iraakse mensensmokkeldossier van Dendermonde de bevoegde magistraat over de mogelijkheid om gegevens op te vragen bij Facebook: “*Verzoek opdracht Facebook: Wij verwijzen naar het aanvankelijk proces-verbaal waaruit blijkt dat wij informatie hebben opgevraagd over het open Facebook profiel X. om de eventuele verblijfplaats van “S.” te kunnen achterhalen. Zij [andere politie-eenheid] delen ons mee dat via het open Facebook profiel de volgende cruciale informatie zichtbaar is (...). Wij brengen volledigheidshalve ter kennis dat bij Facebook een historiek kan opgevraagd worden van de logins op het betreffend Facebook profiel binnen een bepaalde periode. Bovendien kan ook het email-adres opgevraagd worden waarmee het Facebook profiel werd aangemaakt. In een tweede fase kunnen IP-identificaties leiden naar welbepaalde adressen/personen.*”

De magistraat stelde hierop in het kader van een opsporing van telefonische mededelingen een verzoekschrift in tot Facebook voor een vordering van identificatie en lokalisatie van de verdachte smokkelaar.²²⁶ Het resultaat van het onderzoek van Facebook leverde belangrijke gegevens op waarmee de smokkelaar geïdentificeerd kon worden.²²⁷

226 Een proces-verbaal luidt als volgt: “Vordert mijn Ambt de technische medewerking van Facebook om mijn Ambt volgende inlichtingen te verstrekken: om overeenkomstig artikel 46bis van het Belgisch Wetboek van Strafvordering alle beschikbare informatie te verstrekken omtrent de persoon die gebruik maakt van de volgende account of pseudoniem op de website www.facebook.com met de twee volgende Facebook profielen: (...) de complete identificatie/registratiegegevens (inclusief eventuele gekoppelde oproepnummers) van de gebruiker van voormelde pseudoniemen; IP-adres/datum/uur/tijdzone van de creatie van de accounts; een lijst van de beschikbare IP-adressen met data, uren en tijdzone, gebruikt om deze pseudoniemen te consulteren.”

227 Een proces-verbaal luidt als volgt: “Uit de historische gegevens blijkt dat de Facebook profielen die afgelopen 3 maanden minstens werden geopend op het netwerk van Internet Service Providers (ISP) in België, Nederland, Duitsland, Zweden, Denemarken en het Verenigd Koninkrijk... De historische gegevens van beide profielen zijn gelijklopend (= binnen dezelfde tijdsframes ingelogd op de netwerken van dezelfde ISP's in dezelfde landen), wat aanwijst dat beide profielen door dezelfde persoon in gebruik zijn. Het IP bij registratie van het Facebook profiel ‘A.’ behoort toe tot de Belgische ISP SkyNet/Belgacom, wat impliceert dat dit Facebook profiel in België is aangemaakt. Het aan dit Facebook profiel gekoppelde oproepnummer (...) blijkt in de ANG gekoppeld te zijn aan de Brusselse notitie (...) onder de naam C. Dit leidt tot de identificatie van de verdachte ‘S.’”

Op basis van de dossiers stellen we vast dat er samengewerkt wordt met sociale media, zoals Facebook, maar dit is nog voor verbetering vatbaar. Volgens EMN stellen zich verschillende problemen op vlak van een omslachtige procedure.²²⁸ Eurojust moet dit trachten te standaardiseren.²²⁹

6. INTERNATIONALE SAMENWERKING

Het gebruik van sociale media en internet leidt tot een internationale schaalvergroting van het fenomeen van mensensmokkel en mensenhandel. Volgens Europol²³⁰ moet dit resulteren in een betere internationale samenwerking. Sociale media en internet kunnen hierbij relevante hulpmiddelen zijn. In de strijd tegen mensensmokkel heeft de internetresearchdienst van Europol reeds zijn nut bewezen.²³¹

Het EMN beveelt aan dat internationale instanties zoals Eurojust de internationale samenwerking faciliteren door

228 Samenvatting van de EMN ad-hoc vraag nr. 1055 van 18 april 2016, *Addressing and preventing the use of social media in migrant smuggling*: “De samenwerking in dat domein verloopt moeizaam door de nationale wetgeving inzake privacy. De meeste online service providers zijn in het buitenland gevestigd, wat de samenwerking ingewikkeld maakt. Vaak verloopt de samenwerking traag en gaat informatie verloren omdat platforms snel kunnen veranderen. De procedures om toegang te krijgen tot gegevens, nadat een verzoek bij de providers is ingediend, zijn vaak omslachtig.”

229 EMN Inform, *The Use of Social Media in the Fight Against Migrant Smuggling*, september 2016: EMN beveelt aan “dat Eurojust zou helpen bij het stroomlijnen van de juridische samenwerking, door mee te streven naar een efficiënte samenwerking met private (sociale media) bedrijven, door met name mee te werken aan het opstellen van standaard aanvraagformulieren, of door te helpen met het stroomlijnen van het huidige MLA-systeem via gestandaardiseerde procedures en opleidingen.”

230 EUROPOL, *Intelligence Notification 15/2014*, Den Haag, oktober 2014. www.europol.europa.eu/publications-documents/trafficking-in-human-beings-and-internet: “Door internet gefaciliteerde mensenhandel gebeurt wereldwijd, wat het onderzoekswerk bemoeilijkt. Het efficiënt delen van informatie tussen verschillende rechtsgebieden is van essentieel belang voor wetshandhavinginstanties.”

231 Europol, *EU Internet Referral Unit year one report: Highlights*, 22 februari 2016: “Overeenkomstig haar mandaat heeft de IRU van de EU haar controles op de open sources en het internet opgevoerd, om mee te helpen aan het ontmantelen van illegale netwerken van migrantensmokkel. De IRU van de EU heeft op verzoek van het European Migrant Smuggling Centre (EMSC), of centrum tegen mensensmokkel, 122 accounts doorgelicht, die gelinkt werden aan illegale immigratie.” Voor meer informatie over het IRU, zie externe bijdrage: “Presentatie van de dienst DJOC/12 in de strijd tegen de mensenhandel: een ondersteunende rol in het onderzoek op internet en sociale media”

het uitwisselen van best practices.²³² We kunnen hierin nog verder gaan en vragen dat dit structureel zou ingebed worden in een op te richten forum dat het gebruik van sociale media bij internationale samenwerking stimuleert en de best practices geregeld uitwisselt.

In België werden al enkele van dergelijke best practices vastgesteld in de dossiers. Bij financieel onderzoek kwam dit ook al even ter sprake, maar er zijn nog andere dossiers.

In een mensenhandeldossier van een Thais massagesalon kon de politie op basis van een internetonderzoek bijkomende relevante vragen stellen voor een internationale rogatoire commissie. Met deze gegevens kon volgens het vonnis²³³ in Thailand de internetshop van het reisagentschap opgespoord worden waar de slachtoffers gerekruteerd werden: “Aan de hand van het IP-adres van waaruit de mails van het reisagentschap T.C. werden gestuurd,... kon middels een internationale rogatoire commissie in Thailand worden vastgesteld dat het reisagentschap T.C. bleek te werken vanuit een telefoon- en internetwinkel/reisbureau in Bangkok, dat werd uitgebaat door de beklagde en haar echtgenoot.”

In een Iraaks smokkeldossier²³⁴ van Dendermonde spoorde de politie via een rogatoire commissie naar het Verenigd Koninkrijk een smokkelaar op en gebruikte hiervoor naast gegevens van de telefoontap ook zijn Facebook profiel. Mede dankzij zijn profielfoto kon de smokkelaar in het VK duidelijk geïdentificeerd worden.²³⁵

232 EMN Inform, *The Use of Social Media in the Fight Against Migrant Smuggling*, september 2016: EMN beveelt aan “dat Eurojust zou helpen bij het stroomlijnen van de juridische samenwerking, door besprekingen te vergemakkelijken over betere praktijken tussen juridische experts over thema's zoals procedure en internationale samenwerking rond de aspecten cybercriminaliteit van migrantensmokkel, conform het Boedapest-verdrag inzake cybercriminaliteit en het European Judicial Cybercrime Network”.

233 Zie verder, deel 3, hoofdstuk 3 (rechtspraak): Corr. Oost-Vlaanderen, afdeling Dendermonde, 11 oktober 2016, k. D19D.

234 Zie verder, deel 3, hoofdstuk 2, punt 2 (dossieranalyse mensensmokkel).

235 Een proces-verbaal luidt als volgt: “De verdachte onder nummer 13 is nog niet geïdentificeerd. Hij wordt aangesproken met de roepnamen: “H.” en “H. B.” en is al minstens 6 jaar actief als smokkelaar. Het betreft een Iraakse Koerd. Hij verblijft op een onbekende plaats in het Verenigd Koninkrijk. Hij gebruikt(e) minstens de telefoonnummers (...) en (...). Hij is gebruiker van de Facebook nickname: H.B. via account (...). Hij stond in contact met zowel de verdachten in België als in het Verenigd Koninkrijk. Hij voert op korte tijd verschillende smokkel-gerelateerde geldtransacties uit ter attentie van de gebruiker van het nummer (...) onder drie verschillende schuilnamen, namelijk ‘A.O.’, ‘A.A.’ en ‘A.M.’. Vergelijkend onderzoek bij het Home Office (vergelijkbaar met de Dienst Vreemdelingenzaken in België) resulteerde positief. Zo kon deze man formeel geïdentificeerd worden als A. Dit zou met zekerheid dezelfde persoon zijn als diegene die voorkomt op de profielfoto van het door: “H.” gebruikte Facebookaccount (...).”

Hoofdstuk 3

Internet en sociale media: nieuwe uitdagingen voor het beleid, de politie en justitie

Deze focus gaat dieper in op de verschillende facetten van het gebruik van internet en sociale media in het kader van mensenhandel en mensensmokkel. Mensenhandelaars maken er intussen gretig gebruik van voor het ronselen en de controle van slachtoffers en ook om hun zaakjes te beheren. Zoals we hebben gezien gebruiken ook politie en justitie internet en de sociale media in hun strijd tegen mensenhandelaars en smokkelaars. En toch is er nog een lange weg te gaan, vol hindernissen.

De uitdagingen in dat verband zijn dan ook niet van de minste.

1. HET JURIDISCHE KADER VAN DE ONDERZOEKSMETHODES WAAROVER DE GERECHTELIJKE INSTANTIES BESCHIKKEN

Een eerste uitdaging heeft te maken met het juridische kader van de onderzoeksmethodes waarover de gerechtelijke instanties beschikken.

Het wetgevend kader loopt altijd één, of zelfs meer stappen achter op de vindingrijkheid van de criminelen. Heel wat bepalingen uit ons Wetboek van strafvordering waren niet langer aangepast aan de razendsnelle technologische evoluties van de afgelopen jaren. Daardoor hadden politie en justitie minder middelen beschikbaar om bewijzen in de informatiesystemen te verzamelen.

In de strijd tegen het terrorisme en om magistraten en speurders de middelen te geven die aan hun tijd en de realiteit op het terrein zijn aangepast, heeft de minister van Justitie in juli 2016 een wetsontwerp in het parlement ingediend. Het wetsontwerp beoogt de vervolmaking van het Belgisch recht met betrekking tot de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en telecommunicatie.²³⁶ De bedoeling was een juridisch kader te scheppen, dat beter afgestemd was op het zoeken in een informaticasysteem. De nieuwe wet werd op 22 december 2016 in het parlement goedgekeurd en op 17 januari in het Belgisch Staatsblad gepubliceerd.²³⁷ De meeste van die nieuwe bepalingen zijn op 27 januari 2017 in werking getreden.²³⁸

De laatste grote wijzigingen op vlak van onderzoeksmaatregelen dateerden uit 2000 met de wet op

²³⁶ Wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Doc.parl.*, Kamer, zitting 2015-2016, Doc 54-1966/001.

²³⁷ Wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken, *BS.*, 17 januari 2017.

²³⁸ Voor een aantal van die wijzigingen moet echter nog een koninklijk besluit worden goedgekeurd, vooraleer ze in werking kunnen treden.

informaticacriminaliteit.²³⁹ Zo had deze wet nieuwe onderzoeksmogelijkheden ingevoerd in het Wetboek van strafvordering zoals het databeslag in een informaticasysteem (artikel 39 bis)²⁴⁰ en de netwerkzoeking (artikel 88ter).²⁴¹

De nieuwe wet past deze artikelen aan de evolutie van de behoeften aan door de inhoud van artikel 88ter in artikel 39bis op te nemen. Dat wordt het referentieartikel voor de *niet-heimelijke* zoeking in informaticasystemen (een smartphone bijvoorbeeld).²⁴²

Zo kan een officier van gerechtelijke politie (OGP) voortaan een zoeking gelasten in een in beslag genomen informaticasysteem (een smartphone zonder toegangscode bijvoorbeeld).²⁴³ Het is evenwel aan de procureur des Konings om een zoeking te gelasten in een niet in beslag genomen informaticasysteem maar die dat zou kunnen zijn (een computer in een cybercafé of een bank bijvoorbeeld, waarbij de in beslagname in dat geval onmogelijk of niet opportuun zou zijn).²⁴⁴ Het is ook de procureur des Konings die over een netwerkzoeking kan beslissen²⁴⁵ (een zoeking in een “cloud” bijvoorbeeld, op voorwaarde dat de gegevens toegankelijk zijn zonder nieuw paswoord).²⁴⁶ In het verleden was de onderzoeksrechter daarvoor bevoegd. Zowel de zoeking in een informaticasysteem als die in een beslagbare drager kunnen enkel worden uitgevoerd nadat de externe verbindingen vooraf zijn gedeactiveerd²⁴⁷ (zo moet een smartphone in vliegtuigmodus worden gezet). De door de procureur des Konings gelaste netwerkzoeking blijft dan weer enkel beperkt tot de toegankelijke delen.²⁴⁸

239 Wet van 28 november 2000 op informaticacriminaliteit, *BS*, 3 februari 2001.

240 We hebben het dan over databeslag, in tegenstelling tot de inbeslagname van de informaticadrager (een gsm of computer bijvoorbeeld). Daar gaat het om een beslag op roerend goed in de zin van artikel 35 Sv. Onder databeslag wordt het kopiëren van gegevens op ad hoc dragers verstaan, wanneer de inbeslagname van de drager niet wenselijk is.

241 De onderzoeksrechter kon een zoeking in een informaticasysteem gelasten of in een deel ervan. Deze zoeking kon onder bepaalde omstandigheden ook worden uitgebreid naar een informaticasysteem of naar een deel ervan, dat zich op een andere plaats bevindt dan die waar de zoeking wordt uitgevoerd (zoeking binnen een netwerk).

242 Artikel 39bis is van toepassing in geval de houder van de smartphone zijn instemming weigert.

243 Nieuwe §2, alinea 1 van artikel 39bis Sv. . Bv: nadat een smartphone in vliegtuigmodus is gezet, verschijnt op het scherm een email. De OGP is bevoegd om van het scherm een foto te nemen maar wil hij erop klikken..., dan is dat niet langer zijn bevoegdheid.

244 Artikel 39bis, §2, alinea 2 Sv.

245 Artikel 39bis, §3 Sv.

246 Verslag van de eerste lezing binnen de commissie voor de Justitie van het wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Doc.parl.*, Kamer, zitting 2016-2017, Doc 54-1966/006, p. 5.

247 Artikel 39bis, §2, alinea 3 Sv.

248 Artikel 39bis, §3, alinea 2 Sv.

Elke andere niet-heimelijke zoeking in een informaticasysteem tenslotte kan enkel door een onderzoeksrechter worden gelast (bijvoorbeeld: wanneer de toegang tot de “cloud” extra wordt beschermd).²⁴⁹

Bij de interpellatie van een verdachte in het bezit van een smartphone bijvoorbeeld²⁵⁰, kan een onmiddellijke controle van het toestel noodzakelijk zijn. Daarover kan een officier van gerechtelijke politie (OGP) beslissen maar enkel als de toegang tot de gegevens geen paswoord of een specifiek technische handeling vereist, en als de smartphone in vliegtuigmodus wordt gezet. Wanneer een ontgrendeling of technische handelingen zijn vereist, is de toelating van de procureur des Konings nodig.

Het wetgevend kader loopt altijd één, of zelfs meer stappen achter op de vindrijkheid van de criminelen.

Als de smartphone toegang biedt tot een Gmail- of Facebook account en de gebruiker zijn login en paswoord in het toestel heeft opgeslagen, kan de procureur des Konings een netwerkzoeking gelasten. De externe verbindingen mogen dan ook worden geactiveerd (toestel staat dus niet langer in vliegtuigmodus) en de zoekingen worden uitgevoerd op de accounts die zonder paswoord toegankelijk zijn. Wanneer login en paswoord evenwel niet in het toestel zijn geparometreerd, dan is de toelating nodig van een onderzoeksrechter. De onderzoeksrechter zal dan de nodige operaties kunnen gelasten om de codes op te halen, omdat voor de activering van de externe verbindingen om zoekingen op de toegankelijke accounts te kunnen doen, paswoorden moeten worden ingevoerd.

Een andere situatie doet zich voor wanneer een toegang nodig is tot niet-toegankelijke accounts. Het gaat dan om een heimelijke zoeking waarvoor de toestemming van een onderzoeksrechter nodig is (cf. infra, wijzigingen aan artikel 90ter).

De nieuwe wet voert ook nieuwe onderzoeksmethodes in het Wetboek van strafvordering in.

249 Artikel 39bis, §4. Zie ook het verslag van de eerste lezing binnen de commissie voor de Justitie van het wetsontwerp, *op. cit.*, Doc 54-1966/006, p. 5.

250 Dit voorbeeld wordt aangehaald in de presentatie van de gespecialiseerde hoofdinspecteur van de RCCU van Namen, H. COLIN: “La saisie des données informatiques en pratique”, tijdens de studiedag georganiseerd door het ‘Centre de recherche information, droit et société’ van de universiteit van Namen (CRIDS): “Les méthodes d’enquête pénale dans le domaine des nouvelles technologies”, op 12 mei 2017.

Voorbeelden daarvan zijn:

- interacties en infiltraties die uitsluitend op internet plaatsvinden (“digitale” infiltratie of “light” infiltratie (nieuw artikel 46*sexies*)). In dit geval worden, desgevallend onder een fictieve identiteit, contacten via internet onderhouden met een of verschillende personen. De voorwaarden voor dat soort infiltratie zijn soepeler dan die voor “fysieke” infiltratie. Overigens is daar ook geen bevel van een onderzoeksrechter voor nodig. Een toelating van het Openbaar Ministerie volstaat.
- de inijkoperatie (binnendringen in een informatiesysteem (artikel 46*quinquies*)).

Tenslotte wordt ook artikel 90*ter*, dat de voorwaarden regelt waarbinnen telefoontaps mogen plaatsvinden, grondig gewijzigd. Dit artikel was aanvankelijk opgesteld in functie van de klassieke telefonie en was enkel van toepassing op communicaties en telecommunicaties tijdens de transmissie. In het internettijdperk moest het artikel dus worden aangepast aan de communicaties op de informatiesnelwegen.²⁵¹ Behalve op telefoons mogen heimelijke zoekingen en taps voortaan ook worden uitgevoerd op e-mails, Skype, Whatsapp, Facebook, Snapchat, enz. De lijst van inbreuken waarvoor de maatregel van artikel 90*ter* mogelijk is (taplijst) is uitgebreid. Mensenhandel en mensensmokkel stonden reeds op die lijst maar deze maatregel is intussen uitgebreid naar “eenvoudige” mensenhandel en mensensmokkel, terwijl in het verleden verzwarende omstandigheden waren vereist.²⁵²

Deze wet is ongetwijfeld een doorbraak in een wereld waarin de technologie razendsnel evolueert en hij biedt zeker nieuwe onderzoeksmogelijkheden. Toch zijn er ook punten van kritiek. De aangebrachte wijzigingen lijken veel verder te gaan dan een loutere modernisering.²⁵³ Zo deden zowel actoren uit de gerechtelijke (onderzoekrechters en advocaten)²⁵⁴ en academische

wereld²⁵⁵, als mensenrechtenverenigingen²⁵⁶ alsook parlementsleden²⁵⁷ verschillende vaststellingen die vragen oproepen. De verschuiving van de bevoegdheden van de onderzoeksrechter, een onafhankelijke en onpartijdige rechter, naar het Openbaar Ministerie, betrokken partij bij een strafproces, en dit zonder echte gerechtelijke controle, de hogere risico's op schending van het recht op eerbiediging van het privéleven²⁵⁸ en van het recht op een eerlijk proces²⁵⁹ zijn de belangrijkste punten van kritiek op de nieuwe wet. De Liga voor de mensenrechten en *La Ligue des Droits de l'Homme* hebben trouwens een beroep ter vernietiging ingediend bij het Grondwettelijk Hof.²⁶⁰

2. DE (INTERNATIONALE) SAMENWERKING MET OPERATOREN EN PROVIDERS

Een tweede uitdaging is de (internationale) samenwerking met o.a. operatoren en providers.

Een van de problemen is dat de in België gevoerde communicaties, via officieel in het buitenland gevestigde providers verlopen. Zoals de minister van Justitie erop heeft gewezen, “is het probleem van de territorialiteit bijzonder complex geworden met de ontwikkeling van nieuwe technologieën en sociale media”.²⁶¹ Het Wetboek van strafvordering gaat overigens maar beperkt in op deze problematiek van de territorialiteit bij het bepalen van de toepassingsvoorwaarden van elke onderzoeksmaatregel,

251 Memorie van toelichting bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, Doc.parl., Kamer, zitting 2015-2016, Doc 54-1966/001, p. 7.

252 Deze maatregel wordt bedoeld in artikel 90*ter*, §2, 22° (mensenhandel) en §2, 37° (mensensmokkel).

253 M. KEITA, “De wet bijzondere opsporingsmethoden: een delicaat evenwicht”, *TvMR*, 2017, nr. 1, p. 12.

254 Zie in dit verband nota E. BROCKMANS, “Minister wil opsporings- en onderzoeksbeleid op internet versterken”, *De juristenkrant*, 28 september 2016, nr. 334, p.11 en het verslag van de eerste lezing binnen de commissie voor de Justitie van het wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Doc.parl.*, Kamer, zitting 2016-2017, Doc 54-1966/006, pp. 33-34 et 56-57.

255 Op de risico's van mogelijke ontsporing en op het ontbreken van voldoende controle is reeds gewezen tijdens de door het CRIDS op 12 mei 2017 georganiseerde studiedag, die ging over de: “méthodes d'enquête pénale dans le domaine des nouvelles technologies”.

256 Zie ook de hoorzittingen met de vertegenwoordigers van de: “Liga voor mensenrechten” en de: “Ligue des droits de l'homme” tijdens het onderzoek van het wetsontwerp in de Kamer (verslag van de eerste lezing binnen de commissie voor de Justitie, *op. cit.*, Doc 54-1966/006, pp. 67-74).

257 Zie ook het verslag van de eerste lezing binnen de commissie voor de Justitie van het wetsontwerp, *op. cit.*, Doc 54-1966/006, pp. 8-9 et 12-15.

258 We mogen niet vergeten dat dit grondrecht wordt gewaarborgd door artikel 8 van het Europees Verdrag inzake de Rechten van de Mens (EVRM) en door artikel 22 van de Grondwet.

259 Dit recht wordt met name gewaarborgd door artikel 5 van het EVRM.

260 Rolnummer 6711.

261 Memorie van toelichting bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *op. cit.*, Doc 1966/001, p. 10.

omdat die in principe door het internationaal recht worden geregeld.²⁶²

De EU-lidstaten hebben bovendien op verschillende moeilijkheden gewezen in het kader van de samenwerking met providers van sociale media en internet, met name op vlak van preventie en bestrijding van mensensmokkel: moeilijke samenwerking omwille van de nationale wetgeving inzake privacy; hoofdkantoren van de providers die zich in het buitenland bevinden, wat tot een logge en bureaucratische samenwerking leidt; trage samenwerking en informatie die verloren gaat omdat de platformen snel kunnen veranderen; lange procedures om toegang te krijgen tot de gegevens, eens een verzoek is ingediend.²⁶³

Verschillende bevraagde actoren wezen op een positieve samenwerking met verschillende van die operatoren (zoals Facebook), maar dat is lang niet voor allemaal het geval. Bovendien bestaat er geen echt formeel kader voor een samenwerking in dat domein.²⁶⁴ Zo moest in België verschillende keren Justitie worden ingeschakeld om bepaalde operatoren tot samenwerking te verplichten. In een arrest van 18 januari 2011 inzake het bedrijf Yahoo heeft het Hof van Cassatie immers geoordeeld dat de medewerkingsplicht van toepassing was op “iedereen die diensten van elektronische communicatie verstrekt, zoals onder meer de transmissie van communicatiegegevens”, en dat de medewerkingsplicht van artikel 46*bis* van het wetboek van strafvordering niet beperkt is tot operatoren van een elektronisch communicatienetwerk of verstrekkers die hun elektronische communicatiediensten enkel verstrekken via hun eigen infrastructuur.²⁶⁵ Zo kan ook als verstrekker van een dienst van elektronische communicatie worden beschouwd, “de persoon die een dienst aanbiedt die erin bestaat zijn klanten toe te laten via een elektronisch netwerk informatie te verkrijgen of te ontvangen of te verspreiden”.

De nieuwe wet van 25 december 2016 is in dit verband een doorbraak omdat deze rechtspraak daarmee in verschillende bepalingen ingang vindt. Zo moeten de

ondernemingen die op het Belgische grondgebied een internetdienst aanbieden samenwerken met de Belgische gerechtelijke overheden in het kader van de maatregelen met het oog op de identificatie van een dienst of een abonnee (artikel 46*bis*), die met het oog op de opsporing van communicatie (artikel 88*bis*) of die met het oog op de onderschepping van communicatie of de heimelijke zoeking in een informaticasysteem (artikel 90*ter*). De medewerkingsplicht geldt dus ook voor de operatoren van elektronische communicatienetwerken en de verstrekkers van elektronische communicatiediensten, met name “iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden”.²⁶⁶

Tijdens het onderzoek van het wetsontwerp in de Kamer heeft de minister van Justitie er trouwens op gewezen dat “iedere internetdienst aangeboden op het Belgische grondgebied het Belgische recht moet naleven, met inbegrip van de tenuitvoerlegging van rechterlijke beslissingen over de toegang tot de gegevens”.²⁶⁷ Hij heeft er echter ook op gewezen dat er op dat vlak nood is aan een doorgedreven Europese regeling.²⁶⁸

Ook werd gewezen op de noodzaak van een efficiëntere en snellere internationale wederzijdse rechtshulp.²⁶⁹

Voorts kan er best werk worden gemaakt van samenwerking met private operatoren van sociale media om een dialoog op gang te trekken over de beste methodes in de bestrijding en preventie van mensenhandel.²⁷⁰

Ook moet de uitwisseling van goede praktijken op vlak van samenwerking tussen nationale instanties, sociale media en andere dienstverstrekkers worden aangemoedigd.

Tenslotte zouden de private bedrijven die de sociale media beheren moeten erkennen (sommigen doen het

262 *Ibid.* Het gaat o.a. om het Verdrag van Boedapest van 23 november 2001 van de Raad van Europa over cybercriminaliteit en richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken, *PB.*, L130 van 1 mei 2014, p. 1. Zo voorziet artikel 31 van deze richtlijn in een specifiek systeem van interceptie van de communicaties, al naargelang de plaats waar de persoon op wie de interceptie betrekking heeft zich bevindt, en al naargelang de staat, waar de persoon op wie de interceptie betrekking heeft zich bevindt, al dan niet technische bijstand nodig heeft.

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

264 *Ibid.*

265 Cass., 18 januari 2011 (besluit beschikbaar op www.juridat.be): “Die verplichting bestaat ook voor iedereen die een dienst aanbiedt die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronische communicatienetwerken.”

266 Zie artikel 46*bis*, §1, 2° Sv. (identificatie).

267 Verslag van de eerste lezing binnen de commissie voor de Justitie van het wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *op. cit.*, Doc 54-1966/006, p. 4.

268 *Ibid.*

269 O.a. professor V. FRANSSEN heeft dit punt benadrukt tijdens zijn interventie op 30 oktober 2015 in het kader van de: “De middagen van het recht” georganiseerd door de FOD Justitie rond het thema: “Internet en nieuwe technologieën: welke nieuwe middelen voor de opsporings- en vervolgingsautoriteiten?”

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

al) dat daders van mensenhandel en mensensmokkel gebruik maken van hun platformen. Deze bedrijven zouden dan maatregelen moeten treffen om werk te maken van voorstellen en technologieën die mensenhandel aanpakken zoals bijvoorbeeld het online meldingsmechanisme bij Facebook.²⁷¹

3. DE MOGELIJKHEDEN VAN DE EERSTELIJNSDIENSTEN

Een derde uitdaging houdt verband met de mogelijkheden van de eerstelijnsdiensten.

In het kader van de samenwerking met Europol is de oprichting van een ondersteuningsdienst zoals de IRU²⁷²

ongetwijfeld een goeie zaak. De eerstelijnsdiensten daarentegen zijn nog onvoldoende gewapend om met internet en sociale media om te gaan: verouderde computers, niet-opgeleide politieagenten, enz. Het zou

De eerstelijnsdiensten zijn nog onvoldoende gewapend om met internet en sociale media om te gaan.

zeker nuttig en aangewezen zijn om in informatica te investeren en om de nodige financiële en menselijke middelen te voorzien. In dit verband zijn concrete “on the job” opleidingen gepland.

Ook de diensten die zich bezighouden met economische uitbuiting zouden trouwens beter moeten worden opgeleid rond internetcontrole (voor online jobadvertenties bijvoorbeeld).²⁷³

4. WETENSCHAPPELIJK ONDERZOEK

Een laatste uitdaging heeft betrekking op wetenschappelijk onderzoek.

Men zou onderzoek naar internet en sociale media, die voor mensenhandel en mensensmokkel worden gebruikt, kunnen financieren. Het lijkt immers belangrijk om in het kader van de strijd tegen mensenhandel blijvend inzicht te krijgen in de rol van internet en van de nieuwe technologieën, en in het gebruik ervan. Er is vandaag evenwel weinig wetenschappelijke informatie beschikbaar. Er zou bijvoorbeeld een vergelijkend wetenschappelijk onderzoek over de rol en de impact van sociale media en internet als bron van objectief bewijsmateriaal voor de rechtspraak kunnen ondernomen worden.

²⁷¹ Ibid., p. 80.

²⁷² In juli 2015 heeft de Raad JBZ, samengesteld uit de ministers van Justitie en van Binnelandse Zaken van alle EU-lidstaten, beslist binnen Europol een nieuwe eenheid op te richten: de EU-IRU (Internet Referral Unit). Elk land, waaronder ook België, heeft een nationaal contactpunt opgericht. Zie in dit verband *infra*, de externe bijdrage: “Presentatie DJOC/12 in de strijd tegen mensenhandel: ondersteunende rol bij onderzoeken op het internet en sociale media”.

²⁷³ In die zin ook, H. WATSON and others, *op. cit.*, p. 80.