Mathias Vermeulen[a]
Paul De Hert[b]

Toegang tot sociale media en controle door politie

Een eerste juridische verkenning vanuit mensenrechtelijk perspectief [1]

Abstract

Access to social media and control by police: a first legal exploration from the human rights perspective
In this paper the legal framework of Belgian police access to social media is outlined, including the impact that such access has on human rights such as the right to privacy and freedom of expression. After analysing in part 1 how the police can make use of social media, we examine in part 2 police access to public information on social media. Part 3 analyses how the police can have access to non-public information on social media. The question whether the Belgian police has the ability to deny individuals access to social media is assessed in part 4 and the – related – question whether there exists a right to anonymous access to social media is examined in part 5.

Key words: social media – human rights – police – privacy – kill switch
Kernwoorden: sociale media – mensenrechten – politie – privacy – kill switch

Panopticon, 33 (3), 258-272
© 2012 Maklu | ISSN 0771-1409 | Mei 2012

[a] Research Fellow aan de Law Faculty van het European University Institute in Firenze en phd-kandidaat aan de Vrije Universiteit Brussel (corresp.: mathias.vermeulen@gmail.com).
[b] Vrije Universiteit Brussel en *associate professor* aan het Tilburg Institute for Law and Technology.

In deze bijdrage schetsen we het juridische kader dat de toegang van de politie tot informatie op sociale media regelt, waarbij we speciale aandacht geven aan de potentiële impact die dergelijke toegang heeft op onder meer het recht op privacy en de vrijheid van meningsuiting. Na in deel 1 na te gaan op welke manieren de politie sociale media kan gebruiken, onderzoeken we in deel 2 de regulering van politietoegang tot publieke informatie op sociale media. Deel drie behandelt dan de (complexere) vraag hoe en wanneer de politie toegang heeft tot niet-publieke informatie. Aangezien op internationaal vlak stemmen opgaan om het mogelijk te maken om de toegang tot sociale media te blokkeren omwille van veiligheidsoverwegingen, gaan we in deel 4 kort in op de wettelijke mogelijkheid van een dergelijke maatregel door politie en justitie in België. Het vijfde deel van deze bijdrage behandelt de vraag of er een recht bestaat op anonieme toegang tot sociale media. We sluiten af met een aantal conclusies.

[1] Deze bijdrage werd mede mogelijk gemaakt door steun van het Agentschap voor Innovatie door Wetenschap en Technologie in het kader van het EMSOC project – User empowerment in a social media culture.

1. Sociale media gebruik door de politie

Er is geen algemeen aanvaardde definitie van sociale media, maar voor dit artikel beschouwen we sociale media als die verzameling van internetsites en applicaties die het creëren van 'user generated content' mogelijk maken (Kaplan & Haenlein, 2010). Het gebruik van dergelijke media door publieke actoren biedt in het algemeen een drietal mogelijkheden (Bertot, Jaeger & Hansen, 2011). Ten eerste kunnen sociale media gebruikt worden om de burger nauwer te betrekken bij het werk dat een (overheids)dienst doet door een participatieve dialoog op te starten. Centraal bij sociale media is immers het tweerichtingsverkeer: burgers kunnen actief hun stem laten horen in discussies over beleidsontwikkeling en -uitvoering. Naast het bevorderen van dergelijke participatie in de democratie, kan het gebruik van sociale media ook leiden tot het gemeenschappelijk ontwikkelen, verstrekken en verbeteren van de dienstverlening van de overheid. Zo kan het gebruik van sociale media de reactiesnelheid van overheden gevoelig vergroten. Tot slot kunnen sociale media ook ingezet worden om het publiek te betrekken in het zoeken van oplossingen van bepaalde problemen, het zogenaamde 'crowdsourcing'. De kennis en de talenten van de burger worden dan gebruikt om oplossingen te ontwikkelen voor maatschappelijke vraagstukken. Om dit mogelijk te maken wordt er verondersteld dat de overheid bepaalde data met het publiek deelt zodat die laatste een stevig vertrekpunt heeft om te kunnen meedenken. We zullen zien dat deze drie mogelijkheden ook daadwerkelijk benut worden door de politie.

Sociale media in België worden op verschillende onschuldige manieren gebruikt door de politie. Deze media bieden de politie allereerst een ongefilterd kanaal aan waarmee snel een groot publiek kan bereikt worden. Het lijkt dan ook logisch dat een belangrijk functie van het gebruik van sociale media door de politie ligt in het informeren van de burgers over het werk dat een politie(zone) uitvoert. Het publiek kan geïnformeerd worden via Facebook of Twitter over belangrijke activititeiten die in de politiezone plaatsvinden (zoals grote sportmanifestaties of muziekfestivals). De Politiezone Rupel gebruikt bijvoorbeeld actief Facebook en Twitter om de bezoekers van muziekfestivals Tomorrowland en Casa Blanca te informeren over bijvoorbeeld file-problemen op weg naar de festivals en hoe deze te vermijden. In Leuven is de 'doelgroepinspecteur studenten' beter bekend als 'de Facebookflik', die via zijn Facebookpagina de studenten informeert over fietscontroles en activiteiten van de politie. Tegelijkertijd is zijn Facebookpagina een laagdrempelig aanspreekpunt voor de studenten. Een eerste contact wordt snel gelegd via Facebook, wat daarna verder opgevolgd kan worden (Vermeulen, 2011).

Dat informeren kan echter veel verder gaan. In de Verenigde Staten zijn er politiekorpsen die in real time weergeven op Twitter of Facebook wat het korps momenteel aan het doen is. Dat resulteert in tweets zoals: "***bocapolice*** *are investigating an early morning crash into a canal. The driver has been arrested and charged. Details bit.ly/bFdQOx*." Het valt nog af te wachten of we ook in België een dergelijke *real-time* inkijk zullen krijgen in de activiteiten van een korps.

In het verlengde hiervan ligt het gebruik van sociale media om aan crisiscommunicatie te doen. Het Pukkelpopdrama toonde aan dat de burger verwacht dat officiële instanties aanwezig zijn op deze kanalen om objectieve informatie te verstrekken over een crisis. Toenmalig Minister van Binnenlandse Zaken Annemie Turtelboom ondersteunde deze redenering. Snelle communicatie tijdens een crisissituatie is essentieel, stelt de Minister, en daarom zijn sociale media "een absoluut geschenk" voor de overheid. Ze ijverde resoluut voor het opnemen van het gebruik van sociale media in de noodplanning van evenementen (Turtelboom, 2011).

Ten slotte benut de politie ook de 'crowdsourcing' functie van nieuwe media door actief burgers te betrekken bij het oplossen van misdrijven. Sociale media zijn immers een ideaal kanaal om opsporingsberichten en child focus alerts te verspreiden. Via gerichte advertenties op Facebook kan een politiezone in theorie zelfs beslissen om bijvoorbeeld alle Facebookgebruikers in – bijvoorbeeld – de buurt van Wuustwezel een bepaald opsporingsbericht te laten zien. Naar analogie met het gebruik van sms-berichten (De Hert, Nouwt, Voets & Van Der Wees, 2008) kan via hetzelfde mechanisme ook gericht naar getuigen gezocht worden. Daarbij wordt dankbaar gebruik gemaakt van het drempelverlagend effect van de nieuwe media. Tijdens het Tomorrowlandfestival bijvoorbeeld kreeg de politie ook foto's van drugsdealers – gemaakt door festivalgangers – doorgestuurd (Boey, 2011). Het spreekt voor zich dat hier privacy-aspecten aan verbonden zijn. In België kan een burger bijvoorbeeld niet zomaar foto's van dergelijke verdachten publiceren op de publieke Facebook- of Twitterpagina van een politiezone. Dat zou immers een schending betekenen van de privacywet van 8 december 1992, waarin de wetgever bepaalde dat je geen informatie mag verwerken van een andere persoon die kan leiden tot individuele herkenning zonder de toestemming van de persoon in kwestie. Dergelijke informatie kan alleen via een vertrouwelijke 'direct message' of een e-mail worden verstuurd (De Hert en Vermeulen, 2011).

Deze bijdrage focust vooral op het 'preventief' gebruik van sociale media door de politie. Via websites zoals http://youropenbook.org/ kan er actief gezocht worden in de statusupdates van mensen die een publiek profiel hebben op Facebook (Koops, 2012). Het gedrag van bepaalde verdachten kan ook gevolgd worden via sociale media, en via die sociale media is het gemakkelijk om de verschillende relaties tussen verdachten te analyseren – al dan niet met gespecialiseerde apparatuur. Sommige – niet al te snuggere – verdachten werden betrapt omdat ze foto's van hun misdaden op dergelijke sites zetten. Met 'metatagging' van foto's kan de politie zelfs de locatie bepalen van de foto's die iemand op Facebook of Twitter zette. Het juridische kader voor de toegang tot dergelijke 'publieke' informatie is niet helemaal duidelijk in België: valt het systematisch checken van dergelijke publieke informatie bijvoorbeeld onder de stelselmatige observatie? Welke privacy-risico's zijn er verbonden aan een dergelijk monitoren van sociale media?

De politie kan ook toegang zoeken tot informatie die niet publiekelijk verkrijgbaar is.. De politie zou bijvoorbeeld kunnen infiltreren in gesloten Facebook groepen om bepaalde verdachten te monitoren, of een politieman kan de identiteit aannemen van iemand anders om bevriend te worden met een verdachte zodat hij diens privéprofiel kan checken. Dat is vooral het geval in het kader van de opsporing van kindermisbruik. De politie kan ook direct aan sociale mediasites vragen om inzage te krijgen in de persoonlijke berichten van verdachten. In een opmerkelijk onderzoek van *The Guardian* beantwoordde drie kwart van de Britse respondenten positief de vraag of de politie onvoorwaardelijk inzage zou moeten hebben in de data van alle sociale mediagebruikers om de georganiseerde misdaad te bestrijden (Ball, 2011). Ook hier is het juridisch kader niet helemaal duidelijk in België. Wanneer kan de politie precies inzage krijgen in de privécommunicatie van de burger op een sociale netwerksite?

Een laatste situatie die behandeld wordt is deze waarin de politie een (sociale netwerk) site, of een deel ervan, uit de lucht wil halen omwille van veiligheidsoverwegingen. Op deze laatste situatie wordt in een aparte sectie teruggekomen, waarbij speciale aandacht wordt gegeven aan de impact die dit kan hebben op de vrijheid van meningsuiting.

In wat volgt maken we een eerste verkenning van het Belgisch juridisch kader (Dewandeleer, 2010; Van Linthout & Korfs, 2008; De Hert & Van Leeuw, 2010; Beirens, 2010) en plaatsen we enkele mensenrechtelijke vraagtekens.

2. Toegang tot publieke informatie op sociale media: juridisch kader

Ten eerste is de context van het open bronnenonderzoek, i.e. het onderzoek van publiek toegankelijke informatie zoals publieke *tweets*, *status-updates* op Facebook en YouTube filmpjes die (al dan niet bewust) voor iedereen zichtbaar zijn. Beirens staat niet lang stil bij de situatie van dergelijke publieke gegevens en stelt dat kopieën kunnen gemaakt worden van publiek toegankelijke informatiediensten of diensten waarop elkeen zich zonder enige voorwaarde kan registreren om er gebruik van te maken (Beirens, 2010). In België bestaat er immers een juridische basis van algemene strekking voor het verzamelen van persoonsgegevens door de politie: de wet op het politieambt machtigt de politiediensten inlichtingen en informatie in te winnen en te verwerken over personen en groeperingen die een concreet belang vertonen voor de uitoefening van de opdrachten van bestuurlijke en gerechtelijke politie (art. 44/1 WPA). Meer staat er niet. Er is geen wettelijke basis voor het systematisch opslagen van publieke gegevens over één persoon of over het verder gebruik van publieke gegevens met behulp van profielen en misdaadanalysemethoden (Van Den Wyngaert, 2011, 961; De Hert & Saelens, 2011). Die situatie steekt schril af tegen het gedetailleerd karakter van de bepalingen over misdaadanalyse in het Europolbesluit of de Nederlandse Wet Politieregisters. Publiek 'grijpbare' gegevens zijn onzes inziens echter niet helemaal vrij te gebruiken, aangezien de systematische opslag of het verdere gebruik van dergelijke informatie aan de hand van profielen en misdaadanalyse, een weerslag zouden kunnen hebben op de fundamentele rechten en vrijheden van de burger. Concreet betekent dit dat de politie niet zonder redelijk vermoeden van een (ophanden zijnde) strafbaar feit de burger de klok rond mag bespioneren of observeren op sociale netwerksites. Het equivalent van een dergelijke online observatie in de 'echte' wereld lijkt immers vergelijkbaar te zijn met een politieman die elk gesprek van een individu op een publieke plaats afluistert en opneemt.

Deze redenering kan ook juridisch onderbouwd worden. Centraal in de privacywet van 8 december 1992, staan wettelijke vereisten zoals rechtmatigheid, juistheid en nauwkeurigheid en doelbinding (art. 4-6 WVP). Het verwerken van gegevens voor andere doeleinden dan waarvoor gegevens zijn verzameld, is in beginsel niet toegelaten en verklaart waarom open brongegevens nooit volledig vrije gegevens zijn. Bovendien legt deze wet zeer restrictieve regels op voor gevoelige persoonsgegevens, zoals gegevens betreffende ras of gezondheid – die bijvoorbeeld uit foto's zijn af te leiden; de politie mag dergelijke gegevens slechts verzamelen als dit onvermijdelijk is voor het doel dat wordt beoogd (Koops, 2012).

De WVP vormt één argument om open bronnenonderzoek in België en de moderne methoden van misdaadanalyse op de aldus bekomen gegevens, nader te regelen. Een ander argument vormt de gebrekkige regeling van de observatie, zeker met betrekking tot de nieuwe sociale media. In België bestaat geen regeling voor de 'gewone' observatie omdat aangenomen wordt dat dit nu net is wat de politie altijd doet: een oogje in het zeil houden op publieke plaatsen. Toch wordt deze invulling van de taak van de politie wat uitgerekt in de zin dat ook "*het occasioneel schaduwen, bijvoorbeeld door een politieofficier in burger die plaatsneemt in een café of een dancing en gesprekken mee beluistert*" er onder gerekend wordt (Van Den Wyngaert, 2011, 963). Een specifieke wettelijke grondslag voor deze observaties bestaat niet, maar kan gevonden worden in de algemene taakstelling van de politie (artikel 8 Sv. en 15 WPA). In Nederland bestaat een analoge constructie en baseert men de gewone constructie op het algemene art. 2 Politiewet 1993. Koops suggereert terecht dat dergelijke algemene bepalingen geen toereikende grondslag betekenen voor politieel openbronnenonderzoek als het argument is dat het hier om "publiek beschikbare

gegevens" gaat. "Ik (kom) tot de conclusie dat dit artikel onvoldoende voorzienbaarheid biedt voor burgers om de inbreuk op hun privacy te rechtvaardigen. Vanwege het gebruik van technische hulpmiddelen (*bedoeld worden misdaadanalysemethoden*) en vanwege de intensiteit van het zoeken in uiteenlopende Internetbronnen, is open-brononderzoek op Internet snel als stelselmatige observatie aan te merken. Alleen als op slechts enkele specifieke webpagina's gedurende een beperkte periode informatie wordt verzameld over concrete personen, is er geen sprake van stelselmatige observatie" (Koops, 2012). Het onderscheid tussen gewone observatie en stelselmatige observatie is van groot belang in het licht van de koppeling van deze laatste aan stringente voorwaarden die ingevoerd werden door de BOM-wetgeving (De Nauw & Schuermans, 2003).

De stelselmatige observatie wordt gedefinieerd en geregeld in *47sexies* Sv als het stelselmatig waarnemen door een politieambtenaar van één of meerdere personen, hun aanwezigheid of gedrag, of van bepaalde zaken, plaatsen of gebeurtenissen. De bepaling is 'streng' vanuit politieperspectief omdat alleen de procureur des Konings het bevel tot een stelselmatige observatie kan geven en dit alleen in het kader van strafonderzoek. Bovendien moet de voorwaarde vervuld zijn 'dat het onderzoek zulks vereist en de overige middelen van onderzoek niet lijken te volstaan om de waarheid aan de dag te brengen'. Een observatie met gebruik van technische hulpmiddelen kan bovendien enkel gemachtigd worden wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben (artikel *47sexies*, § 2 Sv.). Artikel *47sexies*, § 2 Sv omschrijft een aantal situaties die op 'objectieve' wijze aangeven dat we in de hypothese van een stelselmatige observatie zitten: een observatie van meer dan vijf opeenvolgende dagen of van meer dan vijf niet-opeenvolgende dagen gespreid over een periode van een maand, een observatie waarbij technische hulpmiddelen worden aangewend, een observatie met een internationaal karakter, of een observatie uitgevoerd door de gespecialiseerde eenheden van de federale politie. Er bestaat weinig twijfel over de toepassing van artikel artikel *47sexies* Sv op het bekijken van Facebook pagina's. Wordt het bekijken van nieuwe media gelijkgesteld met het gebruik van technische hulpmiddelen, dan is er geen enkele ruimte voor de politie om buiten de voorwaarden in artikel *47sexies* Sv. dagenlang de bewegingen en uitspraken van een gebruiker op verschillende sociale media te observeren.

Beirens maakt eerder melding van een initiatief van het college van procureurs-generaal, het federaal parket, de lokale parketten, de vereniging van onderzoeksrechters en van verschillende diensten van de federale politie, die in 2007 een document met conclusies opgesteld hebben waarin gepoogd wordt binnen de grenzen van het huidige wettelijk kader de bewegingsruimte voor internetonderzoeken vast te leggen (Beirens, 2010, 64). Het document is niet beschikbaar en de bespreking, die niet bedoeld is als systematisch, geeft ons geen volledige helderheid, maar de kern van het document zou neerkomen op volgende afspraken. Enerzijds is er verkennend onderzoek naar mogelijke criminele activiteiten op internet, zonder dat er al concrete aanwijzingen zijn van gepleegde of nog te plegen feiten. Deze zijn slechts toegelaten binnen het kader van een pro-actief onderzoek, waarvoor het Openbaar Ministerie vooraf en schriftelijk zijn toestemming heeft gegeven. Anderzijds zijn er de reactieve onderzoeken, waarbij, aldus Beirens, de politiemensen onder leiding van de dossiermagistraat iets meer speelruimte krijgen voor hun internetonderzoeken. "Heel vlug zitten we echter tegen de grens aan van de bijzondere opsporingsmethodes, waardoor het niet eenvoudig zal zijn om bijvoorbeeld internetdossiers op een efficiënte manier te laten verlopen. We kunnen in een reactief dossier een neutrale nickname aannemen om in een publiek chatkanaal polshoogte te nemen, maar we mogen niet echt in debat gaan met de andere chatters; dat zou immers al een infiltratie uitmaken" (Beirens, 2010,

64). We komen op de infiltratie in een volgende sectie terug. Het ontbreekt ons aan meer informatie om het gemaakte onderscheid bedacht in 2007 volledig te doorgronden. Wel is duidelijk dat er op discutabele wijze van uitgegaan is dat internetonderzoeken geen observatie met technische hulpmiddelen zijn, want daarvoor is krachtens artikel 47*sexies* **§ 2.** Sv. vereist dat er ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van een jaar, of een zwaardere straf, tot gevolg kunnen hebben. De praktijkoplossing schreeuwt om een wettelijke verduidelijking temeer omdat ook een verkennend onderzoek naar mogelijke criminele activiteiten op internet veel informatie over een persoon kan opleveren waarvoor krachtens artikel 8, § 2 EVRM een uitdrukkelijke wettelijke grondslag vereist is.

3. Toegang tot niet-publieke informatie op sociale media: juridisch kader

De tweede situatie die we onderscheiden is deze waarin de politie niet-publiek toegankelijke informatie zoekt. We belanden opnieuw in een juridische zone met vele complexiteiten en onduidelijkheden. In regel kan de politie hier niet eigenmachtig optreden en moet ze het initiatief overlaten aan hetzij de Procureur, hetzij de onderzoeksrechter.

Eenvoudig verloopt het opvragen van bepaalde gegevens over het gebruik van sociale media op grond van artikel 46*bis* van het Wetboek van Strafvordering dat de procureur machtigt identificatiegegevens op te vorderen bij operatoren van elektronische netwerken en bij verstrekkers van elektronische communicatiediensten. Ingeval van hoogdringendheid kan zelfs een officier van gerechtelijke politie de identiteit van de betrokkene(n) opsporen, zij het mits instemming van de procureur des Konings (Kerkhofs & Van Linthout, 2011). Deze privacy intrusie is minder verregaand dan inzage in de inhoud van de communicatie omdat alleen de identiteit van de deelnemers bekend wordt gemaakt en niet de inhoud van de communicatie.

Wil men de inhoud van de communicatie kennen dan volstaat de bevoegdheid van de procureur niet meer en zal een onderzoeksrechter moeten worden ingeschakeld (Beirens, 2010, 65). Deze heeft eveneens een bevoegdheid tot het opvragen van communicatiegegevens (88*bis* Sv.) en kan daarenboven voor meer doorgedreven onderzoeken gebruikmaken van een netwerkzoeking (88*ter* Sv.), en communicatietap van alle communicaties van de verdachte(n) of van de plaatsen en de telecommunicatiemiddelen die geregeld worden gebruikt door de verdachte (art. 90*ter* Sv.).

De politie kan bijgevolg niet zomaar inzage krijgen in de communicatie van de burger op een sociale netwerksite. We denken hierbij aan hier artikel 314*bis* en 259*bis* Sw. Deze bepalingen bestraffen niet alleen het afluisteren van communicatie maar ook het kennisnemen van communicatie. Het kennis nemen van de inhoud van (elektronische) communicatie kan in principe alleen door tussenkomst van de onderzoeksrechter. Wanneer een politieman bijvoorbeeld inzage zou wensen in de communicatie van een bepaalde burger (laat staan een onbepaald aantal burgers) op een sociale netwerksite zoals Netlog, dan kan Netlog niet zonder meer op de vraag van de politie in te gaan. Dat kan alleen mits bevel van de onderzoeksrechter en voor zover er sprake is van ernstige feiten. Het lukraak opvragen van communicatie aan een sociale netwerkbedrijf is niet aanvaardbaar. Desgevallend pleegt de politieman een inbreuk op artikel 259*bis* Sw (ambtsmisdrijf).

Er zijn enkele problemen aan te wijzen met de genoemde onderzoeksbevoegdheden. Zo is de netwerkzoeking vervat in artikel 88*ter* § 2 Sv. 'beperkt tot waar bepaalde persoon toe gerechtigd is/was', wat onder meer de vraag oproept of een netwerkzoeking kan gebeuren vanaf de computer van de overheid (Dewandeleer, 2010). Artikel 88*ter* § 2 Sv.

laat ook een zoeking toe tijdens een gerechtelijk onderzoek waarbij het gerecht buiten de grenzen gaat. In beginsel is dus een netwerkzoeking met het oog om Facebookgegevens te bekomen (die in de Verenigde Staten zijn opgeslagen) geen probleem. Wel is het zo dat België met deze bepaling internationaal vooruit loopt en dat vele landen dergelijke grensoverschrijdende bevoegdheden als een inbreuk op hun soevereiniteit zien (Koops & Brenner, 2006). Internationale afspraken zijn meer dan nodig. Aangezien de grote sociale media spelers (Facebook, Twitter, Linkedin) Amerikaanse bedrijven zijn, is het nuttig om op te merken dat in de V.S. er niet noodzakelijk dezelfde geplogendheden op nahoudt als België. Belgische gebruikers van deze sites moeten zich realiseren dat hun privé-informatie gemakkelijker toegangelijk is tot Amerikaanse agenten. In een opgemerkte uitspraak in een zaak over drie Wikileaks-sympathisanten (waaronder zich een Nederlander en een Ijslands parlementslid bevonden) oordeelde het Eastern District Court van Virginia dat er geen privacy bezwaren konden ingeroepen worden tegen het overdragen van informatie over de Twitter-accounts van de drie activisten, inclusief informatie over de tijdstippen wanneer persoonlijke berichten werden gestuurd en vanop welk ip-adres dat gebeurde (United States District Court for the Eastern District of Virginia, 2011).

Beirens bespreekt ten slotte een 'zwakke plek' die ontstaat als criminelen doordringen tot de cybernetwerken en deze netwerken hacken. De netwerkzoeking maakt het immers alleen mogelijk om een zoeking uit te voeren op een systeem waarop de verdachte toegangsrechten heeft – en dat is niet echt het geval op een gehackte computer. Evenmin is hacking toegelaten in beveiligde omgevingen, wat Beirens doet besluiten dat deze wetgeving uit 2000 tot de prehistorie van cyberspace behoort (Beirens, 2010).

Een laatste probleem heeft betrekking op de telecommunicatietap (artikel 90*ter* Sv.). Van alle besproken bevoegdheden vormt dit de meest stringente, qua randvoorwaarden en motivering. Deze bepaling vormt de enige toegelaten uitzondering op het verbod in artikel 314*bis* en 259*bis* Sw. op het afluisteren en kennisnemen van communicatie. Probleem is evenwel dat deze bepalingen alleen bescherming bieden voor de communicatie 'tijdens de overbrenging' – wat sommigen uit de magistratuur en de politiewereld ertoe brengt om de strafbepalingen niet van toepassing te achten op bijvoorbeeld een 'aangekomen', maar ongeopende mail in de mailbox (De Hert, 2003). Zolang deze interpretatiekwestie niet beslecht is, blijft er onduidelijkheid over de fundamentele vraag naar de reikwijdte van de bescherming geboden door artikel 314*bis* en 259*bis* Sw. en over de technische vraag wanneer gebruik gemaakt moet worden van een telecommunicatietap (artikel 90*ter* Sv.) dan wel van een iets minder strikt geregelde netwerkzoeking (88ter Sv.).

Een tweede reeks bevoegdheden die relevant zijn betreffen deze van de infiltratie en van de wettelijk geregelde observaties. Hier wordt de analyse erg complex daar de politie zoveel als mogelijk ruimte wil behouden en uit het vaarwater van de 'strenge' bepalingen van de reeds genoemde BOM-wetgeving wil blijven. De stelselmatige observatie uitgewerkt in 47*sexies* Sv. is hoger (sectie 2) reeds besproken inclusief de in 2007 uitgewerkte interpretatie en versoepeling, die ons vanuit mensenrechtelijke standpunt niet overtuigde.

De infiltratie wordt uitgewerkt in artikel 47*octies* Sv. Infiltratie in de zin van dit wetboek is het door een politieambtenaar (de infiltrant) onder een fictieve identiteit, duurzaam contact onderhouden met een of meerdere personen, waarvan er ernstige aanwijzingen zijn dat zij strafbare feiten in het kader van een criminele organisatie (zouden) plegen of in het kader van één van de misdrijven waarvoor een telecommunicatietap toegelaten is (opgesomd in artikel 90ter, §§ 2 tot 4 Sv.). Opnieuw dus strenge voorwaarden. Volgens de in 2007 uitgewerkte interpretatie is niet elke afscherming van de politie-identiteit een infiltratie. De politie kan, aldus Beirens, in reactieve dossiers een neutrale nickname aannemen om in een publiek chatkanaal polshoogte te nemen, maar "daarbij mag ze niet echt

in debat gaan met de andere chatters; dat zou immers al een infiltratie uitmaken" (Beirens, 2010, 64). Wat de situatie is bij verkennende proactieve onderzoeken is niet duidelijk. De regeling van de nicknames wijst opnieuw op een constructie die veel vragen oproept en vraagt om wettelijke verduidelijking om tegemoet te komen aan de mensenrechtelijke eis dat privacyinbreuken uitdrukkelijk bij wet worden geregeld. Duidelijk is alleszins wel dat politie en gerecht vragen om een aangepaste (lees: minder strenge) variant om aan *cyberinfiltratie* te kunnen doen (bv. onder valse identiteit chatten). Wij denken dat de verduidelijking een meer algemene draagwijdte moet hebben. Een begin van oplossing vormt de Nederlandse bevoegdheid tot het stelselmatig inwinnen van informatie over de verdachte door een opsporingsambtenaar 'zonder dat kenbaar is dat hij optreedt als opsporingsambtenaar' (art. 126j Nl. Sv). Deze bevoegdheid laat toe om in burger gesprekken te voeren met een verdachte en zijn omgeving (Koops, 2012, sub 3.1), en geeft o.i. aan hoe de regularisering van politiepraktijken die men uit de toepassing van de infiltratie wil houden, vorm moet krijgen.

4. Beperken van toegang tot sociale media omwille van veiligheidsoverwegingen

Een derde situatie die we hoger hebben geïdentificeerd is deze waarin de politie de toegang tot door burgers bekendgemaakte informatie wil afsnijden en blokkeren. Volgens de Raad van Ministers van de Raad van Europa heeft het internet een 'public service value' (Council of Europe, 2007), omdat mensen steeds meer vertrouwen op het internet "als een essentieel onderdeel voor hun dagelijkse activeiten inzake communiceren, informatie, kennis en commerciële activiteiten". Daaruit volgt dat burgers een legitieme verwachting mogen hebben dat internetdiensten voortdurend toegangelijk, betaalbaar, veilig en betrouwbaar zijn. Volgens de meest recente cijfers gebruiken 78% van alle Belgen het internet (Internetworldstats, 2011), en van die intergebruikers zitten ongeveer 4.44 miljoen Belgen op Facebook en 1 miljoen op Linkedin. Voor Twitter zijn de cijfers minder duidelijk, maar geschat wordt dat er 150 à 250.000 accounts aan Belgen kunnen worden gekoppeld (Belgian Social Media Monitor, 2012). De Raad benadrukte dat het internet een steeds belangrijkere rol speelt in het verstrekken en verspreiden van diverse bronnen van informatie aan het publiek, "*inclusief user generated content.*" De waarde van sociale media ligt volgens de raad dus niet per se in haar (unieke) infrastructuur, maar in de informatie die ze verspreidt. Die waarde werd duidelijk in 2011, het jaar waarin sociale media gelauwerd werden voor hun bijdrage in het organiseren en mogelijk maken van de verschillende revoluties tijdens de Arabisch lente. Het gebruik van sociale media was niet de oorzaak van de revoluties, maar vergemakkelijkte deels de uitvoering van die revoluties: mensen konden sneller in contact komen met gelijkgezinden.

Het 'revolutionair potentieel' van sociale media werd erkend door verschillende autoritaire regimes – niet alleen in het Midden Oosten, maar ook in China, Rusland en Congo. Sommige staten hebben deze 'bedreiging' in de kiem proberen te smoren door een waaier aan maatregelen zoals het blokkeren, filteren, of volledig afsluiten van sociale media sites (Kelly & Cook, 2011). De reeks voorbeelden is helaas eindeloos. Nadat er geruchten opdoken dat er gewonden waren gevallen tijdens een protest van werknemers in de energiesector, sloot Kazakhstan Twitter af (Committee to Protect Journalists, 2011). De oprichter van de Russische sociale netwerksite Vkontakte werd gedagvaard nadat hij geweigerd had om de Facebookpagina's van zeven groepen te blokkeren die oproepen om te protesteren tegen de uitslag van de Russische parlementsverkiezingen (EDRI, 2011). Syrië en Wit-Rusland monitoren actief al de berichten van hun burgers op sociale netwerksites op zoek naar tegenstanders. Syrië sloot, net zoals Egypte, de internet toegang gewoon af in het land

toen de revolutie eenmaal uitbrak. Het land verbood zelfs het gebruik van iPhones zodat er minder makkelijk filmpjes van demonstraties gemaakt konden worden die snel op sociale media gezet konden worden (BBC, 2011).

Wanneer autoritaire regimes de toegang tot (bepaalde informatie op) sociale netwerksites willen beperken om de organisatie van protesten in de kiem te smoren, dan schreeuwt de (Westerse) media en publieke opinie moord en brand. Anders wordt het wanneer democratische landen oproepen om meer controle te krijgen over het gebruik van sociale media, en zelfs de toegang tot die media (tijdelijk) willen opschorten. Dergelijke signalen werden gegeven naar aanleiding van het gebruik van Twitter en Facebook bij de Britse rellen van 2011 en krijgen ook bij ons een echo wanneer vastgesteld wordt dat chauffeurs gebruik maken van smartphone-apps en Facebookpagina's die waarschuwen voor alcoholcontroles (Somers, 2011).

Na de rellen tijdens de zomer van 2011 in het Verenigd Koninkrijk zei de Britse premier David Cameron tegen het Parlement dat zijn regering overwoog om mensen te verbieden om nog sociale media zoals Twitter en Facebook te gebruiken als ze verdacht werden van het plannen van criminele activiteiten: "*So we are working with the Police, the intelligence services and industry to look at whether it would be right to stop people communicating via these websites and services when we know they are plotting violence, disorder and criminality*" (Cameron, 2011). De minister van Binnenlandse Zaken, Theresa May, nodigde daarop vertegenwoordigers van Facebook, Twitter en RIM uit om samen met de politie te bespreken of en hoe dit eventueel mogelijk zou zijn (May, 2011; Bradshaw, 2011). Uiteindelijk werd de soep niet zo heet gegeten en bleek dat het gesprek meer een discussie was over hoe te voorkomen dat hun diensten gebruikt werden om geweld te organiseren. De overheid zocht uiteindelijk geen nieuwe bevoegdheden die hen zou toelaten om sociale media te sluiten in tijden van crisis. Anders liep het in San Francisco, waar de politie van het Bay Area Rapid Transit (BART) metronetwerk het mobiele netwerk in de metro afsloot om gecoördineerde protesten tegen te houden nadat een passagier na een incident was neergeschoten door een van een veiligheidsmedewerker van het bedrijf. BART, een speciaal agentschap van de State of California, kon het mobiele netwerk in zijn metronetwerk uitschakelen, omdat het de apparatuur daarvoor in eigen beheer heeft. Door de maatregel kon geen enkele gebruiker van het metronetwerk meer bellen, sms'en of mobiel internetten in de metro's en metrostations van de vervoerder (Elinson, 2011).

Het gevaar van suggesties zoals deze van Cameron en de acties van BART in Californië schuilt in het feit dat in se de denkwijze tussen democratische en authoritaire voorstanders van een zogezegde 'afzetknop' van sociale media (in het Engels bekend als de 'kill switch') op hetzelfde idee berust, namelijk dat de toegang tot informatie gelimiteerd moet worden omwille van veiligheidsredenen. In het Westen wordt dan snel teruggegrepen naar de balans-metaphoor, waarin het verspreiden van informatie – via het gebruik van sociale media – aan banden moet gelegd kunnen worden als daar veiligheidsoverwegingen voor bestaan.

Wij beschikken niet over informatie over de mogelijkheden voor politie en justitie in België om de toegang tot informatie te blokkeren. Zeker is dat filter- en blokkeringsystemen in sommige gevallen verenigbaar zijn met de Europese mensenrechten, hoewel Stol toch met goede argumenten de vraag stelt of dit wel een taak is voor de politie (Stol, 2010). In het kader van een strafprocedure kan alleszins teruggevallen worden op de ruime bevoegdheid tot databeslag (artikel 39*bis* Sv.) die toelaat om informatie ontoegankelijk te maken en te verwijderen van informaticasystemen (artikel 39*bis* § 1Sv.). De derde paragraaf van deze bepaling laat de procureur toe om passende technische middelen aan te wenden om de toegang tot gegevens te verhinderen. Indien de gegevens strijdig zijn

met de openbare orde of de goede zeden wendt hij alle passende technische middelen aan om deze gegevens ontoegankelijk te maken (artikel 39*bis* § 1Sv.). Artikel 88*quater* § 2 Sv. laat de onderzoeksrechter dan weer toe iedere geschikte persoon bevelen om zelf een informatiesysteem *ontoegankelijk te maken of te verwijderen*, in de door hem gevorderde vorm.

Iedere inperking op de mogelijkheid tot communiceren ligt evenwel zeer gevoelig in een democratische rechtstaat. Frank La Rue, de VN Special Rapporteur on the right to freedom of opinion and expression, benadrukt de noodzaak aan goede, gerechtelijke procedures met betrekking tot elke overheidshandeling die een weerslag heeft op de vrijheid van meningsuiting via moderne media zoals het Internet. In de praktijk van vele landen ziet hij te vaak willekeur en te ruim toezicht en de controle van communicaties. Belangrijke rechtsgoederen zoals de nationale veiligheid of de bestrijding van terrorisme kunnen alleen inbreuken op deze vrijheden rechtvaardigen wanneer, aldus La Rue, de overheid kan aantonen dat a) een bepaalde handeling of boodschap gericht is tot 'dreigend' geweld aan te zetten, b) er de handeling of boodschap ook aannemelijk kan leiden tot geweld, en c) dat er een rechtstreeks en onmiddellijk verband tussen het gebruik van de media en de kans dat geweld zal volgen (UN, 2011).

De noodzaak van dergelijke criteria werden duidelijk in de 'Twittergrap' rechtszaak in het Verenigd Koninkrijk. In de winter van 2010 vroor het stevig in het Verenigd Koninkrijk, wat resulteerde in verschillende geschrapte vluchten – en zelfs gesloten luchthavens. Op 6 januari 2010 stond Paul Chambers voor zo'n gesloten luchthaven dichtbij Sheffield. Ontgoocheld omdat hij zijn vliegtuig zou missen die hem naar zijn blind date zou leiden, nam hij zijn smartphone waarop hij de volgende status-update invoerde op zijn Twitter-account: "Crap! Robin Hood airport is closed. You've got a week and a bit to get your shit together otherwise I'm blowing the airport sky high!!" Voor zijn 600 volgers was er waarschijnlijk geen vuiltje aan de lucht; maar een manager van de luchthaven vond de tweet tijdens een toevallige zoekopdracht, en waarschuwde de politie. Die arresteerde Paul Chambers een week later op zijn werk, en tijdens een huiszoeking werden zijn iPhone, laptop en desktop computer in beslag genomen (Wainwright, 2010). Hij werd later aangeklaagd voor het "verzenden van een publieke elektronische boodschap die uitzonderlijk grof, beledigend, of van een onfatsoenlijke, obscene of bedreigende aard is" zoals in strijd met sectie 127 van de UK Communications Act 2003. De rechter in Doncaster Magistrates' Court oordeelde dat er inderdaad sprake was van een 'bedreigende' boodschap, en op 10 mei 2010 werd Chambers schuldig bevonden en veroordeeld tot het betalen van 1000 pond aan boetes en gerechtskosten. De uitspraak werd op veel ongeloof onthaald en velen stelden zich de vraag of de huidige generatie rechters wel genoeg vertrouwd waren met de finesses en modaliteiten van het gebruik van sociale media. Huidige UN Special Rapporteur on the protection of human rights while countering terrorism, Ben Emmerson QC, behandelt momenteel de zaak Chambers in hoger beroep. Zijn conclusie: "One has to inject common sense to avoid the law ending up looking silly" (BBC, 2012).

Op een studiedag in het Belgische Parlement over cybersurveillance op 16 december 2011 georganiseerd door de Universiteiten van Brussel en Namen werd eenzelfde opmerking gemaakt over een vergelijkbare situatie. Arbeidsgerechten reageren te krampachtig op klachten van werkgevers over Facebookberichten van werknemers. Voor Steve Gilson, *maître de conference* aan de ULC was het ook duidelijk dat rechters ook niet in staat waren om berichten om sociale media te begrijpen in hun ware betekenis. Zo hielden rechters geen rekening hielden met begeleidende *smileys* bij een Facebook bericht van een man over zijn werkgever. De 'humor' werd niet gezien en het ontslag werd door de rechters geredelijk aanvaard. (Gilson, 2011)

5. Een recht op anoniem gebruik van sociale media?

Uiteindelijk is het niet de staat, maar sociale media zelf die gebruiksregels aannemen die een eerste impact kunnen hebben op de rechten van de mens, vooral dan met betrekking tot het recht op vrije meningsuiting. Een onderdeel van dit debat betreft de noodzaak aan anoniem gebruik van sociale media. Er zijn veel goede redenen om een pseudoniem te gebruiken online, of om anoniem te willen blijven wanneer men het internet gebruikt. Pseudoniemen kunnen gebruikt worden om zich te beschermen tegen stalkers of andere gebruikers met onfrisse doeleinden. Soms is men bang om een echte identiteit aan te nemen wanneer men wantoestanden aanklaagt, zowel in autoritaire regimes (activisten) als in constitutionele democratieën (klokkenluiders). Maar de laatste jaren zien we een trend om anonimiteit online terug te dringen. Die trend is gekoppeld aan een drang van de grote sociale mediaspelers om ook als 'identity-management tool' te fungeren. Meer en meer krantensites en blogs in de V.S. laten nu pas commentaar toe op bepaalde online artikels als je ingelogd bent met je Facebook-account.

Als grootste sociale netwerksite hanteert Facebook een duidelijke 'real name policy': gebruikers moeten hun echte naam gebruiken, mogen geen valse informatie over zichzelf verspreiden, en mogen niet meer dan een online profiel aanmaken. Als een gebruiker zich hier niet aan houdt, kan hem de toegang tot Facebook ontzegd worden door het bedrijf zelf. Natuurlijk bestaan er duizenden mensen met een pseudoniem op Facebook, maar het bedrijf zelf is duidelijk: niet-afdwinging betekent niet dat er geen schending van de overeenkomst is. Die regels gelden voor iedereen. In 2011 sloot Facebook bijvoorbeeld de profielpagina af van een bekende Chinese politieke blogger (Zhao Jing) die schreef onder de naam Michael Anti. Zelfs bekend schrijver Salman Rushdie zag zijn Facebookprofiel verdwijnen aangezien hij op zijn paspoort officieel bekend staat als Ahmed Rushdie. Facebook stelt dat zo'n politiek de kwaliteit en de beschaafdheid van de commentaren en de interacties tussen de gebruikers op de site verhoogd. De Raad van Europa roept lidstaten op "het recht op privacy en private correspondentie tijdens het gebruik van het Internet" te respecteren, inclusief "de wil van gebruikers om niet hun identiteit kenbaar te maken" (Council of Europe, 2007) Maar in welke mate is er in Europa een recht op het anoniem gebruik van sociale media?

Volgens het Europees Hof van de Rechten van de Mens is er alvast geen absoluut recht op anonimiteit online. In de zaak K.U. vs. Finland plaatste een onbekende een advertentie op een Finse datingsite met een foto van KU en een verwijzing naar zijn website, lichaamsbouw en leeftijd waarin wordt gesuggereerd dat de twaalfjarige K.U. op dat moment op zoek is naar jongens om hem seksueel "de weg te wijzen." De vader van K.U. vraagt aan de ISP de identiteit te achterhalen van de persoon die de advertentie heeft geplaatst zodat een klacht wegens laster kan ingediend worden. De service provider weigert echter de identiteit van de houder van het ip-adres te onthullen. Het wil wel een schadevergoeding betalen. De zaak komt voor het Europese Hof, en het Hof oordeelt dat er een schending was van artikels 8 en 13 EVRM. Het Hof wijst erop dat we hier te maken hebben met het kwetsbaar opstellen van een minderjarige voor toenaderingen door pedofielen. Een dergelijke zware schending van het privéleven vereist efficiënte strafrechtelijke voorzieningen. Maar volgens het Hof was Finland er niet in geslaagd haar positieve verplichtingen onder artikel 8 na te komen, aangezien er voor een dergelijk scenario geen mogelijkheid was om een schadevergoeding te krijgen van de eigenlijke dader. Praktische en efficiënte beschermingsmaatregelen waren daarom nodig om de identiteit van de betrokkene te achterhalen. Het Hof oordeelde dat men zich immers niet onttrekken aan bepaalde verantwoordelijkheden door zich te beroepen op de expressievrijheid en het daaraan gerelateerde recht op anonimiteit:

> *"Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such a guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others."* (EHRM, 2008, §49)

Uit deze uitspraak volgt natuurlijk niet dat anonieme profielen op sociale media verboden moeten zijn. Integendeel, het Hof stelt ook duidelijk in *K.U. versus Finland* dat een land positieve verplichtingen heeft om maatregelen aan te nemen die het recht op respect voor het privéleven kunnen verzekeren, inclusief de bescherming van de identiteit van een persoon. Sommige activisten of klokkenluiders kunnen alleen hun boodschap onder een pseudonieme verspreiden via sociale media – bijvoorbeeld als het te gevaarlijk is om te protesteren in een land, of als er geen effectieve toegang is tot traditionele media om een boodschap te verkondigen. Volgens deze redenering zou een staat stappen moeten ondernemen die bijvoorbeeld ervoor moeten zorgen dat een klokkenluider zich moet kunnen verschuilen achter een pseudoniem wanneer hij wandaden wil aanklagen – al dan niet via een sociale netwerksite. Artikel 10 EVRM voorziet de vrijheid om meningen te verstrekken voor een ieder "zonder inmenging van enig openbaar gezag en ongeacht grenzen." Maar als Facebook beslist om dergelijke anonieme profielen niet toe te staan, dan beknot het indirect de vrijheid van meningsuiting. Zou Ierland (als zetel van Facebook Europe) dan bijvoorbeeld verantwoordelijk kunnen gesteld worden voor het schenden van artikel 10?

De kans is klein. De zaak Appleby e.a. tegen het Verenigd Koninkrijk uit 2003 kan verhelderend zijn in deze context. In deze zaak voor het Europees Hof liet een lokaal winkelcentrum (dat tevens de functie van nieuw stadscentrum vervulde) niet toe dat bepaalde dorpsbewoners (onder wie mevrouw Appleby) campagne voerden tegen lokale bouwplannen. Doel van de actie was een informatiestandje op te zetten en een handtekeningenactie te organiseren in het publieke gedeelte van het winkelcomplex. Hoewel de inperking op de vrijheid van meningsuiting en vergadering uitging van een private actor, aanvaardde het Hof dat het Verenigd Koninkrijk aangeklaagd kon worden door middel van de "indirecte horizontale werking" van het verdrag. Onder die redenering moet de overheid maatregelen nemen om niet gewenste beperkingen van de expressievrijheid door de eigenaar van het winkelcomplex tegen te gaan. In dit concrete geval oordeelde de rechter echter dat er geen schending was van artikel 10, aangezien mevrouw Appleby genoeg andere fora had om haar grieven te formuleren. Het Hof preciseert dat artikel 10 geen keuzevrijheid schenkt qua (publiek) forum voor de uitoefening van dat recht (EHRM, 2003, §47).

6. Conclusie

In deze bijdrage behandelden we juridische aspecten van de toegang van de politie tot sociale media die relevant zijn in een mensenrechtencontext. Na een kort overzicht van relatief onschuldig gebruik van sociale media door de politie focusten we op het gebruik van sociale media als hulpmiddel bij rechercheactiviteiten. Hier rijzen er meer potentiële problemen – vooral vanuit het recht op privacy. Het onderzoeken van publieke informatie op sociale media valt volgens de Belgische wetgeving binnen het open bronnenonderzoek. Hier werd beargumenteerd dat artikel 47sexies SV betreffende de stelselmatige observatie ook van toepassing kan zijn op het langdurig bekijken van openbare tweets of Facebook-

updates. Een in 2007 uitgewerkte regeling die de politie toelaat onder voorwaarden het Internet te observeren moet omwille van de mensenrechtelijke legaliteitseis beter in de wetgeving verankerd worden. Ook de politietoegang tot niet-publieke informatie is momenteel onduidelijk. Naargelang de aard van de gezochte informatie is de tussenkomst van de onderzoeksrechter nodig. Activiteiten die een grote impact hebben op het recht op privacy, zoals infiltratie via sociale media, of chatten onder een andere identiteit, zijn momenteel niet duidelijk geregeld en de indruk rijst dat de BOM-wetgeving een minimale interpretatie krijgt. Een verduidelijking van het Belgisch wettelijk kader dringt zich hier aan.

In het vierde deel van deze bijdragen gingen we na in welke mate de politie eventueel de toegang tot sociale media moet kunnen afsluiten omwille van veiligheidsoverwegingen. Het lijkt onwerkbaar om mensen te verbieden sociale media te gebruiken, zelfs wanneer er een verdenking rust op die personen dat ze sociale media gebruiken om criminele activiteiten te plannen. Er is in ieder geval momenteel geen wettelijk kader dat een dergelijke afsluiting zou toelaten. In kader van strafonderzoek zijn er wel de mogelijkheden tot interventie van artikel 39*bis* en 88*quater* Sv.

Het moge duidelijk zijn dat recht in binnen- en buitenland nog geen passend antwoord heeft gevonden om de toegang van de politie tot sociale media te regelen. Dat is geen verrassing, aangezien de wetgever altijd achterloopt op de nieuwste technologieën. Een computerwet uit 2000 wordt vandaag al tot de digitale prehistorie gerekend. Omwille van de mensenrechten moeten gebalanceerde, krampvrije oplossingen gevonden worden in de rechtszaal en op de tekentafel van de wetgever. Dat ook de Grondwet op de tekentafel moet herbekeken worden, lijdt geen twijfel (Kindt, Lievens, Kosta, Leys & De Hert, 2008; Lemmens, 2010; Uyttendaele, 2002). De oproepen tot de erkenning van een recht op toegang tot het Internet moet op dat moment zeker ook aandacht krijgen. Zo'n recht kan niet alleen belangrijk zijn als een hefboom voor het dichten van de digitale kloof, maar kan ook tevens een nuttig instrument vormen ter ontrading van te vergaande controlebevoegdheden en censuurbevoegdheden, weze het in handen van de politie of van een private actor.

Referenties

Ball, J. (2011), *Two-thirds support social networking blackout in future riots*. Verkregen op 8 November 2011, via http://www.guardian.co.uk/media/2011/nov/08/two-thirds-support-social-media-blackout

BBC (2011), *Syria 'bans iphones' over protest footage*. Verkregen op 2 december 2011 via http://www.bbc.co.uk/news/world-middle-east-16009975

BBC (2012), Judgment reserved in Doncaster Twitter airport threat appeal. Verkregen op 8 februari 2012, via http://www.bbc.co.uk/news/uk-england-south-yorkshire-16943333

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

Boey, J. (2011), Politie tevreden over gebruik sociale media als Facebook en Twitter. *Gazet van Antwerpen*, 6 Augustus 2011.

Bradshaw, T. (2011), *Mixed messages from Twitter, Facebook and RIM over Cameron's riot block threat*. Verkregen op 11 Augustus 2011, via http://blogs.ft.com/fttechhub/2011/08/social-media-block-response/#axzz1n48Rf8Up

Cameron, D. (2011), *PM Statement on disorder in England*. Verkregen op 11 Augustus 2011, via http://www.number10.gov.uk/news/pm-statement-on-disorder-in-england/

Committee To Protect Journalists, *Kazakh authorities censor news on deadly clashes*. Verkregen op 20 December 2011, via http://cpj.org/2011/12/kazakh-authorities-censor-news-on-deadly-clashes.php

Council Of Europe (2007), *Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet* (Adopted by the Committee of Ministers on 7 November 2007 at the 1010th meeting of the Ministers' Deputies). Verkregen op 10 oktober 2011 via https://wcd.coe.int/ViewDoc.jsp?id=1207291
De Hert, P. (2003), C.A.O. nr. 81 en advies nr. 10/2000 over controle van internet en e-mail. *Rechtskundig weekblad,* 66, 1281-1294.
De Hert, P., J. Nouwt, I. Voets & J.G.L. Van Der Wees (2008), Sms, opsporing en privacy. *Computerrecht*, 4, 154-160.
De Hert, P. & Saelens, R. (2011), Lokale besturen, informatienoden en de nood aan een wet verwerking politiegegevens. Gedaan met deeloplossingen. *Vigiles. Tijdschrift voor politierecht*, 17(2), 1-5.
De Hert, P. & Van Leeuw, FR. (2011), Cybercrime Legislation in Belgium, Country report of the Cybercrime Section of the IACL Congress in Washington 2010. In Dirix, E., & Leleu, Y.H. (eds.), *The Belgian reports at the Congress of Washington of the International Academy of Comparative Law* (pp.867-956). Brussel: Bruylant.
De Hert, P., & Vermeulen, M. (2011), De Twitterschandpaal en de privacy. *Juristenkrant,* 237, 11.
De Nauw, A. & Schuermans, F. (2003), De wet betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden. *R.W.*, 921-936.
Dewandeleer, D. (2010), Misdrijven en strafonderzoek in de IT-context. In Verstraeten, R. & Verbruggen, F., (ed.), *Strafrecht en strafprocesrecht. Themis 2009-2010* (pp.125-163). Brugge: Die Keure.
Edri (2011), Russian Government's new attempts to censor the Internet. *EDRi-gram newsletter*, (9)24.
Elinson, Z. (2011), After cellphone action, Bart fasces escalating protests, *New York Times*, 20 Augustus 2011.
Gilson, S. (2011), *Is de werkgever de beste vriend van de werknemer op Facebook?*. Verkregen op 15 januari 2012 via http://www.privacycommission.be/nl/new/event/studienamiddag-cybersurveillance-161211.html
Kaplan, A. & Haenlein, M. (2010), Users of the world, unite! The challenges and opportunities of social media. In Business Horizons, 53, 59-68.
Kelly, S. & Cook, S. (2011) *Freedom on the Net 2011: A global assessment of Internet and digital media*. Washington: Freedom House.
Kerkhofs, J. & Van Linthout, Ph. (2011), Artikel 46bis van het Wetboek van Strafvordering en de motiveringsplicht: de minimis non curat praetor?, noot bij Cassatie, 29 maart 2011. *Tijdschrift voor Strafrecht*, 6.
Kindt, E., Lievens, E., Kosta, E., Leys, Th. & De Hert, P. (2008), Constitutional Rights and New Technologies in Belgium (pp.11-56). In Leenes, R., Koops, E.J., & De Hert, P., *Constitutional Rights and New Technologies. A Comparative Study*. The Hague:T.M.C. Asser Press.
Koops E.J. & Brenner S.W. (2006) *Cybercrime and Jurisdiction. A Global Survey*. The Hague: TMC Asser Press.
Koops, E.-J. (2012), Politieonderzoek in open bronnen op Internet: strafvorderlijke aspecten. *Tijdschrift voor Veiligheid*, te verschijnen.
Lawless, J. (2011), *Facebook, Twitter, RIM Meet For Riot Talks With U.K. Government*. Verkregen op 25 Augustus 2011 via http://www.huffingtonpost.com/2011/08/25/facebook-twitter-rim-uk-government-riot_n_936058.html
Lemmens, K. (2010), Misbruiken van de meningsvrijheid via internet: is het recht Web 2.0-compatibel? Pleidooi voor een technologieneutrale bescherming van de uitingsvrijheid. *Orde van de dag*, 49, 15-22.

May, Th. (2011), *Speech on riots*. Verkregen op 11 Augustus 2011 via http://www.homeoffice.gov.uk/media-centre/speeches/riots-speech?version=1
Somers, S. (2011), Politie machteloos tegen Bob-verklikkers. *De Morgen*, 31 december 2011, 3.
STOL, W. (2010), Filteren van inter net: een politietaak? *Orde van de dag*, 49, 43-49.
Turtelboom, A. (2011), *Pukkelpop: Hoe moet het beleidsniveau omgaan met sociale media*. Verkregen op 12 September 2011, via http://annemieturtelboom.be/2011/09/12/pukkelpop-hoe-moet-het-beleidsniveau-omgaan-met-sociale-media/
Un Human Rights Council (2011), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 6 May 2011, A/HRC/17/27.
Uyttendaele, C. (2002), Bescherming van de communicatievrijheid in digitale omgevingen: verminderde bruikbaarheid van nationaal (grondwettelijk) recht (pp.11-44). *Jaarboek ICM 2000-2001*, Antwerpen: Maklu.
Van Den Wyngaert, Ch. (2011), *Strafrecht en strafprocesrecht (in hoofdlijnen)*. Antwerpen: Maklu.
Van Linthout, Ph. en Kerkhofs, J. (2008), Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel. *T. Strafr.,* 2, 79-95.
Vermeulen, M., *Belgische politie tast gebruik van sociale media af*. Verkregen op 14 december 2011 via http://emsoc.be/1900-belgische-politie-tast-gebruik-van-sociale-media-af/
Wainwright, M. (2010), Wrong kind of tweet leaves air traveller £1000 pound out of pocket. *The Guardian*, 10 Mei 2010.
Wet van 5 augustus 1992 op het politieambt (WPA)
Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, gewijzigd door de wet van 11 december 1998 tot omzetting van de richtlijn 95/46/EG van het Europees parlement en de raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *B.S.*, 3 februari 1999 (WVP).
Wet van 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *B.S.*, 12 mei 2003, 25357 (BOM-wet).
EHRM, K.U. v. Finland, 2 december 2008, verzoekschrift nr. 2872/02.
EHRM, Appleby e.a. t. Verenigd Koninkrijk, 6 mei 2003, verzoekschrift nr. 44306/98.
United States District Court for the Eastern District of Virginia, Alexandria Division, Memorandum Opinion – Case 1:11-dm-00003-TBC-LO, 10 November 2011.
Belgian Social Media Monitor – http://bvlg.blogspot.com/2012/01/belgian-social-media-monitor-januari.html.
Internet World Stats – http://www.internetworldstats.com/europa.htm#be