Sociale media

Een nieuwe uitdaging voor politie en justitie

Charlotte Conings [a]
Philippe Van Linthout [b]

Abstract

Social media: a new challenge for law enforcement

Over the last decade, several technical evolutions made it possible for each one of us to take actively part in the creation of a new phenomenon which we like to call the web 2.0. With the emergence of different forms of social media we can create webpages without any help of computer experts and easily share all sorts of information through different types of platforms. We can sell or buy goods on the internet, we can communicate by chat, by video or by voice, we can share our latest holiday photos or ever our deepest thoughts. However, the possibilities that cyberspace has to offer are not only beneficial to well-intended people but also to diverse types of (cyber)criminals. Crimes can not only be committed in this new, virtual world. Social media are also an important tool to help criminals to commit crimes in real world or to facilitate the communication and organization of criminal groups. That is why social media enclose a precious load of information for law enforcement. This contribution looks at the different legal possibilities and problems which law enforcement can experience while taking access to social media, while investigating within these social media and while using gathered 'social-media-evidence' before court. Due to the fact that criminal procedural law is still in general aimed at the real world, law enforcement faces several legal difficulties which scream for legislative action. Nevertheless this text makes clear that a creative and open-minded approach of the matter can lead to important opportunities in investigating crime. In other words, law enforcement can as well enjoy the possibilities of social media, even today, but these possibilities are only a small part of the bigger picture, which the legislator urgently has to draw.

Key words: Social media – types of information – access – law enforcement — applicable law – digital evidence– evidence assessment in court
Kernwoorden: Sociale media – informatie – toegang – opsporingsinstanties — toepasselijk recht – digitaal bewijs – appreciatie bewijs door rechter

Panopticon, 33 (3), 205-230
 | ISSN 0771-1409 | Mei 2012

[a] Assistente Instituut voor Strafrecht, KU Leuven; gastdocent UHasselt; medewerker *Belgian Cybercrime Centre of excellence for training, research&education (*corresp.: charlotte.conings@law.kuleuven.be).
[b] Onderzoeksrechter bij de Rechtbank van Eerste Aanleg te Mechelen; medewerker *Belgian Cybercrime Centre of excellence for training, research&education*; vrijwillig wetenschappelijk medewerker Instituut voor strafrecht, KULeuven.

Inleiding

Samen met het begin van de eenentwintigste eeuw situeert zich de start van het Web 2.0[1]. Het internet evolueerde toen van een eerder passief en een consultatief gebruik (Web 1.0:

[1] http://nl.wikipedia.org/wiki/Web_2.0.

vergelijk het met het bekijken van een televisiescherm) naar een interactief gebeuren waar de internetgebruikers mee de inhoud van het internet gingen bepalen. Men spreekt van 'user generated content'. Bekende voorbeelden zijn de zogenaamde sociale netwerksites (Facebook, Netlog, Hyves...), weblogs, webvideo sites zoals Youtube en webservice sites zoals Wikipedia (gratis encyclopedie), Twitter (korte gedachten uitwisseling), Flickr (fotodelen) enz. Zij horen allen thuis onder de noemer 'sociale media'.

Deze evolutie bracht een enorme expansie van internetgebruikers met zich mee. De eerder gespecialiseerde gebruikers ('techneuten', specialisten, academici) kregen het gezelschap van iedereen die een GSM kon bedienen of een computer kon opstarten. Het internet vond zo zijn weg tot in elke huiskamer, elk klaslokaal en werkelijk elke plaats waar, bv. via een Wi-Fi hotspot, verbinding mogelijk is. Deze expansie ging daarbovenop gepaard met het enerzijds goedkoper worden van de beschikbare middelen (computers en telefoons) en het anderzijds exponentieel uitbreiden van de technische mogelijkheden van deze middelen (computers bevatten tegenwoordig ook functies om te bellen; moderne telefoons hebben dan weer meer weg van kleine handige computers).

Het is evident dat in die internet- en ICT-gedreven wereld – helaas – ook plaats is voor allerlei vormen van misbruik, waarbij de ergste onder de noemer informaticacriminaliteit of cybercrime vallen. Wanneer die ICT criminaliteit gefaciliteerd of gepleegd wordt met behulp van sociale media, kunnen die media uiteraard een onmiskenbare rol spelen bij het vergaren van bewijsmateriaal. Sociale media zijn op de eerste plaats bijzonder interessant voor politie en justitie wanneer zij de plaats delict zelf uitmaken. Maar ook buiten die hypothese vormen ze een onuitputtelijke bron van informatie die van groot belang kan zijn voor de misdaadbestrijding.

Doordat in het Belgisch strafrecht de bewijsvoering vrij is (Verstraeten 2007, 859; Van Den Wyngaert, 2006, 1127) en het Hof van Cassatie bovendien een ruime visie hanteert voor wat betreft de bewijswaardering[2], opent zich een poort voor politie en justitie. Enerzijds krijgen zij immers nieuwe opportuniteiten, maar anderzijds worden zij geconfronteerd met heel wat juridische uitdagingen met betrekking tot de beschikbaarheid, de wijze van verzamelen en het exploiteren van deze nieuwe vormen van bewijs.

Deze bijdrage bekijkt vooreerst hoe de sociale media voor politie en justitie nuttig kunnen zijn (Hoofdstuk I). Vervolgens wordt de wenselijkheid van specifiek internetstraf(proces)recht in algemene termen onderzocht (Hoofdstuk II). Verantwoorden de bijzonderheden van de cybercontext over het algemeen een afzonderlijke juridische aanpak op strafrechtelijk gebied? In hoofdstuk III bekijken we welke concrete handelingen politie en justitie al dan niet kunnen stellen in de sociale media in het huidige juridische kader en formuleren we waar nodig de nood aan aanpassing van de wetgeving. Daarbij komen achtereenvolgens het verschaffen van toegang tot sociale media en het verzamelen van bewijsmateriaal in sociale media aan bod. Ten slotte verdienen ook de eventuele problemen van het gebruik van dit digitale bewijs voor de rechtbank bijzondere aandacht (Hoofdstuk IV). Het grenzeloze karakter van het internet, dat verschillende problemen met zich meebrengt op het gebied van rechtsmacht, wordt in deze bijdrage grotendeels buiten beschouwing gelaten. Dat probleem is immers dermate complex dat het een specifieke behandeling noodzakelijk maakt (Zie hieromtrent: *Cybercrime and jurisdiction. A global survey, 2006).*

[2] Verwezen wordt naar de zogenaamde 'Antigoon' rechtspraak die het Hof van Cassatie sinds de mijlpaalarresten van 14 oktober 2003 en 23 maart 2004 hanteert (Cass. 2003 & Cass. 2004).

I. Sociale media: een interessante bron van informatie voor politie en justitie

Sociale media stellen mensen in staat om op relatief gemakkelijke wijze informatie, foto's, bestanden en gedachten met elkaar te delen. Niet alleen is de inhoud, die op die manier in de (soms relatieve) openheid wordt gebracht, dikwijls interessant voor politie en justitie (1). Ook het gegeven dat de mensen die deze informatie delen, sporen achterlaten op het internet die het mogelijk maken om hen te identificeren en te lokaliseren, is van onschatbare waarde (2).

1. De inhoud van sociale media

Een onderscheid tussen twee categorieën inhoud dringt zich op. De eerste categorie bestaat uit inhoud die op zich strafbaar is (*'illegal content')* en die daarom het voorwerp kan uitmaken van een strafrechtelijk onderzoek. De tweede categorie omvat de inhoud die in se slechts communicatie is tussen partijen en dikwijls een alternatief is voor het vroegere telefoneren tussen gesprekspartners. Het onderscheppen van dergelijke communicatie kan uiteraard een belangrijk hulpmiddel zijn in de bewijsvoering.

A. Illegal content

Wat betreft de eerste categorie is de mogelijkheid tot het vastleggen van de inhoud erg belangrijk om het op het op internet gepleegde en vastgestelde misdrijf te kunnen bewijzen. In de sociale media gaat het meestal om klassieke misdrijven, waarbij het medium van de informatica als facilitator wordt gebruikt om het misdrijf makkelijker of op grotere schaal te kunnen plegen (*'old crimes, new tools'*[3]). Het gaat dan meestal over informaticacriminaliteit *sensu lato*[4]. Voorbeelden hiervan zijn kinderpornografie, negationistische propaganda, *'hatespeach'*, aanzetten tot discriminatie, lasterlijke of eerrovende berichten, oplichting, heling en pestberichten in het kader van belaging.

B. Communicatie-inhoud

De tweede categorie houdt verband met verschillende alternatieve communicatiemethoden die zich hebben ontwikkeld op het Web 2.0 en specifiek in de sociale media. Het internet biedt verschillende, meestal gratis, applicaties die het mogelijk maken om contacten te leggen (bijv. Facebook of MSN Messenger), al dan niet openlijk voor iedereen, of afgeschermd in zogenaamde *'private chatrooms'* (bijv. Paltalk.com). In sommige gevallen krijgen gebruikers bovendien de garantie van bijna volledige anonimiteit of privacy doordat de communicatie op een geëncrypteerde of versleutelde wijze plaatsvindt (bijv. Skype.com). Het hoeven daarbij trouwens niet per se applicaties te zijn die zich in een eerste plaats richten op die communicatie. Zo maken platforms bij spelapplicaties op het internet (bijv. World of Warcraft[5]) of virtuele (speel)werelden (bijv. second life[6]) het mogelijk met medespelers te communiceren. Ook in het crimineel milieu had men al snel door dat elk alternatief voor de klassieke telefoonlijn, die afgeluisterd kan worden overeenkomstig art. 90ter Sv en volgende, handig kan zijn om afspraken te maken of deals te regelen.

---

3 Tegenover *'new tools, new crimes'* die de nieuwe ICT misdrijven *sensu stricto* omvatten. (Kerkhofs & Van Linthout, 2010, 179).

4 De informaticacriminaliteit *sensu stricto* zijn de bij wet inzake informaticacriminaliteit ingevoerde ICT specifieke misdrijven: informaticavalsheid en gebruik van valse informaticagegevens (art. 210bis Sw), informaticabedrog (art. 504quater Sw), hacking (art. 550bis Sw) en informaticasabotage (art. 550ter Sw).

5 http://eu.battle.net/wow/en/.

6 http://secondlife.com/.

Het is dan ook een jammere vaststelling dat twee criminelen die communiceren in een digitale en virtuele omgeving nauwelijks riskeren een echte of zelfs virtuele 'flik' tegen het lijf te lopen, die hun kan identificeren en hun gesprek, indien daartoe gemachtigd, kan opvangen of afluisteren.

Met de opkomst van de 'smartphones', dit zijn telefoons die eigenlijk de mogelijkheden bieden van kleine computers, zijn er verschillende applicaties bijgekomen die het opnieuw makkelijker en goedkoper maken om met elkaar te communiceren buiten de klassieke telefoontoepassingen om (geen sms of mms of telefoongesprek maar berichten die men verstuurt via een Wifi-netwerk, 3G netwerk of specifiek Blackberry netwerk)[7]. Ook hier zien politie en justitie soms met lede ogen aan hoe moeilijk of onmogelijk dit internet gebaseerd dataverkeer valt te onderscheppen. Het wordt, gelet op hun verspreiding en gebruik, echter des te relevanter om ook deze nieuwe manieren van communicatie onder controle te kunnen krijgen. Dit dataverkeer laat naast sporen bij de operatoren of bij de verstrekkers van internetdiensten echter soms wel zijn sporen achter op de smartphones zelf, wat het interessant maakt om deze toestellen op zich te onderzoeken waar daar grond toe bestaat.

2. Sporen naar verdachten en nuttige bronnen in sociale media

Rechercheren naar misdrijven die zich in of met behulp van sociale media voltrekken, stelt echter niets voor zonder de mogelijkheid om personen te identificeren en te lokaliseren. Op de eerste plaats is het uiteraard interessant om daders van online-misdrijven op te sporen. Men zoekt dan bijvoorbeeld naar een antwoord op de vraag wie bepaalde pornografische foto's van kinderen heeft ge-upload en tussen wie die bestanden circuleren[8] of wie een profiel heeft aangemaakt en vervolgens dreigberichten heeft gepost. Daarnaast kunnen sporen in sociale media naar verdachten van offline misdrijven ook relevant zijn. Zo kan bijvoorbeeld de identificatie van deelnemers aan een chatconversatie met tijdsaanduiding een alibi bevestigen[9]. Het is echter niet enkel interessant verdachten te identificeren via sporen die zij nalaten op het internet. Ook de identificatie van gesprekspartners in de sociale media kan nuttig zijn gelet op de mogelijkheid om hen vervolgens op te roepen voor verhoor waarbij zij eventueel bruikbare informatie kunnen leveren voor het strafrechtelijk onderzoek. Tot slot is het in het licht van opsporingen naar vermiste personen eveneens noodzakelijk te kunnen nagaan wanneer en waar iemand een laatste teken van leven heeft achtergelaten, zo ook in de sociale media.

A. Identificatie en localisatie met de hulp van ISP's en IAP's

Het opsporen van personen gebeurt meestal door de aanbieder van een dienst op het internet (een internet service provider of ISP) te vragen of deze beschikt over logbestanden die kunnen onthullen wie, wanneer en waar van hun dienst gebruik heeft gemaakt. Wanneer deze gegevens effectief gelogd werden, verstrekt de ISP een IP-adres met vermelding

7 Het gaat om verschillende soorten draadloze netwerken: Het Blackberry netwerk vormt zo bijvoorbeeld een afzonderlijk draadloos netwerk waarin wordt voorzien door de reguliere mobiele-telefonieproviders.

8 Het verslag van de Europese Commissie over de evaluatie van de richtlijn inzake gegevensbewaring bevestigt dat bewaarde gegevens in gevallen van seksueel misbruik van kinderen met behulp van internet onmisbaar zijn gebleken. Het project 'measurement and analysis of p2p activity against paedophile content', gefinancierd vanuit het Europees programma Veiliger internet, zou zo bijvoorbeeld nauwkeurige informatie hebben opgeleverd over pedofiele activiteiten in het eDonkey peer-to-peer systeem. Dit leidde tot de identificatie van 178 000 gebruikers die kinderporno opvroegen (p.27).

9 Dat dit effectief gebeurt blijkt uit het verslag van de Commissie aan de Raad en het Europees Parlement over de evaluatie van de richtlijn inzake gegevensbewaring (p.27).

van een tijdstip (met tijdzone) en een datum van wie toegang nam tot een bepaalde dienst[10]. Met deze gegevens kunnen de onderzoekers terecht bij de betrokken internet toegangsprovider (internet access provider of IAP) die kan nagaan wie effectief gebruik maakte van het door hen toebedeelde IP adres. Zo een IP adres kan immers het best vergeleken worden met een 'jettonnetje' of een tijdelijk toegangspasje[11], dat aan iemand wordt verstrekt om op het internet te kunnen gaan. In de huidige voorraad van toegangspasjes voor het internet zijn er niet genoeg adressen om iedereen ter wereld continu toegang tot het internet te verschaffen (de huidige versie is IPv4, dat 2^{32} = 4.294.967.296 adressen of toegangspasjes inhoudt). Wanneer iemand zijn internetverbinding stopzet, wordt daarom zijn toegang aan een andere internetgebruiker ter beschikking gesteld. Voorzichtigheid is dus geboden met het opsporen van IP gebruikers omdat een verschil in bevraagd tijdstip kan leiden tot een andere gebruiker[12].

De artikelen 46*bis* en 88*bis* van het Wetboek van Strafvordering vormen de basis voor het opvragen van deze gegevens bij de ISP's en IAP's. Beide artikelen voorzien in een medewerkingsplicht voor de providers. Bij gebrek aan medewerking riskeren de providers een strafrechtelijke geldboete. Artikel 46bis Sv. regelt de opvraging van identificatiegegevens (De Hert & Van Leeuw, 2011,926). Het gaat meer bepaald om de vraag 'wie zit achter een bepaald IP'. De procureur des Konings en onderzoeksrechter kunnen op basis van dat artikel bijvoorbeeld aan een IAP vragen om aan de hand van een dynamisch IP-adres samen met de tijdsaanduiding de gebruiker van een bepaald e-mailadres te identificeren (De Wandeleer, 2009-2010, 136). Art. 88*bis* Sv. maakt het mogelijk telecommunicatie op te sporen en te lokaliseren, zonder de inhoud van de communicatie op te sporen. De onderzoeksrechter, of in uitzonderlijke gevallen de Procureur des Konings[13], gebruikt art. 88*bis* Sv. meestal om een lijst met IP adressen te bekomen van personen die gebruik maakten van een e-mail adres (bv. hotmail account) of van een dienst op het internet (bv. van een facebook account). Belangrijk is wel te weten dat in de praktijk de voornoemde vorderingen niet steeds resultaat blijken op te leveren nu niet alle IAP's en ISP's de door politie en justitie gewenste gegevens blijken te bewaren (of niet onder de juiste technisch leesbare vorm).

Het is bijgevolg enorm belangrijk voor een succesvolle internetrecherche dat de ISP's en IAP's de verrichtingen van hun cliënteel loggen en deze gegevens voldoende lang bijhouden om verdere opsporingen mogelijk te maken. De richtlijn gegevensbewaring van 15 maart 2006 regelt deze materie. Ze verplicht de ISP's en IAP's enkel tot het bewaren van communicatie en lokalisatiegegevens waaruit de inhoud van communicatie niet kan blijken (Art. 5 laatste lid richtlijn gegevensbewaring). Deze richtlijn maakt echter het contrast tussen termijnen voor het bijhouden van bewijsmateriaal (om het daarna te vernietigen) en de in België geldende verjaringstermijnen voor misdrijven zeer groot. De richtlijn schuift immers dataretentietermijnen naar voor tussen zes en vierentwintig maanden (Art. 6

10 Facebook deelt bijvoorbeeld mee dat de gebruiker van het IP adres 78.22.36.66 dat behoort tot de aan TELENET toebedeelde IP adressen op 2011-12-27 10.31.22 (GMT) een laatste maal heeft ingelogd met het profiel 'Cowboy Henk'; het onderzoek kan nu aan de hand van deze gegevens worden verder gezet bij TELENET.

11 Variabel IP – soms wordt ook gebruik gemaakt van vaste IP adressen, wanneer het bijvoorbeeld noodzakelijk is dat iemand of een dienst steeds op hetzelfde adres kan worden gecontacteerd (denk bijvoorbeeld aan de IP adressen van bedrijven).

12 Nog grotere voorzichtigheid zal vereist zijn in de overgang van IPv4 naar IPv6 waar de IAP's tijdelijk om het tekort aan internetadressen op te vangen gebruik maken van Carrier Grade Network Address Translation of Carrier Grade NAT. Daarbij zal één IP adres gedeeld worden door verschillende personen, door gebruik van verschillende poorten achter eenzelfde IP adres; de identificatie zal dan noodzakelijkerwijze niet ophouden bij het terugvinden van een IP adres, maar zal verder moeten worden gezet naar de – al dan niet geregistreerde – poortinformatie.

13 Bv. in geval van ontdekking op heterdaad van misdrijven opgesomd in art. 90 ter §2-4 Sv.

Richtlijn gegevensbewaring). Verjaringstermijnen van misdrijven bedragen al snel vijf jaar en kunnen bovendien oplopen tot maximum dertig jaar (Art. 21 en 22 Sv.). ISP's en IAP's moeten na verloop van de dataretentietermijn wel enkel die gegevens vernietigen die niet reeds werden geraadpleegd en vastgesteld (Art. 7 Richtlijn gegevensbewaring). Wanneer de politie dus binnen de voorziene termijn nuttig bewijsmateriaal verzamelt, kan dit zo lang als nodig bewaard blijven. Wanneer men daar niet in slaagt, gaat het bewijsmateriaal echter verloren. De gedachte dat dit ook bewijsmateriaal à décharge[14] kan zijn, beangstigt daarbij.

De wettelijke bewaringstermijn kan echter niet zomaar worden verlengd. Het bewaren van deze gegevens vormt immers een inmenging in het recht op eerbiediging van de privacy en de bescherming van persoonsgegevens. Die rechten zijn grondrechten in de Europese unie[15] en worden eveneens gewaarborgd door art. 8 EVRM en art. 22 van de Belgische Grondwet. Een inmenging in die rechten is enkel rechtmatig indien zij bij wet is voorzien, noodzakelijk is in een democratische samenleving, beantwoordt aan een doelstelling van algemeen belang zoals erkend in de internationale normen die deze rechten waarborgen en het evenredigheidsbeginsel eerbiedigt[16]. Het bewaren van gegevens moet bijgevolg evenredig zijn met het doel waarvoor de gegevens worden verzameld (EHRM, 2008b). Dat houdt in dat er minimumwaarborgen moeten worden voorzien met betrekking tot, onder andere, de duur. Een wettelijke verlenging van de termijn is enkel mogelijk indien wordt aangetoond dat dit noodzakelijk is voor de opsporing en vervolging van ernstige criminaliteit (het door de richtlijn vooropgestelde doel) en slechts in die mate dat de inmenging niet onevenredig wordt ten aanzien van dat doel. Ondanks voldoende praktijkvoorbeelden blijkt het helaas, bij gebrek aan bijgehouden statistische gegevens, moeilijk aan de Europese instellingen uit te leggen welke de belangrijke impact van dataretentie is op de misdaadbestrijding. Doordat zowel parketmagistraten als onderzoeksrechters rekening houden met de actueel zeer korte dataretentietermijnen en geen vorderingen opstellen waar bij voorbaat een negatief antwoord op te verwachten is, lijkt het trouwens dat korte datatermijnen toekomen. Dit is echter een vertekend beeld.

Hoewel een verlenging van de termijnen bijzonder wenselijk is met het oog op misdaadbestrijding, lijkt dat op dit moment politiek niet haalbaar. Dit blijkt uit het verslag van 18 april 2011 van de Commissie aan de Raad en het Europees Parlement inzake de evaluatie van de richtlijn gegevensbewaring. In dat verslag erkent de Commissie op de eerste plaats het belang van dataretentie voor strafrechtssystemen en rechtshandhaving binnen de EU. Aan de andere kant signaleert ze echter enkele problemen op het vlak van privacybescherming en bescherming van persoonsgegevens. De Commissie verwoordt daarbij de kritiek van een aantal maatschappelijke organisaties die vinden dat het *'ongevraagd, algemeen en ongedifferentieerd bewaren van verkeers-, locatie- en abonneegegevens van personen'* een onwettige beperking van de grondrechten uitmaakt (Verslag gegevensbewaring, 2011, 33). Ze geeft o.a. ook de kritiek van de Europese Toezichthouder voor gegevensbescherming weer. Die kaart vooral het probleem aan van het gebrek aan Europese minimumregels voor de toegang en verder gebruik van

14 Persoon X kon in een zaak waar hij verdacht werd van een gewapende overval, aantonen niet op de plaats delict te zijn geweest aan de hand van de bijgehouden sporen van telecommunicatie die aantoonden dat hij was ingelogd op een computer op een adres dat honderden kilometers verwijderd was van de plaats delict.

15 Zie hiervoor Art. 7 en 8 Handvest van de grondrechten van de Europese Unie. Ook art. 16 VWEU garandeert het recht op bescherming van persoonsgegevens.

16 Toepassing inzake gegevensbewaring (meer bepaald DNA-profielen en vingerafdrukken) : EHRM 2008b.

de gegevens door rechtshandhavingsautoriteiten (Verslag gegevensbewaring 2011, 34). Voor wat de Belgische situatie betreft, lijkt echter wel een duidelijke wettelijke regeling voorhanden, verwoord in de artikelen 46*bis* en 88*bis* Wetboek van Strafvordering. Daarnaast uiten gegevensbeschermingsautoriteiten kritiek op de tekortschietende nationale gegevensbeveiliging. Gelet op technologische ontwikkelingen en de daarmee gepaard gaande nieuwe communicatiemogelijkheden dreigt dit probleem bovendien nog toe te nemen (Verslag gegevensbewaring 2011, 34). Zolang die problemen niet op Europees niveau worden aangepakt, riskeert men dat de richtlijn gegevensbewaring, zelfs zonder verlenging van de termijn, een onrechtmatige inbreuk vormt op het recht op bescherming van de privacy en bescherming van persoonsgegevens. Het is voorlopig afwachten wat het Hof van Justitie zal antwoorden op de prejudiciële vraag van het hooggerechtshof van Ierland hieromtrent[17].Indien het Hof van Justitie een strijdigheid vaststelt zal naar een passende oplossing gezocht moeten worden. De Commissie spreekt in het verslag o.a. van een eventuele verkorting van de termijnen (Verslag gegevensbewaring 2011, 36). De problematiek inzake de privacybescherming situeert zich blijkbaar echter niet zozeer op het niveau van de termijnen. Vanuit de praktijk kan bovendien nu reeds gesteld worden dat zo'n eventuele verkorting van de termijnen desastreuze gevolgen zal hebben voor de strijd tegen cybercrime in het algemeen en de waarheidsvinding in het bijzonder. Een gepaste oplossing zou bijgevolg niet liggen in een verkorting van de termijnen maar eerder in Europese waarborgen inzake de toegang en het gebruik van de gegevens door de rechtshandhavingsautoriteiten en Europese richtsnoeren inzake gegevensbescherming. Het is aan de lidstaten om de Europese instellingen gevoelig te maken voor de nood aan langere gegevensbewaring, die in de praktijk wel degelijk blijkt te bestaan. Zij zouden hen er op kunnen wijzen dat efficiënte gegevensbewaring en adequate privacybescherming hand in hand kunnen gaan.

B. GeoTagging en face recognition

Zeer recente internettoepassingen bieden bovendien nog andere mogelijkheden voor politie en justitie. Waar vroeger de gedachte dat iemand verplicht een lokalisatie instrument op zich zou moeten dragen als *'Orwelliaans'* en politiestatelijk zou zijn afgedaan, kiezen mensen nu blijkbaar zelf, en met plezier, voor multimediaproducten (zoals de nieuwste iPhone, of fototoestellen die zijn uitgerust met *'Geotagging'* software) die er voor zorgen dat aan elk gemaakt mediabestand[18] een (verborgen) GPS locatie wordt verbonden zodat later effectief kan worden nagegaan waar een bestand werd gecreëerd. Zo kan men bijvoorbeeld via de *'geotag'* informatie (GPS-coördinaten) van een op een sociale netwerk site teruggevonden foto met daarop kinderporno, achterhalen waar de foto effectief werd genomen. Wanneer deze bestanden op geldige wijze in beslag zijn genomen (digitaal beslag geregeld door artikel 39*bis* van het Wetboek van Strafvordering), kunnen deze op eenvoudige wijze, d.i. zonder bijzondere vorderingen, worden geëxploiteerd door de met het onderzoek gelaste politiemensen.

Een andere interessante evolutie is de opkomst van de gezichtsherkenningssoftware die onschuldig lijkt binnen te sijpelen in de meeste sociale media om makkelijker door vrienden geposte foto's terug te vinden (toepassing bij bv. Facebook) of om foto's van familie en vrienden te catalogeren (bv. Picasa van Google). Toepassingen voor politie en justitie zijn echter niet moeilijk te bedenken. Gezichtsherkenningssoftware zou het bijvoorbeeld mogelijk kunnen maken op het internet een zoekopdracht in te geven naar

[17] http://www.contentandcarrier.eu/?page_id=371; http://www.thejournal.ie/ecj-asked-to-rule-on-mandatory-retention-of-phone-and-internet-data-339434-Jan2012;

[18] Bv. foto, sms, video, website.

alle foto- of videobestanden waar de op te zoeken persoon in herkend wordt aan de hand van zijn biometrische gegevens[19]. De politie zou dan een foto kunnen uploaden van een bewakingscamera die een bankoverval registreerde, om vervolgens via een zoekmachine na te gaan wie de gefilmde persoon, en dus de vermoedelijke dader is. Politieagenten kunnen trouwens nu reeds uitgerust worden met bijvoorbeeld een iPhone[20] die toelaat niet enkel foto's, maar ook een irisscan en vingerafdrukken door te sturen naar een centrale computer. Naast reeds lopende en voor het grote publiek reeds gekende projecten waarbij nummerplaatherkenning wordt toegepast, worden ook in België de eerste stappen gezet naar gezichtsherkenning[21].

De inzameling en verwerking van politionele informatie wordt geregeld in de artikelen 44/1 t.e.m. 44/11 Wet op het politieambt (WPA,1992). Op grond van die artikelen en onder de daar omschreven voorwaarden kan de politie persoonlijke gegevens, zoals foto's en afbeeldingen, inzamelen en verwerken indien die betrekking hebben op gebeurtenissen, groeperingen of personen die een concreet belang tonen voor de opdrachten van de bestuurlijke en gerechtelijke politie. De inzameling en verwerking dient te gebeuren overeenkomstig de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (art. 44/2 WPA). De gegevens worden opgeslagen en verwerkt in de algemene nationale gegevensbank (ANG) (art. 44/4 WPA). Het toepassen van face recognition op de afbeeldingen die in de ANG geldig zijn opgeslagen vormt een verwerking in de zin van de wet van 8 december 1992. Overeenkomstig art. 1§2 van die wet valt het met elkaar in verband brengen van persoonsgegevens immers onder het begrip 'verwerking'. Persoonsgegevens kunnen onder andere verwerkt worden indien dit noodzakelijk is voor de vervulling van een taak van openbaar belang (Art. 5 e, Wet bescherming persoonlijke levenssfeer, 1993). Aangezien criminaliteitsbestrijding een openbaar belang is kan face recognition dus worden toegepast op de foto's en afbeeldingen opgeslagen in de ANG, zonder dat daartoe een afzonderlijke wettelijke basis nodig is. Maar kan de politie ook gezichtsherkenningssoftware toepassen op afbeeldingen uit sociale media? Wanneer de politie op geldige wijze toegang kan nemen tot de sociale media (onder de voorwaarden omschreven in hoofdstuk III, titel 1) en daar vervolgens bewijzen kan verzamelen (onder de voorwaarden omschreven in hoofdstuk III, titel 2) belet niets dat de politie met het blote oog afbeeldingen met elkaar vergelijkt. Het lijkt op het eerste zicht geen probleem dat zij in dat kader gebruik maakt van software die dat proces alleen maar versnelt en automatiseert[22]. Ook in dat geval gaat het om een op criminaliteitsbestrijding gerichte verwerking van persoonsgegevens die op een geldige manier werden verkregen.

19 http://www.tineye.com/

20 Amerikaanse politie zou zo bijvoorbeeld de iPhone gebruiken om gezichten te scannen met MORIS (Mobile Offender Recognition and Identification System); http://www.popsci.com/technology/article/2011-07/amid-privacy-fears-police-across-nation-will-roll-out-face-recognizing-iphone-tech-year.

21 Tijdens het programma '*Villa Vanthilt*' werden in september 2011 camera's, uitgerust met gezichtsherkenningsoftware, getest. De camera's slaagden erin proefpersonen te herkennen tussen de grote massa bezoekers. O.a. Roeselare zou overwegen de moderne camera's te installeren in het centrum: http://www.standaard.be/artikel/detail.aspx?artikelid=MF3G01G0.

22 Zie over de relevantie van het 'technisch hulpmiddel' als onderscheidingscriterium: randnrs 17 & 37.

II. Wenselijkheid specifiek internetstrafrecht?

1. Nood aan 'update' strafrecht en strafprocesrecht

Internauten, en dus ook criminele internauten, genieten bijzonder veel mogelijkheden in de virtuele internetwereld om te communiceren, om informatie te delen, om zich desgevallend weg te steken achter instrumenten die hun aanwezigheid op het internet anoniem maken (zogenaamde anonymizers), enz. Politie en justitie worden in die wereld daarentegen geconfronteerd met belangrijke beperkingen van het huidige juridische kader, dat voornamelijk gericht is op de reële wereld. Die beperkingen maken het optreden van de cybercop bijzonder moeilijk. De nood aan aanpassing van de wetgeving aan de internetrealiteit valt dan ook niet te ontkennen.

Voor de politie is het voorlopig moeizaam roeien met de riemen die ze hebben. Het gebrek aan aangepaste wetgeving maakt het bijzonder moeilijk voor parketmagistraten of onderzoeksrechters om te bepalen hoe en in welke mate zij, hun politiemensen toelaten zich in de cyberwereld te begeven om er bewijsmateriaal te vergaren. In de schoot van het Federaal Parket, in de werkgroep internetrecherche, werd deze denkoefening alvast voorgedaan, welke resulteerde in interne richtlijnen voor politie en parket. Voortbouwend op eerdere denkoefeningen in concrete zaken en geïnspireerd door de inzichten van de voornoemde werkgroep internetrecherche, dienen voor de praktijk een aantal voorafgaande principes te worden verduidelijkt, vooraleer in hoofdstuk III gradueel elke beweging en steeds dieper gaande intrede in de sociale media op het internet van dichterbij wordt bekeken.

2. Uitgangspunt bij 'update-proces': online = offline.

Hoewel de reële wereld en de virtuele wereld als twee verschillende omgevingen kunnen worden beschouwd, lijkt een zo groot mogelijke juridische gelijkschakeling tussen offline en online te verkiezen. Een aparte cyberregelgeving zou de wetgeving immers onnodig complex kunnen maken. Zeker in online/offline grensoverschrijdende situaties zou een afzonderlijke juridische regeling voor overbodige problemen zorgen. '*online = offline'* als uitgangspunt aannemen verdient daarom de voorkeur, zowel voor het materieel strafrecht als voor het procedureel strafrecht. Enkele voorbeelden kunnen dit illustreren.

A. Materieel strafrecht

Wanneer een gedraging strafbaar is, zou het geen verschil mogen uitmaken of die gedraging in de online- dan wel in de offlinewereld wordt gesteld. Het te beschermen rechtsbelang staat centraal, het middel waarmee het rechtsbelang wordt aangetast zou geen criterium van onderscheid mogen zijn. Waar misdrijven niet zijn aangepast aan de internetrealiteit, dient de wetgever bijgevolg geen nieuwe misdrijven te creëren maar kan hij vaak beter een 'update' van de regelgeving doorvoeren. Zo is bijvoorbeeld het misdrijf valse naamdracht, gericht op de reële wereld en houdt het weinig rekening met het erg courante gebruik van *nicknames* in de virtuele wereld. Een herformulering, die het misdrijf werkbaar maakt in de reële en in de virtuele wereld, dringt zich op.

In de geïnformatiseerde wereld wordt veel frequenter gebruik gemaakt van *'nicknames'* dan in de reële wereld. Dit verschil kan logisch worden verklaard. Om toegang te krijgen tot bepaalde applicaties op het internet (bv. facebook, hyves) moet u een hele reeks persoonlijke gegevens ingeven. Alleen in België zouden er al meer dan 4 miljoen Facebookgebruikers zijn (Lorre, 2010-11, 1498). Dit is dus te vergelijken met volledige gemeenschappen die enkel toegankelijk zijn voor degenen die bereid zijn persoonlijke gegevens te delen. Ook in de reële wereld worden bepaalde gemeenschappen slechts toegankelijk gemaakt

na het delen van persoonlijke gegevens. Zo moeten niet-Amerikanen die Amerika willen binnentreden hun identiteitsgegevens meedelen, een vingerafdruk laten afnemen, meedelen waarom ze naar Amerika komen, waar ze verblijven en voor hoelang. Door de strenge controles is het zo goed als onmogelijk om hier fictieve gegevens mee te delen. De mogelijkheid om Amerika binnen te treden op anonieme wijze is daardoor zo goed als onbestaande. In de virtuele wereld wordt de waarachtigheid van persoonlijke gegevens echter nauwelijks gecontroleerd. Het is op de eerste plaats dus veel makkelijker om een fictieve identiteit aan te nemen in de virtuele wereld. Bovendien zal men op internet veel sneller gebruik maken van schuilnamen dan in de fysiek tastbare wereld omdat men de mogelijkheid tot sociale controle wil beperken en zijn privacy niet zomaar te grabbel wil gooien. Geschreven woorden of geposte afbeeldingen op het World Wide Web zijn immers makkelijk voer voor pottenkijkers, in tegenstelling tot vluchtige woorden uitgesproken in de reële wereld of foto's, veilig opgeborgen in een of ander fotoalbum. Bovendien worden op het internet geregistreerde gegevens vaak opgeslagen en kan men met behulp van het internet verschillende gegevens met elkaar in verbinding brengen waardoor meer aan het licht komt over de betrokken persoon dan dat die in eerste instantie wou vrijgeven[23]. De nood aan afwering van online controle, bescherming van het recht op privacy en het recht op vrije meningsuiting doet een recht op anonimiteit op het internet stilaan doorsijpelen in ons rechtssysteem[24]. Dat recht is echter niet absoluut, net zoals het recht op privacy en het recht op vrije meningsuiting. Het recht gaat bijvoorbeeld verloren wanneer men valse of lasterlijke informatie op een datingsite post (EHRM, 2008a; Voorhoof, 2009, 5). Ook worden er grenzen gesteld door het misdrijf valse naamdracht[25].

Art. 231 Sw. omschrijft valse naamdracht als '*het in het openbaar aannemen van een naam die hem niet toekomt*'. Het misdrijf beperkt zich tot het aannemen van een valse familienaam (Delbrouck, 2008, N10/26). Het subjectief delictsbestanddeel bestaat in de vraag of men wetens en willens de valse naam heeft aangenomen om te doen geloven dat dit de werkelijke naam is (Delbrouck, 2008, N10/27). Een dergelijk subjectief delictsbestanddeel zal vaak aanleiding geven tot bewijsproblemen, ook in geval van gebruik van *'nicknames'*. Gelet op de definitie van valse naamdracht is een veroordeling wegens het gebruik van een '*nickname'* niet uitgesloten, maar in de meeste gevallen wel absurd. Het risico op een veroordeling haalt het recht op anonimiteit op het internet volledig onderuit. Daarom is het misdrijf niet aangepast aan de virtuele wereld. Het subjectief delictsbestanddeel kan beter vervangen worden door een ander handig criterium, dat zowel dienst kan doen in de virtuele als in de reële wereld, nl. de redelijke en geloofwaardige schijn vanuit het standpunt van de gebruiker (*'subjectieve dadernotie'*): Heeft de gebruiker misbruik gemaakt van de redelijke en geloofwaardige schijn van de naam[26]? Dit criterium van een *'subjectieve dadernotie'* werd ontleend aan de beoordeling van een eventueel voorliggende valsheid in informatica (Kerkhofs & Van Linthout, 2010, 181). Daar werd reeds aangetoond dat dergelijk criterium zowel geschikt is in de virtuele wereld als in de reële wereld[27].

---

23 Het in verbinding brengen van verschillende gegevens wordt gereguleerd door de wet bescherming persoonlijke levenssfeer.

24 Zie : Principe 7 van de verklaring betreffende de expressievrijheid op het internet van de Raad van Europa, 2003.

25 Art. 231 Sw. Zo werd bijvoorbeeld een vrouw veroordeeld door de correctionele rechtbank te Gent omdat zij een facebookprofiel aanmaakte onder de naam van haar ex-baas om hem van overspel te beschuldigen: 'Vals Facebook-profiel voor eerst veroordeeld' in *De Tijd,* 21 september 2011.

26 Jan.jansens@hotmail.com kan redelijk en geloofwaardig overkomen als een echte identiteit; cowboy.henk@yahoo.fr niet.

27 Dat criterium komt immers neer op de vraag of de gebruiker misbruik heeft gemaakt van de bewijsfunctie van een drager van informatie. Werd er misbruik gemaakt van de redelijke en

Daar waar elke internaut gebruik kan maken van (ongeloofwaardige) fictieve identiteiten, zonder enige vorm van controle door de dienstenaanbieder, mag de politie dit ook om verder informatie in te winnen(Zie *infra* randnr. 22)[28].Het recht op anonimiteit op het internet ontzeggen aan de politie zou immers het gerechtelijk apparaat in een groot gedeelte van de cyberwereld lam leggen, wat de deur naar misbruik zou openzetten en van het internet eerder een World Wild West zou maken.

B. Procedureel strafrecht

In België bestaat een zeer ruim arsenaal aan regelgeving omtrent verschillende onderzoeksdaden en -methodes, zoals huiszoeking, tapmaatregelen, observatie, infiltratie, enz. Bovendien zijn in een opsporingsonderzoek andere regels van toepassing dan in een gerechtelijk onderzoek. Daarenboven gelden nog andere procedures bij ontdekking op heterdaad. Aan deze uitgebreide regelgeving specifieke regels toevoegen betreffende onderzoeksdaden in de virtuele wereld moet zoveel als mogelijk worden vermeden. Te veel onderscheiden procedures zou de efficiëntie van het strafrechtelijk onderzoek immers niet ten goede komen. Nieuwe wetgeving zou in eerste instantie moeten gericht zijn op het aligneren van de juridische benaderingen van de reële en virtuele wereld.

Wanneer een undercover agent bijvoorbeeld in de reële wereld contacten heeft met zijn target lijkt dit probleemloos te worden vertaald naar vaststellingen in het strafdossier. Wanneer echter een undercover agent in de virtuele wereld dezelfde (digitale) contacten onderhoud met een target op het internet, blijkt deze vertaling minder evident. Volstaat de machtiging tot infiltratie; dient die gepaard te gaan met een machtiging tot observatie en / of dient die op straffe van nietigheid gedekt te worden door een tapbevel?

Het juridisch verschil tussen het volgen van een voertuig in het kader van een kortstondige (en dus niet stelselmatige) observatie en het even frequent volgen van datzelfde voertuig via een ingebouwde chip (tracking device) lijkt onverantwoordbaar. Door het louter gebruik van het technisch hulpmiddel (de chip) is in het tweede geval wel sprake van een stelselmatige observatie en moet bijgevolg voldaan zijn aan de voorwaarden van art. 47*sexies* ev. Sv. In concreto komen beide situaties echter op hetzelfde neer.

Op grond van voorgaande argumenten kan gepleit worden voor een doorgedreven modernisering van het strafprocesrecht op dit vlak. In hoofdstuk III wordt daarom voor de verschillende mogelijke handelingen van politie en justitie in de sociale media gezocht naar de gepaste tegenhanger in de reële wereld, om vervolgens na te gaan of een aanpassing van de regelgeving nodig is.

3. Geen blinde toepassing van het uitgangspunt

Een te rigide toepassing van dit voorafgaande principe is echter niet werkbaar. Er zal steeds onderzocht moeten worden waarom bepaalde regels of voorwaarden tot stand zijn gekomen en of die ratio legis ook geldt in de virtuele wereld. Bovendien zijn er bepaalde mogelijkheden of fenomenen aanwezig in de virtuele wereld, die gewoonweg niet bestaan in de reële wereld. Uiteraard dringt een specifieke cyberregelgeving zich in die gevallen op.

Zo valt het nut van specifieke wetgeving die gericht is op de bescherming van informaticasystemen als zodanig, zoals de wet van 28 november 2000 inzake informaticacrimi-

geloofwaardige schijn van de drager en van de inhoud? In essentie is het dergelijk misbruik dat door de valshedenwetgeving wordt bestraft. (Conings, 2012; Van Dyck, 2007, 230).

[28] In vele gevallen volstaat het bijvoorbeeld om wanneer een profiel dient te worden aangemaakt om bij 'Naam:', 'naam' in te vullen, bij 'Voornaam:', 'voornaam' enz. Het valt dus op dat de aanbieder van de betreffende dienst op het internet in deze gevallen echt niet geïnteresseerd is in het bekomen van echte identiteiten, noch deze controleert.

naliteit, niet te ontkennen[29]. Ook het fenomeen van cloud-computing heeft bijvoorbeeld geen vergelijkbare tegenhanger in de reële wereld. Wanneer gegevens (data) of zelfs besturingssystemen in de 'cloud' worden opgeslaan impliceert dit dat zelfs de normale gebruikers niet echt weten waar hun data of besturingssysteem op dat moment staan. Dat dit in een ander land kan zijn dan het land waar de computer staat die toegang geeft tot de 'cloud' is heel gewoon. Het toepassen van klassieke regels van territoriale bevoegdheid, zowel voor wat betreft procedurele territoriale bevoegdheid, als voor wat betreft de bevoegdheid om eventueel data te vergaren in het buitenland, lijkt hier onmogelijk. Een nieuwe benadering van cyberspace en territoriale bevoegdheid dringt zicht op[30].

III. Politie en justitie in de sociale media

1. Toegang tot sociale media: Informatie achter een open of gesloten deur?

A. Met welke computer?

Wat voor het publiek zonder enige voorwaarde toegankelijk is in de cyberwereld is vergelijkbaar met een openbare straat of een andere openbare plaats in de reële wereld. Dit zijn plaatsen die uit hun aard en op elk ogenblik zonder enig onderscheid toegankelijk zijn (Verstraeten, 2007, 283; Viane, 1962, nr. 44). De politie kan zich bijgevolg zonder meer toegang verschaffen tot dit gedeelte van de cyberwereld (Beirens, 2010, 65). In de eerste plaats des te meer wanneer de politie zich open en bloot toegang verschaft van op haar eigen computers, waarvan de IP-adressen soms publiek gekend zijn, of al dan niet makkelijk opzoekbaar zijn op het internet[31]. Die situatie valt namelijk te vergelijken met een politieman die zich in uniform begeeft op een openbare plaats.

Verder lijkt het ook geen probleem te zijn wanneer de politie gebruik maakt van reguliere computers buiten het politienetwerk. Dit blijkt immers noodzakelijk te zijn voor sommige websites die voor iedereen toegankelijk zijn, behalve voor de gekende IP-adressen van *law enforcement*. Die situatie valt op zijn beurt immers te vergelijken met een politieman die in burger toegang neemt tot een straat van een probleemwijk waar politiemensen in uniform steeds reacties van de omstanders oproepen.

Tot slot lijkt het ook juridisch geen probleem te zijn, wanneer de politie websites of sociale media bezoekt gebruik makend van op het internet vrij toegankelijke tools (veelal gericht op de bescherming van het recht van vrije meningsuiting) om geen onmiddellijk traceerbare sporen achter te laten. Het gaat meer bepaald over websites die een extra (dikwijls buitenlands) IP-adres beschikbaar stellen (proxyservers[32]) of om een *peer to peer*

---

[29] Het lijkt echter een gemiste kans van de wetgever om, daar waar geen volledig nieuwe misdrijven nodig waren (in tegenstelling tot datasabotage en hacking), reeds bestaande artikels te moderniseren (bijvoorbeeld herschrijving van artikel 196 Strafwetboek in plaats van het creëren van een nieuw artikel 210bis Strafwetboek) (Conings, 2012)

[30] Een eerste aanzet ligt vervat in §3 van artikel 88ter Sv. dat bepaalt: *'Wanneer blijkt dat deze gegevens zich niet op het grondgebied van het Rijk bevinden, worden ze enkel gekopieerd. In dat geval deelt de onderzoeksrechter dit, via het openbaar ministerie, onverwijld mee aan het ministerie van Justitie, dat de bevoegde overheid van de betrokken Staat hiervan op de hoogte brengt, indien deze redelijkerwijze kan worden bepaald.';* het is duidelijk dat de wetgever hier toelaat om ondanks de soevereiniteit van een eventueel andere betrokken staat toch bewijsmateriaal op een in deze vreemde staat gelokaliseerde server te vergaren. Ten aanzien van een klassieke benadering van statelijke soevereiniteit is dit Copernicaans.

[31] Bijvoorbeeld: http://www.ip-adress.com/ip_tracer/fccu.be.

[32] Men bekomt met zijn eigenlijk IP adres (het toegangsjetonnetje tot het internet) een ander en vreemd IP adres (een tweede jetonnetje) om enkel de sporen van dit – dikwijls buitenlands – IP adres achter te laten en zo geen sporen achter te laten die rechtstreeks naar de eigenlijke gebruiker verwijzen: bv. http://www.publicproxyservers.com.

netwerk dat op geïncrypteerde wijze gebruik maakt van verschillende niet detecteerbare tussenstations (bv. TOR of The Onion Routing Network[33]). Het gaat in concreto over (dikwijls gratis en) vrij toegankelijke hulpmiddelen op het internet die privacy bescherming als doel hebben. Het gebruik van dergelijke tools door de politie kan vergeleken worden met de situatie in de reële wereld waar een politieman in burger in een volledig anoniem voertuig rondrijdt op een openbare weg. Uiteraard kan de politie de tools enkel gebruiken indien zij legaal zijn.

B. Onder welke naam of identiteit?

a. Voorafgaande principes

Wat betreft het aannemen van een *nickname*, een fictief e-mailadres of het gebruik maken van een fictief profiel wordt het criterium van de subjectieve dadernotie in herinnering gebracht (zie *supra*). Concreet toegepast op het aannemen van een fictieve identiteit door politiemensen op het internet, bepaalt dit criterium mee de grens tussen normaal aanvaard gedrag op het internet en het eventueel plegen van strafbare feiten. Het helpt zodoende de grijze zone te bewaken tussen een loutere cybercrime surveillance en een bijzondere opsporingsmethode onder aangenomen valse identiteit in de sociale media. Het aannemen van een geloofwaardige fictieve identiteit is immers enkel mogelijk in het kader van de bijzondere opsporingsmethoden. De wet voorziet uitdrukkelijk in die mogelijkheid in het kader van een infiltratie (art 47*octies* Sv) maar het lijkt eveneens tot de mogelijkheden te behoren in het kader van de observatie. Art. 47*quinquies* §2 Sv bepaalt namelijk dat een politieambtenaar, in de uitvoering van bijzondere opsporingsmethoden, onder strikte voorwaarden misdrijven mogen plegen. Het moet daarbij gaan om strikt noodzakelijke strafbare feiten die worden gepleegd in het kader van de opdracht, met het oog op het welslagen daarvan of ter verzekering van hun eigen veiligheid of deze van andere bij de operatie betrokken personen. Dergelijke misdrijven kunnen slechts gepleegd worden mits uitdrukkelijke toestemming van de procureur des Konings. Zij mogen bovendien niet ernstiger zijn dan de strafbare feiten waarvoor de bijzondere methoden worden aangewend en moeten noodzakelijkerwijze evenredig zijn met het nagestreefde doel[34]. De mogelijkheid tot het aannemen van een fictieve identiteit kan best eveneens uitdrukkelijk worden opgenomen in art. 47*sexies* Sv. Immers, waar de observant in de reële wereld geen identiteit moet opgeven, moet hij dat wel in de cyberwereld. Net zoals het noodzakelijk is om de identiteit van de infiltrant in de reële en virtuele wereld af te schermen, is dat eveneens zo voor de observant in de virtuele wereld. Dat niet alleen om de observatie werkbaar te maken maar ook om de observant en zijn familie te beschermen tegen represailles[35]. Ook in de reële wereld kan een fictieve identiteit trouwens nuttig zijn voor de observant. Wanneer de observatie bijvoorbeeld plaatsvindt in een private plaats waar registratie nodig is, is het veiliger voor de observant zich te registreren onder een fictieve naam.

Als uitgangspunt voor politioneel optreden geldt dat een *nickname*, een fictief e-mail adres of een fictief profiel nooit suggestief of provocerend mag zijn (Art. 30 V.T. Sv.) en in eerste instantie niet extra ondersteund mag worden door fictieve documenten[36]. Wanneer

33 https://www.torproject.org: dit netwerk vergaarde recent veel bekendheid enerzijds (positief) als nuttig instrument tijdens de Arabische lente en anderzijds (negatief) als speeltuin voor pedofielen en andere criminelen.

34 Zie voor een uitvoerige bespreking: Berkmoes & Delmulle, 2011, 558 ev; De Roy & Vandromme, 2004, 18-25.

35 In het kader van de infiltratie: Berkmoes & Delmulle, 2011, 674-675; De Roy & Vandromme, 2004, 46.

36 Dergelijke documenten zijn er immers op gericht de identiteit geloofwaardig te maken. Het aannemen van een geloofwaardige identiteit is enkel mogelijk in het kader van de bijzondere

de noodwendigheden van een strafrechtelijk onderzoek daarentegen een geloofwaardige fictieve identiteit vereisen, komt men terecht onder de BOM-wetgeving, dat strenge toepassingsvoorwaarden kent. Enkel in dat geval kan er ook gebruik worden gemaakt van fictieve ondersteunende documenten. Het is voor de politiediensten dus aangewezen om steeds vooraf controle te doen van het feit of de aangenomen identiteit niet echt bestaat en in samenspraak met de betrokken magistraat kan het (on)geloofwaardigheidscriterium steeds op zijn deugdelijkheid worden getest.

Vanaf het moment dat een website of forum vraagt om een soort van minimale registratie, gaat een vergelijking met een openbare plaats niet langer op. De website of het forum is immers niet langer uit zijn aard, op elk ogenblik en zonder enig onderscheid toegankelijk voor eenieder die dat wenst. Afhankelijk van de formaliteiten die moeten worden vervuld om toegang te krijgen, kan een vergelijking gemaakt worden met een plaats toegankelijk voor het publiek, dan wel een soort privéclub. Terwijl de politie een privéclub slechts kan betreden onder dezelfde voorwaarden als een huis (Bockstaele, 2009, 23), kan zij een plaats toegankelijk voor het publiek vrij betreden gedurende de tijd dat het publiek er toegelaten is (art. 26 lid 2 WPA; Cass. 1932a; Cass. 1932b). Er is sprake van een privéclub wanneer voor de toegang formaliteiten zijn voorgeschreven die effectief worden nageleefd en die beletten dat iedereen die dat zou wensen de plaats kan betreden (Cass. 1939; Cass. 1972; Verstraeten, 2007, 291). Wanneer de formaliteiten niet effectief worden nageleefd of de toegang niet beletten, is er sprake een voor het publiek toegankelijke plaats.

b. De voor het publiek toegankelijke virtuele plaats

Sommige sites vereisen, vooraleer zij toegang verschaffen tot hun inhoud, de opgave van een e-mail-adres en soms een daaraan gekoppeld paswoord, zonder dat op enige wijze de echtheid van dat adres of van de persoon achter het adres door de dienstverstrekker wordt gecontroleerd. In dat geval is het de bedoeling dat men zijn identiteit inschrijft in een soort van register. Die formaliteit belet echter niet dat iedereen die dat wenst, toegang kan nemen tot de site (Bockstaele, 2009, 24; De Valkeneer, 2004, 16). Bovendien wordt de formaliteit niet op een degelijke manier nageleefd aangezien er absoluut geen controle is op de echtheid van de identiteit. Hier kan dus identiteit gevonden worden met een voor het publiek toegankelijke plaats. Het lijkt dus zeker geen probleem voor politiediensten om binnen het huidig wettelijk kader toegang te nemen tot dergelijke websites of chatforums. De politie kan daarbij een niet-geloofwaardige fictieve identiteit aannemen. Zo kan zij bijvoorbeeld toegang nemen met behulp van een e-mailadres zoals number1@hotmail.com of ann63@hotmail.com[37].

Wanneer men zich niet bedient van een eigen naam, maar gebruik dient te maken van de gegevens van een andere persoon of van iemand anders zijn of haar sleutel(s)[38], ligt alles gevoeliger. Wanneer op een open (chat)forum sleutels vrij ter beschikking worden gesteld en iedereen (dus ook de politie) daarvan gebruik kan maken, lijkt er geen probleem voor wat betreft de loutere toegangsverschaffing. De sleutels vormen in dat geval immers geen effectieve beperking van de toegang. Daardoor is een vergelijking met een voor het

opsporingsmethoden. Daar geldt echter een subsidiariteitsvereiste. Omwille van het ingrijpend karakter van de bijzondere opsporingsmethoden, mogen zij slechts worden toegepast indien hetzelfde resultaat niet door andere middelen van onderzoek kan worden bereikt. Zie: Berkmoes & Delmulle, 2011, 523.

37 Ook hier is geen sprake van een valse naamdracht aangezien dat misdrijf enkel de familienaam beschermt.

38 Wanneer van sleutel wordt gesproken gaat dit in de meeste gevallen over een login en een daaraan verbonden paswoord.

publiek toegankelijke plaats ook hier op zijn plaats. Eenieder kan immers door gebruik van de publieke sleutels toegang nemen tot de vergrendelde site, zo ook de politie.

c. De cyberprivéclub

Anders is het wanneer een anonieme bron de sleutel ter beschikking stelt (bijvoorbeeld door een melding op stopchildporno.be of op ecops.be), of wanneer men de sleutel verkrijgt van een slachtoffer of van een verdachte (die bijvoorbeeld onder een tapmaatregel staat). De sleutel vormt in dat geval een effectief beletsel voor een hele groep mensen om toegang te nemen tot de site of het forum. Het gaat hier dus wel degelijk om een soort 'cyberprivéclub' die de politie niet zonder meer mag betreden. Wanneer de politie de verkregen sleutel gebruikt om toegang te krijgen tot een website, waartoe ze normaliter niet gerechtigd is, riskeert de overheid zich schuldig te maken aan het misdrijf van hacking (art. 550*bis* SW). Het misdrijf van externe hacking is reeds gepleegd wanneer men louter wetens en willens toegang neemt tot een informaticasysteem waartoe men niet gerechtigd is. Er is geen bedrieglijk opzet vereist[39]. Bovendien neemt de politie andermans identiteit aan, waardoor ze zich schuldig maakt aan identiteitsfraude (art. 231 Sw.). De overheid lijkt in die situatie op het eerste zicht vrijwel machteloos te staan tegenover bijvoorbeeld gruwelijke feiten van kindermisbruik, waarvan het bewijsmateriaal en de gegevens om de eventuele daders te identificeren verscholen liggen achter een virtuele deur waarvan men de digitale sleutel in handen heeft. De mogelijkheden voor de politie zijn beperkt gelet op het private karakter van de site of het forum en gelet op de misdrijven hacking en identiteitsfraude.

Kan de inkijkoperatie in de zin van art. 46*quinquies* Sv.[40] hier een oplossing bieden? Bij een inkijkoperatie verschaft de politie zich immers ook toegang tot een plaats waartoe men in eerste instantie niet gerechtigd is. De huidige bewoordingen van de wet lijken virtuele plaatsen niet uit te sluiten. Een inkijkoperatie kan echter slechts plaatsvinden in private omgevingen waarvan men op basis van precieze aanwijzingen vermoedt dat men er zaken kan vinden zoals bedoeld in art. 46*quinquies* §2, 1° Sv.[41], dat er bewijzen kunnen worden verzameld of dat ze gebruikt worden door personen op wie een verdenking rust (art. 46*quinquies* §3 Sv). De inkijkoperatie is bovendien enkel mogelijk wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een misdrijf uitmaken of zouden uitmaken zoals bedoeld in art. 90*ter* §2-4 of gepleegd worden of zouden worden in het kader van een criminele organisatie, zoals bedoeld in art. 324*bis* Sw (art. 46*quinquies* §1 Sv). Dit lijken eveneens terechte beperkingen in de cyberwereld gelet op het recht op bescherming van de privacy in de afgesloten virtuele ruimtes. In het reeds gebruikte voorbeeld waarbij de politie de sleutels verkrijgt tot een site met kinderporno van een anonieme bron, kan de dubbele proportionaliteitsvereiste vervuld zijn, nl. wanneer deze afgifte gepaard gaat met een aangifte die voldoende precies, gedetailleerd en geloofwaardig is.[42] Een 'cyberinkijkoperatie' lijkt in dat geval mogelijk. Ter verduidelijking zou de wetgever er goed aan doen de woorden 'reële of virtuele' toe te voegen aan de term 'private plaats'. De politie kan in

39 Artikel 550bis §1 Sw.: *'Hij die, terwijl hij weet dat hij daartoe niet gerechtigd is, zich toegang verschaft tot een informaticasysteem of zich daarin handhaaft,…'.*

40 De inkijkoperatie in een private plaats die niet tot woning dient, noch een door de woning omsloten aanhorigheid uitmaakt, noch een lokaal aangewend voor beroepsdoeleinden of de woonplaats van een advocaat of arts is.

41 Zaken die het voorwerp van het misdrijf uitmaken, die gediend hebben of bestemd zijn tot het plegen ervan of die uit een misdrijf voortkomen, de vermogensvoordelen die rechtstreeks uit het misdrijf zijn verkregen, de goederen en waarden die in de plaats ervan zijn gesteld of de inkomsten uit de belegde voordelen.

42 Zie: Cass. 2001 & Cass. 2002: Een anonieme maar zeer gedetailleerde en derhalve geloofwaardige verklaring kan een ernstige aanwijzing uitmaken.

het kader van zo een 'cyberinkijkoperatie' gebruik maken van verstrekte sleutels, maar kan indien nodig tevens gebruik maken van hackertools (cf. een digitale slotenmaker).

Indien de politie de sleutel verkrijgt van de verdachte (al dan niet vrijwillig) geldt een bijkomende mogelijkheid, nl in het kader van een netwerkzoeking. Het gaat daarbij echter niet meer om het louter toegang nemen tot de sociale media om daar eens een kijkje te nemen maar om een werkelijke zoeking naar bewijsmateriaal. Met het oog op die zoeking is een toegang echter wel mogelijk (Kerkhofs & Van Linthout, 2010, 39-40).

C. Wat als meer gevraagd wordt dan enkel een naam en login?

Sommige sites vragen bijkomende gegevens om toegang te kunnen krijgen, zonder dat er sprake is van een echte interactie met de bezoeker. Deze sites zijn hoogdrempeliger dan de sites die onmiddellijk voor iedereen toegankelijk zijn, maar bieden in vele gevallen wel degelijk aan iedereen toegang van zodra een extra gegeven wordt aangereikt. Voor zover de toegang niet effectief wordt beperkt is ook hier de vergelijking met een voor het publiek toegankelijke plaats terecht.

Zo vragen bepaalde websites de opgave van een kredietkaartnummer om bijvoorbeeld na te gaan dat de bezoeker van de website meerderjarig is. Hier lijkt het perfect toegelaten dat de politie gebruik maakt van kredietkaarten die verbonden zijn aan de betrokken politiedienst. De in ogenschouw te nemen grens is hier, zoals ook hierboven voor andere situaties reeds aangekaart, het verbod van het aannemen van een geloofwaardige fictieve identiteit, eventueel ondersteund door fictieve documenten (waar de overstap zou gemaakt dienen te worden naar een bijzondere opsporingsmethode).

Andere websites vragen de voordracht van een andere deelnemer. In zoverre de politie op rechtsgeldige wijze deze voordracht bekomen heeft is er ook hier geen wettelijk beletsel om zich toegang te verschaffen. Al zal in het spanningsveld tussen de rechten van verdediging en de eventuele bescherming van de bron in samenspraak met de betrokken magistraten naar een oplossing gezocht moeten worden die beide belangen kan verzoenen. Wanneer de opgave van een code of een extra paswoord wordt gevraagd, kan dezelfde redenering worden toegepast als hierboven betreffende het gebruik van sleutels (zie *supra*).

Verder zijn verschillende websites betalend, soms aan de hand van een kredietkaart, soms aan de hand van een GSM-betaling (sms of inbellen). Dit mag in se geen beletsel zijn voor de politie om hier verder onderzoek op te verrichten. Het loutere element van betaling maakt iets immers niet minder toegankelijk voor de politie. Een krant kost bijvoorbeeld ook geld, toch maakt een krant een open bron uit die de politie zonder meer mag kopen en consulteren.

Het wordt veel delicater wanneer, zeker in zaken van kinderpornografie, enkel toegang wordt verstrekt wanneer men ofwel zelf eerst (zonder dat er verder ook maar gecommuniceerd moet worden met iemand) illegaal materiaal moet uploaden of waar men door de configuratie van het systeem zelf (denk aan *peer to peer* netwerken of een toepassing zoals Freenet[43]) noodgedwongen deel gaat uitmaken van het verspreidingssysteem van dat netwerk. In die gevallen is elke politionele *'solo slim'* absoluut af te raden en

43 http://freenetproject.org/; volgens Wikipedia: *'Freenet is een op peer-to-peertechniek gebaseerd programma/netwerk dat het mogelijk maakt om volledig anoniem allerlei soorten data te bekijken en te publiceren. Het is daarom een populair programma onder mensen die lokale of nationale misstanden onder de aandacht willen brengen. Dit vooral in dictatoriale landen als China waar anonimiteit voor critici voor hen van levensbelang is. Maar ook illegale zaken als kinderporno kunnen verspreid worden via Freenet. … Wanneer iemand verbinding maakt met Freenet stelt hij dus een stukje schijfruimte beschikbaar aan de rest van de gebruikers. Op deze schijfruimte kan elke willekeurige gebruiker versleutelde data plaatsen; deze data kan degene die ruimte beschikbaar stelt,*

moet zeer precies worden uitgezocht hoe het systeem juist werkt en tot waar men met goedkeuring van de betrokken parketmagistraat of onderzoeksrechter als politieman kan gaan. Een schriftelijke opdracht of kantschrift is in deze gevallen zeer aan te raden. Het actief aanbieden van illegaal materiaal door een politieman is evident niet zomaar toegelaten, want een strafbaar feit. Wanneer daarentegen defectueuse of onschadelijk gemaakte bestanden worden aangeboden, die er echt uitzien, maar niet kunnen geopend worden[44] en ze enkel dienen om toegang te kunnen nemen tot een site, lijkt er juridisch geen probleem. Het gaat enkel over de toegang tot sites zodat enige verdere reflectie over eventuele provocatie zich alsnog niet opdringt.

Het lijkt ook aanvaardbaar dat de politie, zonder dat de ze actief illegale bestanden verspreidt, tijdelijk toegang neemt tot zo'n netwerk met het oog op het verzamelen van bewijsmateriaal en de identificatie van mogelijke daders. Van zodra het bewijsmateriaal werd verzameld, dient wel het nodige te worden gedaan om elke verdere verspreiding te voorkomen of te doen ophouden. Men dient er zich zeer bewust van te zijn, dat zolang men deel uitmaakt van het te onderzoeken *peer to peer* netwerk de eigen computer zal ingeschakeld worden door het netwerk als extra computerkracht of als opslagstation. Toch lijkt er geen sprake van deelneming aan het misdrijf door de politie. Juridisch is allicht belangrijk om mee in rekening te brengen dat men veelal slechts een deel van de bestanden (nullen en enen die op zich niets voorstellen) bij zich krijgt en in het geval van bijvoorbeeld Freenet zelfs enkel geëncrypteerde bestanden waarvan men dus niet weet wat ze voorstellen. Men heeft dus de facto geen 'volledige' illegale bestanden in handen en kan niet weten wat men eventueel juist meehelpt (ten dele) te verspreiden. *A forteriori* ontbreekt de wil om illegale bestanden te helpen verspreiden. Doordat men toegang neemt tot het netwerk, waar meestal ook legale bestanden op worden gedeeld, maakt de computer, ongewild, ook deel uit van het illegale circuit. Er kan bijgevolg geen sprake zijn van deelnemingsopzet[45].

2. Bewijsvergaring in sociale media

A. Het zich ophouden en interageren in sociale media

Daar waar de politie in de hierboven beschreven gevallen op een rechtsgeldige wijze toegang heeft genomen tot de sociale media kan zij er in principe zonder problemen een kijkje nemen. Drie situaties zijn te onderscheiden. Een eerste situatie is te vergelijken met een openbare plaats. Op grond van art. 8 Sv. kan de politie op openbare plaatsen steeds een opsporing doen of een zoeking uitvoeren, dit geldt dus ook voor de openbare plaatsen in de cyberwereld. De tweede situatie is die van de voor het publiek toegankelijke virtuele plaats. Ook die plaatsen kunnen door de politie worden betreden om er een kijkje te nemen (art. 26 WPA). De derde situatie is de cyber-privéclub. Wanneer een cyber-inkijkoperatie mogelijk is, kan men daar eveneens rondkijken (art. 46*quinquies* Sv).

Eens de politie in de sociale media vertoeft komt ze echter al snel in aanraking met specifieke onderzoeksdaden waarvoor specifieke en strengere vereisten gelden. Wanneer ze er namelijk *live* getuige is van gesprekken en van eventuele data in transmissie en deze registreert, loert de toepassing van de tapwetgeving om de hoek. Van zodra er sprake is

niet zelf bekijken of veranderen. Op deze manier is er dus geen centrale server nodig en is iemand alleen traceerbaar binnen een vriendengroep waarmee hij wel direct een verbinding heeft.'

44 Bijv. een bestandje 'preteen-with-grandpa.jpg' dat niet kan geopend worden maar doet vermoeden dat het kinderporno bevat.

45 Enkel een te ver doorgedreven toepassing van het eventuele (deelnemings)opzet zou deze handeling door de politie onmogelijk maken. Wanneer de politie bovendien te actief deelneemt aan het netwerk komt ze terecht onder de BOM-wetgeving.

van een stelselmatige controle op het internet rijst al snel de vraag naar de grens met de bijzondere opsporingsmethode observatie. Ook is het denkbaar dat een politieambtenaar zich actief moet opstellen en met aanwezigen begint te communiceren. In dat geval dient men in te schatten of er sprake is van de bijzondere opsporingsmethode infiltratie en dient men zich bovendien te behoeden voor elke vorm van provocatie (art. 30 Vt. Sv.).

a. Grens met informaticatap?

Wanneer op de bezochte site, chatroom of andere toepassing van sociale media geen actieve communicatie plaatsvindt, vindt de tapwetgeving uiteraard geen toepassing. In het kader van sociale media zal echter al snel sprake zijn van actieve communicatie. Immers, niet alleen taaluitingen vallen onder het begrip communicatie maar ook het uitwisselen van foto's, tekeningen of ander beeldmateriaal (Verslag namens de commissie, 1992-93, 34). Telecommunicatie omvat zo bijvoorbeeld ook de overdracht van, in files opgeslagen, bewegend beeldmateriaal (bv. video's met kinderporno) via e-mailberichten of via het internet (Arnou, 2008, 26; De Cang & Pitieus & Van Wassenhove, 2001, 302).

Het enkele feit dat er sprake is van actieve communicatie maakt de tapwetgeving niet automatisch van toepassing. Er gelden immers nog andere toepassingsvoorwaarden. Zo bepaalt art. 90 ter Sv. dat de (tele)communicatie privé moet zijn. Bovendien zal er enkel sprake zijn van een tap indien de communicatie in de fase van overbrenging is.

Communicatie dient enkel als privé te worden beschouwd wanneer zij niet bestemd is om door iedereen gehoord of ontvangen te worden (Wetsontwerp, 1992-93, 7; Verslag namens de commissie, 1992-93, 10). Het criterium hierbij is de intentie van de deelnemers aan de communicatie en de context waarin deze plaatsvindt (Wetsontwerp, 1992-93, 6; Verslag namens de commissie, 1992-93, 10). Noch de plaats, noch het gebruikte communicatiemiddel (noch het al dan niet beveiligd zijn van het communicatiemiddel), noch het aantal deelnemers aan de communicatie zijn van doorslaggevend belang (Verstraeten, 2007, 469-470). Het gebruikte communicatiemiddel kan echter wel aantonen dat de communicatie niet privé is (Arnou, 2008, 29). Bovendien kan een gesprek niet privé zijn wanneer het gesprek zo verloopt dat anderen het zonder probleem of zonder speciale inspanningen kunnen volgen (Arnou, 2008, 29). Iemand die boodschappen verstuurt op een forum dat duidelijk voor iedereen toegankelijk is en waar eenieder die dat wenst, de gedeelde boodschappen kan lezen, kan achteraf niet beweren dat de communicatie privé was. Er kan slechts sprake zijn van privécommunicatie wanneer de persoon die communiceert in alle redelijkheid kan verwachten dat de communicatie niet wordt bekeken of beluisterd door niet-bestemmelingen[46]. De persoon zal in volgende gevallen bijvoorbeeld mogen verwachten dat de communicatie beschermd is: wanneer de toegang tot de sociale media effectief gecontroleerd en beperkt wordt; wanneer er sleutels nodig zijn die niet gedeeld worden; wanneer sleutels nodig zijn en niet algemeen geweten is dat die openlijk ter beschikking zijn gesteld op openbare fora; wanneer de betrokkene zijn privacy beschermd door de aanpassing van zijn privacyinstellingen; wanneer het forum de illusie creëert dat er private communicatie kan worden gevoerd.

Communicatie is in overbrenging gedurende het traject tussen afzender en ontvanger. Die voorwaarde is in het kader van sociale media echter erg moeilijk toe te passen. Op de eerste plaats is het niet altijd gemakkelijk uit te maken of data statisch dan wel in transmissie zijn. Denk bijvoorbeeld aan een mededeling achter iemands naam op facebook. Daarnaast is ook de duur van de transmissie moeilijk te bepalen. Wanneer komt bv. een chatbericht aan bij de bestemmeling? Wanneer de bestemmeling heeft geantwoord is duidelijk dat de voorgaande berichten zijn aangekomen maar een bericht kan ook reeds

[46] Ook het EHRM hanteert dat criterium. Zie: EHRM, 1999 & EHRM, 2007.

zijn ontvangen zonder dat de bestemmeling antwoord. Wat als er bovendien meerdere bestemmelingen zijn? Dan kan het bericht bij sommigen zijn aangekomen en bij anderen niet. De werkbaarheid van dit criterium in de virtuele wereld wordt sterk in vraag gesteld, zoals dit ook al gebeurde in het kader van e-mailverkeer (Arnou, 2008, 32 ev.; Dumortier, Vanhecke & Missotten, 1997, 145-150; Kerkhofs & Van Linthout, 2008, 79-94).

Het is echter wel belangrijk te weten of de tapwetgeving toepassing vindt. In dat geval is het registeren van de communicatie immers onderworpen aan de op straffe van nietigheid voorgeschreven vormen van artikel 90quater Sv. Bovendien is het 'afluisteren' en registreren van de communicatie dan enkel mogelijk in de beperkte gevallen omschreven in art. 90*ter* Sv. Een herschrijving van de tapwetgeving dringt zich bijgevolg op.

b. Grens met observatie?

Daarnaast rijst de vraag vanaf wanneer er sprake is van de bijzondere opsporingsmethode observatie. Artikel 47*sexies* Sv. omschrijft die bijzondere opsporingsmethode als '*het stelselmatig waarnemen door een politieambtenaar van één of meerdere personen, hun aanwezigheid of gedrag, of van bepaalde zaken, plaatsen of gebeurtenissen'*. In de virtuele wereld zijn plaatsen bijvoorbeeld internetsites of chatrooms. Onder de term gebeurtenissen kan bijvoorbeeld uitwisseling van bestanden of discussies begrepen worden, voor zover hun kennisname niet valt onder de tapwetgeving.

In de reële wereld is het onderscheidingscriterium tussen een 'normale' observatie en deze zoals bedoeld in artikel 47*sexies* Sv., het al dan niet *'stelselmatig'* karakter van de observatie (Berkmoes & Delmulle, 2011, 586; De Roy & Vandromme, 2004, 38). De wetgever koos bewust voor een objectieve invulling van het begrip *'stelselmatige observatie'*[47]. Er is namelijk sprake van een stelselmatige observatie wanneer die langer duurt dan vijf opeenvolgende dagen of vijf niet-opeenvolgende dagen gespreid over een periode van een maand. Een observatie is eveneens stelselmatig wanneer technische hulpmiddelen worden aangewend of wanneer ze een internationaal karakter vertoont of wanneer ze wordt uitgevoerd door de gespecialiseerde eenheden van de federale politie. Het stelselmatig karakter moet vóór het opstarten van de observatie worden beoordeeld en niet post factum of in functie van de finaliteit van de observatie (Memorie van toelichting, 2001-02, 30).

In een internetomgeving lijkt echter al snel sprake te zijn van een stelselmatige observatie. Zo is in de eerste plaats het gebruik van een *'technisch hulpmiddel'* geen efficiënt criterium in de virtuele wereld[48]. Een technisch hulpmiddel is *'een configuratie van componenten die signalen detecteert, deze transporteert, hun registratie activeert en de signalen registreert' (*art. 47*sexies* §1, lid 3 Sv). Ook de computers van de politie, die noodzakelijk zijn om toegang te kunnen nemen tot sociale media, lijken onder deze definitie te vallen. Aangezien geen enkele mogelijkheid bestaat om zonder het gebruik van dat 'technisch hulpmiddel' te observeren in een digitale context zou dit betekenen dat elke observatie die plaatsvindt in de virtuele wereld automatisch stelselmatig is. Verrekijkers en camera's die louter als oog functioneren, worden aanschouwd als louter zintuigversterkende middelen dus niet als een *'technisch'* hulpmiddel in de zin van art. 47*sexies* Sv.(Berkmoes & Delmulle, 2011, 596). Dezelfde redenering lijkt enige uitweg te bieden voor zover de computers gebruikt worden om personen, hun gedrag, zaken, plaatsen of gebeurtenissen in de sociale media waar te nemen. Of de software programma's, die

47 Art. 47*sexies*, §1, tweede lid Sv. Een subjectieve invulling werd op die manier van de hand gewezen: nl. een observatie die toelaat een vrij volledig beeld te vormen van iemands privéleven of van een facet daarvan.

48 Bovendien lijkt het ons ook geen efficiënt criterium te zijn in de reële wereld, gelet op alle uitzonderingen die reeds zijn gemaakt door de wetgever, rechtspraak en rechtsleer (Berkmoes & Delmulle, 2011, 596 ev.).

het observeren menselijk mogelijk maken (bijv. door filtering van bepaalde informatie waardoor een bulk van data exploiteerbaar wordt), louter zintuigversterkend zijn is niet duidelijk. Van zodra de computers van de politie de aanwezigheid van personen of zaken, gedragingen of activiteiten registreren is duidelijk dat de gelijkschakeling niet langer op gaat. Voor het maken van een print screen lijkt dan weer wel een mogelijkheid te bestaan zonder automatisch te vallen onder stelselmatige observatie. Het maken van een print screen kan immers vergeleken worden met het fotograferen van (een gedeelte van) de site die op dat moment open staat. De wet sluit toestellen die worden gebruikt om foto's te maken uitdrukkelijk uit van de definitie van 'technisch hulpmiddel' (art. 47*sexies* §1, lid 4 Sv). Zelfs wanneer meerdere print screens achtereenvolgens worden gemaakt van pagina's waarop misdrijven worden gepleegd, kan men argumenteren dat het louter gaat om vaststellingen van strafbare feiten zodat er geen sprake is van een observatie[49]. Aangezien in geval van registratie van data sprake is van een observatie met technisch hulpmiddel is dit enkel mogelijk in geval van ernstige aanwijzingen van strafbare feiten, strafbaar met een gevangenisstraf van minimum één jaar (art. 47*sexies* §2 Sv).

Er stelt zich echter nog een bijkomend probleem. In een internetomgeving zal immers zeer snel sprake zijn van een observatie met internationaal karakter, gelet op het grenzeloze karakter van het internet. Nu de wetgever bij de redactie van de BOM-wet geen rekening lijkt gehouden te hebben met de internetrecherche, lijkt het raadzaam als parketmagistraat of onderzoeksrechter om toch in deze het zekere voor het onzekere te nemen en de nuttige en noodzakelijke beschikkingen te verlenen, wat uiteraard slechts mogelijk is onder de voorwaarden van art. 47*quinquies* ev. Sv. In ieder geval moet de wetgever de criteria voor het stelselmatig karakter van de observatie dringend herbekijken.

c. *Grens met infiltratie?*

De praktijk leert dat wanneer men toegang neemt tot sociale media, men meestal geconfronteerd wordt met sites waarop vermeld staat wie op dat moment aanwezig of online is. In het merendeel van de gevallen volgt al snel een reactie van de aanwezige personen wanneer zij merken dat er een schijnbaar vreemde eend in de bijt is, zeker wanneer deze laatste niets doet en enkel luistert of toekijkt. Dit schijnbaar voyeurisme wordt meestal gesanctioneerd door verwijdering uit de chatroom of van de site of resulteert in een virtuele aanval met malware op de computer van de 'voyeur'. Het zal dus in vele gevallen noodzakelijk zijn dat de politie – veiligheidshalve – met andere politiemensen een minimum minimorum communiceert, liefst over koetjes en kalfjes.

Wanneer men echter verder gaat en in contact treedt met anderen loert de toepassing van de bijzondere opsporingsmethode infiltratie wel heel snel om de hoek. Het lijkt dan ook evident dat van zodra met derden wordt gecommuniceerd, er veiligheidshalve dient geopteerd te worden voor – waar wettelijk mogelijk – een infiltratie. Dat is echter niet nodig wanneer de communicatie niet duurzaam is (art. 47*octies* §1 Sv).Het louter verzenden van een vriendschapsverzoek valt zodoende bijvoorbeeld niet onder infiltratie. Om van een duurzaam contact te kunnen spreken is immers vereist dat de infiltrant niet louter met het criminele milieu in contact treedt, maar dat hij bovendien het contact enige tijd aanhoudt (Berkmoes, Delmulle, 2011, 675; De Roy & Vandromme, 2004, 46).

Agenten die een infiltratie uitvoeren moeten speciaal daartoe opgeleid en getraind zijn (Memorie van toelichting, 2001-02, 33). Die voorwaarde vloeit voort uit de terechte bezorgdheid voor de risico's die gepaard gaan met een fysieke integratie in een crimineel milieu met het oog op duurzame contacten Berkmoes & Delmulle, 2011, 673). Hoewel die risico's vrijwel onbestaande zijn in de virtuele wereld bestaat ook daar de nood aan een

49 Gent 30 oktober 2006, onuitg. Vermeld door Berkmoes & Delmulle, 2011, 588-589.

specifieke, weliswaar aangepaste training voor infiltranten. Een bijkomende voorzichtigheid is bij de cyberinfiltratie immers op zijn plaats om eventuele provocatie te vermijden. Dat maakt immers vaak een zeer moeilijke evenwichtsoefening uit. Denk bijvoorbeeld aan gespecialiseerde en beveiligde chatrooms waar kinderporno wordt verspreid en men zich dient te handhaven door een minimum aan geloofwaardigheid te creëren.

De vraag dient wel hardop gesteld te worden, waarom er geen eigen *'light'* versie van de figuur van de infiltratie bestaat die toepasbaar is voor internetrecherche, gelet op het beduidend minder risicovolle karakter ervan.

B. Mededelingsplicht in hoofde van IAP's en ISP's

Politie en justitie genieten echter ook een mogelijkheid om bewijsmateriaal uit de cyberwereld te vergaren zonder zelf toegang te moeten nemen tot sociale media. Dit ingevolge de wet betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij[50]. Die wet regelt in eerste instantie de verantwoordelijkheden van de diensten die instaan voor het louter doorgeven van informatie ('mereconduit': artikel 18), voor de opslag in de vorm van het tijdelijk kopiëren van gegevens (artikel 19) en voor 'hosting', dit is de opslag van de door een afnemer van een dienst verstrekte informatie (artikel 20). Gelet op het feit dat Internet Access Providers (IAP's) en Internet Service Providers (ISP's) gigantisch veel informatie over hun datalijnen en datasystemen krijgen, stelt de wet dat deze diensten in principe geen inhoudelijke controletaak hebben (dit zou trouwens in de praktijk ook niet mogelijk zijn). Artikel 21 van de wet bepaalt daarom: *'Met betrekking tot de levering van de in de artikelen 18, 19 en 20 bedoelde diensten hebben de dienstverleners geen algemene verplichting om toe te zien op de informatie die zij doorgeven of opslaan, noch om actief te zoeken naar feiten of omstandigheden die op onwettige activiteiten duiden.'*

Maar, en hier liggen de opportuniteiten voor de cyberrecherche, waar deze IAP's en ISP's geen verplichting hebben om actief toe te zien en op zoek te gaan naar onwettige activiteiten, dienen zij wel de bevoegde gerechtelijke of administratieve autoriteiten onverwijld in kennis te stellen van vermeende onwettige activiteiten of onwettige informatie indien zij hiervan op de hoogte zijn (§2, al.1) en zijn zij verplicht om op verzoek van de bevoegde gerechtelijke of administratieve autoriteiten alle informatie te verschaffen waarover zij beschikken en die nuttig is voor de opsporing en de vaststelling van de inbreuken gepleegd door hun tussenkomst, onverminderd andere wettelijke bepalingen (§2, al.2). Het volstaat met andere woorden dus dat deze verstrekkers van diensten op het internet, bijvoorbeeld door middel van kantschrift van de procureur des Konings of van de onderzoeksrechter, op de hoogte worden gesteld van het bestaan van onwettige activiteiten op hun netwerk of op hun servers, om van hen – gegrond op een wettelijke basis – alle informatie te verkrijgen die nodig is voor het verdere onderzoek.

Politie en justitie hebben bovendien nog een aantal stokken achter de deur waardoor de dienstverleners op het internet er alle belang bij hebben om mee te werken. Voor wat betreft de hosting diensten stelt artikel 20 van de wet van 11 maart 2003 dat de dienstverlener enkel niet aansprakelijk is voor de informatie die bij haar is opgeslagen op voorwaarde dat: 1° zij niet daadwerkelijk kennis heeft van de onwettige activiteit of de informatie en 2° zij van zodra zij daadwerkelijk kennis heeft, prompt handelt om de informatie te verwijderen of de toegang ertoe onmogelijk te maken[51]. Daartoe brengt zij onverwijld de procureur des Konings in kennis van de onwettige activiteit of informatie. De procureur des Konings neemt op zijn beurt de nodige maatregelen overeenkomstig artikel

[50] 'dienst van de informatiemaatschappij': elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg op afstand en op individueel verzoek van een afnemer van de dienst verricht wordt.

[51] De zogenaamde 'notice and take down' procedure

39*bis* Sv. Zolang de procureur des Konings geen beslissing heeft genomen met betrekking tot het kopiëren, ontoegankelijk maken en verwijderen van de in een informaticasysteem opgeslagen gegevens, kan de dienstverlener enkel maatregelen nemen om de toegang tot de informatie te verhinderen. Verder is de weigering om medewerking te verlenen zoals vereist door het artikel 21 van de wet strafbaar met een geldboete van 1.000 tot 20.000 euro (art. 26 §5 3° wet betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij).

IV. Bewijsmateriaal uit sociale media voor de rechter ten gronde

Het lijkt al eens vergeten te worden maar de laatste kritische stap in de bewijsvoering is het voorleggen van het bewijsmateriaal voor de rechter(s) ten gronde met het oog op een tegensprekelijk debat tussen openbaar ministerie, verdediging en eventuele burgerlijke partijen. Bewijsmateriaal is slechts dienstig wanneer de rechtbank het in aanmerking kan nemen. Zoals reeds hoger beschreven, is de bewijsvoering in België vrij en laat het hoogste Hof aardig wat marge voor de rechter ten gronde bij de waardering van eventueel onregelmatig bekomen bewijs. Op grond van de Antigoonrechtspraak van het Hof van Cassatie (Cass. 2003 & Cass. 2004), die ondertussen ook zijn zegen heeft gekregen van het EHRM (EHRM 2009; De Decker, 2009, 201; Schuermans, 2009, 1-2) en het Grondwettelijk Hof (GwH 2010 & GwH 2011; Berkmoes, 2011, 11-17; Schuermans, 2011, 580-585), moet onregelmatig verkregen bewijs immers enkel uit de debatten worden geweerd in 3 gevallen: wanneer de geschonden regel op straffe van nietigheid is voorgeschreven[52], wanneer de schending de betrouwbaarheid van het bewijs aantast of wanneer de rechten van verdediging zijn geschonden.

Met betrekking tot de laatste grond tot uitsluiting verduidelijkte Het Hof dat de rechter ten gronde, in het licht van de artikelen 6 EVRM en 14 IVBPR, rekening mag houden met de elementen van de zaak in haar geheel genomen. De rechter heeft daarbij o.a. oog voor de wijze waarop het bewijs werd verkregen en de omstandigheden waarin de eventuele onrechtmatigheid werd begaan. Hij mag onder meer de volgende omstandigheden in afweging nemen: hetzij dat de overheid die met de opsporing, het onderzoek en de vervolging van misdrijven is belast, al dan niet de onrechtmatigheid opzettelijk heeft begaan, hetzij dat de ernst van het misdrijf veruit de begane onrechtmatigheid overstijgt, hetzij dat het onrechtmatig verkregen bewijs alleen een materieel element van het bestaan van het misdrijf betreft, hetzij dat de onrechtmatigheid geen invloed heeft op het recht of de vrijheid die wordt beschermd door de overtreden norm (Cass. 2003; Cass. 2005; Cass. 2008). Het Hof van Cassatie stelde in het arrest van 31 oktober 2006 bovendien dat de omstandigheid dat de overheid die met de opsporing, het onderzoek en de vervolging van misdrijven is belast, bij de bewijsverkrijging opzettelijk een onrechtmatigheid heeft begaan, niet noodzakelijk moet leiden tot bewijsuitsluiting door de rechter (Cass. 2006a). Wanneer de overheid bijvoorbeeld bewust onrechtmatig gebruik maakt van sleutels, wordt het verkregen bewijs bijgevolg niet noodzakelijk uitgesloten. Toch behoudt de rechter ten gronde de mogelijkheid om louter op grond van het opzettelijke karakter van de onrechtmatigheid het bewijs uit de debatten te weren[53].

---

52 De nietigheidssancties in het Wetboek van Strafvordering zijn echter zeer beperkt.

53 Zie Cass. 2006b: '*In principe is niet geoorloofd het gebruik van bewijs dat de overheid die met de opsporing, het onderzoek en de vervolging van misdrijven is belast, of een aangever met het oog op het leveren van dat bewijs hebben verkregen ingevolge een misdrijf, met miskenning van een regel van het strafprocesrecht, ingevolge een schending van het recht op privacy, met miskenning van het recht van verdediging of met miskenning van het recht op menselijke waardigheid.*'.

In het kader van de betrouwbaarheid van het verkregen bewijs, is het relevant te verwijzen naar artikel 39*bis* Sv. dat de inbeslagname van digitaal bewijs regelt. Paragraaf 6 van dat artikel bepaalt: '*De procureur des Konings wendt de passende technische middelen aan om de integriteit en de vertrouwelijkheid van deze gegevens te waarborgen*'. In tegenstelling tot andere Europese landen waar het verzamelen van digitaal bewijs nauwkeurig beschreven staat in de wetgeving, laat de Belgische wetgever voorlopig raden wat dan wel die passende technische middelen zijn. De uitdaging voor elke raadsman van de verdediging ligt nu bijgevolg in het overtuigen van de rechtbank dat niet de passende technische middelen werden aangewend en dat zodoende de betrouwbaarheid van het bewijs is aangetast.

Er moet dringend worden nagedacht over hoe de digitale vaststellingen zich vertalen naar het niet digitale dossier en over hoe de integriteit en de tegenspreekbaarheid van het digitaal bewijs wordt gegarandeerd. Een wettelijke regulering omtrent de 'chain of custody' is hier zeker en vast op zijn plaats. Dat lijkt de enige manier waarop daadwerkelijk de integriteit en betrouwbaarheid van het digitale bewijs kan worden verzekerd en bewezen en ellenlange discussies daarover uit de weg kunnen worden gegaan. Om de tegenspreekbaarheid van het digitale bewijs te garanderen dringt het gebruik van gedetailleerde deskundige rapporten zich op. Een blik over de grens naar deskundige rapporten van het Nederlands Forensisch Instituut (NFI)[54] doet watertanden. Daarin staat namelijk zeer nauwkeurig beschreven (1) wie het digitaal bewijs onderzocht heeft, (2) waarom de mensen die dat gedaan hebben mogen verondersteld worden deskundig te zijn (3) wat werd gedaan, (4) waarom wat werd gedaan nodig was (5) hoe de integriteit van het bewijsmateriaal werd bewaakt[55] en (6) wat het resultaat is van het deskundig onderzoek. Het spreekt voor zich dat een dergelijk deskundig verslag van het NFI een tegensprekelijk debat niet enkel mogelijk maakt, maar ook waarschijnlijk overleeft. In België lijkt men in vele gevallen zich te beperken tot punt (6). Zeker in het kader van de internationalisering van bewijsoverdracht[56], is de prehistorische wijze van omgaan met bewijsmateriaal in België is niet langer duldbaar.

V. Conclusie

De sociale media vormen een bijzondere uitdaging voor politie en justitie. Aangezien ze een zeer rijke bron aan informatie vormen, is het van groot belang dat de overheid er, met het oog op misdaadbestrijding, op efficiënte wijze gebruik van kan maken. De huidige wetgeving laat een dergelijk efficiënt gebruik echter niet toe. In deze bijdrage werden de voornaamste moeilijkheden bij internetrecherche in de sociale media aangekaart. Het ging daarbij over problemen in verband met de toegang, het verzamelen van bewijsmateriaal en het gebruik van bewijs voor de rechter ten gronde. Onze huidige wetgeving blijkt onvoldoende aangepast aan de nieuwe Web 2.0 realiteit. Op het terrein is het momenteel zoeken naar oplossingen met de beschikbare wetgeving. Daarbij dient enige creativiteit aan de dag gelegd te worden om aan de hand van de combinatie van artikels en de combinatie van rechtsfiguren naar een zo goed mogelijke oplossing te zoeken voor de voorliggende problemen.

54 http://www.forensischinstituut.nl/.

55 Er wordt bijvoorbeeld omstandig uitgelegd wat een hashwaarde is; welke hash waarde berekend werd en waarom dat nodig is (Een hash-waarde is de uitkomst van een wiskundige berekening over de inhoud van een bestand en is altijd uniek. Een hash-waarde kan na berekening bijvoorbeeld een indicatie geven dat een bestand is veranderd zonder dat dit aan de uiterlijke kenmerken te zien is (breekpunt.nl)).

56 Zie in het Europese kader: **Kaderbesluit betreffende het Europees bewijsverkrijgingsbevel.**

Niet in het minst dienen de zich nieuw aandienende en razendsnel verspreidende vormen van communicatie tot bijzondere reflectie te leiden bij onze strafwetgever. Een upgrade van wetgeving 1.0 naar wetgeving 2.0 dringt zich op. Zonder deze upgrade dreigt de politionele en justitiële antivirusbescherming immers onvoldoende weerstand te bieden tegen het wijdverspreide, alsmaar sterker wordende en meest dreigende virtuele virus, de cybercriminaliteit. Bij die upgrade moet de wetgever zoveel mogelijk het uitgangpunt, *offline = online,* in het achterhoofd houden. Bovendien zal de wetgever vanzelfsprekend ook steeds oog moeten hebben voor de grenzen gesteld door het recht op privacy en het recht op vrije meningsuiting. De vraag stelt zich daarbij luidop hoe die privacy moet worden ingevuld, nu de meeste mensen er niet voor terugschrikken een groot deel van hun persoonlijke gegevens in de relatieve openheid van de virtuele wereld te brengen.

Referenties

Arnou, L. (2008). afluisteren tijdens het gerechtelijk onderzoek. In X, *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer* (afl. 59, pp. 1-95). Mechelen: Kluwer.

Beirens, L. (2010). De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace. *Orde van de dag*, *13*(49), 51 – 68.

Berkmoes, H. (2011).Het grondwettelijk Hof geeft zijn zegen aan de antigoonrechtspraak. *Vigiles*, *17*(2), 11-17.

Berkmoes, H., & Delmulle, J. (2011). *De bijzondere opsporingsmethoden en enige andere onderzoeksmethoden.* Brussel: Politeia.

Bockstaele, M. e.a. (2009). *De zoeking onderzocht.* Antwerpen: Maklu.

Conings, C. (2012). Reële valsheid versus virtuele valsheid: hetzelfde garen op een ander klosje. *Nieuw Juridisch Weekblad,* nog te publiceren.

Cybercrime and jurisdiction. A global survey (2006). Den Haag: T.M.C. Asser Press.

De Cang, T., Pitieus, K., & Van Wassenhove, I. (2001). Kinderpornografie. In G. Vermeulen (ed), *Strafrechtelijke bescherming van minderjarigen* (pp. 277-336) . Antwerpen: Maklu.

De Decker, S. (2009). Antigoon vooruit? Straatsburg heeft geen bezwaar tegen de Antigoonrechtspraak. *Vigiles*, *15*(5), 201.

De Hert, P., & Van Leeuw, F. (2011). Cybercrime legislation in Belgium. In E. Dirix & Y. Leleu (eds), *De Belgische rapporten voor het Congres van de 'Académie internationale de Droit Comparé' te Washington*, (pp 867-956) Brussel: Bruylant.

Delbrouck, I. (2008). Naam, naamdracht en valse naam. In X, *Postal Memorialis. Lexicon strafrecht, strafvordering en bijzondere wetten* (pp N 10/01 – N10/32). Mechelen: Kluwer.

De Roy, C., & Vandromme S. (2004). *Bijzondere opsporingsmethoden en aanverwante onderzoeksmethoden.* Antwerpen: Intersentia.

De Valkeneer, C. (2004). La perquisition: principes généraux. In M. Bockstaele (ed), *Huiszoeking en beslag* (pp. 13-30). Brussel: Politeia.

Dewandeleer, D. (2009-10). Computermisdrijven en strafonderzoek in een ICT-context. In R. Verstraeten & F. Verbruggen (eds), *Straf- en strafprocesrecht* (pp 125-163), Brugge: Die Keure.

Dumortier, J., Vanhecke, R., & Missotten, S. (1997). Laat de Belgische wetgeving gerechtelijk aftappen van privé-communicatie via GSM of internet toe?. *Computerrecht: Tijdschrift voor Informatica, Telecommunicatie en Recht*, *14*(4), 145-150.

Kerkhofs, J., & Van Linthout, Ph. (2008). Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel. *Tijdschrift voor Strafrecht*,*9*(2), 79-95.

Kerkhofs J., & Van Linthout, Ph. (2010). Cybercriminaliteit doorgelicht. *Tijdschrift voor Strafrecht*, *11*(4), 179-199.

Lorre, J. (2010-11) Facebook en arbeidsrecht: mysterium tremendum et fascinans. *Rechtskundig Weekblad, 74*(36), 1498-1510.
Schuermans, F. (2009). Straatsburg geeft zegen aan Antigoonrechtspraak. *Juristenkrant, 11* (196), 1-2.
Schuermans, F. (2011). Na Straatsburg betonneert nu ook het Grondwettelijk Hof de Antigoonrechtspraak. *RABG, 9*(8), 580-585.
Van den Wyngaert, C. (2006). *Strafrecht en strafprocesrecht en internationaal strafrecht: in hoofdlijnen.* Antwerpen: Maklu.
Van Dyck, S. (2007). *Valsheid in geschriften en gebruik van valse geschriften.* Antwerpen: Intersentia.
Verstraeten, R. (2007). *Handboek strafvordering.* Antwerpen: Maklu.
Viaene, L. (1962). *Huiszoeking en beslag in strafzaken.* Gent: Story-Scientia.
Voorhoof, D. (2009). Recht op anonimiteit op internet brokkelt af. *Juristenkrant*, *11*(181), 5.
Handvest van de grondrechten van de Europese Unie, *Pb. C.* 30 maart 2010, afl. 83, 389.
Kaderbesluit 2008/978/JBZ van de Raad van 18 december 2008 betreffende het Europees bewijsverkrijgingsbevel ter verkrijging van voorwerpen, documenten en gegevens voor gebruik in strafprocedures, Pb L. 30 december 2008, afl. 350, 1.
Memorie van toelichting, *Parl. St.* Kamer 2001-02, nr. 1688/1.
Richtlijn 2006/24/EC van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG (Richtlijn gegevensbewaring), *Pb. L.* 13 april 2006, afl. 105, 54.
Verklaring van 28 mei 2003 betreffende de expressievrijheid op het internet van de Raad van Europa, 2003, https://wcd.coe.int/ViewDoc.jsp?id=37031.
Verslag namens de commissie, *Parl. St.* Senaat, 1992-93, nr. 843-2.
Verslag van de Commissie aan de Raad en het Europees Parlement, Evaluatie van de richtlijn gegevensbewaring (Verslag gegevensbewaring), COM (2011)225, 1-47.
Wet 5 augustus 1992 op het politieambt (WPA), *BS* 22 december 1992, 27124.
Wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (Wet bescherming persoonlijke levenssfeer), *BS* 18 maart 1993, 5801.
Wet 28 november 2000 inzake informaticacriminaliteit, *BS* 3 februari 2001, 2909.
Wet 11 maart 2003 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, *BS* 17 maart 2003, 12962.
Wetsontwerp, *Parl. St.* Senaat 1992-93, nr. 843-1.
Cass. 14 maart 1932a, *Pas.*1932, I, 108.
Cass.12 december 1932b, *Pas.* 1933, I, 50.
Cass. 16 januari 1939, *Pas.* 1939, I, 22.
Cass. 25 mei 1972, *Pas.* 1972, I, 885.
Cass. 4 april 2001, *Arr. Cass.* 2001, afl. 4, 616.
Cass. 12 februari 2002, *Arr. Cass.* 2002, afl. 2, 425.
Cass. 14 oktober 2003, *Pas.* 2003,afl. 9-10, 1607, concl. De Swaef.
Cass. 23 maart 2004, *Arr. Cass.* 2004, afl. 3, 500.
Cass. 12 oktober 2005, *JLMB* 2006, afl. 14, 585.
Cass.,31 oktober 2006a, *Vigiles* 2007, afl. 3, 93, noot F. Schuermans.
Cass. 21 november 2006b, *Pas.*2006, afl. 11, 2437.
Cass. 10 maart 2008, *JLMB* 2009, afl. 13, 580, noot R. De Baerdemaeker.
EHRM 25 juni 1999, Halford/Verenigd Koninkrijk, http://echr.coe.int.echt/fr/hudoc.

EHRM 3 april 2007, Copland/Verenigd Koninkrijk, http://echr.coe.int.echt/fr/hudoc.
EHRM 2 december 2008a, K.U./Finland, http://echr.coe.int.echt/fr/hudoc.
EHRM 4 december 2008b, Marper/Verenigd Koninkrijk, http://echr.coe.int.echt/fr/hudoc.
EHRM 28 juli 2009, Lee Davis/België, *Rev. dr. Pen.* 2010, 324-335, noot N. Collette-Basecqz.
GwH 22 december 2010, nr. 158/2010, *Arr. GwH* 2010, afl. 5, 2445.
GwH 27 juli 2011, nr. 139/2011, http://www.const-court.be.