OFFLINE VS. ONLINE INFILTRATIE: EVALUATIE VAN DE BIJZONDERE ONDERZOEKSMETHODE VAN INFILTRATIE IN DE INFORMATICA CRIMINALITEIT IN BELGIË

Masterproef van de opleiding ‘Master in de rechten’

Academiejaar 2017-2018

Ingediend door Van Eyken Louise
(studentennummer: 01207356)

Promotor: Prof. dr. Gert Vermeulen
Commissaris: Sofie Depauw
Aantal woorden: 51 053
Aangezien het schrijven van deze masterproef symbolisch als het sluitstuk van mijn academisch parcours kan worden beschouwd, lijkt het opportuun om hierbij een paar mensen te bedanken.

Ten eerste gaat mijn zeer oprechte dank uit naar Prof. dr. Vermeulen voor de hulp en de vrijheid dat hij me heeft gelaten bij het schrijven van mijn masterproef. Dit was een zeer uitdagende en leerrijke ervaring die perfect mijn opleiding in de Rechten kan afronden.

Daarnaast wil ik ook mijn familie bedanken voor de ondersteuning die ze mij gegeven hebben deze vijf laatste jaren, en zeker tijdens de lastige blokperioden waar de onzekerheid en de stress die ermee verbonden was, vaak overheerste. Ook wil ik Carmen in het bijzonder bedanken voor het leer- en verbeterwerk, zeker omdat ik als Franstalige soms veel spelfouten in mijn tekst liet.

Uiteindelijk wil ik ook mijn rechtenvriendinnen, zowel van de Université Saint-Louis als van de Universiteit Gent bedanken voor hun steun en de vele uren die we samen in de bibliotheek hebben gewerkt.

Louise Van Eyken

Gent, mei 2018
<table>
<thead>
<tr>
<th>Hoofdstuk</th>
<th>Titel</th>
<th>Pagina</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>De plaats van het internet in onze maatschappij</td>
<td>4</td>
</tr>
<tr>
<td>2.</td>
<td>Nieuwe gevaren verbonden aan de informatisering van de maatschappij</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>2.1. Opkomst van de informaticacriminaliteit</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>2.2. Politiële criminaliteitsstatistieken</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>2.3. Cyberterrorisme</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>2.4. Toekomstige toename van de informaticacriminaliteit</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>2.5. Het dark web</td>
<td>9</td>
</tr>
<tr>
<td>2.</td>
<td>Begripsomschrijving</td>
<td>11</td>
</tr>
<tr>
<td>3.</td>
<td>Types misdrijven</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>1. Opsplitsing van het Cybercrimeverdrag</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>2. Opsplitsing tussen specifieke en niet-specifieke informaticacriminaliteit</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>2.1. Specifieke informaticacriminaliteit</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>2.2. Niet-specifieke informaticacriminaliteit</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>2.3. Misdadiigers die de informatica toevallig gebruiken</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>2.4. Accidentele cybercriminelen</td>
<td>15</td>
</tr>
<tr>
<td>4.</td>
<td>Kenmerken informaticacriminaliteit</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>1. Anonimiteit</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>2. Globaliteit en grensoverschrijdende natuur</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>3. Stijgende trend</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>4. Reikwijdte</td>
<td>20</td>
</tr>
<tr>
<td>2.</td>
<td>Hoofdstuk 2. Belang van IT-systemen voor het onderzoek</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Afdeling 1. IT-systemen als hulpmiddelen van het onderzoek</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Afdeling 2. De toegankelijke plaatsen op het internet voor de politiediensten</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Afdeling 3. Rol van de sociale media’s</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>Afdeling 4. Nood aan bijzondere kennis en expertise</td>
<td>27</td>
</tr>
</tbody>
</table>

DEEL II. IMPACT VAN DE INVOERING VAN DE ONLINE INFILTRATIE DOOR DE WET VAN 25 DECEMBER 2016 OP DE BESTRIJDING VAN DE INFORMATICACRIMINALITEIT
Hoofdstuk 1. Legislatief kader en evolutie ........................................................................... 31
Afdeling 1. Nood aan aanpassing van het legislatief kader aan de cyberwereld ................. 31
1. Ongeschikt wettelijk kader ......................................................................................... 31
2. Aanbevelingen ........................................................................................................ 33
Afdeling 2. Wetgevend kader .......................................................................................... 35
1. Wijzigingen aangebracht door de wet van 28 november 2000 inzake informaticacriminaliteit ................................................................. 35
   1.1. Wijzigingen aangebracht aan het materieel strafrecht ........................................... 36
   1.2. Wijzigingen aangebracht aan het procedureel strafrecht ...................................... 37
       1.2.1. Het databeslag ................................................................................................. 37
       1.2.2. Het opsporen en lokaliseren van telecommunicatie ......................................... 38
       1.2.3. De netwerkzoeking ......................................................................................... 38
       1.2.4. De informatietap .............................................................................................. 39
       1.2.5. De medewerkingsplicht ................................................................................... 40
       1.2.6. De bewaringsplicht van oproep- en identificatiegegevens voor operatoren en dienstverstrekkers ....................................................... 41
   1.3. Wijzigingen van de wet van 28 november 2000 inzake informaticacriminaliteit ...... 42
2. Wijzigingen aangebracht door de wet van 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden .................... 42
   2.1. Bijzondere opsporingsmethoden ........................................................................... 44
       2.1.1. De observatie .................................................................................................. 44
       2.1.2. De infiltratie .................................................................................................. 44
       2.1.3. De informantenwerking .................................................................................... 44
       2.2. Andere onderzoeksmethoden ............................................................................. 45
       2.3. Algemene principes bij de toepassing van de bijzondere opsporingsmethoden ...... 45
       2.3.1. Het subsidiariteitsbeginsel ............................................................................ 45
       2.3.2. Het proportionaliteitsbeginsel ........................................................................ 46
       2.3.3. Het provocatieverbod ..................................................................................... 46
       2.3.4. Het verbod om misdrijven te plegen .............................................................. 46
   2.4. Wijzigingen van de BOM-wet door wet van 27 december 2005 ......................... 46
3. Wijzigingen aangebracht door de Potpourri II-wet .................................................... 48
4. Wijzigingen aangebracht door de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie ..................................................................................... 48
5. Wijzigingen aangebracht door de wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van Strafvordering en het Strafwetboek ............... 50
   5.1. De openlijke zoekings in informaticasystemen ....................................................... 50
   5.2. De heimelijke zoekings in informaticasystemen ..................................................... 51
   5.3. De snelle bewaring van gegevens ....................................................................... 52
   5.4. De online infiltratie .............................................................................................. 53
Hoofdstuk 2. De online infiltratie .................................................................................. 54
Afdeling 1. Probleemstelling voor de invoering van de online infiltratie ............... 54
1. Wettelijke hindernissen ............................................................................................. 54
2. Waarde bewijsmateriaal verkregen door middel van een illegale infiltratie ....... 56
Afdeling 2. De online infiltratie van artikel 46sexies van het Wetboek van Strafvordering .................................................................57
1. Toepassingsvoorwaarden .................................................................58
   1.1. Het subsidiariteitsbeginsel ..........................................................58
   1.2. Het materieel toepassingsgebied ...............................................58
   1.3. Voorbeelden ...............................................................................60
2. De machting tot infiltratie .................................................................60
   2.1. Vormvoorwaarden ....................................................................60
   2.2. Persoonlijke interacties die de verificatie van misdrijven of de arrestatie van verdachten tot doel hebben en internetpatrouilles ..................................................61
3. Bevoegde infiltranten .....................................................................62
4. Het plegen van misdrijven door de infiltranten ..................................64
   4.1. De strafuitsluitende verschoningsgrond .....................................64
   4.2. De voorafgaandelijke toestemming ............................................65
   4.3. Kritiek .......................................................................................66
5. Het proces-verbaal en de opnames van de contacten .............................68

Hoofdstuk 3. De klassieke offline infiltratie .............................................69
1. Toepassingsvoorwaarden .................................................................69
   1.1. Het proportionaliteitsbeginsel ....................................................70
   1.2. Het subsidiariteitsbeginsel .........................................................70
2. De machtiging tot infiltratie ...............................................................71
   2.1. Vormvoorwaarden ....................................................................71
   2.2. Latere wijziging, aanvulling of verlenging van de machtiging ..........72
   2.3. Politieke onderzoekstechnieken ...............................................72
3. Bevoegde infiltranten .....................................................................73
   3.1. Politieke infiltratie ....................................................................73
   3.2. Burgerinfiltratie .......................................................................74
4. Bescherming van de infiltranten .......................................................75
5. Het plegen van misdrijven door de infiltranten ....................................77
   5.1. De strafuitsluitende verschoningsgrond .....................................77
   5.2. De voorafgaandelijke toestemming ............................................78
6. Het proces-verbaal en het vertrouwelijk dossier ....................................79

Hoofdstuk 4. Vergelijking tussen de online en de offline infiltratie ...............81
Afdeling 1. Gemeenschappelijke kenmerken ..........................................81
   1. Heimelijk karakter van de operatie ................................................81
   2. Deelname van de politie aan de strafbare feiten .........................81
Afdeling 2. Verschillen tussen de twee soorten infiltraties ..........................82
   1. Fysieke contacten .......................................................................82
   2. Opname van de communicaties ....................................................83
ALGEMENE INLEIDING

Met de huidige toename van de elektronische communicatiemiddelen, van het elektronisch handelen en meer in het algemeen van de informatisering van de maatschappij in al haar aspecten, merken we een exponentiële toename van de informaticacriminaliteit.\(^1\) Internet en de telecommunicatiemiddelen worden dus vandaag de dag steeds belangrijker zowel in onze dagelijkse leven, voor het plegen van georganiseerde criminaliteit, terroristische acties en in de strafrechtelijke opsporingspraktijken.\(^2\) Het internet en de informaticatechnologieën in het algemeen bieden inderdaad veel nieuwe mogelijkheden om strafbare feiten te plegen en het onderzoek naar deze misdrijven te bemoeilijken. Daarnaast biedt het ook belangrijke middelen aan de politiediensten om het onderzoek te voeren en bewijsmateriaal te verzamelen. Omdat tal van dagelijkse activiteiten en communicaties door middel van de ICT geschieden, vinden we op het internet belangrijke bronnen van informatie die nuttig kunnen zijn voor het onderzoek. Het gebruik van de middelen die de informatie- en communicatietechnologie (ICT) en internet biedt is dus zeer belangrijk in de hedendaagse samenleving voor de rechtshandhaving. Er dient tevens rekening gehouden te worden met het feit dat de kenmerken van de informaticacriminaliteit grondig verschillen van de strafbare feiten die gepleegd worden in de fysieke wereld. Het is dus belangrijk dat de overheid, de opsporingsdiensten en de politiediensten in het bijzonder, de middelen die ze aanwenden om misdrijven te onderzoeken en op te sporen, aanpassen aan de technologische realiteit, gezien de algemene informatisering die de maatschappij aan het ondergaan is en die trouwens enkel zal toenemen in de toekomst. Het lijkt dan opportuun om zich te buigen over de vraag of we in België over een wettelijk kader beschikken dat de nodige en aangepaste middelen kan bieden voor de bestrijding van de informaticacriminaliteit en van de misdrijven die kunnen toenemen door middel van de ICT.

Met als titel “**Offline vs. Online infiltratie: evaluatie van de bijzondere onderzoeksmethode van infiltratie in de informaticacriminaliteit in België**” gaan we ons in deze masterproef in het bijzonder afvragen of de wetgever een optimale wettelijke regeling van de nieuwe onderzoeksmethode of opsporingsmethode van online infiltratie, die zich voordoet als een aangepaste versie van de bijzondere opsporingsmethode van de klassieke


offline infiltratie voor het onderzoek op het internet, in het Wetboek van Strafvordering heeft ingevoerd? Biedt de regeling van deze nieuwe onderzoeksmethode een werkelijke up-to-date versie van de offline infiltratie, die effectieve resultaten kan meebrengen voor de bestrijding van de informaticacriminaliteit?

Om deze vragen te kunnen beantwoorden moeten we eerst een algemeen kader schetsen om de informaticacriminaliteit en de cyberwereld goed te begrijpen. In het eerste deel van dit werk gaan we daarvoor de informaticacriminaliteit en zijn kenmerken omschrijven. Deze omschrijving en nadere verklaring van de uitdagingen die de cyberwereld vormt, gaat ons in staat stellen om te beseffen dat de bijzondere opsporingsmethoden en onderzoeksmethoden, en in het bijzonder de offline infiltratie, aangepast moeten worden aan de aan de complexiteit van de cyberwereld om effectieve resultaten te kunnen behalen in de strijd tegen de informaticacriminaliteit en andere misdrijven die een link kunnen hebben met de ICT. Het belang dat de ICT vertoont voor het onderzoek zal in dit deel ook worden besproken en de eisen van de Kadernota Integrale Veiligheid 2016-2019 voor de bestrijding van het fenomeen van het internet als faciliterend instrument voor het plegen van misdrijven.

In deel II gaan we op basis van het algemene kader van deel I trachten te beoordelen of de recente wetswijzigingen en in het bijzonder de invoering van de online infiltratie in het Wetboek van Strafvordering, die aangebracht werden in 2016, voldoende tegemoet komen aan de nood aan efficiënte middelen die voldoende aangepast zijn aan de technologische evolutie. Daartoe gaat een overzicht van de belangrijkste wetswijzigingen die plaats hebben gevonden op het vlak van de informaticacriminaliteit en de opsporing ervan, ons toelaten om de leemtes te duiden die in het wettelijke kader bestonden om de informaticacriminaliteit effectief te bestrijden. Dit onderwerp is dus zeer actueel en interessant, omdat we hier gaan proberen te beoordelen of de nieuwe opsporingsmethode van de online infiltratie, ingevoerd via artikel 46sexies van het Wetboek van Strafvordering (Sv.) door de wet van 25 december 2016, een nuttige bijdrage kan leveren aan de bestrijding van de criminaliteit. In een tijdsperiode van amper meer dan één jaar kunnen we niettemin niet verwachten dat deze infiltratie al veel toegepast zal zijn, zeker gezien de strenge toepassingsvoorwaarden die eraan


verbonden zijn, maar we zullen de online en de offline infiltratie met elkaar vergelijken om te bekijken of de wetgever de eigenschappen en de kenmerken van de cyberwereld voldoende voor ogen heeft gehouden bij de invoering van de nieuwe opsporingsmethode. We gaan ons dus afvragen of de wettelijke regeling van de online infiltratie voldoende aangepast is aan de werkelijkheid van de cyberwereld en of deze maatregel op de meest optimale manier is geregeld om de informaticacriminaliteit effectief te kunnen bestrijden. Hiervoor moeten wij ook de bezwaren en de eisen van de Kadernota Integrale Veiligheid voor ogen houden. Om de regeling van de online infiltratie door de Belgische wetgever te kunnen beoordelen, gaan we deze ook vergelijken op bepaalde aspecten met de Franse en de Nederlandse regeling van de cyberinfiltratie.

Tot slot gaan we in deel III bepaalde gevaren die verbonden kunnen zijn aan de uitvoering van indringende onderzoeksmethoden zoals de online infiltratie, nader bekijken. Omdat de online infiltratie slechts in de cyberwereld plaatsvindt en op meerdere vlakken als minder indringend en risicovol dan de offline infiltratie kan worden beschouwd, moeten wij ons afvragen of de regeling over dezelfde rechtswaarborgen als de offline infiltratie moet beschikken? De bepaling van de grenzen die tijdens de uitvoering van de cyberinfiltratie door de politiediensten, om de fundamentele rechten van de burgers, en in het bijzonder het recht op eerbiediging van het privéleven, niet op een ongeoorloofde manier te schenden en de grenzen van de handelingsvrijheid van de infiltranten te bepalen, die ervoor zorgen dat ze zich niet schuldig maken aan het uitlokkingsverbod, is een zeer moeilijke en complexe vraag. De effectiviteit van de toepassing van de operatie voor het welslagen van het onderzoek, en dus de veiligheid, staat hier tegenover de bescherming van de fundamentele rechten en vrijheid van de burgers. Het zijn dus twee legitieme belangen die men voortdurend moet afwegen bij de uitvoering van de online infiltratie. We gaan dan in dit deel eerst beoordelen in welke mate de online infiltratie een inmenging in het recht op privéleven kan teweegbrengen en of artikel 46 *sexies* Sv. voldoende waarborgen voor de fundamentele rechten kan bieden, zonder dat de effectiviteit die de operatie voor het onderzoek kan hebben, daarmee op ongewenste wijze vermindert. Daarnaast, zoals we zullen zien zijn beperkingen onder bepaalde voorwaarden van bepaalde fundamentele rechten toelaatbaar. Er dient dus tevens te worden gekeken, *in concreto*, of de toepassing van de cyberinfiltratie, wanneer ze een aantasting van de fundamentele rechten kan teweegbrengen, wel gerechtvaardigd kan zijn.
Voordat we de verschillende opsporingsmethoden en onderzoeksmethoden die de politiediensten kunnen aanwenden om de informaticacriminaliteit te bestrijden, kort gaan bekijken, en in het bijzonder de online en de offline infiltratie, is het essentieel om een algemeen kader van de informaticacriminaliteit te schetsen. In dit deel gaan we dus nader bekijken wat de informaticacriminaliteit precies is en de huidige plaats van informatica en informaticamisdrijven in onze samenleving om daarna het belang van de ICT voor het onderzoek aan te tonen, en de maatregelen die dienen genomen te worden volgens de Kadernota Integrale Veiligheid 2016-2019.

Hooftstuk 1. Informaticacriminaliteit

Afdeling 1. Context

1. De plaats van het internet in onze maatschappij

Het internet is vandaag de dag één van de meest snelgroeiende gebieden van de technische infrastructuuronwikkelingen geworden. Dit betekent dat de digitalisering van de maatschappij aan het toenemen is en dat deze geleidelijk alomtegenwoordig is in onze dagelijkse leven. Inderdaad, er wordt niet meer enkel beroep gedaan op het internet en de cyberwereld voor media en communicatie. We merken vandaag dat de meeste sectoren van de maatschappij, zoals de werkgelegenheid, het onderwijs, de overheidsdiensten, het recht, de openbare orde en de gezondheidszorg, en zelfs essentiële infrastructuren en voorzieningen zoals het bankwezen, water en elektriciteit zich steeds meer beroepen op de ICT om hun dagelijkse werkwijze te vergemakkelijken en er soms zelfs volledig afhankelijk van zijn geworden.\(^5\) Men wordt dus meer en meer geconfronteerd met producten die vroeger zonder internet- of computerconnectiviteit werkten, zoals wagens, en woningen, nu worden geïntegreerd met computertechnologie.\(^6\) De technologische ontwikkelingen en uitvindingen zoals mobile banking, online shopping en mobiele data, waardoor we bijna altijd en overal verbonden kunnen blijven met de digitale wereld, zorgen voor de verbetering van onze dagelijkse leven, zodat het steeds moeilijker wordt vandaag om zonder het internet te kunnen

---


Het internet heeft dus een belangrijke plaats in ons leven ingenomen, zodat we zeer aandachtig moeten blijven over zijn toekomstige ontwikkeling in onze steeds meer onderling verbonden wereld. Met de opkomst en het belang van netwerkgebaseerde diensten zoals de mails, internetgebaseerde communicaties en telefoondiensten in onze moderne informatiemaatschappij kunnen wij zelfs stellen dat het internet de moeder van alle netwerken is geworden.8

We kunnen dus merken dat leven in onze maatschappij al sinds de laatste decennia onderhevig is geweest aan tal van belangrijke veranderingen, die ertoe hebben geleid dat men nu een onderscheid maakt in de praktijk en in de beleidsvoering tussen online en offline situaties. Dit onderscheid is van belang omdat er verschillende deskundigheden en benaderingen vereist zijn, naargelang men zich in de online of offline wereld bevindt. Niettemin merken wij ook dat het onderscheid soms moeilijk te maken is, omdat mensen tegelijkertijd in beide werelden kunnen handelen door het gebruik van smartphones bijvoorbeeld. Inderdaad, voor tal van dagelijkse handelingen doen we beroep op het internet, al dan niet bewust, door bijvoorbeeld tijdens een fysiek gesprek informatie online op te zoeken.9

2. Nieuwe gevaren verbonden aan de informatisering van de maatschappij

2.1. Opkomst van de informaticacriminaliteit

Naast de huidige toename van de elektronische communicatiemiddelen, het elektronisch handelen en meer in het algemeen de informatisering van de maatschappij in al haar aspecten, merken we, spijtig genoeg, een exponentiële toename van de informaticacriminaliteit.10 Het misbruik van informatietechnologieën is nochtans geen nieuw fenomeen, omdat we het reeds tegenkomen sinds de introductie van deze technologieën. Reeds in de jaren zestig, wanneer de transistor-gebaseerde computer op de markt werd geïntroduceerd, werd er een stijging waargenomen van het gebruik van informaticatechnologie. Misdrijven en aanvallen waren op dat moment wel eerder gericht op het fysiek schaden van computers en op hun opgeslagen gegevens. Het is pas in de jaren zeventig dat er nieuwe vormen van computercriminaliteit tot stand kwamen, namelijk de

8 B.J. KOOPS, “Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research”, p. 5.
computerfraude. De verschuiving van fysieke misdrijven naar misdrijven die slechts door manipulatie van elektronische gegevens of het illegaal gebruik van een computer plaatsvonden, bracht al sinds het begin tal van uitdagingen voor de onderzoeksdiesten met zich mee, zodat er al vroeg wetswijzigingen nodig en wenselijk waren. In de jaren tachtig, bracht de interconnectie van computers een andere type van dreiging met zich mee, namelijk dat door de opkomst van netwerken crimineelen zich niet meer dienden te bevinden op de misdaadplek. Sindsdien vallen ook softwareprogramma’s ten prooi aan piracy en aan misdrijven die verband houden met octrooien en intellectuele eigendomsrechten. Dit was dus het begin van de informaticacriminaliteit zoals we die nu kennen en die nog veel voorkomt. De informaticacriminaliteit nam daarna aanzienlijk toe in de jaren negentig met de opkomst van het wereldwijde web en de daarmee gepaard gaande beduidende toename van internetgebruikers. Men werd hier geconfronteerd met nieuwe uitdagingen zoals het feit dat informatie die in een bepaald land wettelijk op het internet werd gebracht, wereldwijd toegankelijk was, dus eventueel ook in landen waar de publicatie van dit soort informatie normaal gezien bestraft wordt. Sinds de eeuwisseling ontstonden er ook ingewikkelde nieuwe methoden om misdrijven te plegen die door de ordehandhavingsdiensten moeilijker te bestrijden zijn, zoals phishing, wat kan omschreven worden als een poging tot het frauduleus verwerven van gevoelige en geheime informatie, zoals paswoorden, door zich te verschuilen als een betrouwbaar persoon of bedrijf in een schijnbare officiële elektronische communicatie.11 In de toekomst van onze steeds hoe langer hoe meer verbonden maatschappij zal het ook steeds moeilijker worden om zich misdrijven voor te stellen die zonder het gebruik van ICT worden gepleegd.12 De nieuwe technologieën vergemakkelijken op een aanzienlijke manier de werkwijze van daders. Ze kunnen nu bijvoorbeeld via het internet contact onderhouden en communiceren met hun klanten in het geval van drugshandel of hun verslagen en de boekhouding van hun activiteiten op hun computers bijhouden.13

Door de alomtegenwoordigheid van de ICT is de samenleving onderhevig aan nieuwe dreigingen en gevaren, zoals gebreken in de informatica-infrastructuren en aanslagen daartegen, net als nieuwe types van misdrijven die vaak een up-to-date versie zijn van misdrijven die uitsluitend plaatsvonden in de fysieke wereld en waarvan de uitvoering

13 M. CHAWKI, A. DARWISH, M.A. KHAN en S. TYAGI, Cybercrime, Digital Forensics and Jurisdiction, p. 16.
vergemakkelijkt werd door de technologische evolutie van de ICT. In deze opzicht kunnen we bijvoorbeeld een ongeoorloofde toegang tot een computer vergelijken met een ongeoorloofde toegang tot een privaat eigendom, een kantoor of een auto.\textsuperscript{14} De cybercriminaliteit verspreidt zich nu met een grote verscheidenheid en diversiteit van vormen van criminaliteit, zoals drugs- en wapenhandel, diensten van huurmoordenaars, mensenhandel, mensensmokkel, fraude, seksuele exploitatie van kinderen of kinderpornografie.\textsuperscript{15}

2.2. 

\textit{Politie\'e\'en criminaliteitsstatistieken}

Volgens de politie\'e\'en criminaliteitsstatistieken van de jaren 2000 tot en met het eerste semester van 2017 merken wij dat de zuivere inbreuken op de informaticawet, die bestaan uit de valsheid in informatica, de hacking, de informaticabedrog en de sabotage, met 14,15\% in 2016 zijn gestegen ten opzichte van 2015. In 2015 werden er 18 044 informaticamisdrijven geregistreerd terwijl er 20 598 feiten in 2016 geregistreerd werden. Volgens dezelfde statistieken waren er al 9 840 informaticamisdrijven gemeld tijdens het eerste semester van 2017.\textsuperscript{16} Verder als we de cijfers en de statistieken van de verschillende informaticamisdrijven apart bekijken, merken we dat de valsheid in informatica in tegenstelling tot de andere zuivere inbreuken op de informaticawet die hierboven zijn vermeld, aan het dalen is sinds 2016.\textsuperscript{17} Daarnaast kan de stijging ook worden verklaard door het feit dat er nieuwe misdrijven, die verbonden zijn aan de ICT in het Strafwetboek zijn ingevoerd, zoals grooming van artikel 377quater Strafwetboek (Sw.) door de wet van 10 april 2014\textsuperscript{18}. Men moet ook voor ogen houden dat het slechts gaat over het aantal geregistreerde feiten en niet alle misdrijven in verband met informaticacriminaliteit, zodat de dark number van feiten die niet gekend zijn bij de politie hier niet meegeteld zijn. Bovendien, wanneer we met recente gegevens werken zijn deze nog onderhevig aan veranderingen door latere vermeldingen en aangifte door derden en slachtoffers. Betreffende informaticacriminaliteit is er ongetwijfeld een groot dark number. Slachtoffers verliezen soms meer door de misdrijven die ze hebben ondergaan te melden, dan dat ze verliezen door het misdrijf zelf. Dit is te verklaren door het feit dat er vaak cruciale

\textsuperscript{14} M. CHAWKI, A. DARWISH, M.A. KHAN en S. TYAGI, \textit{Cybercrime, Digital Forensics and Jurisdiction}, p. 16.
\textsuperscript{15} B.J. KOOPS, “Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research”, pp. 5-6.
\textsuperscript{18} Wet van 10 april 2014 betreffende de bescherming van minderjarigen tegen benadering met als oogmerk het plegen van strafbare feiten van seksuele aard, B.S. 30 april 2014.
belangen op het spel staan. Men denkt hier namelijk aan hun eer in sommige gevallen of de blootstelling van hun kwetsbaarheden en gebreken omtrent de veiligheid.\textsuperscript{19} Deze statistische gegevens zijn van uiterst belang omdat het de aandacht gaat vestigen op het voortdurend groeiende belang van de informaticacriminaliteit. Gebrek aan kennis omtrent het fenomeen en vooral gegevens die de verschillende informaticamisdrijven onderscheiden en verdelen is één van de grootste uitdagingen voor beleidsmakers, omdat het de kwantificering van de impact van de cybercriminaliteit om een effectief beleid op te stellen, bemoeilijkt.\textsuperscript{20}

2.3. Cyberterrorisme

Daarnaast worden het internet en de telecommunicatiemiddelen ook steeds meer en meer aangewend door terroristische groepen om terroristische activiteiten en georganiseerde criminaliteit te plannen en te plegen.\textsuperscript{21} Cyberterrorisme is dus een misdrijf die ontstaan is uit de convergentie van cybercriminaliteit en de traditionele vorm van terrorisme. Internet biedt inderdaad een relatief ongereguleerde en ongelimiteerde plaats waar terroristen hun propaganda kunnen verspreiden om radicalisering te promoten door een onbeperkt aantal van websites en sociaal media platformen. Dit gebeurt ook vaak door middel van de verborgen internetcommunicatiediensten. Een groot aantal nieuwe rekruten zijn dus door het internet makkelijk te bereiken om de terroristische organisaties te vergezellen. De Islamitische Staat in Irak en al-Sham (ISIS) heeft tot nu toe de meest technologisch geavanceerde propaganda gevoerd waarmee ze bewust jongvolwassenen als doelgroep wensen te bereiken, door verkeerde beelden van een utopisch en heldhaftige leven te verspreiden.\textsuperscript{22} Door sociale media en het internet kunnen terroristen nu informatie zonder limiet met een groot publiek delen. Controle op het gehele van berichten en informatie die op het internet en door de sociale media in het bijzonder zijn verspreid, is zo goed als onmogelijk, aangezien dat ze vaak onmiddellijk gepubliceerd worden. Bovendien worden publicaties op het internet niet gereguleerd als nieuwsbronnen, zodat onjuiste informatie gemakkelijk kan worden gepost zonder bijna enig toezicht of regulatie.\textsuperscript{23} Het internet heeft daarnaast ook de wijze waarop de terroristen hun daden plegen, veranderd. De ICT biedt namelijk de mogelijkheid aan de

\textsuperscript{19} M. CHAWKI, A. DARWISH, M.A. KHAN en S. TYAGI, Cybercrime, Digital Forensics and Jurisdiction, p. 10.


\textsuperscript{21} C. CONINGS en S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken”, NC 2017, afl. 4, p. 312.

\textsuperscript{22} A.V. LIEBERMAN, “Terrorism, the Internet, and Propaganda: A Deadly Combination”, Journal of National Security Law and Policy 2017, afl. 9, p. 95 (hierna: A.V. LIEBERMAN, “Terrorism, the Internet, and Propaganda: A Deadly Combination”).

\textsuperscript{23} A.V. LIEBERMAN, “Terrorism, the Internet, and Propaganda: A Deadly Combination”, p. 102.
terroristen om misdrijven op afstand voor te bereiden en te plegen. Zo kunnen ze hun aanslagen nu via beelden van Google Earth plannen en schade berokkenen in verre landen, waar ze hun acties via computers uitvoeren.²⁴

2.4. Toekomstige toename van de informaticacriminaliteit

Er valt dus te verwachten dat het aantal informaticamisdrijven in de toekomst zal stijgen, aangezien het internet de ruggengraat van tal van elementen en diensten van onze maatschappij is geworden.²⁵ Er bestaat inderdaad een hoge waarschijnlijkheid dat cybercriminaliteit en cyberterrorisme de voornaamste vorm van criminaliteit in de komende jaren zal worden, zodat men een andere aanpak dient aan te wenden om deze vorm van criminaliteit te bestrijden. Er moet dus een juiste middel gevonden worden tussen maatregelen die zich exclusief op de online wereld richten en maatregelen die zich exclusief op de offline wereld richten.²⁶

Eén van de grootste bedreigingen die de evolutie van de informatica voor de cybercriminaliteit kan meebrengen, is dat men misdrijven niet meer zou kunnen toeschrijven aan mensen, maar slechts aan zelfstandige computers. Tot nu toe is de menselijke tussenkomst nog altijd nodig om misdrijven te plegen via de computer, maar dit zou wel eens kunnen veranderen door de vooruitgang op het vlak van de artificiële intelligentie, zodat de menselijke tussenkomst steeds minder noodzakelijk wordt voor de cybercriminaliteit. Dit zou tot nieuwe problemen leiden aangaande de mogelijkheid om misdrijven aan bepaalde daders toe te schrijven.²⁷

2.5. Het dark web

Slechts een klein deel van alle websites die op aanwezig zijn op het internet, met name de geïndexeerde webpagina’s, zijn opzoekbaar via zoekmachines zoals Google. De meeste van de webpagina’s zijn dus slechts toegankelijk door het rechtstreeks ingeven van hun URL. Deze websites vormen het deep web samen met nog meer verborgen websites die slechts

²⁴ A.V. LIEBERMAN, “Terrorism, the Internet, and Propaganda: A Deadly Combination”, p. 101.
toegankelijk en zichtbaar zijn door het hanteren van speciale software of hardware. We gebruiken het begrip dark web of darknet om te verwijzen naar de inhoud van de websites die gehost zijn op een infrastructuur die een specifieke software vereisen om de content provider te bereiken. Het dark web is niet slechts voor illegale doeleinden gebruikt maar was oorspronkelijk ontwikkeld voor legitieme doeleinden, met name rechtmatige privacy aanbieden aan zijn gebruikers. Het is inderdaad vaak gehanteerd door politici en journalisten om hun communicaties geheim te houden. Nochtans heeft het snel een grote aantrekkingskracht gevormd voor het plegen van illegale handelingen, omwille van het feit dat de opspoorbaarheid van diens gebruikers vermoeilijkt is door de anonimiteit die deze netwerken bieden.

De bekendste en belangrijkste software om het dark web te bereiken is TOR die afgeleid is van The Onion Router. Het TOR-netwerk is ontstaan en voor het eerst voorgesteld in 2002 door de U.S. Naval Research Laboratory. Het heeft dus hetzelfde ontstaansgeschiedenis als het internet dat ook door het U.S.-leger werd ontwikkeld. Het was oorspronkelijk ontwikkeld om anonieme communicaties mogelijk te maken door de exploitatie van een netwerk van vrijwillige knooppunten die verantwoordelijk zijn voor de routing van gecodeerde en beveiligde verzoeken, zodat de communicaties verborgen en ontraceerbaar kunnen blijven voor bewakingsinstrumenten. Daartoe werkt TOR met een meer complex routingprogramma, omdat ook de adressen gecodeerd en beveiligd zijn in tegenstelling tot het reguliere internet, waar de adressen van de afzender en het doelwit van de communicatie wel bekend zijn. Zelfs als het darknet dezelfde communicatie-infrastructuren hanteert als het gewoon internet, vormt het een parallelle wereld.

Het dark web is dus een bevorderlijke plaats geworden voor het plegen van allerlei kwaadaardige, commerciële activiteiten, criminele transacties en uitwisselingen. In het TOR-netwerk, dat het netwerk is met de grootste aantrekkingskracht voor het plegen van illegale transacties in de illegale underground markt, bevinden zich marktplaatsen die als e-commerce functioneren, zoals Silk Road dat sinds oktober 2013 niet meer actief is, en een hoop kleinere

---

31 M. WASCHKE, Personal Cybersecurity, pp. 117-118.
websites die individuele diensten aanbieden. De uitschakeling van een website houdt natuurlijk niet tegen dat het ergens anders op het internet zal opduiken, maar de ordehandhavingsdiensten kunnen er wel voor zorgen dat voldoende consumenten en operatoren geneutraliseerd worden, zodat de website zich nooit volledig zou kunnen herstellen. Illegale drugshandel, wapenhandel, witwassen, mensenhandel en meer specifiek sekshandel en het uitwisselen van technische informatie voor het hacken, worden door犯罪elijke darknet websites aangeboden. De toegang tot deze illegale en犯罪elijke darknet websites wordt echter vaak gecontroleerd en vereist ook vaak een goedkeuring van andere leden om de aanwezigheid van ordehandhavingsdiensten te vermijden. De transacties die op het dark web plaatsvinden worden gerealiseerd door middel van cryptogeld zoals Bitcoin, Perfect Money en Litecoin. Het is dus perfect mogelijk voor terroristische en犯罪ele organisaties om via het anoniem betalingssysteem, dat vaak gehanteerd wordt op het dark web, ontraceerbare transacties uit te voeren.

**Afdeling 2. Begripsomschrijving**

Om de informaticacriminaliteit op een juiste manier te kunnen omschrijven, is het eerst van belang om de relatie tussen cybercriminaliteit en computer gerelateerde misdrijven te grijpen. Computergerelateerde misdrijven zijn een breder begrip dan cybercriminaliteit, omdat het geen computernetwerk behoeft in tegenstelling tot deze laatste. Dit betekent dat misdrijven die slechts een op zichzelf staande computer betreffen en niet door een netwerk zijn gedragen, ook tot de categorie van computergerelateerde misdrijven behoren. In een poging om een gemeenschappelijke en brede definitie van de cybercriminaliteit of kortweg cybercrime te geven, zouden we het kunnen omschrijven als om het even welke activiteit waarin computers of computernetwerken als een hulpmiddel, een doel of een plaats van犯罪ele activiteiten fungeren. Nochtans is er geen consensus over een definitie van het misdrijf, omdat er verschillende invullingen aan het begrip kunnen worden gegeven. Deze definitie kan als te breed worden beschouwd door sommigen, omdat het ook traditionele misdrijven omvat die slechts worden begaan met computers als materiële goederen. Deze definitie kan dus ook een op zichzelf staande computer betreffen en dus geen

---

33 M. WASCHKE, *Personal Cybersecurity*, p. 120.
computernetwerk vereisen, zodat er hier geen onderscheid wordt gemaakt tussen de cybercriminaliteit en computergerelateerde misdrijven. We kunnen hier denken aan het misdrijf van slagen en verwondingen, wanneer de dader het slachtoffer slaagt met behulp van een toetsenbord bijvoorbeeld of wanneer hij een computer gooit naar het slachtoffer die daardoor gewond geraakt. Daarom is het misschien beter om een nauwere definitie te geven van cybercriminaliteit die een reeks van misdrijven omvat, zoals netwerkmisdrif en traditionele computermisdrif met uitsluiting van traditionele misdrif die slechts vergemakkelijkt werden door het gebruik van computer hardware. Dit blijft steeds een zeer brede omschrijving die een grote waaier van misdrijven dekt zoals we het in de volgende afdeling kunnen zien. In het algemeen als we het over cybercriminaliteit hebben, hebben we het meestal over de twee hoofdcategoriën van informaticamisdrijven: de traditionele misdrijven zoals fraude en diefstal die worden gepleegd door middel van een computer die verbonden is aan een netwerk of verwante informatietechnologieën en de misdrijven die computers verbonden aan een netwerk als doelwit hebben. We denken hier namelijk aan misdrijven tegen de integriteit en de confidentialiteit.

Om een adequate en nauwkeurige definitie te kunnen geven van de informaticacriminaliteit is het ook van belang om met een goede beeldvorming en met volledige en juiste statistische gegevens te kunnen werken. Zoals reeds gezien, worden misdrif vaak niet aangegeven, zodat de statistische gegevens niet volledig zijn en men dus geen integraal beeld krijgt van het fenomeen.

Afdeling 3. Types misdrijven

Omdat de informaticacriminaliteit of cybercriminaliteit een zeer brede waaier van soorten misdrif omvat, is het zeer moeilijk om een classificatiesysteem of typologie te vinden die alle misdrif dekt en die ze kan opdelen.

1. Opsplitsing van het Cybercrimeverdrag

Een opsplitsing die we kunnen hanteren, is die van het Cybercrimeverdrag van Boedapest van de Raad van Europa die de misdrif verdeelt in vier categorieën: delicten tegen de vertrouwelijkheid, integriteit en beschikbaarheid van computergegevens en...

---

38 M. CHAWKI, A. DARWISH, M.A. KHAN en S. TYAGI, Cybercrime, Digital Forensics and Jurisdiction, p. 5.
computersystemen, computergerelateerde delicten en fraude, inhoudgerelateerde delicten en delicten met betrekking tot inbreuken op auteursrecht en naburige rechten.\(^\text{40}\)

Sommige auteurs zoals Gercke merken op dat deze categorisering, alhoewel ze als een nuttige basis kan dienen, niet volledig consistent is, omdat ze niet gebaseerd is op één enkel criterium om de misdrijven in categorieën op te splitsen. Hij wijst namelijk op het feit dat, terwijl de drie eerste categorieën zich steunen op het onderwerp van de legale bescherming, de vierde categorie van delicten, die delicten met betrekking tot inbreuken op auteursrecht en naburige recht omvat, zich focust op de methode waarmee de misdrijven worden gepleegd. Bovendien, merkt hij ook op dat bepaalde misdrijven, zoals phishing, in meerdere categorieën kunnen terechtkomen.\(^\text{41}\)

2. Opsplitsing tussen specifieke en niet-specifieke informaticacriminaliteit

Andere auteurs zoals Meunier en Collard steunen zich daarentegen, op een onderscheid in de informaticacriminaliteit tussen de specifieke informaticacriminaliteit, ook intrinsieke informaticamisdrijven of informatica als crimineel doel genoemd, en de niet-specifieke informaticacriminaliteit, ook instrumentele informaticamisdrijven of informatica als crimineel middel genoemd.\(^\text{42}\) Dit conceptueel onderscheid werd ook al gedaan in de memorie van toelichting van de wet inzake informaticacriminaliteit van 28 november 2000\(^\text{43}\).\(^\text{44}\) Aan deze tweedelige indeling kunnen we nog twee andere categorieën toevoegen om een meer volledige classificatie te bekomen van de misdrijven die gepleegd worden met al dan niet een nauwe band met informaticatechnologieën, namelijk de misdrijven die gepleegd worden door misdadigers die de informatica toevallig gebruiken en de accidentele cybercriminel.

2.1. Specifieke informaticacriminaliteit

Dit betreft de gedragingen van misdadigers gericht tegen een informaticasysteem of de gegevens dat het omvat, om de vertrouwelijkheid, de integriteit of de beschikbaarheid ervan te schenden. Het gaat hier dus over informatica-inbreuken als zodanig omdat de informatica hier


\(^{44}\) Memorie van Toelichting, Wetsontwerp inzake informaticacriminaliteit, Parl.St., Kamer, 1999-2000, nr. 50-0213/001, 50-0214/001, p. 5.
als het doelwit van het misdrijf wordt beschouwd.\textsuperscript{45} In deze categorie kunnen wij bijgevolg de misdrijven als hacking, heling van gehackte gegevens en informaticasabotage samenbrengen.\textsuperscript{46} Deze misdrijven vormen een nieuwe versie die geen up-to-date versie van “oude” klassieke misdrijven uitmaakt, maar er zich gewoon van onderscheidt door het hanteren van een nieuwe \textit{modus operandi}. Deze misdrijven hebben zich dus parallel ontwikkeld en zijn uitgegroeid tot de bestaande misdrijven met de opkomst van het internet en het netwerk.\textsuperscript{47}

2.2. Niet-specifieke \textit{informaticacriminaliteit}

Hier wordt de informatica gebruikt als een middel, een instrument, een \textit{modus operandi} om andere traditionele misdrijven te plegen zodat er geen impact is op de bestanddelen van het bestaande misdrijf.\textsuperscript{48} We kunnen deze categorie dus beschrijven als “\textit{old crimes, new tools}”\textsuperscript{49}. Deze misdrijven worden dus gepleegd door middel van de ICT, die het plegen van het misdrijf gaan vergemakkelijken, maar deze kunnen ook net zo goed op een andere, meer traditionele manier, worden gepleegd. Het gaat hier dus niet over nieuwe misdrijven die volledig zijn ontstaan door de ontwikkeling van de informatietechnologieën, maar over de integratie van de cyberruimte in de sfeer van meer traditionele misdrijven die al bestonden voor de opkomst van de nieuwe technologieën.\textsuperscript{50} We denken hier onder meer aan de valsheid in informatica, de manipulatie van data, het gebruik van valse informaticagegevens, bezit en verspreiding van kinderporno, belaging, verspreiding van racistische uitingen op het internet, het houden van een valse boekhouding, oplichting via het internet, intimidatie via mails, witwassen door middel van beleggingen in elektronisch geld, etc.\textsuperscript{51}

De toepasbaarheid van de bestaande strafbepalingen blijft hier ongewijzigd, maar problemen kunnen zich stellen omtrent de opsporing van deze misdrijven en de identificatie van de daders omdat deze andere middelen hebben gehanteerd om de misdrijven te plegen.52

2.3. Misdadigers die de informatica toevallig gebruiken

Om deze indeling aan te vullen, kunnen we nog de categorie van misdadigers toevoegen die het internet toevallig gebruiken voor het plegen van een misdrijf. Het internet en al de faciliteiten die het aanbiedt, worden hier niet gehanteerd als middel om als dusdanig in actie te komen en illegale activiteiten te plegen, maar kunnen de daders helpen om hun misdrijven voor te bereiden. We denken hier aan het gebruik maken van het internet om te communiceren met misdaadpartners in het kader van de voorbereiding van hun misdrijf, het bijhouden en doorsturen van boekhouding van illegale activiteiten op zijn computer, zoals drugshandel of gokspelen, of het zoeken van eventuele slachtoffers door sociale media. Op zich zijn al deze handelingen niet strafbaar maar bevatten belangrijke bewijzen van de misdrijven die ze voorbereiden of organiseren. Voor de uiteindelijke uitvoering van het misdrijf zal hier geen verder gebruik van de informatica worden gemaakt. In dit geval speelt het netwerk een belangrijke rol in de opsporing- en vervolgingsfase omdat het belangrijke bewijs elementen bevat, die de onderzoeksdiensten zullen helpen om de misdadigers op te sporen.53

2.4. Accidentele cybercriminelen

Als laatste kunnen we nog een aparte categorie toevoegen voor mensen die in de fysieke wereld niet als misdadigers worden beschouwd, maar die zich wel schuldig maken aan misdrijven in de cyberwereld. Deze behoren niet helemaal tot de andere categorieën, omdat ze zich onderscheiden door het feit dat ze de feiten stellen en dus de misdrijven plegen, zonder enig opzet. Misdrijven worden hier gepleegd door gebrek aan vertrouwdheid met de technologie of onwetendheid van de wetten. We denken hier aan toegang krijgen zonder toestemming tot andermans computer, die niet goed beveiligd was en het bekijken van documenten en gegevens die daarop staan, zonder dat men er zich ervan bewust is.54

53 M. CHAWKI, A. DARWISH, M.A. KHAN en S. TYAGI, Cybercrime, Digital Forensics and Jurisdiction, pp. 18-19.
Afdeling 4. Kenmerken informaticacriminaliteit

1. Anonimiteit

Eén van de meest attractieve factoren van het internet en de online wereld voor het plegen van misdrijven is dat het in de cyberwereld veel eenvoudiger is om de identiteit te verbergen. Anonieme netwerken zoals TOR, die gecodificeerde communicatie hanteert, brengen veel complicaties en extra werk mee voor de opsporingsdiensten. Men laat hier veel minder voetafdrukken achter bij het plegen van misdrijven, zodat het een zware taak wordt voor de onderzoekers en de rechtshandhaving om de misdadigers te ontmaskeren. Het opsporen van misdrijven die online plaatsvinden kan dus zeker een moeilijke taak worden, wanneer de daders ervoor hebben gezorgd dat hun communicaties geëncrypteerd zijn of elementen ervan verspreid zijn over verschillende landen door omleiding via verscheidene computers.\(^5\)

Men kan een onderscheid maken tussen werkelijke anonimiteit en pseudo-anonimiteit wanneer men het over het internet heeft. Bij werkelijke anonimiteit is het onmogelijk om de identiteit van de individuen die zich achter bepaalde handelingen verstoppen, te ontdekken. Het is bijna onmogelijk vandaag de dag om de identiteit van professionele cybercriminelen te achterhalen, behalve wanneer zij fouten begaan of wanneer zij over hun prestaties opscheppen.\(^6\) Professionele cybercriminelen kunnen zelfs de sporen vervalsen en ervoor zorgen dat onwillige mededaders worden ontmaskerd en schuldig worden verklaard voor de misdrijven, terwijl de eigenlijke daders, die de leiding van de operaties hebben, onbekend blijven.\(^7\) Pseudo-anonieme communicatie is, in tegenstelling tot de eerste soort anonimiteit wel opspoorbaar, zelfs als het ontmaskeren van de identiteit van de individuen zeer bemoeilijkt wordt door allerlei mechanismen.\(^8\)

Zelfs buiten het darknet is het gebruiken van pseudoniemen, fictieve identiteiten en valse gegevens gebruikelijk op het internet. Dit is op zich niet strafbaar, omdat het bijdraagt tot de vrijheid van meningsuiting en het recht op de persoonlijke levenssfeer. Persoonlijke

---

informatie wordt bovendien niet altijd gecontroleerd bij het opmaken van een profiel op een website of een e-mailadres, zodat het gemakkelijk is om zich te schuilen achter een valse identiteit in de cyberwereld. Communicatie gebeurt vaak ook vlotter op het internet en dit is te wijten aan het feit dat mensen zich achter hun scherm kunnen verbergen en dus minder snel persoonlijke informatie moeten prijsgeven. Deze neiging om terughoudend te zijn ten aanzien van de bekendmaking van de eigen identiteit op het internet, verklaart zich door het feit dat er meer en meer gegevens en persoonlijke elementen zoals sociale zekerheidsnummers, adressen, e-mailadressen en foto’s bijvoorbeeld worden verzameld en eenvoudig vindbaar zijn op het internet. Veel persoonlijke gegevens worden tevens ook verkocht door sociale media aan bedrijven, zodat men dus vaak de neiging heeft om toch niet alles openbaar te maken om de eigen identiteit toch zo veel mogelijk te beschermen.59 Hier hebben we dus te maken met pseudo-anonimiteit. Als keerzijde van de medaille merken wij ook dat het verbergen van de identiteit leidt tot een ontsporing van de zeden. Mensen durven meer schrijven en overschrijden de grenzen die ze zich stellen in het dagelijkse leven door zich minder verboden op te leggen, zodat ze zich losser en vrijer voelen om zich te uiten. Dit blijkt ook vaak op fora van politieke discussies.60 Dit kan natuurlijk leiden tot misbruiken en tot de vermeerdering van sociaal-afwijkende handelingen, antisociale gedragingen en illegale handelingen, zeker op de sociale media. We kunnen hier denken aan zedendelinquenten die via de sociale media hun toekomstige slachtoffers zoeken en met hen contact opnemen onder een valse identiteit of onder een pseudoniem handelen of situaties waarbij mensen de eer en de goede naam van iemand pogen aan te tasten.61

De anonimiteit op het internet blijft dus een gevoelig onderwerp, omdat het vooral fundamentele rechten beschermt en het meestal voor legitieme doeleinden wordt gebruikt. Men moet dus voorzichtig omgaan met onderzoeken van misdrijven die op het internet plaatsvinden. Een beleid dat te veel binnendringt in de persoonlijke levenssfeer van de burgers dient men blijvend te vermijden om de fundamentele rechten en waarborgen van de rechtsstaat te vrijwaren. Helaas maakt de strijd tegen de informaticacriminaliteit van vandaag het onmogelijk om nooit het recht op vrije meningsuiting en privacy te moeten in te perken voor het welslagen van het onderzoek. Voor de bescherming van het groter algemeen belang

59 M. CHAWKI, A. DARWISH, M.A. KHAN en S. TYAGI, Cybercrime, Digital Forensics and Jurisdiction, p. 98.
en de veiligheid dienen de opsporingsdiensten dus soms de individuele rechten in te perken en er tegelijkertijd voor te zorgen dat de pseudo-anonimiteit van de burgers zo veel mogelijk wordt geëerbiedigd.\textsuperscript{62}

2. **Globaliteit en grensoverschrijdende natuur**

Met de opkomst en de evolutie van de ICT is het vandaag de dag niet meer noodzakelijk dat misdadigers zich op de plaats van het misdrijf bevinden. Het is dus nu perfect mogelijk voor misdadigers om aanslagen en misdrijven te plegen tegen individuen, regeringen en bedrijven die zich overal in de wereld bevinden en illegale elementen in computers in een ander land dan waar ze zich bevinden, te bewaren en over te dragen in luttete seconden door de technologie van de "cloud computing".\textsuperscript{63} De informatietechnologieën doen de logistieke hindernissen, zoals het vervoer, die zich traditioneel stelden, verdwijnen. Links tussen de feiten en de misdadigers zijn dus moeilijker vast te stellen voor de opsporingsdiensten.\textsuperscript{64}

Daarnaast zijn de internetprotocollen (IP), die in de verschillende landen van de wereld worden gebruikt, door de standaardisering van het internet gelijkgeschakeld, zodat men overal in de wereld van dezelfde diensten die op het internet staan, kan genieten.\textsuperscript{65} Dit voegt dus een globale dimensie toe aan de misdrijven die zich op het internet kunnen afspelen. Door deze standaardisering kan men in een problematische situatie terechtkomen wanneer men zich toegang kan verschaffen tot informatie die als legaal wordt beschouwd in het oorspronkelijke land, maar die in andere landen als illegaal wordt beschouwd en dus strafbaar wordt gesteld, terwijl de informatie niet per se bestemd was voor dat land. De grensoverschrijdende natuur en de globaliteit van het internet brengt dan nieuwe vragen met zich mee voor de rechtshandhaving, omdat het nationaal strafrecht van de verschillende landen niet altijd overeenstemt. Er zijn wel mechanismen die het mogelijk maken voor de aanbieders van internettoegang om de toegankelijkheid tot bepaalde websites in bepaalde landen te beperken en aan de dienstverleners die websites beheren om de toegang tot bepaalde informatie te weigeren aan gebruikers die afkomstig zijn van bepaalde landen op basis van

\textsuperscript{62} M. CHAWKI, A. DARWISH, M.A. KHAN en S. TYAGI, Cybercrime, Digital Forensics and Jurisdiction, p. 98.


\textsuperscript{64} M. CHAWKI, A. DARWISH, M.A. KHAN en S. TYAGI, Cybercrime, Digital Forensics and Jurisdiction, p. 20.

\textsuperscript{65} M. GERCKE, “Understanding Cybercrime: phenomena, challenges and legal response”, p. 77.
hun IP-adressen. Dit lost het probleem echter niet volledig en definitief op, omdat het wel nog steeds mogelijk is voor mensen met bepaalde kennis en ervaring om dit te omzeilen.\textsuperscript{66}

De kenmerkende anonimitéit die aan het internet gelinkt wordt, kan de globaliteit van zulke misdrijven bovendien nog versterken, omdat men vaak niet weet van waar een bepaalde internetgebruiker afkomstig is. De cyberruimte biedt dus de mogelijkheid aan cybercriminelen om wijdverspreide misdrijven te plegen zodat grenzen geen hindernissen meer vormen in de cyberwereld.\textsuperscript{67} Internationale samenwerking is dan nodig om de cybercriminaliteit effectief te kunnen opsporen, zodat het een grote uitdaging vormt voor de rechtshandhavingsdiensten. De samenwerking dient ook op het nationaal vlak tussen de verschillende politiediensten, de publieke en private sector en de wetgevende macht plaats te vinden.\textsuperscript{68}

3. **Stijgende trend**

Volgens het eerste jaarverslag van het European Cybercrime Center (ECC) hadden in 2014 ongeveer 2,5 miljard mensen toegang tot het internet wereldwijd.\textsuperscript{69} Twee jaar later in 2016 waren er volgens de statistieken van de International Telecommunications Union (ITU) 3,385 miljard internetgebruikers in de wereld.\textsuperscript{70} De cijfers nemen dus snel toe, zeker in Zuidoost-Azië, Afrika en in Zuid-Amerika. Omdat de groei hoofdzakelijk plaatsvindt in landen waar de gerechtelijke samenwerking niet zeer uitgewerkt is, leidt het tot een grote uitdaging voor de rechtshandhaving van de Europese Unie om het hoofd te bieden aan de misdadigers en de bedreigingen die afkomstig zijn van die landen.\textsuperscript{71} Cybercriminaliteit kent inderdaad een parallelle exponentiële groei met die van het aantal internetgebruikers zodat het probleem steeds meer aanwezig zal zijn. In België hebben we tussen 2010 en 2015 een stijging van 342\% van de misdrijven die gepleegd zijn via of middels het internet waargenomen.\textsuperscript{72} Dit kan eenvoudig verklaard worden door het feit dat in 2016 in België 86,52\% van de burgers het internet gebruikten, terwijl in 2010 slechts 75\% van de Belgen

\textsuperscript{67} M. CHAWKI, A. DARWISH, M.A. KHAN en S. TYAGI, Cybercrime, Digital Forensics and Jurisdiction, p. 97.
\textsuperscript{68} M. CHAWKI, A. DARWISH, M.A. KHAN en S. TYAGI, Cybercrime, Digital Forensics and Jurisdiction, p. 20.
internet gebruikt.\textsuperscript{73} De cijfers nemen dus redelijk snel toe. Dit is wel ruimer dan de specifieke informaticacriminaliteit, maar het geeft wel goed de tendens van de toename van het gebruik van het internet weer voor het plegen van misdrijven. Omtrent de specifieke informaticacriminaliteit zoals we het \textit{supra} in de derde afdeling hebben beschreven en de misdrijven die daaromtrent in het Strafwetboek werden ingevoerd door de wet inzake informaticacriminaliteit van 28 november 2000, is er een stijging van 14,15\% van de informaticacriminaliteit waargenomen tussen 2015 en 2016 volgens de politiële criminaliteitsstatistieken.

4. Reikwijdte

Een ander belangrijk kenmerk van het internet als plaats om misdrijven te plegen is dat het een vaste en goedkope omgeving vormt om met kleine middelen misdrijven met een grote draagwijdte te kunnen plegen.\textsuperscript{74} De expertisedrempel om informaticamisdrijven te kunnen plegen wordt steeds lager, zodat het nu mogelijk is om zonder specifieke voorkennis misdrijven te plegen, zoals hacking\textsuperscript{75} aan de hand van programma’s of hackertools, terwijl dertig jaren geleden de hackers over een grote expertise in de materie dienden te beschikken.\textsuperscript{76} Niettemin merken we dat cybercriminelen nu vaker op een georganiseerde manier handelen, zodat we alleen kunnen verwachten dat de draagwijdte van de schade van de misdrijven gaat toenemen. De grote reikwijdte en grote omvang van de misdrijven verklaart zich ook door de standaardisering van de software, die het mogelijk maken om een groot aantal computers te bereiken zonder enige logistieke hindernissen. Daarnaast is er ook minder een persoonlijke band of enige link tussen de slachtoffers en de daders, zoals het meestal het geval is bij traditionele offline misdrijven. Dit maakt het ook moeilijker voor de opsporingsdiensten om misdadigers te ontmaskeren.\textsuperscript{77} De cybercriminaliteit heeft dus een grote aantrekkingskracht omdat de winsten van zulke misdrijven al dan niet omvangrijker zijn dan bij misdrijven zoals

\textsuperscript{73} Zie Excel-tabel “Percentage of Individuals using the Internet” beschikbaar op https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx, (geraadpleegd op 17 april 2018), en uittreksel betreffende België vindbaar in bijlage 3.
\textsuperscript{74} M. CHAWKI, A. DARWISH, M.A. KHAN en S. TYAGI, \textit{Cybercrime, Digital Forensics and Jurisdiction}, p. 102.
\textsuperscript{75} Overeenkomstig artikel 550\textit{bis} Sw. betreft dit misdrijf het wederrechtelijke toegang verkrijgen door een buitenstaander of een insider tot een informaticasysteem of een deel daarvan.
\textsuperscript{76} P. VANDENBRUWAENE, “Uitdagingen voor de rechtshandhaving in cyberspace”, \textit{R.W.} 2016-2017, afl. 20, p. 765.
drugshandel en dat het risico om gepakt te worden kleiner is dan bij misdrijven gepleegd in de fysieke wereld.\(^{78}\)

Zoals reeds gezien gebeuren ook meer en meer activiteiten en handelingen in het dagelijkse leven via het internet, zoals de online banking, zodat de cybercriminaliteit zich kan uitstrekken tot veel verschillende domeinen. Zeker in de bankwereld kan het een grote omvang aannemen en de cybercriminelen veel winst opleveren. Winst maken is overigens het grootste motief om cybermisdrijven te plegen (65%), met ruime afstand gevolgd door het hacktivisme (20%).\(^{79}\) De gevolgen van de informaticamisdrijven kunnen zich dus laten voelen op een even grote waaier van gebieden dan misdrijven die traditioneel in de offline wereld worden gepleegd.\(^{80}\)

\(^{78}\) B.J. KOOPS, “Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research”, pp. 5-6.


Hoofdstuk 2. Belang van IT-systemen voor het onderzoek

Afdeling 1. IT-systemen als hulpmiddelen van het onderzoek

Door de eigenschappen van de informaticacriminaliteit is het duidelijk dat de traditionele en klassieke opsporingsmethoden geen geschikte middelen meer kunnen bieden om dit type van criminaliteit te bestrijden. Het is bijvoorbeeld niet meer mogelijk om de traditionele beslagleggingen of huiszoekingen uit te voeren, aangezien we hier te maken hebben met immateriële gegevens en bewijsmiddelen. Het is bovendien niet evident om inmengingen in het dark web door politiediensten te verantwoorden, omdat het dark web oorspronkelijk voor niet-criminelle doeleinden werd ontwikkeld.

De inzet van informatietechnologie als opsporingsinstrument is, zoals we het kunnen opmerken, complex. Enerzijds wordt het opsporings- en vervolgingsproces van deze criminaliteit vereenvoudigd, anderzijds wordt het ook bemoeilijkt. Inderdaad, terwijl de technologieën de opsporing van misdadigers door de politiediensten bemoeilijken, kunnen deze ook dienen voor de opsporing, omdat ze nieuwe opportuniteiten en middelen om onderzoeken op te lossen en om de veiligheid te verhogen, meebrengen. Opsporingsdiensten kunnen dus voordeel halen uit de middelen die het internet biedt om onderzoeken uit te voeren. Zelfs als er snel dient te worden ingegrepen door de opsporingsdiensten om te vermijden dat bewijsstukken verdwijnen door tussenkomst van de misdadigers of per ongeluk door manipulaties van de opsporingsdiensten, kan de bewijsvoering met de gegevens die op het internet staan als betrouwbaar en neutraal worden beschouwd. De informatie die bevat ligt in informaticasystemen kunnen dienen om alibi’s te bevestigen ofwel te ontkrachten, maar kunnen ook door geïntegreerde GPS-systemen bijvoorbeeld dienen om verdachte en personen te lokaliseren. Dit is zeker van belang gezien het feit dat de bewijsvoering vrij is in het Belgisch strafrecht en de ruime visie die omtrent de bewijswaardering wordt gehanteerd door het Hof van Cassatie.

---

86 Zie daaromtrent de sectie over “de waarde van het bewijsmateriaal verkregen door middel van een illegale infiltratie” en de Antigoonrechtspraak van het Hof van Cassatie infra in deel II, hoofdstuk 2, afdeling 1.
Afdeling 2. De toegankelijke plaatsen op het internet voor de politiediensten

Een belangrijke vraag omtrent de bestrijding van de informaticacriminaliteit is die van de toegankelijkheid van de gegevens en de bewijsstukken die zich op het internet bevinden voor de opsporingsdiensten. Het Hof van Cassatie heeft in een arrest van 28 maart 2017 verklaard dat het internet een publieke toegankelijke plaats is, zodat het autonoom mag doorgezocht worden door politiediensten in het kader van de strijd tegen misdrijven zoals seksuele uitbuiting, verboden radicalisme en drugs- en wapenhandel. Het Hof baseert zich hier op artikel 8 van het Wetboek van Strafvordering, die vorm geeft aan de algemene opsporingsbevoegdheid van de gerechtelijke politie, en artikel 26 van de Wet op het Politieambt van 1992 (WPA), terwijl dit artikel oorspronkelijk niet werd bedoeld voor de online wereld, die verklaart dat “de politieambtenaren kunnen steeds de voor het publiek toegankelijke plaatsen alsook de verlaten onroerende goederen betreden teneinde toe te zien op de handhaving van de openbare orde en de naleving van de politiewetten en -verordeningen. Zij kunnen steeds diezelfde plaatsen betreden teneinde opdrachten van gerechtelijke politie uit te voeren. (...”)”. Het internet wordt dus hier als een plaats beschouwd volgens het Hof van Cassatie, terwijl het in de letterlijke zin van de wet niet zo gezien wordt. Sinds 2015 bestaat er een wettelijk initiatief om dit artikel uitdrukkelijk uit te breiden tot “plaatsen op het internet of op andere elektronische communicatienetwerken”. In dit opzicht kunnen we dus websites die zonder enige voorwaarde toegankelijk zijn in de cyberspace, vergelijken met openbare plaatsen in de reële wereld. Deze interpretatie door het Hof van een plaats is te verklaren door de noodzaak om aan de politiediensten op een gelijkaardige manier als aan het publiek toegang te verschaffen tot de cyberwereld om bewijzen te kunnen verzamelen voor het onderzoek via haar eigen computers, waarvan de IP-adressen openbaar zijn of al dan niet gemakkelijk opzoekbaar zijn op het internet. Het louter feit dat er vormelijke toegangsvoorwaarden zijn opgelegd, die geen persoonsgebonden controle vergen,

90 Dit artikel luidt als volgt: “De gerechtelijke politie spoort de misdaden, de wanbedrijven en de overtredingen op, verzamelt de bewijzen ervan en levert de daders over aan de rechtbanken belast met hun bestraffing”.
92 Advies nr. 13/2015 van de Commissie voor de Bescherming van de Persoonlijke levenssfeer betreffende de voorontwerpen van wet houdende diverse bepalingen – wijzigingen aan de wet tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, aan de wet op het politieambt en aan de wet van 18 maart 2014 betreffende het politieonse informatiebeheer, p. 6.
betekent niet dat de website niet toegankelijk is voor het publiek. Ook het feit dat de website betalend is, maakt het niet minder toegankelijk voor de politiediensten. Het is dus aanvaardbaar voor de politie om in bepaalde gevallen gebruik te maken van reguliere computers buiten het politienetwerk, wanneer ze geconfronteerd worden met bepaalde websites die voor iedereen, behalve voor computers met de IP-adres van de rechtshandhavingsdiensten, toegankelijk zijn.

Voor websites die de opgave van een e-mailadres en soms een daaraan gekoppeld paswoord vereisen, zonder dat er een controle over de identiteit van de internetgebruiker of de echtheid van het adres wordt uitgevoerd, mogen de politiediensten een alias gebruiken, voor zover deze niet van aard is om een misdrijf uit te lokken of een geloofwaardige fictieve identiteit. Het opgeven van een adres is hier enkel bedoeld als een soort van register, maar iedereen krijgt in feite toegang tot de website. Het aanwenden van een geloofwaardige fictieve identiteit is slechts mogelijk in het kader van de bijzondere opsporingsmethode van observatie of infiltratie zoals we het infra in het deel II zullen zien.

In zijn redenering stelt het Hof vast, dat het zelfs mogelijk is voor de politie, zonder zich daarvoor schuldig te maken aan het misdrijf van hacking, om op het darknet te gaan in het kader van een onderzoek. Dit is te verklaren door het feit dat het niet juridisch problematisch is voor de politie om websites of sociale media te bezoeken door gebruik te maken van op het internet vrij toegankelijke instrumenten om niet onmiddellijk traceerbaar te zijn, zoals TOR, die dikwijls vanuit het buitenland een extra IP-adres beschikbaar stellen en die dus vaak gericht zijn op de bescherming van het recht op vrije meningsuiting.

Dit arrest is niettemin niet zo innovend, omdat het slechts de situatie betreft waar de politiediensten niet hadden moeten binnendringen in privé-accounts of in het privé gedeelte van websites waar het paswoord en de gebruikersnaam van de beklaagde nodig waren. Het forum, waarvan sprake in het arrest, was open op de computer op het moment van de huiszoeeking. Verdere toelichtingen over de toegankelijkheid van de gegevens die zich op het internet bevinden, moeten dus nog het licht zien.

---

Samenvattend kunnen we dus vaststellen dat websites als publieke plaatsen kunnen worden beschouwd, zolang er geen toetredingsvoorwaarden worden opgesteld die belemmeren dat eenieder die toegang wenst te krijgen tot deze website, het kan verkrijgen. Toetredingsvoorwaarden zoals leeftijd, geslacht, registratie op naam of de betaling van een geldsom maken deze websites niet privaat. Dit betekent dus dat er niet zoveel aandacht wordt besteed aan het onderscheid tussen vormelijke en inhoudelijke of persoonsgebonden voorwaarden. Het is dus slechts wanneer een private kring van personen, die niet louter te maken heeft met het geslacht of de leeftijd, zich de toegang kan verschaffen, dat er geen sprake is van een publieke toegankelijke plaats.\(^{98}\)

De situatie is echter anders en ingewikkelder wanneer politiediensten gebruik moeten maken van een sleutel die hun ter beschikking werd gesteld door een anonieme bron, zoals bijvoorbeeld een melding op een website zoals www.ecops.be, of door een verdachte die onder een tapmaatregel staat of een slachtoffer, om toegang te krijgen tot een bepaalde website. De website kan hier worden beschreven als een cyberprivéclub, omdat het door de noodzaak van het gebruik van bepaalde sleutels, een beletsel vormt voor een hele groep mensen om zich toegang te verschaffen tot die bepaalde website. De politie kan zich hier schuldig maken aan het misdrijf van externe hacking van artikel 550bis Sw. door zich wetens en willens, zonder enige vereiste van bedrieglijke opzet, toegang te verschaffen tot een informaticasysteem waar ze niet toe gerechtigd is en aan het misdrijf van identiteitsfraude van artikel 231 Sw. door andermans identiteit aan te nemen.\(^{99}\)

Een andere problematische situatie ontstaat, wanneer de toegang tot een bepaalde website enkel wordt verstrekt door deelname aan het verspreidingssysteem van het netwerk, door de configuratie van het systeem zelf of dat men eerst illegaal materiaal moet uploaden voordat men zich toegang kan verschaffen. Hier moeten de politiediensten voorzichtig, met de goedkeuring van de betrokken parketmagistraat of onderzoeksrechter handelen en bij voorkeur met een schriftelijke opdracht. Dit zou enkel kunnen worden gerechtvaardigd, en dan nog, alleen voor zolang het nodig is, bijvoorbeeld om de nodige bewijsstukken te verzamelen en/of om de misdadigers te kunnen identificeren. Daarbij mogen ze enkel gebruik maken van onschadelijke en gebrekkige bestanden, die niet geopend kunnen worden of ze mogen enkel deelnemen aan het netwerk als extra computerkracht of als opslagstation zonder.

---


er actief bestanden uploaden. Als de politiediensten voorzichtig handelen en geen volledige illegale bestanddelen bijhouden, kan er dus geen sprake zijn van deelnemingsopzet omdat de politie hier aantoont dat ze niet de wil heeft om deel te nemen aan de verspreiding van illegale bestanden.100

**Afdeling 3. Rol van de sociale media’s**

Vanwege de diepgaande en groeiende integratie van computertechnologieën en van sociale netwerken in de handelingen en interacties van het dagelijks leven is het zo dat de steun en hulp die opsporingsdiensten kunnen vinden in de ICT voor hun onderzoeken zich niet beperken tot de opsporing van cybermisdrijven. Zoals we het *supra* in het eerste hoofdstuk hebben gezien zijn er misdadigers die de informatica slechts toevallig gebruiken om hun misdrijven voor te bereiden door bijvoorbeeld voorafgaande opzoeken te maken voordat ze hun misdrijven plegen. Ook bij het opmaken van vervalste documenten kunnen er sporen achtergelaten worden door metadata, die de identiteit van de vervalser kunnen aanwijzen. Zelfs als het hier geen cybermisdrijf betreft, is het van belang de opsporing uit te voeren op de computers van misdadigers en in de online wereld.101 Sociale media vormen in deze context een belangrijke en niet te onderschatten bron van informatie zelfs als de sociale netwerken niet de plaats zelf van het misdrijf uitmaken.102 Door de identificatie met tijdsaanduiding van deelnemers van een chatconversatie kunnen de politiediensten bijvoorbeeld een alibi bevestigen of gesprekpartners van verdachten identificeren om ze vervolgens eventueel te verhoren en daardoor eventueel bruikbare informatie te bekomen voor het strafrechtelijk onderzoek.103

Daarnaast kunnen de sociale media ook het onderzoek verstoren door de politiediensten op valse sporen te wijzen door de massa aan valse informatie die we op deze netwerken kunnen terugvinden. Het wordt ook steeds moeilijker voor de politiediensten om met zekerheid te kunnen bepalen wanneer bepaalde beelden gemanipuleerd werden zodat de reputatie van de politie soms op het spel kan staan.104

---

Een groot pluspunt van de aanwending van sociale media voor het onderzoek, is dat deze de verschillende oordelen, informatie en kennis van grote groepen mensen bijeenbrengen om zo veel mogelijk een waarheidsgetrouw beeld van de publieke opinie te verkrijgen. Het opvangen van signalen van de maatschappij, de slachtoffers, de burgers, de verdachte en van de politiediensten zelfs, gebeurt ook gemakkelijker via de aanwending van sociale netwerken dan bij lokale politiediensten, omdat het dichter bij de mensen ligt. Burgers zijn inderdaad geneigd om via de sociale netwerken een actievere rol aan te nemen in het voorkomen en oplossen van misdrijven en kunnen worden beschouwd als een verlengstuk van de politiediensten die alomtegenwoordig zijn.105

Afdeling 4. Nood aan bijzondere kennis en expertise

Terwijl de bewijsvoering in het kader van de opsporing van de informaticacriminaliteit aan dezelfde fundamentele beginselen is onderworpen als de opsporing van misdrijven die niets met informatica te maken hebben, namelijk dat de bewijsmiddelen betrouwbaar, authentiek en volledig moeten zijn en dat bewijzen slechts op een legale wijze mogen worden verkregen, vergt de bestrijding van de informaticacriminaliteit bijzondere kennis en een bijzondere aanpak. De opsporingsdiensten moeten dus de fundamentele beginselen die voor alle onderzoeken gelden, kunnen paren met de eigenaardigheden die de cyberwereld biedt. Gerechtelijke overheden en politiediensten dienen daarvoor over bijzondere middelen, een goede opleiding en expertise te beschikken om te kunnen omgaan met de nieuwe uitdagingen die verbonden zijn met de nieuwe technologieën zoals de wijze van exploiteren en verzamelen van de nieuwe soort van bewijzen en de beschikbaarheid ervan.106 Forensische laboratoria moeten een belangrijke rol spelen om te verzekeren dat er voldoende wetenschappelijke onderzoeken worden uitgevoerd en opleidingen worden verleend. Opsporingsdiensten dienen bovendien het onderzoek in een zeer korte tijdsduur uit te voeren volgens de wetenschappelijke betrouwbare beginselen en het wettelijk voorschrift. Dit is niet gemakkelijk aangezien dat de stand van de technologie voortdurend aan het evolueren is, zodat het noodzakelijk is om een permanente opleiding te kunnen verlenen aan de opsporingsdiensten en verschillende partijen die in het spel zijn tijdens een gerechtelijke

De bestrijding van de informaticacriminaliteit is dus een zeer actueel onderwerp dat nog onderhevig is aan toekomstige veranderingen. Zoals we het infra in het deel II zullen zien zijn er sinds 2016 al grote wijzigingen op het vlak van strafroutele wettelijke bepalingen die de bestrijding van de cybercriminaliteit moeten bespoedigen, zoals de tweede Potpourri-wet\textsuperscript{108} van 5 februari 2016, de dataretentiewet\textsuperscript{109} van 29 mei 2016 en de wet van 25 december 2016.\textsuperscript{110} Politiediensten moeten zich dus nog aanpassen aan alle wettelijke wijzigingen en leren omgaan met hun tijd.

Zoals we in het derde deel zullen zien, dient men eveneens zeer voorzichtig te zijn met de eerbiediging van de fundamentele rechten tijdens het onderzoek om een evenwicht te behouden in de driehoek van mensenrechten, wettelijkheid en veiligheid.\textsuperscript{111} Het is dus van cruciaal belang dat de politiediensten het milieu dat ze onderzoeken en in het bijzonder de cyberwereld goed kennen, om het onderzoek op de meest optimale manier te kunnen uitvoeren zonder belangrijke fundamentele grenzen te overschrijden. Zeker omdat de wettelijke bepalingen nog onderhevig zijn aan eventuele wijzigingen, is de optimale toepassing van de wettelijke opsporingsmethoden en instrumenten om de informaticacriminaliteit te bestrijden geen eenvoudige taak voor de politiediensten.

Afdeling 5. Kadernota Integrale Veiligheid 2016-2019

In de Kadernota Integrale Veiligheid van 2016-2019 wordt er in het transversale thema en uitdaging van “het gebruik van het internet als (faciliterend) instrument bij het plegen van misdrijven” benadrukt dat naast het feit dat het internet als een faciliterend instrument kan worden gebruikt en misbruikt om misdrijven te plegen, “de nieuwe technologische ontwikkelingen, al dan niet via het internet, en de informatie die via de nieuwe communicatiekanalen kan worden geraadpleegd, binnen de wettelijke normen ook ongekende mogelijkheden bieden op het stuk van opsporing en vervolging”.\textsuperscript{112} Opsporingsdiensten moeten dus genieten van de voordelen en opportuniteiten dat de ICT bieden in het kader van de criminaliteitsbestrijding en de handhaving van de veiligheid door bijvoorbeeld bepaalde

\textsuperscript{108} Wet van 5 februari 2016 tot wijziging van het strafrecht en de strafvordering en houdende diverse bepalingen inzake justitie, B.S. 19 februari 2016 (hierna: Potpourri II-wet).
\textsuperscript{109} Wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, B.S. 18 juli 2016 (Hierna: Dataretentiewet).
\textsuperscript{111} W. BRUGGEMAN, “Politie, justitie en (nieuwe) sociale media. De sporen gelegd, (te) weinig reizigers, de trein gemist, de trein ontspoord?”, Panopticon 2012, afl. 3, p. 204.
\textsuperscript{112} Kadernota Integrale Veiligheid 2016-2019, p. 21.
sociale media permanent te bewaken. Cybercrime en cybersecurity worden in de KIV ook beschouwd als één van de tien clusters en veiligheidsfenomenen.

Bij het transversale thema van het internet als faciliterend instrument voor het plegen van misdrijven wordt er benadrukt op de verschillende schakels van de strafrechtsketen. Men dient een integraal en geïntegreerd beleid te voeren en dus sinds de beeldvorming oog te hebben voor het fenomeen. In de Kadernota wordt er inderdaad verklaard, dat er geëngageerd moet worden voor het terugdringen van de illusie dat het internet een vrijplaats is voor het plegen van misdrijven en voor crimineel gedrag door een effectieve detectie en arrestatie van misdadigers en van georganiseerde misdaadgroepen. De opsporingsonderzoeken moeten dus effectiever zijn om het gevoel dat cybercriminelen ongestraft blijven te doen afnemen. Daarnaast moet er ook op het vlak van de preventie gewerkt worden. Er dienen namelijk bewustmakingsstrategieën ontwikkeld te worden om ervoor te zorgen dat zowel de burgers, als de bedrijven, verenigingen, de publieke instellingen en besturen op de hoogte zijn en bewust zijn van de risico’s die kunnen voortvloeien uit een onvoldoende veilig gebruik van het internet. Er moet vooral de nadruk worden gelegd bij kwetsbare groepen en jongeren op de sensibilisatie voor de gevaren van het internet. De overheid moet hier een voorbeeldfunctie aannemen door een veilig surfgedrag aan te leren. Wat ook belangrijk is, is dat de verschillende opsporingsdiensten een actievere rol en opsporingsfunctie aannemen in het kader van de misdaadbestrijding. Betreffende de repressie, wordt er in de KIV vastgesteld dat de online detectie van misdrijven door politiediensten beter moet gebeuren. Internetpatrouilles en de internetrecherche moeten hiervoor verder uitgebouwd worden door hun wettelijk kader verder uit te werken. De wetgeving betreffende de bijzondere opsporingsmethoden en in het bijzonder de maatregelen die verband houden met internet en telecommunicatie, moeten tevens volgens de KIV eventuele aanpassingen doorgaan. Het is inderdaad noodzakelijk dat het wettelijk kader aangepast wordt aan de stand van de technologie en de voortdurende evolutie ervan zonder dat het afbreuk maakt aan het evenwicht dat bestaat tussen de wettelijke regelingen van de opsporing en vervolging en de fundamentele rechten van verdediging en persoonlijke levenssfeer. Het kan dus zijn dat de bestaande wettelijke regeling geen aangepaste middelen heeft om het hoofd te bieden aan de toename van het gebruikmaken van het internet om misdrijven te plegen. Er wordt ook benadrukt dat er geen effectieve bestrijding kan zijn van de criminaliteit zonder een effectieve

---

uitbouw van de internetpatrouilles en de internetrecherche.\textsuperscript{116} Politiediensten en de magistratuur dienen ook gespecialiseerd te worden om het hoofd te kunnen bieden aan de verschillende vormen van informaticacriminaliteit. Opleiding, voortdurende investering in middelen en mensen en uitwisseling van expertise en kennis tussen de verschillende schakels van de veiligheidsketen zijn hiervoor noodzakelijk. Uitwisseling van kennis en expertise kan gebeuren door de oprichting van een permanente overlegstructuur samengesteld uit het openbaar ministerie, de private sector, de academische wereld en specialisten van de politie-, inlichtingen- en veiligheidsdiensten en gespecialiseerde inspectiediensten en door een efficiënte samenbundeling van de verscheidene middelen die soms op een ongecoördineerde wijze over de verschillende diensten verspreid zijn.\textsuperscript{117} Maatregelen dienen inderdaad genomen te worden om ervoor te zorgen dat politiediensten weten hoe ze in de cyberwereld moeten handelen om onderzoek effectief uit te voeren.\textsuperscript{118}

Naast de verschillende schakels van de strafrechtsketen benadrukt de KIV ook het belang van de sociale media en van de burgers en de bedrijven die permanent aanwezig zijn in de online wereld voor de bestrijding van het fenomeen. Zijn dienen een actievere rol te krijgen in de bestrijding van de informaticacriminaliteit door hen de gelegenheid te laten om via bekende en eenvoudige online meldingsmogelijkheden deel te nemen aan de detectie van misdrijven. Politiediensten moeten dus voordeel halen uit de mogelijkheden die de technologie biedt om burgers dichter te benaderen en om zelf aanspreekbaarder te zijn door melpunten op het internet ter beschikking te stellen.\textsuperscript{119} De geïntegreerde politie moet er ook voor zorgen dat er een effectieve bewijsvoering en sporenonderzoek kan plaatsvinden en dat alle betrokkenen in vormen van criminaliteit waarbij ICT wordt gebruikt, worden geïdentificeerd.\textsuperscript{120}

Verder in de Kadernota Integrale Veiligheid wordt ook de nood aan internationale samenwerking met buurlanden, de Europese Unie en non-EU-partners benadrukt, evenals het belang van nazorg voor de slachtoffers van informaticamisdrijven.\textsuperscript{121}

\textsuperscript{116} Kadernota Integrale Veiligheid 2016-2019, p. 22.
\textsuperscript{117} Kadernota Integrale Veiligheid 2016-2019, p. 23.
\textsuperscript{118} Dit sluit aan bij de vorige afdeling.
\textsuperscript{119} Kadernota Integrale Veiligheid 2016-2019, p. 22.
\textsuperscript{120} Kadernota Integrale Veiligheid 2016-2019, p. 86.
\textsuperscript{121} Kadernota Integrale Veiligheid 2016-2019, p. 22.
DEEL II. IMPACT VAN DE INVOERING VAN DE ONLINE INFILTRATIE DOOR DE WET VAN 25 DECEMBER 2016 OP DE BESTRIJDING VAN DE INFORMATICACRIMINALITEIT

In dit deel gaan we een inzicht geven in de belangrijkste wetswijzigingen die tot doel hebben om het Belgisch wettelijk kader van het onderzoek aan de technologische evolutie van de ICT aan te passen. In het bijzonder gaan we hier onze aandacht besteden aan de wijzigingen die aangebracht werden door de wet van 25 december 2016, waaronder de invoering van de online infiltratie. Daarnaast zullen we ook trachten te beoordelen of de online infiltratie kan bijdragen tot een efficiënte en daadwerkelijke aanpak van het internet als facilitator voor de criminaliteit. Daarvoor gaan we tevens de regeling in naburige landen van de online infiltratie vergelijken met de Belgische regeling daarmtrent.

Hoofdstuk 1. Legislatief kader en evolutie

Afdeling 1. Nood aan aanpassing van het legislatief kader aan de cyberwereld

1. Ongeschikt wettelijk kader

Aangezien dat de informaticacriminaliteit één van de snelste groeiende gebieden van de criminaliteit is, zullen we steeds meer en meer aandacht moeten besteden aan opsporingsmethoden en middelen die geschikt zijn voor de bestrijding ervan. In de Kadernota Integrale Veiligheid wordt er trouwens verklaard dat door de alomtegenwoordigheid van het internet een “omvattende mentaliteitswijziging betreffende orde- en rechtshandhaving” nodig is om de cybercriminaliteit effectief te kunnen bestrijden. De toename van de cybercriminaliteit en het cyberterrorisme vormt inderdaad een daadwerkelijke uitdaging voor het beleid, omdat deze zich voordoet in een complexe wereld die onderhevig is aan tal van veranderingen en technologische evoluties. Het internet heeft inderdaad veel grenzen opengesteld en beperkingen weggewerkt voor misdadigers, zodat de aanpak van dit fenomeen steeds complexer wordt. Daarnaast moeten wij voor ogen houden dat de cybercriminaliteit zowel gepleegd kan worden door individuele misdadigers als door internationale

---

123 M. CHAWKI, A. DARWISH, M.A. KHAN en S. TYAGI, Cybercrime, Digital Forensics and Jurisdiction, p. 22.
georganiseerde cybercriminelen die samenwerken en hun expertise samenbrengen om misdrijven te plegen en zo weinig mogelijk sporen achter te laten.¹²⁴

We kunnen hier een paar regelingen van de offline wereld aanwijzen die geen aangepaste middelen bieden om de informaticacriminaliteit in de brede zin te bestrijden of die gewoon niet rekening houden met de eigenaardigheden van de online wereld. De toepassing van de klassieke regels van de fysische wereld omtrent de territoriale bevoegdheid, bijvoorbeeld voor de verzameling van bewijsstukken op het internet is hier bijna onmogelijk, omdat informaticamisdrijven vaker een grensoverschrijdend aspect bevatten dan traditionele misdrijven. Er moet dus rekening worden gehouden met alle bijzonderheden en specifieke aanwinsten dat de cyberspace biedt voor het plegen van misdrijven bij het opstellen van nieuwe wetgevingen of bij het wijzigingen van het bestaande wettelijk kader. Betreffende de bewijsvoering moet er ook worden nagedacht over hoe digitale vaststellingen en bewijsstukken vertaald of omgezet kunnen worden naar niet-digitale juridische dossiers zonder dat ze hun integriteit en tegenspreekbaarheid verliezen. Dit vergt een zeer precieze en uitgewerkte wetgeving die overeenstemt met de techniciteit van de problematiek.¹²⁵

De traditionele deskundigheid en middelen waarover de rechtshandhavingsdiensten beschikken zijn dus onvoldoende om de cybercriminaliteit op een wezenlijke manier te kunnen aanpakken aangezien de kenmerken van deze vorm van criminaliteit nauw zijn verbonden aan de stand van de technologie.¹²⁶ Wijzigingen dringen zich op, want terwijl internetgebruikers reeds in staat zijn om te genieten en soms misbruik te maken van de mogelijkheden die de technologie hen biedt om informatie te delen, te communiceren, of zich te verbergen achter instrumenten die hun toelaten om anoniem te handelen op het internet, zijn de rechtshandhavingsdiensten vaak nog geconfronteerd met wettelijke technieken en middelen die voortvloeien uit een wettelijk kader dat vooral gericht is op misdrijven die in de offline wereld plaatsvinden. De wettelijke achterstand ten opzichte van de technologische realiteit maakt het uiteraard erg moeilijk voor politie en justitie om het fenomeen van de informaticacriminaliteit daadwerkelijk en effectief te kunnen indijken.¹²⁷ Naast dit snel

veranderend fenomeen is het noodzakelijk om snel te reageren en maatregelen ten uitvoer te brengen die een effectieve oplossing kunnen bieden om de achterstand die men heeft tegenover de online wereld, te doen afnemen.\textsuperscript{128} Snelheid is inderdaad zeer belangrijk in het kader van het onderzoek naar cybercriminaliteit omdat gegevens die cruciaal kunnen zijn voor het onderzoek mogelijk vluchtig zijn, zodat er snel dient te worden ingegrepen vóór dat ze verdwijnen. Dit is vaak moeilijk omdat traditionele samenwerkingsprocedures tussen verschillende diensten en op het internationaal gebied tijdrovend zijn, zodat de procedurele hindernissen in het voordeel van de misdaders kunnen spelen.\textsuperscript{129}

Onderzoek en kennis over de informaticacriminaliteit zijn dus van cruciaal belang om maatregelen in te voeren die een effectief beleid voor de bestrijding van cybercriminaliteit mogelijk maken. Niet alleen moet er aandacht worden besteed aan maatregelen die op korte termijn resultaten kunnen meebrengen, maar ook over maatregelen die op langere termijn resultaten kunnen boeken, dient te worden nagedacht.\textsuperscript{130} Er moet nog veel gebeuren opdat de technologieën en de opsporingsdiensten in staat zijn om individuen en criminele organisaties aansprakelijk te stellen voor hun acties en de misdrijven die ze hebben gepleegd. Zelfs de bestraffing van de kleinste informaticamisdrijven moeten mogelijk worden en daadwerkelijk worden uitgevoerd om een effectieve bestrijding en aanpak te hebben. Alles wat er op het internet gebeurt, is op één of andere manier opspoorbaar, maar de juiste middelen en technieken moeten nog ontwikkeld worden om het hoofd te kunnen bieden aan de moeilijkheden en de hindernissen, die het dark web kan meebrengen. Opsporingsdiensten moeten daarom de mogelijkheid krijgen om de ICT op een optimale manier te kunnen aanwenden tijdens hun onderzoeken en dus misdaders op te sporen met dezelfde middelen die ze aanwenden om hun sporen zoveel als mogelijk ontraceerbaar en onbestaand te maken.\textsuperscript{131}

2. Aanbevelingen

Het is dus noodzakelijk dat het wettelijk kader een adequate en effectieve steun biedt aan de opsporingsdiensten ten aanzien van de technologische context.

\textsuperscript{130} B.J. KOOPS, “Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research”, p. 3.
Rechtshandhavingsdiensten moeten duidelijk de mogelijkheid hebben om de grenzen van de maatregelen die ze mogen nemen, te kennen, om te weten hoe ze kunnen bewegen in de online wereld en wat hun actiemogelijkheden zijn. Zelfs als de online en de offline wereld grote verschillen aantonen, is het niet wenselijk om een apart juridische kader te ontwikkelen voor het onderzoek en de opsporing in de cyberwereld, omdat dit tot een te complexe verdeling en organisatie van het wettelijk kader zou leiden, wat nadelig zou zijn voor het strafrechtelijk onderzoek. Het juridische landschap is al genoeg verdeeld en complex met de verschillende regelgevingen omtrent de bijzondere opsporingsmethoden, de specifieke regels die van toepassing zijn voor het gerechtelijke onderzoek en de specifieke regels die van toepassing zijn bij ontdekking op heterdaad.\textsuperscript{132} De beste oplossing zou dus hier zijn om een juridisch compromis te vinden om het juridische kader van beide werelden gelijk te schakelen voor wat betreft zowel het materieel recht als het procedureel strafrecht zodat de bestaande wetsbepalingen ook de nieuwe misdrijven die afzonderlijk op het internet plaatsvinden kunnen omvatten. Er zou dus geen onderscheid moeten worden gemaakt in de manier waarop het rechtsbelang aangetast werd. We denken hier bijvoorbeeld aan het gebruik van bijnamen op het internet, wat ondergebracht kan worden bij het misdrijf van valse naamdracht.\textsuperscript{133} Niet voor alle situaties en fenomenen die plaatsvinden in de online wereld is echter een vergelijkbaar fenomeen of situatie te vinden in de offline wereld. Voor deze situaties is het dan wel noodzakelijk om nieuwe wetsbepalingen in het leven te roepen. Verder betekent het niet dat gelijkaardige situaties, die in de twee verscheidene werelden plaatsvinden, per se onder dezelfde wetsbepaling moeten vallen. In bepaalde gevallen kan een uitbreiding van het toepassingsgebied van de wetsbepalingen niet zomaar gebeuren, omdat er eerst moet worden gekeken naar de ratio legis van de wetsbepalingen om te zien of deze wel geschikt kunnen zijn voor de cyberwereld.\textsuperscript{134}

In de grote inspanning die verwacht wordt van de wetgever, om het wettelijk kader up-to-date te brengen, dient hij bovendien een evenwicht te vinden om de wetsbepalingen zo technologisch neutraal mogelijk te formuleren, zodat deze ook van toepassing kunnen zijn op toekomstige technologische ontwikkelingen zonder dat er andere wijzigingen moeten worden aangebracht en zonder dat de bepalingen evenmin te abstract en niet duidelijk genoeg zijn.\textsuperscript{135}

\textsuperscript{132} C. CONINGS en P. VAN LINTHOUT, “Sociale media: een nieuwe uitdaging voor politie en justitie”, p. 215.
\textsuperscript{133} C. CONINGS en P. VAN LINTHOUT, “Sociale media: een nieuwe uitdaging voor politie en justitie”, p. 213.
\textsuperscript{134} C. CONINGS en P. VAN LINTHOUT, “Sociale media: een nieuwe uitdaging voor politie en justitie”, p. 215.
\textsuperscript{135} B.J. KOOPS, “Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research”, p. 11.
Afdeling 2. Wetgevend kader

In deze afdeling wordt er een overzicht en een korte bespreking gegeven van verschillende wetten die belangrijk zijn voor de bestrijding van de informaticacriminaliteit en die het bestaande wettelijk kader hebben gewijzigd.

1. Wijzigingen aangebracht door de wet van 28 november 2000 inzake informaticacriminaliteit\(^{136}\)

Deze wet heeft wijzigingen aangebracht aan het Strafwetboek en het Wetboek van Strafvordering die noodzakelijk waren rekening houdend met de technologische evolutie en het feit dat bepaalde constitutieve bestanddelen van traditionele misdrijven onvoldoende technologieneutraal waren geformuleerd, zodat het een hindernis vormde om bepaalde kwaadaardige handelingen te vervolgen en rechtsbelangen te beschermen.\(^{137}\) Voor de wet van 28 november 2000 was België op het vlak van de informaticacriminaliteit geen goede leerling en vertoonde een achterstand ten aanzien van de meeste Europese landen die al wetgevingen daaromtrent hadden aangenomen.\(^{138}\) Deze wet inspireert zich op de aanbeveling R(89)9 van de Raad van Europa inzake computer gerelateerde criminaliteit\(^{139}\), maar wijkt er nauwgezet van af, omdat de wetgever deze aanbevelingen al als achterhaald beschouwde ten aanzien van de technologische evolutie, en de perceptie van de criminaliteit op bepaalde vlakken en op de aanbeveling R(95) 13 inzake problemen van strafprocesrecht die gelieerd zijn aan de informatietechnologie\(^{140}\).\(^{141}\)

Er worden met deze wet twee precieze doelstellingen nagestreefd. Ten eerste, voert deze wet nieuwe strafbepalingen in om tegemoet te komen aan het feit dat de bepalingen van de traditionele misdrijven die zich bevinden in het Strafwetboek niet van toepassing of moeilijk van toepassing kunnen zijn op misdrijven die zich in de online wereld voordoen.\(^{142}\) Hiermee beoogde de wetgever de specifieke noden van de informatietechnologieën te vervullen. Ten tweede, werden er wijzigingen aangebracht aan de strafrechtelijke procedure om ervoor te zorgen dat de rechtshandhavingsdiensten over de gepaste juridische middelen

---

\(^{136}\) Hierna: WIC.
\(^{139}\) Aanbev.Raad, R (89) 9 van 13 september 1989 inzake computergerelateerde criminaliteit.
\(^{140}\) Aanbev.Raad, R (95) 13 van 11 september 1995 over problemen inzake strafrechtelijke procedures in verband met de informatietechnologie.
\(^{142}\) J. COPPENS, “Informatisering en criminaliteit: de advocaat in cyberspace”, *Ad Rem* 2012, afl. 4, p. 22.
zouden beschikken om hun onderzoeken omtrent cybercriminaliteit uit te voeren. Terwijl deze wet wijzigingen en aanvullingen heeft aangebracht aan het Strafwetboek en het Wetboek van Strafvordering om een evenwicht uit te bouwen tussen enerzijds de bescherming van nieuwe waarden, en anderzijds het behoud van traditionele waarden, beoogde deze wet geen diepe structurele hervormingen te brengen aan deze wetboeken.

1.1. Wijzigingen aangebracht aan het materieel strafrecht

Aangaande het materieel strafrecht wordt het onderscheid tussen specifieke en niet-specifieke informaticacriminaliteit gehanteerd om te bepalen welke laakbare gedragingen een nieuwe strafbepaling nodig hebben en welke zich kunnen aansluiten bij de bestaande wetsbepalingen van de traditionele misdrijven. Niet-specifieke informaticamisdrijven waarbij de informatica slechts als een nieuwe *modus operandi* voor het plegen van het misdrijf wordt gehanteerd, sluiten zich voldoende aan bij de bestaande wetgeving, zodat de wetgever het niet nodig heeft geacht om nieuwe strafbepalingen in te voeren. Hiervoor hanteerde men een teleologische interpretatie van de strafwet om de strafbepalingen op een evolutieve manier te beschrijven door rekening te houden met de wijzigingen die plaatsvinden in de samenleving. Dit is echter slechts mogelijk wanneer men met zekerheid de wil van de wetgever kent en als de feiten onder de wettelijke definitie kunnen vallen.

Daarnaast heeft de wetgever nieuwe strafbepalingen ingevoerd voor de gevallen waar de informatica zelf het doel van de strafbare gedraging is, zodat er geen aangepast antwoord kon worden gevonden in het bestaande juridisch arsenaal, zelfs na een teleologische interpretatie. De wetgever heeft hier zo veel mogelijk gebruik gemaakt van een technologieneutrale woordenschat om te vermijden dat door de ontwikkeling in de informatietechnologie de strafbepalingen te snel achterhaald zouden zijn. De nieuwe strafbaarstellingen die in het leven werden geroepen met de wet van 28 november 2000 zijn

---


samengevoegd in drie categorieën: valsheid in informatica\textsuperscript{147}, informaticabedrog\textsuperscript{148} en de inbreuken op de vertrouwelijkheid, de integriteit en de beschikbaarheid van informaticasystemen of van de daarin opgenomen gegevens\textsuperscript{149} die een nieuwe titel in het Strafwetboek samenstellen. De twee eerste categorieën betreffen de “\textit{instrumentele IT-misdrijven}” waarbij het gebruik van een bepaalde IT-modus operandi een strafbaar doel nastreeft, terwijl de misdrijven van de derde categorie kunnen worden aangeduid als “\textit{intrinsieke IT-misdrijven}” omdat ze de IT-omgeving als zelfstandige rechtswaarde aantasten.\textsuperscript{150} Hierna wordt er een kort overzicht en voorstelling van de nieuwe misdrijven geschetst.

1.2. Wijzigingen aangebracht aan het procedureel strafrecht

Betreffende het formeel IT-stafrecht of het procedureel strafrecht heeft de wetgever met de wet van 28 november 2000 nieuwe onderzoekshandelingen in het raam van de IT-recherche ingevoerd om adequate middelen voor de bestrijding van de informaticacriminaliteit aan de rechtshandhavingsdiensten aan te reiken.

1.2.1. Het databeslag

Er werd een nieuw artikel 39\textit{bis} in het Wetboek van Strafvordering ingevoerd, die het databeslag regelt met dezelfde doelstellingen als de inbeslagneming van artikelen 35 e.v. Sv. In tegenstelling tot de reële fysieke wereld kunnen de digitale gegevens niet ter hand genomen worden om ze in beslag op de griffie neer te leggen. Er was dus een nieuw artikel nodig die de praktische moeilijkheden zou regelen omtrent de onmogelijke toepassing van de klassieke benadering van inbeslagneming van bewijsmateriaal voor immateriële gegevens. Door de inwerkingtreding van dit artikel is zowel de materiële inbeslagname van gegevens via het in beslagnemen van een computer of een gsm volgens de klassieke regels, als de inbeslagname

\textsuperscript{147} Het betreft een nieuwe versie van het traditioneel misdrijf van valsheid in geschrifte van artikelen 194 tot 196 Sw. die ingevoerd is in een nieuw artikel 210\textit{bis} Sw. door artikel 4 WIC.
\textsuperscript{148} Artikel 5 WIC heeft een nieuwe afdeling \textit{Informaticabedrog} in het hoofdstuk II “Betrog” van Titel IV “Misdrijven en wanbedrijven tegen eigendommen” van Boek II van het Strafwetboek ingevoerd.
\textsuperscript{149} Artikel 6 WIC heeft een nieuwe titel IX\textit{bis} in Boek II van het Strafwetboek ingevoerd waarin wij de misdrijven van hacking in artikel 550\textit{bis} Sv. en van data en informaticasabotage in artikel 550\textit{ter} Sv. terugvinden.
van de gegevens enkel door een kopie van deze gegevens op een officiële drager van de overheid mogelijk.  

1.2.2. Het opsporen en lokaliseren van telecommunicatie

De lokalisatie van communicatie en de opsporing ervan zijn ook zeer belangrijk in het kader van een strafrechtelijk onderzoek. Daarom heeft de wetgever artikel 88bis van het Wetboek van Strafvordering ingevoerd, dat toelaat in het geval dat er “ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf tot gevolg kunnen hebben en de onderzoeksrechter van oordeel is dat er omstandigheden zijn die het doen opsporen van elektronische communicatie of het lokaliseren van de oorsprong of de bestemming van elektronische communicatie noodzakelijk maken om de waarheid aan de dag te brengen” om de dynamische gegevens van communicatie op te vragen bij de operatoren en verstrekkers van een dienst op het internet. Deze onderzoeksmaatregel laat niettemin niet toe om kennis te nemen van de inhoud van de communicatie, omdat het enkel betrekking heeft op de gegevens van de communicatie. Kennis van de inhoud van een communicatie is dan slechts mogelijk door de tapmaatregel, al dan niet gekoppeld aan de maatregel van artikel 88bis Sv.

1.2.3. De netwerkzoeking

Met de invoering van de *sui generis* figuur van de netwerkzoeking van artikel 88ter Sv., wat losstond van de huiszoeking, beoogde de wetgever tegemoet te komen aan het probleem dat zich stelde wanneer er een klassieke huiszoekingsplatsvond en er vastgesteld werd dat er niet slechts één computer werd aangetroffen, maar dat die verbonden was aan een netwerk van computers. Het klassieke huiszoekingsmandaat kan per definitie enkel worden uitgevoerd op de plaats waar het wordt bevolen, zodat het in bepaalde situaties geen aangepast antwoord kan bieden. Het onderzoek naar het informaticasysteem moet in dit geval op verschillende plaatsen geschieden, zodat er meerdere bevelen tot huiszoekings nodig zijn. Dit was problematisch, omdat er vaak niet *a priori* kon worden vastgesteld waar de zoekings plaats diende te vinden, welke bestanddelen relevant waren, zelfs waar de computers of dragers van het informaticasysteem zich geografisch bevinden, omdat deze ook mobiel kunnen zijn en tevens door het niet-gelijktydig optreden kon het ook zijn dat er bewijsmateriaal verloren

---


ging.\textsuperscript{153} Door artikel 88\textit{ter} Sv. werd het dus mogelijk onder bepaalde voorwaarden\textsuperscript{154} om een zoekings in een informaticasysteem, of een deel ervan, uit te breiden naar een informaticasysteem, of een deel ervan, dat zich op een andere plaats bevond dan de plaats van de zoekings.\textsuperscript{155} Deze wetsbepaling had niet enkel betrekking op computers die in een gebouw staan, maar ook op draagbare computers en telefoons om te vermijden dat het artikel te vug achterhaald zou zijn tegenover de technologische realiteit.\textsuperscript{156} Zelfs als deze maatregel ruim werd bedoeld en dat informaticasystemen\textsuperscript{157} op een brede manier worden omschreven in de memorie van toelichting van de wet\textsuperscript{158}, mogen de politiediensten zich niet schuldig maken aan hacking, zodat de netwerkzoekings niet mogelijk is op informaticasystemen die niet openstaan voor het publiek en waarvoor de politiediensten niet over de toegangscodes en een gemotiveerd netwerkzoekingsmandaat beschikken.\textsuperscript{159}

\subsection*{1.2.4. De informatietap}

Door artikelen 11 tot 13 van de wet van 28 november 2000 werd de telefoontap van artikelen 90\textit{ter} e.v. van het Wetboek van strafvordering, aangepast aan de nieuwe vormen van informaticacriminaliteit. Er was dan geen sprake meer van “telefoontap” maar van “informatietap” zodat de nieuwe vormen van communicatie op het internet, onder welke vorm ook, sindsdien tijdens hun overbrenging van de zender naar de ontvanger tapbaar of afluisterbaar waren. De tapmaatregel is echter verboden op communicatie die nog niet in transmissie is en communicatie die al volledig ter bestemming bij het geïndiceerd noodzakelijk eindstation is aangekomen.\textsuperscript{160} De tapwetgeving, die tot stand is gekomen door

\begin{itemize}
\item De uitbreiding naar informaticasystemen is slechts mogelijk wanneer deze noodzakelijk is om de waarheid te achterhalen in de feiten waarvoor de onderzoeksrechter gevat is, ofwel wanneer het disproportioneel zou zijn om andere maatregelen te treffen, zoals het uitschrijven van meerdere huishoudingsbevelen, ofwel wanneer er een risico dat er bewijsobjecten kwijt zullen gaan bestaat.
\item P. VAN LINHTHOUT en J. KERKHOFS, “Inleiding tot het materieel en strafprocedureel cyberstrafrecht: uitdagingen voor de advocatuur”, p. 41.
\item Informaticasystemen worden omschreven als alle systemen voor de opslag, de verwerking of de overdracht van data. Er wordt hier vooral gedacht aan computers, chipkaarten en dergelijke, netwerken en delen daarvan, en telecommunicatiesystemen of onderdelen daarvan die een beroep doen op IT.
\item Memorie van Toelichting, Wetsontwerp inzake informaticacriminaliteit, Parl.St., Kamer, 1999-2000, nr. 50-0213/001, 50-0214/001, p. 12.
\item P. VAN LINHTHOUT en J. KERKHOFS, “Inleiding tot het materieel en strafprocedureel cyberstrafrecht: uitdagingen voor de advocatuur”, p. 43.
\item P. VAN LINHTHOUT en J. KERKHOFS, “Inleiding tot het materieel en strafprocedureel cyberstrafrecht: uitdagingen voor de advocatuur”, p. 32.
\end{itemize}
de Nieuwe Afluisterwet van 30 juni 1994\textsuperscript{161}, was oorspronkelijk geschreven zonder rekening te houden met de vooruitgang in de digitale wereld en was daardoor gebaseerd op de klassieke spraketelefonie. De Wet Informaticacriminaliteit heeft drie wijzigingen aangebracht aan de toenmalige regelingen omtrent telefoontap en in het bijzonder aan de artikelen 90\textit{ter}, 90\textit{quater} en 90\textit{septies} van het Wetboek van Strafvordering, om adequate juridische middelen te kunnen bieden aan de politiediensten en gerechtelijke diensten in het kader van de bestrijding van de informaticacriminaliteit.\textsuperscript{162} Eerst werd de lijst van de straftabie feiten waarvoor een tapmaatregel kan bevolen worden, uitgebreid met de nieuwe misdrijven die reeds door de wet van 28 november 2000 werden ingevoerd en de misdrijven van de artikel 259\textit{bis}\textsuperscript{163} en 314\textit{bis} Sw.\textsuperscript{164} Ten tweede, heeft het artikel 12 WIC een bijzondere medewerkingsplicht ingevoerd voor personen waarvan de onderzoeksrechter vermoedt dat ze een bijzondere kennis hebben van telecommunicatiediensten, met name de operatoren en dienstverleners, bij het zoeken naar bewijsmateriaal in een nieuwe vierde paragraaf in het artikel 90\textit{quater} Sv. Teneinde werd er een nieuw lid ingevoegd in het artikel 90\textit{septies} Sv. door artikel 13 WIC die waarborgen voorziet voor de vertrouwelijkheid en de integriteit van een tapmaatregel, zoals de digitale handtekening.\textsuperscript{165}

1.2.5. De medewerkingsplicht

Naast de invoering van een nieuwe paragraaf in artikel 90\textit{quater} Sv., heeft de wet van 28 november 2000 ook een nieuw artikel 88\textit{quater} in het Wetboek van Strafvordering in het leven geroepen die de medewerkingsplicht bevat. Door dit artikel is het mogelijk voor de onderzoeksrechter om “iedere geschikte persoon bevelen om zelf het informaticasysteem te bedienen of de ter zake dienende gegevens, die door middel daarvan worden opgeslagen, verwerkt of overgedragen, naargelang het geval, te zoeken, toegankelijk te maken, te kopiëren, ontoegankelijk te maken of te verwijderen, in de door hem gevorderde vorm. Deze personen zijn verplicht hieraan gevolg te geven, voorzover dit in hun mogelijkheden ligt”\textsuperscript{166}. Deze medewerkingsverplichting is vanzelfsprekend niet van toepassing op de verdachten die

\textsuperscript{161} Wet 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en –telecommunicatie, B.S. 24 januari 1995.


\textsuperscript{163} Het betreft het misdrijf van afluisteren, kennisnemen en opnemen van privécommunicatie en –telecommunicatie.

\textsuperscript{164} Het betreft de misdrijven betreffende het geheim van privé-communicatie en –telecommunicatie.


\textsuperscript{166} Artikel 88\textit{quater} §2 van het Wetboek van Strafvordering.
niet verplicht kunnen zijn om lastens zichzelf bewijsmateriaal te verzamelen of om tegen zichzelf te getuigen en op de personen die opgesomd zijn in artikel 156 Sv., namelijk de aanverwanten en bloedverwanten bijvoorbeeld.

Daarnaast wanneer we in aanwezigheid zijn van versleutelde gegevens toelaat de eerste paragraaf van het artikel 88quater Sv. aan de onderzoeksrechter om “personen van wie hij vermoedt dat ze een bijzondere kennis hebben van het informaticasysteem dat het voorwerp uitmaakt van de zoekong of de uitbreiding ervan bedoeld in artikel 39bis, § 3 of van diensten om gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, te beveiligen of te versleutelen, bevelen inlichtingen te verstrekken over de werking ervan en over de wijze om er toegang toe te verkrijgen, of in een verstaanbare vorm toegang te verkrijgen tot de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen”’. In de derde tot de vijfde paragraaf van het artikel zijn er sancties vastgesteld in geval van niet-naleving of van verhindering van de verplichtingen van de twee eerste paragrafen.

1.2.6. De bewaringsplicht van oproep- en identificatiegegevens voor operatoren en dienstverstrekkers

Ten laatste, heeft de Wet Informaticacriminaliteit het artikel 109ter van de wet van 21 maart 1991167, ook wel de Belgacomwet genoemd, gewijzigd door een tweede en derde paragraaf toe te voegen die aan de Koning de kracht geeft om de verplichtingen voor “de operatoren van telecommunicatienetwerken en de verstrekkers van telecommunicatiediensten om de oproepgegevens van telecommunicatiemiddelen en de identificatiegegevens van de gebruikers van telecommunicatiemiddelen te registreren en gedurende een bepaalde termijn te bewaren met het oog op de opsporing en de vervolging van strafbare feiten” te bepalen via koninklijke besluit.168 De bewaringsperiode van de gegevens was één van de meest controversiële punten van het parlementaire debat en er werd uiteindelijk beslist dat het aan de Koning was om deze te bepalen, maar dat het niet minder dan twaalf maanden mocht inhouden.169

---

1.3. Wijzigingen van de wet van 28 november 2000 inzake informaticacriminaliteit

Door de ratificatie door België in 2013 van het Cybercrimeverdrag van Boedapest van 23 november 2001 zijn er aanpassingen aan de Wet Informaticacriminaliteit moeten gebeuren om de Belgische wetgeving in overeenstemming te brengen met het minimum wettelijk procedureel arsenaal, waarin de lidstaten dienen te voorzien volgens het verdrag om de informaticacriminaliteit op een geharmoniseerde manier te kunnen bestrijden.\(^{170}\) Wijzigingen werden dan aangebracht door de wet van 15 mei 2006\(^{171}\) aan de misdrijven van de schending van de integriteit van gegevens en de schending van de integriteit van informaticasystemen van art. 550\(\text{ter} \) Sw., het misbruik van instrumenten van artikel 550\(\text{bis} \) §5 en 550\(\text{ter} \) §4 Sw. en het misdrijf van informaticabedrog van artikel 504\(\text{quater} \) Sw.\(^{172}\)

2. Wijzigingen aangebracht door de wet van 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden\(^{173}\)

De wet van 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethode – ook al BOM-wet genoemd- is op 22 mei 2003 in werking getreden. Deze wet schept een wettelijk kader voor de bijzondere opsporingsmethoden van observatie, infiltratie, informantenerwerking en enige andere onderzoeksmethoden in de strijd tegen terrorisme en zware georganiseerde criminaliteit, zoals de inkkijkoperatie, het onderscheppen van post, het direct afluisteren, het inwinnen van gegevens over bankrekeningen en banktransacties en de uitgestelde tussenkomst. Volgens het tweede lid van de eerste paragraaf van artikel 47\(\text{ter} \) Sv. kunnen de bijzondere opsporingsmethoden worden omschreven als de methoden “door de door de minister van Justitie aangewezen politiediensten aangewend in het kader van een opsporingsonderzoek of een gerechtelijk onderzoek (…), met als doel het vervolgen van daders van misdrijven, het opsporen, verzamelen, registreren en verwerken van gegevens en inlichtingen op grond van ernstige aanwijzingen van te plegen of reeds gepleegde, al dan niet aan het licht gebrachte strafbare feiten”. Deze bijzondere opsporingsmethoden zijn bijzonder omdat ze discreet en misleidend kunnen zijn en “omdat de toepassing ervan de fundamentele rechten en vrijheden kan


\(^{171}\) Wet van 15 mei 2006 tot wijziging van de artikelen 259\(\text{bis} \), 314\(\text{bis} \), 504\(\text{quater} \), 550\(\text{bis} \) en 550\(\text{ter} \) van het Strafwetboek, \textit{B.S.} 12 september 2006.

\(^{172}\) B. VAN ROY, “Wijzigingen aan de Belgische bepalingen inzake informaticacriminaliteit”, \textit{Computerr.} 2006, p. 188.

aantasten en afbreuk kan doen aan de fundamentele beginselen van de strafrechtspelging, zoals het loyaliteitsprincipe, en zijn heimelijk karakter, niet enkel in de uitvoering ervan maar ook in zijn strafvorderlijke neerslag, aangezien bepaalde elementen in een vertrouwelijk dossier worden bijgehouden”.  

Er werd nochtans al sinds de jaren 70 beroep gedaan op deze bijzondere methoden, zelfs als er nog geen wettelijk kader voor bestond en deze soms een zware inmenging in het recht op eerbiediging van het privéleven uitmaakten, omdat ze soms, al dan niet in combinatie met het gebruik van spijtoptanten en klassieke opsporingsmethoden, de enige maatregelen zijn die effectieve middelen bieden om de zware criminaliteit op een aangepaste manier te bestrijden.

Op de noodzaak van een wettelijk kader voor de bijzondere onderzoeks- en opsporingsmethoden werd voor het eerst in 1990 gewezen door de parlementaire onderzoekscommissie, met name de Bendecommissie I, die de wijze waarop de bestrijding van het banditisme en het terrorisme georganiseerd was na de aanvallen van de Bende van Nijvel onderzocht. Een strikte reglementering van de aanwending van de bijzondere methoden was volgens het verslag van de Bendecommissie I nodig, omdat het in sommige gevallen, zoals bij de infiltratie, bijna onvermijdelijk was om bij het gebruik van zulke methoden strafbare feiten te plegen. Men ging echter niet verder dan het opstellen van een vertrouwelijke ministeriële omzendbrief die bestemd was voor de procureurs-generaal van het land, zodat er steeds een tussenkomst van de wetgever nodig was. Deze wettelijke tussenkomst werd verder noodzakelijk ten aanzien van het toenemende aantal grensoverschrijdende operaties, die onder meer plaatsvonden in het raam van de Schengenakkoorden, waar er beroep werd gedaan op bijzondere opsporingsmethoden, en de tegenstrijdigheid die deze methoden kunnen vertonen ten aanzien van artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM).

---

177 Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, ondertekend te Rome op 4 november 1950, B.S., 19 augustus 1955.
2.1. Bijzondere opsporingsmethoden

In deze sectie worden de verschillende de bijzondere opsporingsmethoden die een wettelijke basis hebben gekregen door de BOM-wet kort omschreven.

2.1.1. De observatie

De bijzonder opsporingsmethode van observatie heeft door de BOM-wet een wettelijke regeling gekregen in artikel 47sexies Sv. De observatie wordt in het artikel omschreven als “het stelselmatig waarnemen door een politieambtenaar van één of meerdere personen, hun aanwezigheid of gedrag, of van bepaalde zaken, plaatsen of gebeurtenissen. Een stelselmatige observatie in de zin van dit wetboek is 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”.

De toepassing van deze opsporingsmethode is niet slechts beperkt tot verdachten, maar kan ook aangewend worden ten aanzien van andere personen die eens in contact zijn geweest met het criminele milieu of een link ermee hebben, en ten aanzien van zaken, plaatsen en bepaalde gebeurtenissen.\footnote{A. DE NAUW en F. SCHUERMANS, “De wet betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden”, R.W. 2003-04, afl. 1, p. 937.}

2.1.2. De infiltratie

De infiltratie wordt geregeld in artikel 47octies Sv., waar het omschreven wordt als “het door een politieambtenaar, infiltrant genoemd, 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, zoals bedoeld in artikel 324bis van het Strafwetboek, of misdaden of wanbedrijven als bedoeld in artikel 90ter, §§ 2 tot 4 plegen of zouden plegen”.

2.1.3. De informantenwerking

Als derde bijzondere opsporingsmethode heeft de informantenwerking een wettelijke basis gekregen in artikel 47decies Sv. Dit artikel omschrijft de informantenwerking als “het onderhouden van regelmatige contacten door een politieambtenaar met een persoon,
informant genoemd, waarvan vermoed wordt dat hij nauwe banden heeft met één of meerdere personen, waarvan er ernstige aanwijzingen zijn dat ze strafbare feiten plegen of zouden plegen, en die de politieambtenaar hierover, al dan niet gevraagd, inlichtingen en gegevens verstrekkt”.

2.2. Andere onderzoeksmethoden

Naast de bijzondere opsporingsmethoden, heeft de BOM-wet tevens een wettelijk kader ingevoerd voor de verdere uitwerking van een aantal andere onderzoeksmethoden. Deze worden hier niet verder omschreven maar worden enkel vermeld. Het betreft namelijk het onderscheppen en openen van post geregeld in artikel 46ter Sv., het direct afluisteren van privé-communicatie of -telecommunicatie door de plaatsing van technische middelen in een private plaats zonder toestemming of medeweten van de eigenaar of de bewoner, geregeld in artikel 90ter §1, tweede lid Sv., de inkijkoperatie geregeld in artikel 89ter §1 Sv., de uitgestelde tussenkomst geregeld in artikel 40bis Sv. en het inwinnen van gegevens over bankrekeningen en banktransacties geregeld in artikel 46quater Sv.

2.3. Algemene principes bij de toepassing van de bijzondere opsporingsmethoden

De BOM-wet neemt de vier grote algemene principes over die in acht moeten worden genomen bij de aanwending van bijzondere opsporingsmethoden, en die reeds aan bod kwamen in de ministeriële omzendbrief van 24 april 1990, met name de subsidiariteit, de proportionaliteit, het verbod van provocatie en het verbod om misdrijven te plegen.180

2.3.1. Het subsidiariteitsbeginsel

Het subsidiariteitsbeginsel houdt in dat er eerst moet worden nagegaan als het niet mogelijk is om hetzelfde resultaat te bereiken door andere middelen van onderzoek, omdat deze bijzondere opsporingsmethoden zeer ingrijpend kunnen zijn. Dit beginsel is algemeen geformuleerd in de bepalingen omtrent de observatie181, de infiltratie182 en de inkijkoperatie183.

181 Artikel 47sexies §2 Sv.
182 Artikel 47octies §2 Sv.
183 Artikel 89ter §1 Sv.
2.3.2. Het proportionaliteitsbeginsel

Door het proportionaliteitsbeginsel wordt er verwacht dat de gebruikte maatregel in evenredigheid moet zijn met de ernst van het misdrijf. Hier wordt het beginsel niet algemeen geformuleerd in de wet, maar worden er verschillende drempels gehanteerd in de verschillende opsporingsmethoden in functie van de zwaarte van de straf die aan het misdrijf verbonden is.

2.3.3. Het provocatieverbod

De BOM-wet heeft artikel 47quater Sv. ingevoerd die het provocatieverbod omvat door te bepalen dat “een politieambtenaar mag bij de tenuitvoerlegging van een bijzondere opsporingsmethode een verdachte niet brengen tot andere strafbare feiten dan deze waarop diens opzet reeds tevoren was gericht”. Een inbreuk van dit verbod heeft de onontvankelijkheid van de strafvordering voor de uitgesproken feiten als gevolg. Dit artikel werd echter door het arrest van 21 december 2004 door het Arbitragehof vernietigd.

2.3.4. Het verbod om misdrijven te plegen

Het vierde beginsel betreft het verbod om misdrijven te plegen en is ook het voorwerp van een aparte wetsbepaling die ingevoerd werd door de BOM-wet, met name artikel 47quinquies Sv.

Soms is het echter niet mogelijk voor de politiediensten om dit verbod te eerbiedigen, en worden ze voor het welslagen van het onderzoek, voor het verzekeren van hun eigen veiligheid of van de veiligheid van anderen die betrokken zijn bij de operatie, ertoe gebracht om misdrijven te plegen tijdens de uitvoering van hun opdracht. De tweede paragraaf van het artikel bevat daarvoor een strafuitsluitende verschoningsgrond voor de politieambtenaren.

2.4. Wijzigingen van de BOM-wet door wet van 27 december 2005

Deze wet bracht een aantal wijzigingen aan de BOM-wet om tegemoet te komen aan de kritieken die ertegen waren geformuleerd door het vernietigingsarrest van het Arbitragehof

---

186 De strafbare feiten mogen volgens het tweede lid van de tweede paragraaf niettemin niet “ernstiger zijn dan die waarvoor de methoden worden aangewend en moeten noodzakelijkerwijze evenredig zijn met het nagestreefde doel”.
van 21 december 2004 en heeft daarenboven een aantal nieuwe maatregelen en technische bepalingen ingevoerd.

Dit arrest van het Arbitragehof heeft namelijk verschillende bepalingen die ingevoerd werden door de BOM-wet vernietigd, omdat er werd vastgesteld dat een aantal fundamentele rechten, zoals het recht op een eerlijk proces en het recht op privacy, door de BOM-wet werden aangetast. Volgens het Hof kunnen de inkijkoperatie en de observatie met gebruik van technische hulpmiddelen om zicht te verwerven in een woning enkel gevorderd worden in het kader van een gerechtelijk onderzoek en niet meer via een mini-onderzoek. Het artikel 47quater Sv. dat de provocatie omschreef en regelde, werd ook vernietigd omdat de provocatie daar beperkend was omschreven ten aanzien van de definitie van de provocatie van het gemeen recht die we in de overheersende rechtspraak teruggingden188, zodat er een verschil in behandeling ontstond tussen vervolgd personen naargelang de BOM-wet al dan niet werd toegepast. Daarnaast eiste het Hof het toezicht bij de observatie en de infiltratie op de stukken vervat in het vertrouwelijke dossier door een onafhankelijke en onpartijdige rechter teneinde na te gaan of deze operaties niet aangetast zijn door mogelijke onwettigheden. De wetgever kreeg een periode van één jaar tot de 31 december 2005, waarin de vernietigde bepalingen voorlopig gehandhaafd bleven, om een reparatiewet goed te keuren.189

De reparatiewet van 27 december 2005 heeft daaropvolgend een nieuw algemeen provocatieverbod ingesteld via artikel 30 van de wet van 17 april 1878 houdende de voorafgaande titel van het Wetboek van Strafvordering190 (V.T.Sv.) waar de definitie van de provocatie in overeenstemming is met de rechtspraak van het Hof van Cassatie. Daarnaast heeft deze wet ook de inkijkoperatie en de observatie met technische hulpmiddelen in een woning uitgesloten van het minionderzoek en heeft tenslotte artikel 235ter en 235quater toegevoegd aan het Wetboek van Strafvordering, wat voor een controle van de observatie en

---

190 Wet van 17 april 1878 houdende de voorafgaande titel van het Wetboek van Strafvordering, B.S. 25 april 1878, art. 30.
de infiltratie door de Kamer van Inbeschuldigingstelling zorgt.191 Verder heeft deze wet ook de bestaande maatregelen verder uitgewerkt en nieuwe maatregelen ingevoerd die we hier niet verder gaan bekijken192.193

3. Wijzigingen aangebracht door de Potpourri II-wet

In de loop van 2016 werden er belangrijke wijzigingen in de wetgeving omtrent het strafrechtelijk onderzoek aangebracht. Deze waren ook nodig aangezien dat het wettelijk kader ongeveer overeind was gebleven sinds 2005, terwijl er zich sindsdien veel veranderingen in de technologische wereld hebben voorgedaan. De Potpourri II-wet bracht aanpassingen op meerdere punten aan de opsporingsbevoegdheden met betrekking tot elektronische communicatie, en in het bijzonder het telefonieonderzoek. Er werden namelijk aanpassingen aangebracht aan de medewerkingsplicht van artikel 88bis en 90quater Sv. en aan de voorschriften inzake het gerechtelijk onderzoek van artikel 90quater Sv.194 Verder werden de artikelen 90sexies en 90septies Sv. die de opnames betreffen van de communicaties en telecommunicaties opgevangen als gevolg van de maatregel van het afluisteren, kennisnemen en opnemen van privé-communicatie en –telecommunicatie.195 We zullen hier op deze wijzigingen niet verder ingaan.

4. Wijzigingen aangebracht door de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie196

Vandaag de dag nemen telecomonderzoeken een steeds belangrijkere rol in het strafrechtelijk onderzoek. Dit is te verklaren door het feit dat elk internetverkeer of elke vorm van telecommunicatie digitale sporen achterlaat die onderzocht en vroeg of laat achterhaald kunnen worden. De toegang tot de communicatiegegevens, de identificatie en lokalisatie van de gebruikers van een bepaald emailadres of de verkeersgegevens van bepaalde communicatie leiden meestal naar de telecomoperatoren die instaan voor het telefonisch en het digitaal

192 We denken hier namelijk aan de invoering van een derde lid in artikel 47ter, §1 Sv., of de invoering van een derde paragraaf in artikel 47duodecies Sv.
196 Wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, B.S. 18 juli 2016 (hierna: Databetentiewet).
verkeer.\textsuperscript{197} Op het niveau van de Europese Unie werd de beschikbaarheid van de belangrijke gegevens voor het strafrechtelijk onderzoek, door middel van een bewaar- of dataretentieplicht geregeld door de dataretentierichtlijn van 15 maart 2006\textsuperscript{198} die omgezet werd in België door de wet van 30 juli 2013\textsuperscript{199}. Deze richtlijn werd door het arrest Digital Rights van het Hof van Justitie van 8 april 2014\textsuperscript{200} vernietigd omdat het in strijd was met het recht op privacy van artikel 7 en het recht van bescherming van persoonsgegevens van artikel 9 van het Handvest van de grondrechten van de Europese Unie\textsuperscript{201} omdat er geen onderscheid werd gemaakt in de richtlijn tussen de gebruikers voor het toestaan van de telecommunicatiegegevens. De Belgische wet werd dan vervolgens ook nietig verklaard door het arrest van 11 juni 2015 van het Grondwettelijk Hof\textsuperscript{202} omdat het in strijd werd verklaard met de Belgische Grondwet\textsuperscript{203} en artikel 8 EVRM.

In België heeft de wetgever vlug ingegrepen om een nieuwe Dataretentiewet op 25 mei 2016 tot stand te brengen zodat het gebruik van telecommunicatiegegevens in het kader van een strafrechtelijk onderzoek veilig en in overeenstemming met de fundamentele rechten zou zijn.\textsuperscript{204} Deze wet heeft de bewaarplicht gehouden maar heeft het beperkt in de tijd en de voorwaarden om toegang te verschaffen tot de bewaarde gegevens, zowel ten aanzien van de misdrijven die de toegang rechtvaardigen als in de tijd, verstrenget.\textsuperscript{205}

\textsuperscript{198} Richtlijn 2006/24/EG 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 nr. 2002/58/EG, Pb. L nr. 105, 13 april 2006.
\textsuperscript{199} Wet van 30 juli 2013 houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel90decies van het Wetboek van Strafvoering, B.S. 23 augustus 2013.
\textsuperscript{200} HvJ 8 april 2014, nr. C-293/12 en C-594/12, ECLI:EU:C:2014:238, Digital Rights Ireland Ltd. en Kärntner Landesregierung.
\textsuperscript{201} Handvest van de grondrechten van de Europese Unie van 12 december 2007, Pb. C nr. 83, 30 maart 2010.
\textsuperscript{202} GwH 11 juni 2015, nr. 84/2015.
\textsuperscript{203} Gecoördineerde Grondwet van 17 februari 1994, B.S. 17 februari 1994.
5. Wijzigingen aangebracht door de wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van Strafvordering en het Strafwetboek\textsuperscript{206}

Deze wet die doorgevoerd werd door de Minister van justitie Koen Geens “bevat een aantal wijzigingen in het Wetboek van Strafvordering en het Strafwetboek en beoogt vooral een aantal verbeteringen aan te brengen in het opsporingsonderzoek en het gerechtelijk onderzoek, meer in het bijzonder in de toepassing van de bijzondere opsporingsmethoden en bepaalde andere onderzoeksmethoden die in het bijzonder betrekking hebben op de internetrecherche en elektronische en telecommunicaties”.\textsuperscript{207} Deze modernisering en aanpassing van het wettelijk kader van de bijzondere opsporingsmethoden was nodig, omdat deze sinds een geruime tijd niet herzien of hervormd waren, namelijk sinds de wet van 27 december 2005, met uitzondering van punctuele aanpassingen, zodat het wettelijk kader geen voldoende middelen meer kon bieden voor een effectieve bestrijding van de informaticacriminaliteit.\textsuperscript{208} Hieronder zullen er slechts een paar van de belangrijkste wijzigingen die door de wet werden aangebracht, worden voorgelegd.

5.1. De openlijke zoek ing in informaticasystemen

De wet heeft het onderzoek in informaticasystemen grondig hervormd en heeft een onderscheid gemaakt tussen de openlijke en de heimelijke zoek ing in informaticasystemen. Wat de openlijke zoek ing betreft, heeft het artikel 2 van de wet de netwerkzoek ing, die sinds de wet van 28 november 2000 was geregeld in artikel 88ter Sv., integraal overgeheveld naar artikel 39\textsuperscript{bis} S3 Sv. en de bevoegdheid daarover van de onderzoeksrechter verschoven naar de procureur des Konings. Artikel 39\textsuperscript{bis} Sv. wordt hiermee het standaardartikel voor de openlijke zoek ing in informaticasystemen terwijl het vroeger slechts het databeslag regelde. Dit zorgde voor een uitbreiding van de informaticazoe king naar informaticasystemen of delen van systemen die zich op een andere plaats bevinden en “waartoe de personen die gerechtigd zijn het onderzochte informaticasysteem te gebruiken, in het bijzonder toegang hebben”.\textsuperscript{209}

\textsuperscript{206} Wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van Strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken, B.S. 17 januari 2017.


\textsuperscript{209} Artikel 39\textsuperscript{bis}, §3, tweede lid Sv.
Dit wilt zeggen dat het niet gaat over systemen die toegankelijk zijn voor het publiek. Teneinde de maatregelen bedoeld in artikel 39bis Sv. mogelijk te maken, heeft de wetgever een uitdrukkelijke hack- en decryptiebevoegdheid in artikel 39bis §5 Sv. ingevoerd, zodat de beveiliging van informaticasystemen tijdelijk kan worden opgeheven en dat de procureur des Konings en de onderzoeksrechter de gegevens van een informaticasysteem kunnen ontcijferen en decoderen door de plaatsing van een technisch hulpmiddel.\footnote{C. CONINGS en S. ROYER, “Vernieuwingen binnen het digitaal speurwerk”, Actua Leges 2017/30.}

5.2. De heimelijke zoekning in informaticasystemen

Betreffende de heimelijke zoekning, heeft de wet de inkijkoperatie van artikel 46quinquies Sv., die al ingevoerd was met de BOM-wet, mogelijk gemaakt in IT-systemen. De inkijkoperatie in informaticasystemen, die aan de inkijkoperatie in een woning wordt gelijkgeschakeld, wordt met artikel 15 van de wet digitaal speurwerk in artikel 89ter Sv. geregeld. Terwijl de klassieke inkijkoperatie als een soort heimelijke “light” zoekning in private plaatsen kan worden beschreven, kan het sinds de wet digitaal speurwerk worden gezien als een heimelijke variant op de huiszoekning.\footnote{C. CONINGS en S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken”, NC 2017, afl. 4, pp. 316- 317.} De nieuwe inkijkoperatie gaat dus verder en wordt niet meer beperkt tot het zoekend rondkijken, terwijl de toepassingsvoorwaarden van deze maatregel niet door deze wet werden aangepast. De inkijkoperatie in private informaticasystemen van artikel 89ter Sv. heeft dezelfde beperkte finaliteit als de klassieke inkijkoperatie van artikel 46quinquies Sv. en laat namelijk toe om gegevens terug te vinden in informaticasystemen die een link hebben met het misdrijf en bewijzen te verzamelen van de aanwezigheid van deze gegevens door een gerichte kopie van bepaalde data te nemen. De wet digitaal speurwerk heeft zelf het beslag, onder strikte voorwaarden, tijdens de inkijkoperatie voor voorwerpen waarvan een onderzoek ter plaatse niet mogelijk is, mogelijk gemaakt.\footnote{Artikel 46quinquies, §5 Sv.} Ook betreffende de tapmaatregel van artikelen 90ter e.v. Sv. heeft het artikel 17 van de wet digitaal speurwerk aanpassingen aangebracht die als zeer verregaand kunnen worden omschreven. Deze maatregel werd sterk uitgebreid door de wet zodat het huidig artikel het nu toelaat “niet voor het publiek toegankelijke communicatie of gegevens van een informaticasysteem of een deel ervan met technische hulpmiddelen onderscheppen, er kennis van nemen, doorzoeken en opnemen of de zoekning in een informaticasysteem of een deel ervan uitbreiden” onder de toepassingsvoorwaarden en in de
situaties opgesomd in de wet.\textsuperscript{213} Op basis van dit artikel is het nu dus mogelijk voor de speurders, mits machtiging door de onderzoeksrechter, “informaticsystemen zoals laptops, smartphones, online fora, profielen en mailboxen heimelijk doorzoeken en de communicatie in real time opvolgen”.\textsuperscript{214}

5.3. De snelle bewaring van gegevens

Daarnaast heeft de wetgever ook de nieuwe onderzoeksmethode van snelle bewaring in artikel 39\textit{ter} Sv. door artikel 3 van de wet digitaal speurwerk ingevoegd, om tegemoet te komen aan de verplichtingen van artikel 16 en 17 van het Cybercrimeverdrag met betrekking tot de snelle bewaring en onthulling van gegevens. Deze maatregel laat aan iedere officier van gerechtelijke politie toe, om bij het opsporen van misdaden en wanbedrijven, “\textit{wanneer er redenen bestaan om aan te nemen dat gegevens die opgeslagen, verwerkt of overgedragen worden door middel van een informaticasysteem bijzonder kwetsbaar zijn voor verlies of voor wijziging, bij een met redenen omklede en schriftelijke beslissing aan een of meerdere natuurlijke personen of rechtspersonen bevelen de gegevens die in hun bezit zijn of waarover zij controle hebben te bewaren}”.\textsuperscript{215} Dit verleent niettemin geen rechtstreekse toegang voor de speurders tot de gegevens, omdat er enkel gevraagd wordt aan een persoon of een rechtspersoon om de gegevens gedurende een bepaalde termijn veilig te bewaren, maar brengt de speurders ertoe om beroep te doen op andere onderzoeksdaten zoals de huiszoeking, het databeslag of de medewerkingsplicht uit artikelen 46\textit{bis} en 88\textit{bis} Sv.\textsuperscript{216} Deze medewerkingsplicht werd ook aangepast door de wet van 25 december 2016 door de incorporatie van de ruimere definitie van de aanbieders van elektronische communicatiediensten\textsuperscript{217} uit het Yahoo!-arrest van het Hof van Cassatie van 1 december 2015\textsuperscript{218} 219.

\textsuperscript{213} Artikel 90\textit{ter}, §1 Sv.
\textsuperscript{214} C. CONINGS en S. ROYER, “Vernieuwingen binnen het digitaal speurwerk”, \textit{Actua Leges} 2017/30.
\textsuperscript{215} Artikel 39\textit{ter}, §1 Sv.
\textsuperscript{216} C. CONINGS en S. ROYER, “Vernieuwingen binnen het digitaal speurwerk”, \textit{Actua Leges} 2017/30.
\textsuperscript{217} Ze worden in artikel 46\textit{bis}, §1 tweede lid omschreven als: “\textit{iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen}”.
\textsuperscript{219} C. CONINGS en S. ROYER, “Vernieuwingen binnen het digitaal speurwerk”, \textit{Actua Leges} 2017/30, p. 2.
5.4. De online infiltratie

Een andere belangrijke wijziging in het wettelijk kader voor de bestrijding van de informaticacriminaliteit is de invoering van artikel 46sexies Sv. door artikel 7 van de wet van 25 december 2016, die de online infiltratie als nieuwe opsporingsmethode regelt. Deze nieuwe methode, die in het volgende hoofdstuk grondig wordt bestudeerd, laat aan de procureur des Konings toe, mits de naleving van strikte voorwaarden, om de politiediensten te machtigen om op internet contact te onderhouden met personen waarover er ernstige aanwijzingen bestaan dat ze bepaalde misdrijven hebben gepleegd. Het betreft dus namelijk een bijwerking of modernisering van de klassieke infiltratie van artikel 47octies Sv. die aangepast is aan de technologische evolutie en de meerwaarde dat het kan brengen voor het onderzoek.
Hoofdstuk 2. De online infiltratie


In deze afdeling gaan we de nieuwe opsporingsmethode van de cyberinfiltratie die het licht heeft gezien met de wet van 25 december 2016 bestuderen. We gaan daarvoor eerst aandacht besteden aan de problemen die aanwezig waren voor dat de infiltratie mogelijk was voor de politiediensten op het internet, om daarna de nieuwe bepaling van artikel 46\textit{sexies} Sv.\footnote{Zie bijlage 4.} grondig te bestuderen.

Afdeling 1. Probleemstelling voor de invoering van de online infiltratie

1. Wettelijke hindernissen

Voor de invoering van artikel 46\textit{sexies} in het Wetboek van Strafvordering en de wijzigingen aangebracht door de wet van 25 december 2016 aan artikel 47\textit{octies} Sv. die de offline infiltratie regelt, mocht een politieagent slechts een duurzaam contact onderhouden, onder een fictieve identiteit, met één of meerdere personen wanneer “\textit{er ernstige aanwijzingen zijn dat zij strafbare feiten in het kader van een criminelle organisatie, zoals bedoeld in artikel 324bis van het Strafwetboek, of misdaden of wanbedrijven als bedoeld in artikel 90ter, §§ 2}
Zodra dat politieagenten verder gingen dan het aanwenden van een fictieve naam om de algemene sfeer op een openbaar chatplatform in het kader van een reactief onderzoek te peilen, en dus contact opnamen op een duurzame manier met andere personen, moesten ze aan de strikte voorwaarden van de infiltratie van artikel 47octies Sv., die ook van toepassing kon zijn op de cyberwereld, voldoen. Dit artikel kon dus geen geschikte regeling bieden voor de online infiltratie, omdat de politieambtenaren slechts contact konden opnemen met verdachten via het internet in het kader van een onderzoek van zeer ernstige misdrijven, en dus niet konden gebruik maken van de mogelijkheden die het internet hun bood om gemakkelijker in contact te komen met het crimineel milieu en zo het onderzoek vooruit te helpen, wanneer er niet aan alle strenge toepassingsvoorwaarden van artikel 47octies Sv. werd voldaan.

Bovendien was het ook niet toegelaten om beroep te doen op de bijzondere opsporingsmethode van infiltratie voor een periode die langer zou zijn dan drie maanden volgens artikel 47octies §3, 5\textsuperscript{o} Sv., maar die wel verlengbaar is volgens de paragraaf vijf van dit artikel. Deze beperking van de tijdsduur van de infiltratie zou de doelmatigheid van deze opsporingsmethode onderrichten omdat het tot een verdachte situatie zou kunnen leiden wanneer na de periode van drie maanden het niet mogelijk zou zijn om het onderzoek te sluiten en het fictief profiel zo maar zou moeten verdwijnen. Het doelwit van de infiltratie zou inderdaad kunnen vermoeden dat er onderzoek naar hem gedaan wordt en maatregelen nemen om deze te ondermijnen. Verder moest de procureur des Konings ook sowieso zijn toestemming geven in een afzonderlijke schriftelijke beslissing, volgens artikel 47octies §4 Sv., voor het plegen van misdrijven door de politiediensten, omdat de infiltratie niet mogelijk was zonder het begaan van het misdrijf van valsheid in informatica van artikel 210\textit{bis} Sw. of van het aannemen van een valse naam van artikel 231 Sw.\textsuperscript{24}

De regeling van artikel 47octies Sw. was dus te strikt en onvoldoende compleet om een aangepaste basis te kunnen bieden voor de infiltratie die uitsluitend op het internet moest geschieden. Het was namelijk moeilijk of onmogelijk om aan de politiediensten toe te staan om op basis van dit artikel op het internet in contact te komen met verdachten en

\textsuperscript{23} Artikel 47octies, §1 eerste lid Sv.

\textsuperscript{24} M. GIACOMETTI en P. MONVILLE, “Réseaux sociaux, anonymat et faux profils: vrais problèmes en droit pénal et de la procédure pénale”, in M. SALMON (eds.), Les réseaux sociaux et le droit, Bruxelles, Larcier, Coll. de la Conférence du Jeune Barreau de Bruxelles, 1\textsuperscript{e} éd., 2014, pp. 198-199.
bewijsmiddelen tegen hen in te winnen.\textsuperscript{225} De cyberinfiltratie had dus een aparte wettelijke regeling nodig, die minder strikt zou zijn dan de wettelijke regeling die voor offline infiltratie geldt, omdat het eenvoudiger is om de cyberinfiltratie achteraf te controleren en te beheersen door alle contacten met andere personen op het internet te registreren. Volgens de onderzoeksrechter Philippe Van Linthout, die een voorstander is van een lichte versie van de infiltratie, zijn er ook andere capaciteiten dan in de “real life” gevraagd van undercoveragenten, zoals het beheersen van een specifieke taalgebruik, om niet ontmaskerd te worden.\textsuperscript{226}

2. Waarde bewijsmateriaal verkregen door middel van een illegale infiltratie

We moeten ons dan ook afvragen wat de waarde is van het bewijsmateriaal verkregen door middel van een illegale cyberinfiltratie of een infiltratie die niet beantwoordt aan het wettelijk voorschrift van artikel 47\textit{octies} Sw. Volgens het Grondwettelijk Hof in zijn arrest van 19 juli 2007\textsuperscript{227}, vormt het niet-naleven van het wettelijk kader van de bijzondere opsporingsmethoden een schending van een wezenlijk vormvoorschrift van het strafprocesrecht, zodat het bewijs dat eruit voortvloeit als onrechtmatig moet worden beschouwd.\textsuperscript{228} Op grond van de Antigoonrechtspraak van het Hof van Cassatie van 2003, die ondertussen al een wettelijke basis heeft gekregen in artikel 32 V.T.Sv. moet een bewijs element dat op een onrechtmatige wijze is verkregen, slechts in drie gevallen buiten beschouwing worden gelaten: “hetzij wanneer de naleving van bepaalde vormvoorwaarden voorgeschreven wordt op straffe van nietigheid, hetzij wanneer de begane onrechtmatigheid de betrouwbaarheid van het bewijs heeft aangetast, hetzij wanneer het gebruik van het bewijs in strijd is met het recht op een eerlijk proces”.\textsuperscript{229} Het is dus mogelijk dat bewijsmateriaal dat wordt verkregen door middel van een illegale cyberinfiltratie wel als ontvankelijk wordt beschouwd, zelfs als deze op het eerste inzicht in strijd met het recht op een eerlijk proces wordt verkregen, omdat deze aan de subjectiviteit van een toetsing \textit{a posteriori} door de rechter ten aanzien van de gehele procedure wordt overgelaten. Deze lakse aanpak ten aanzien

\textsuperscript{226} D. LEESTMANS, “Er is te weinig bekommernis over cybercriminaliteit”, \textit{De Juristenkrant} 2015, afl. 12, p. 9.
\textsuperscript{227} GwH 19 juli 2007, nr. 105/2007.
van de ontvankelijkheid van opzettelijk onrechtmatig verkregen bewijsmateriaal werd bovendien bevestigd door het Hof van Cassatie in het arrest van 31 oktober 2006\textsuperscript{230}. Met deze rechtspraak wordt het strafprocesrecht steeds meer flexibel en minder strikt, zodat we ons konden afvragen als het nog nodig was om het wettelijk kader te respecteren, wanneer we weten dat de miskenn ing van de wettelijke voorschriften niet altijd negatieve gevolgen zullen hebben. Wijzigingen en aanpassingen van de wettelijke regeling van de infiltratie waren dus nodig om te vermijden dat de toepassing ervan te veel overgelaten wordt aan het willekeur.\textsuperscript{231}

Vóór de inwerkingtreding van de wet digitaal speurwerk op 17 januari 2017, bestond er dus geen wettelijk kader voor de infiltratie aangepast aan de technologische evolutie. Opsporingsdiensten deden te weinig beroep op de sociale media en op de voordelen die de nieuwe ICT-technologie hun boden. Aangezien de cyberinfiltratie een beduidend minder risicovol karakter inhoudt dan de offline infiltratie, was het dus meer dan gewenst om een nieuwe “light” versie van artikel 47\textit{octies} Sv. in te voeren, om tegemoet te komen aan de tekortkomingen die de regeling van de klassieke infiltratie biedt aan de online infiltratie.\textsuperscript{232}

\textbf{Afdeling 2. De online infiltratie van artikel 46\textit{sexies} van het Wetboek van Strafvordering}

Met de wet van 25 december 2016 werd er dus uiteindelijk een nieuw artikel 46\textit{sexies} in het Wetboek van Strafvordering ingevoerd, dat de wettelijke tekortkomingen beoogde te verhelpen door een wettelijke basis te geven aan de nieuwe maatregel van de cyberinfiltratie of de interactie die op het internet gebeurt.\textsuperscript{233}

Het begrip “internet” wordt in deze bepaling in de ruime zin begrepen en omvat zowel het niet-verborgen deel van het internet als het dark web.\textsuperscript{234} Volgens de huidige minister van Justitie Koen Geens moeten er voor deze infiltratie minder strenge voorwaarden gelden, omdat er hier in tegenstelling tot de klassieke infiltratie geen fysiek contact is tussen de infiltrant en de doelwitten van de infiltratie en omdat er sporen worden achter gelaten van de

\textsuperscript{232} C. CONINGS en P. VAN LINTHOUT, “Sociale media: een nieuwe uitdaging voor politie en justitie”, p. 225.
\textsuperscript{234} Memorie van Toelichting, Wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, \textit{Parl.St.}, Kamer, 2015-2016, nr. 54-1966/001, p. 36.
interacties tussen hen. Contacten tussen de infiltranten en de doelwitten zijn inderdaad transparanter volgens de heer Johan Delmulle, procureur-generaal bij het Hof van Beroep te Brussel, dan bij de infiltratie in de fysieke wereld omdat ze allemaal worden geregistreerd zonder enige selectie, in tegenstelling tot de offline infiltratie, tussen de niet-relevante informatie voor het onderzoek en de relevante passages die moeten worden uitgeschreven. Dit maakt het natuurlijk gemakkelijker om misbruiken te voorkomen en de rechten van verdediging te waarborgen, omdat het dossier ter inzage op de griffie ligt. Een registratie van de infiltratie in haar geheel zou niet mogelijk zijn in het kader van de offline infiltratie zonder de infiltranten in gevaar te brengen.

1. Toepassingsvoorwaarden

Online infiltratie zal slechts kunnen worden toegepast wanneer voldaan is aan de twee voorwaarden van de eerste paragraaf, lid één van artikel 46sexies Sv.

1.1. Het subsidiariteitsbeginsel

Eerst kan de cyberinfiltratie slechts aangewend worden in het kader van de opsporing van misdaden en wanbedrijven, “wanneer het onderzoek zulks vereist en de overige middelen van onderzoek niet lijken te volstaan om de waarheid aan de dag te brengen”. Dit vormt de subsidiariteitsvoorwaarde waaraan de infiltratie is ongedaan geworden. Omdat de infiltratie in sommige gevallen aanzienlijke gevolgen en een inmenging in de persoonlijke levenssfeer van de personen die ermee betrokken zijn, kan meebrengen, is het van belang om deze maatregel slechts te gebruiken, wanneer er geen andere opsporingsmethode die minder indringend is, aangewend kan worden.

1.2. Het materieel toepassingsgebied

Ten tweede, kan de procureur des Konings slechts de politiediensten machtigen “om op het internet, desgevallend onder een fictieve identiteit, contact te onderhouden met een of meerdere personen waarvan er ernstige aanwijzingen zijn dat zij strafbare feiten die een

238 Artikel 46sexies, §1 eerste lid Sv.
correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben, plegen of zouden plegen”.

Uit de formulering van de bepaling kunnen we afleiden dat het toepassingsgebied van de infiltratie ruim is en dat het zowel in het kader van een proactief als een reactief onderzoek mag worden aangewend. Zoals Franssen en Tosza het hebben doen opmerken, zou dit vragen kunnen doen oproepen ten aanzien van het artikel 28bis §2 Sv.

Inderdaad, volgens dit artikel kan het opsporingsonderzoek zich slechts uitstrekken tot het proactieve onderzoek wanneer er een redelijk vermoeden van te plegen of reeds gepleegde, maar nog niet aan het licht gebrachte strafbare feiten bestaat, “en die worden of zouden worden gepleegd in het kader van een criminele organisatie, zoals gedefinieerd door de wet, of misdaden of wanbedrijven als bedoeld in artikel 90ter, §§ 2, 3 en 4, uitmaken of zouden uitmaken”. Deze voorwaarden vinden we namelijk niet terug in artikel 46sexies Sv.

aangezien de misdrijven slechts moeten kunnen worden bestraft met een correctionele hoofdgevangenisstraf van één jaar of met een zwaardere straf om het onderwerp te kunnen maken van een infiltratie in het kader van een proactief of reactief onderzoek. Het toepassingsgebied is dus zeer ruim, omdat er zelfs niet vermeld wordt dat de minimale gevangenisstraf een jaar moet bedragen, zodat het volstaat dat de rechter volgens de wettelijke bepalingen gerechtigd is om een gevangenisstraf van één jaar uit te spreken, wat tot gevolg heeft dat er een brede waaier van misdrijven onder de toepassing van artikel 46sexies Sv. kunnen vallen.

Omdat misdrijven, die zelf bestraft kunnen worden door een zeer korte correctionele gevangenisstraf, in aanmerking kunnen komen voor de aanwending van de infiltratieoperatie, is deze bepaling het voorwerp geweest van kritiek in het verslag van de eerste lezing namens de Commissie voor de justitie van het wetsontwerp. Het zou volgens Kamerlid Özlem Özen (PS) en de heer Manu Lambert, vertegenwoordiger van de Liga voor Mensenrechten, in strijd zijn met het evenredigheidsbeginsel, gewaarborgd door het artikel 8.2 EVRM, omdat het zou kunnen betekenen dat bijzonder nadelige technieken voor de individuele vrijheden zouden kunnen worden bevolen voor een groot deel van de in het Strafwetboek opgenomen misdrijven, zoals een gewone diefstal, terwijl zulke technieken eerder zouden moeten worden voorbehouden voor zware misdrijven die de inmenging en de aantasting van de fundamentele rechten van de burgers zouden rechtvaardigen. Zij pleiten dan voor de optrekking van de

239 Artikel 46sexies, §1 eerste lid Sv.
240 V. FRANSEN en S. TOSZA, “Vers plus de droits pour le justiciable sur internet ? Un nouveau cadre légal pour lutter contre la criminalité dans la société de l’information”, p. 239.
drempel. Een andere kritiek die geuit wordt door mevrouw Özlem Özen tegenover deze indringende technieken, is dat ze veel kosten aan de Staat, terwijl het al moeilijk is voor deze om de kosten verbonden met zulke methoden te dekken. Ook volgens de heer Denis Bosquet, vertegenwoordiger van AVOCATS.be, lijkt deze verruiming van het toepassingsgebied “gevaarlijk en past in een repressievere stroming die een veel grotere aantasting vormt van onze fundamentele rechten”.

1.3. Voorbeelden

In de memorie van toelichting worden er concrete voorbeelden gegeven van situaties waar de politiediensten zich kunnen beroepen op de online infiltratie. De procureur des Konings kan bijvoorbeeld een cyberinfiltratie bevelen, wanneer de politie over ernstige aanwijzingen beschikt dat een bepaalde persoon online een handel heeft opgezet in drugs, kinderpornografie of nog in verboden vuurwapens. De infiltratie zou in dit geval de politiediensten toestaan om bewijsmateriaal te verzamelen en de misdadder en eventuele mededaders te kunnen identificeren. Het zou ook mogelijk zijn om de cyberinfiltratie te gebruiken, wanneer we ons in aanwezigheid van het misdrijf van grooming bevinden en waarbij het onmogelijk is om de profiel van de kinderlokker te lokaliseren. Politiediensten zouden dan een profiel met een fictieve identiteit kunnen opmaken, zonder dat deze expliciet, misleidend of provocatief zou zijn, om de aandacht van de kinderlokker te trekken en met hem in contact te raken om informatie te verkrijgen die hen zouden toestaan om hem te identificeren.

2. De machtiging tot infiltratie

2.1. Vormvoorwaarden

De online infiltratie kan slechts bevolen worden door de procureur des Konings. Deze moet dan een voorafgaandelijke en met redenen omklede schriftelijk machtiging, die geldig is

---

244 Dit misdrijf wordt bestraft in artikel 377quater Sw.
voor een termijn van drie maanden onverminderd hernieuwing, verlenen om de infiltratie mogelijk te maken.\footnote{Articles 46sexies, §2 Sv.} De procureur des Konings moet dus expliciet motiveren dat aan toepassingsvoorwaarden van de online infiltratie is voldaan. De verlenging van deze termijn is mogelijk zolang er nog steeds wordt voldaan aan de voorwaarden uit de eerste paragraaf van het artikel.\footnote{Memorie van Toelichting, Wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, Parl.St., Kamer, 2015-2016, nr. 54-1966/001, p. 41.} Verder wordt er nog bepaald in de tweede paragraaf, dat het kan gebeuren dat in spoedeisende gevallen het niet mogelijk is om een machtiging schriftelijk te verkrijgen, zodat er dan een mondelinge machtiging mogelijk is wanneer deze zo vlug mogelijk in een schriftelijke vorm bevestigd en gemotiveerd wordt.

In het kader van een gerechtelijk onderzoek, zal het echter de onderzoeksrechter zijn die de machtigingen tot de online infiltratie zal verlenen en de procureur des Konings die belast zal zijn met de tenuitvoerlegging ervan overeenkomstig paragraaf vijf van het artikel.

2.2. Persoonlijke interacties die de verificatie van misdrijven of de arrestatie van verdachten tot doel hebben en internetpatrouilles

Er wordt in het vierde lid van de eerste paragraaf van het artikel verduidelijkt dat het artikel niet van toepassing is op de persoonlijke interactie die de verificatie van misdrijven tot doel heeft, door bijvoorbeeld contact op te nemen met een verdachte om na te kijken als deze gestolen en gezocht goederen aanbiedt, of die de arrestatie van verdachten tot doel heeft, door bijvoorbeeld met hem een afspraak vast te leggen. Hiervoor is er dus geen voorafgaande toestemming van de procureur des Konings nodig. De situatie is wel anders, wanneer ze daarvoor gebruik maken van een geloofwaardige fictieve identiteit. In zulk geval, zal er toch aan de voorwaarden van artikel 46sexies Sv. moeten voldaan worden. Daarnaast vallen de internetpatrouilles ook niet onder de toepassing van dit artikel, omdat deze al mogelijk waren vóór de wet van 25 december 2016, onder dezelfde voorwaarden dan diegene die gelden voor de patrouilles in de fysieke wereld.\footnote{Deze zijn beperkt tot de publiek toegankelijke plaatsen voor de politie van art. 26 WPA zoals uitgelegd in het deel I, hoofdstuk 2, afdeling 2.} 249. Die verduidelijking in het artikel “strekt ertoe te voorkomen dat een situatie wordt gecreëerd waarin de slagvaardigheid van de politiediensten wordt beperkt ten opzichte van wat thans bestaat, zowel op internet als in de fysieke

---

\footnote{V. FRANSSEN en S. TOSZA, “Vers plus de droits pour le justiciable sur internet ? Un nouveau cadre légal pour lutter contre la criminalité dans la société de l’information”, p. 238.}
wereld. Verder worden er in de memorie van toelichting voorbeelden gegeven van persoonlijke interacties die enkel een gerichte verificatie en arrestatie tot direct doel hebben. Voor wat de eerste soort interacties betreft, wordt er het voorbeeld gegeven van politiediensten die zich baseren op de zoekertjes op tweedehandsverkoopsites om verdachte verkopen op te sporen. Ze kunnen dan een e-mail sturen naar de verkoper om een afspraak met hem te maken om het goed te zien zonder erop te wijzen dat zij politieambtenaar zijn en zonder een fictieve identiteit aan te nemen. Voor wat de persoonlijke interacties die enkel een arrestatie tot doel hebben betreft, wordt er het voorbeeld gegeven van een politieambtenaar die afspraken onder valse voornemens met een internetgebruiker om hem fysiek te ontmoeten, om deze te arresteren. De arrestatie moet hier een direct doel zijn van de interactie, en niet pas nadien het verzamelen van bewijsmateriaal door de interacties voorkomen, en moet rechtmatig zijn omdat artikel 46sexies Sv. geen nieuwe rechtsbasis voor de arrestatie van een verdachte verschaf._251_

3. Bevoegde infiltranten

In het tweede lid van de eerste paragraaf van het artikel wordt er verklaard dat de Koning in een koninklijke besluit de regels en voorwaarden zal bepalen, waaronder de opleiding met het oog op zowel het verzekeren van het goede verloop van de onderzoeken als de bescherming van de persoonlijke levenssfeer, die van toepassing zijn voor de aanwijzing van de politiediensten bevoegd voor de uitvoering van de online infiltratie. Oorspronkelijk werd de aanwijzing van de bevoegde politiediensten in het voorontwerp gedelegeerd aan de minister van Justitie, maar de Raad van State merkte op, dat dit niet toegestaan kon worden en dat de aanwijzing vastgelegd moest zijn in de wet. Uiteindelijk heeft de regering besloten om de bepaling van de voorwaarden en de modaliteiten van de aanwijzing van de bevoegde politiediensten over te laten aan de Koning. Deze bevoegdheid wordt dus niet meer voorbehouden voor de gespecialiseerde eenheden, met name de leden van het undercoverteam bij de Directie Special Units (DSU), zoals het geval is bij de offline infiltratie, maar kan ook uitgevoerd worden door speciaal opgeleide speurders gespecialiseerd in een welbepaald


criminaliteitsdomein zoals terrorisme, mensenhandel, wapenhandel of zedendelicten. Dit geeft de onderzoekers die in deze materie actief zijn, zoals de onderzoekers van internetrecherche-eenheden, volgens de heer Walter Coenraets, diensthofd van de Federal Computer Crime Unit (FCCU), meer armsglag om snel en op een gerichte manier vooruitgang te boeken in de opsporing van verdachten van misdrijven via het internet.

Indien het strikt noodzakelijk is voor het welslagen van zijn opdracht, kan de ambtenaar van de politiediensten, die bedoeld zijn in het tweede lid van de eerste paragraaf, in uitzonderlijke omstandigheden en mits uitdrukkelijke machtiging van de procureur des Konings, kortstondig een beroep doen op de deskundigheid van een persoon die niet tot de politiediensten behoort voor een welbepaalde operatie. Deze mogelijkheid is van uiterste belang als we weten dat het gebrek aan specialisatie volgens de Belgische wetgever de voornaamste reden van inefficiënte bestrijding van cybercriminaliteit is. De infiltrant moet dus over voldoende technische kennis, zoals bijzondere kennis over cryptografie, om het vertrouwen van de criminele groepen in sterke mate te winnen.

De infiltrant moet dus over voldoende technische kennis, zoals bijzondere kennis over cryptografie, om het vertrouwen van de criminele groepen in sterke mate te winnen. De deskundigheid kan ook “bijvoorbeeld bestaan uit vreemde talen” in bepaalde situaties. Zoals de memorie van toelichting het verder toelicht, betekent het niet dat de uitvoering van de maatregel aan de politiediensten zou worden gedelegeerd. Hij uitvoert slechts de handelingen onder rechtstreekse controle van de bevoegde infiltrant. Er worden in het parlementaire document enige voorbeelden gegeven van waar er een beroep op een deskundige zou kunnen worden gedaan. Politiediensten zouden bijvoorbeeld zich kunnen laten bijstaan door een taaldeskundige wanneer ze zich in een milieu begeven waar er een specifieke taal wordt gehanteerd of door een specialist wanneer ze hoogtechnologische kennis nodig hebben in het kader van een onderzoek in een hackersmilieu.

---

255 Artikel 46sexies, §1 derde lid Sv.
4. Het plegen van misdrijven door de infiltranten

4.1. De strafuitsluitende verschoningsgrond

Een belangrijke problematiek die gelinkt is aan de uitvoering van de offline infiltratie is die van het plegen van misdrijven door de politiediensten in het kader van hun opdracht. Daarvoor bepaalt de wetgever in paragraaf drie van artikel 46sexies Sv dat “blijven vrij van straf de politieambtenaren die, in het kader van hun opdracht en met het oog op het welslagen ervan of ter verzekering van hun eigen veiligheid of deze van andere bij de maatregel betrokken personen, strikt noodzakelijke strafbare feiten plegen, mits uitdrukkelijk akkoord van de procureur des Konings”. Zelfs als de online infiltratie niet wordt omschreven als een bijzondere opsporingsmethode, wordt er dus in het artikel een nieuwe strafuitsluitende verschoningsgrond voorzien, die gelijkwaardig is aan diegene die van toepassing is op de bijzondere opsporingsmethoden in artikel 47quinquies, tweede paragraaf Sv. Het provocatieverbod van artikel 30 V.T.Sv., die we infra nauwkeuriger gaan bekijken in het derde deel, vormt niettemin een begrenzing van de vrijheid die aan de politiediensten wordt toegekend.\textsuperscript{260} Meerdere voorbeelden van strafbare feiten die gemachtigd kunnen worden, worden gegeven in de memorie van toelichting zoals het gebruik maken van technieken aan de hand waarvan de verdachte gelokaliseerd kan worden of berichten sturen op een forum van extremisten of radicalen, waar er bijvoorbeeld racistische uitlatingen worden gedaan.\textsuperscript{261}

Deze strafuitsluitende verschoningsgrond is tevens ook van toepassing “op de personen die aan de uitvoering van deze opdracht noodzakelijke en rechtstreekse hulp of bijstand hebben verleend” en op de burgerdeskundigen bedoeld in §1, derde lid.\textsuperscript{262} De magistraat die, met inachtneming van het Wetboek van Strafvordering, de machtiging voor het plegen van een misdrijf in het kader van de uitvoering van de online infiltratie verleent aan een politieambtenaar of aan een burgerdeskundige blijft ook vrij van straf volgens het vierde lid van de derde paragraaf van dit artikel.

Verder moeten de strafbare feiten die de politiediensten plegen aan een proportionaliteitsbeginsel voldoen, zodat ze niet ernstiger mogen zijn “dan die waarvoor de


\textsuperscript{262} Artikel 46sexies, §3 derde lid Sv.
maatregel wordt aangewend en moeten noodzakelijkerwijze evenredig zijn met het nagestreefde doel". Volgens de vertegenwoordiger van de Liga voor Mensenrechten en de Raad van State in zijn advies van 9 mei 2016, moet er absoluut limitatief worden aangegeven welke misdrijven wel toegelaten kunnen worden. De Raad van State bevraagt zich bovendien in zijn advies, waarom er geen beperking bestaat van de toegelaten misdrijven tot feiten die zich uitsluitend in de cyberspace voordoen. Als antwoord beweert de regering, dat het niet wenselijk zou zijn om de strafbare feiten te beperken. Om zijn standpunt te ondersteunen, wordt het voorbeeld van het opmaken van een vals document dat ingescand wordt om doorgestuurd te worden aan de verdachte, gebruikt omdat het een strafbaar feit is, dat zich niet in cyberspace heeft voorgedaan, maar dat wel voorafgaand is aan het contact met de verdachte.

4.2. De voorafgaandelijke toestemming

De politieambtenaren en de andere personen die hierboven zijn vermeld, mogen niettemin niet zomaar misdrijven plegen tijdens de uitvoering van de cyberinfiltratie. Ze moeten inderdaad voorafgaande aan de uitvoering van de maatregel op een schriftelijke manier melden aan de procureur des Konings de misdrijven voornemens zijn te plegen. Het kan gebeuren dat het in bepaalde situaties voor hen onmogelijk is om de procureur des Konings op voorhand in kennis te brengen van de misdrijven die ze gaan plegen. In dergelijke gevallen is het toegelaten dat de politieambtenaren de procureur des Konings onverwijld achteraf in kennis stellen en hem een schriftelijke bevestiging geven van de misdrijven die zij, of de burgerdeskundigen, hebben gepleegd.

De procureur des Konings moet daarna in een afzonderlijke en schriftelijke beslissing, die bewaard wordt in een vertrouwelijk dossier, onderhevig aan het inzagerecht en controle door de Kamer van inbeschuldigingstelling en de onderzoeksrechter, en waarvan de inhoud onder het beroepsgeheim valt, vermelden welke misdrijven de politiediensten en de

263 Artikel 46sexies, §3 tweede lid Sv.
267 Artikel 46sexies, §3 vijfde en zesde lid Sv.
burgerdeskundigen in het kader van de infiltratie, die door hem is bevolen, kunnen plegen.\textsuperscript{268} Ook in het kader van een gerechtelijk onderzoek waar de infiltratie bevolen wordt door de onderzoeksrechter, moet de procureur des Konings de misdrijven die kunnen worden gepleegd, vermelden in een afzonderlijke en schriftelijke beslissing.\textsuperscript{269} Het is om te vermijden dat de procedure te zwaar wordt dat er in het kader van de uitvoering van de cyberinfiltratie niet automatisch een vertrouwelijk dossier moet worden opgemaakt, maar slechts wanneer de procureur des Konings misdrijven machtigt of een burgerdeskundige inschakelt. In de memorie van toelichting wordt er bepaald dat een omzendbrief van het College van procureurs-generaal nadere richtlijnen kan vaststellen van de omstandigheden waarin het aangewezen is om een burgerdeskundige in te schakelen of misdrijven te machtigen.\textsuperscript{270} Zoals Franssen en Tosza het hebben opgemerkt, kunnen we veronderstellen dat het over andere misdrijven gaat dan het misdrijf van het gebruik van een fictieve identiteit van artikel 231 Sw. anders zou er voor bijna alle cyberinfiltraties een vertrouwelijk dossier moeten worden opgemaakt.\textsuperscript{271}

4.3. Kritiek

Het feit dat er misdrijven mogen worden gepleegd door de politiediensten of de burgerdeskundigen, zonder voorafgaand akkoord van de procureur des Konings, wordt door de Liga voor Mensenrechten bekritiseerd. De voorzitter van de Liga voor Mensenrechten, de heer Jos Vander Velpen, betuigt bovendien zijn bezorgdheid ten aanzien van het feit “dat er slechts een vertrouwelijk dossier zal worden aangelegd, indien de politiediensten werden gemachtigd om misdrijven te plegen of er een burgerdeskundige werd ingeschakeld”, omdat het gebrek aan veel controlemogelijkheden ertoe zou kunnen leiden, dat de infiltranten handelingen stellen, die zich op de grens bevinden van wat men als infiltratie zou kunnen beschouwen.\textsuperscript{272} De Raad van State, afdeling wetgeving, heeft ook zijn bezorgdheid geuit tegenover deze bepaling. Het zou namelijk de voorafgaande controle door de procureur des Konings uithollen. De regering beantwoordt dit door te verwijzen naar de memorie van toelichting bij de BOM-wet van 6 januari 2003, omdat de regeling quasi identiek is aan de

\textsuperscript{268} Artikel 46\textit{sexies}, §3 zevende lid Sv.
\textsuperscript{269} Artikel 46\textit{sexies}, §5 tweede lid Sv.
\textsuperscript{271} V. \textsc{Franssen} en S. \textsc{Tosza}, “Vers plus de droits pour le justiciable sur internet ? Un nouveau cadre légal pour lutter contre la criminalité dans la société de l’information”, p. 241.
\textsuperscript{272} Verslag van de eerste lezing namens de Commissie voor de Justitie uitgebracht door G. \textsc{Calomne} en G. \textsc{Uytttersprot}, \textit{Parl.St.}, Kamer, 2016-2017, nr. 54-1966/006, p. 68.
regeling van artikel 47quinquies Sv. en dat de noodzaak om strafbare feiten te plegen zonder voorafgaande machtiging door de procureur des Konings dezelfde is dan bij de offline infiltratie. Er wordt namelijk verklaard dat “bij infiltratie niet steeds te voorzien is welke handelingen nodig zullen zijn, wil de infiltrant zich ten behoeve van zijn opdracht geloofwaardig maken als deelnemer aan een criminele organisatie. Zijn veiligheid kan op het spel staan, als hij (onverwachte) opdrachten weigert die een deelnemer in de organisatie in zijn positie niet behoort te weigeren (...) Het volstaat dat hij onverwacht door de criminele organisatie wordt uitgenodigd een verdachte transactie of een straftoestand feit daadwerkelijk zelf bij te wonen, opdat hij zich in een positie van potentieel medeplichtigheid aan misdrijven bevindt. In dergelijke gevallen is het onvermijdelijk dat de politieambtenaar strafbare feiten pleegt.”

Door het feit dat politiediensten zich soms in een onverwachte situatie kunnen bevinden waar ze misdrijven moeten plegen, vragen Franssen en Tosza zich af in welke mate de online infiltratie een “light” versie van de offline infiltratie is. Beide soorten infiltraties kunnen inderdaad leiden tot verregaande situaties en gevolgen. De online infiltratie kan tot problemen leiden, omdat het een soepel regime van een “light” infiltratie combineert met sommige gelegenheden die het behoud van de strikkere bepaling van de offline infiltratie.

Daarenboven, verwijst de regering nog naar de memorie van toelichting van de BOM-wet om te bewijzen dat de procureur des Konings zijn recht op een controle a posteriori van de gepleegde misdrijven heeft behouden. De procureur des Konings zou “de gepleegde strafbare feiten beoordelen in het licht van het welslagen van de operatie en de veiligheid van de politieambtenaar of andere bij de operatie betrokken personen. Mocht de magistraat van oordeel zijn dat de gepleegde strafbare feiten het kader van de opdracht of van de bijzondere opsporingsmethoden volledig te buiten gaan of werkelijk onrechtmatig en onaanvaardbaar zijn, zal hij hieraan het strafrechtelijk gevolg, dat hij passend acht, verlenen.”

276 Adv. RvS nr. 59.199/3 bij het voorontwerp van wet betreffende de verbetering van de bijzondere onderzoeksmethoden met betrekking tot internet en elektronische communicaties, Parl.St., Kamer, 2015-2016, nr. 54-1966/001, p. 139; Memorie van Toelichting, Wetsontwerp betreffende de bijzondere
5. Het proces-verbaal en de opnames van de contacten

In paragraaf vier van artikel 46sexies Sv. wordt er bepaald dat de officier van de gerechtelijke politie die belast is met het onderzoek, een proces-verbaal van de verschillende fasen in de uitvoering van de cyberinfiltratie en van de relevante contacten moet opstellen. De contacten die de politiediensten onderhouden met de doelwitten van de infiltratie moeten met de passende technische middelen geregistreerd worden. Het proces-verbaal en de opnames van de contacten moeten allebei, voor de laatste al dan niet in een digitale vorm, uiterlijk na het beëindigen van de maatregel bij het strafrechtelijk dossier gevoegd worden. Het is ook mogelijk dat de opnames van de contacten ter griffie worden neergelegd in plaats van toegevoegd te zijn aan het dossier.

De registratie van alle contacten, en dus de garantie van transparantie a posteriori, vormt een essentieel element van de online infiltratie. Het proces-verbaal vormt in zekere zin een samenvatting van alle delen van de opnames van de contacten die de officier van de gerechtelijke politie, onder het toezicht van de procureur des Konings, relevant acht.

Volgens de regering moet het gemeen recht hier van toepassing zijn, zodat de rechtstreeks belanghebbende, overeenkomstig de artikelen 21bis Sv. in het kader van de opsporingsonderzoek en 61ter Sv. in het kader van het gerechtelijk onderzoek, “de procureur des Konings of de onderzoeksrechter [kan] verzoeken om inzage te krijgen in het dossier of er een afschrift van te ontvangen”. Daarnaast is het steeds mogelijk om aan de procureur des Konings, of aan de onderzoeksrechter op grond van artikel 61quinquies Sv., een willig verzoek te richten tot de overschrijving of de weergave in het proces-verbaal van bijkomende delen van de geregistreerde contacten.

---

277 Memorie van Toelichting, Wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, Parl.St., Kamer, 2015-2016, nr. 54-1966/001, p. 44.

278 Memorie van Toelichting, Wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, Parl.St., Kamer, 2015-2016, nr. 54-1966/001, p. 44.
Hoofdstuk 3. De klassieke offline infiltratie

De offline infiltratie werd ingevoegd en geregeld in artikel 47octies van het Wetboek van Strafvordering\textsuperscript{279} door artikel 4 van de BOM-wet van 6 januari 2003 in de onderafdeling 4 van de nieuwe afdeling III “De bijzondere opsporingsmethoden” van het hoofdstuk IV van het eerste boek. In tegenstelling tot de online infiltratie vormt de klassieke infiltratie een bijzondere opsporingsmethode, vandaar dat het strikter wordt geregeld dan de offline infiltratie.

Volgens de eerste paragraaf van het artikel 47ter Sv. kunnen de bijzondere opsporingsmethoden slechts worden aangewend “in het kader van een opsporingsonderzoek of een gerechtelijk onderzoek, onder de controle van het openbaar ministerie (…), met als doel het vervolgen van daders van misdrijven, het opsporen, verzamelen, registreren en verwerken van gegevens en inlichtingen op grond van ernstige aanwijzingen van te plegen of reeds gepleegde, al dan niet aan het licht gebrachte strafbare feiten”. Deze koppeling van de bijzondere opsporingsmethoden aan het opsporings- en het gerechtelijk onderzoek, om deze te onderwerpen aan de controle en de verantwoordelijkheid van de magistratuur, verklaart zich door de vrees van het Parlement dat deze anders zouden worden gebruikt om inlichtingen te verzamelen tegen bepaalde personen of groepen, “zonder duidelijke kortetermijndoelstellingen en zonder veel verantwoording qua duur, keuze of beoogd resultaat”\textsuperscript{280}. De bijzondere inlichtingenmethoden beschikken tevens, zoals de bijzondere opsporingsmethoden, over een aparte regeling in de wet op de Bijzondere Inlichtingenmethoden van 4 februari 2010\textsuperscript{281}.

1. Toepassingsvoorwaarden

In de eerste paragraaf van artikel 47octies Sv. wordt de infiltratie beschreven, in de zin van het Wetboek van Strafvordering, als “het door een politieambtenaar, infiltrant genoemd, 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犯罪ele organisatie, zoals bedoeld in artikel 324bis van het Strafwetboek, of misdaden of wanbedrijven als bedoeld in artikel 90ter, §§ 2 tot 4 plegen of zouden plegen”.

\textsuperscript{279} Zie bijlage 5.


\textsuperscript{281} Wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten, B.S. 10 maart 2010.
Zoals De Nauw en Schuermans het doen opmerken, is er geen definitie of verduidelijking terug te vinden in de wet van wat een duurzaam contact is. Er moet dus worden gekeken naar de memorie van toelichting om een uitleg te vinden. Het begrip “duurzaam contact” moet worden begrepen in verhouding met de intensiteit van de onderhouden contacten. Het zou dus willen zeggen dat een eenmalig contact tussen een politieambtenaar en een verdachte, onder een fictieve identiteit, niet als een infiltratie kan worden beschouwd.282

1.1. Het proportionaliteitsbeginsel

Deze definitie van de infiltratie houdt een proportionaliteitsbeginsel in. Dit betekent dat de operatie slechts kan worden aangewend ten aanzien van zwaardere misdrijven in het kader van een criminele organisatie en de misdrijven die een opzoeking in een informaticasysteem of een tapmaatregel rechtvaardigen. Het betreft namelijk dezelfde misdrijven die de toepassing van een proactief onderzoek van artikel 28bis, §2 Sv. rechtvaardigen. Dit wordt verantwoord door het feit dat de infiltratie gepaard gaat met een hoge graad van inbreuk op de individuele rechten en vrijheden.283

1.2. Het subsidiariteitsbeginsel

Daarnaast is het ook slechts mogelijk om deze bijzondere opsporingsmethode te gebruiken “wanneer het onderzoek zulks vereist en de overige middelen van onderzoek niet lijken te volstaan om de waarheid aan het licht te brengen”.284 Deze subsidiariteitsvoorwaarde wordt verder uitgelegd in de memorie van toelichting van de BOM-wet. Het houdt namelijk in dat de bijzondere opsporingsmethoden “dermate ingrijpend zijn dat eerst moet nagegaan worden of hetzelfde resultaat niet door andere middelen van onderzoek kan bereikt worden”.285 Er wordt niettemin niet vereist dat de klassieke opsporingsmethoden daadwerkelijk worden gebruikt zonder doeltreffende resultaten te behalen, voordat er gebruik wordt gemaakt van de bijzondere opsporingsmethoden. Dit betekent dat het mogelijk is om beroep te doen op de infiltratieanneer er een hoger belang

283 Memorie van Toelichting, Wetsontwerp betreffende de bijzondere opsporingsmethode en enige andere onderzoeksmethoden, Parl.St., Kamer, 2001-2002, nr. 50-1688/001, p. 35.
284 Artikel 47tocties, §2 eerste lid Sv.
op het spel staat, zoals het redden van mensenlevens, of wanneer er een grote tijdswinst kan worden geboekt door het uitvoeren van een bijzondere opsporingsmethode.\(^\text{286}\)

2. **De machtiging tot infiltratie**

2.1. **Vormvoorwaarden**

Deze bijzondere opsporingsmethode wordt door de procureur des Konings gemachtigd. De machtiging moet schriftelijk zijn en moet de ernstige aanwijzingen van het strafbaar feit die de infiltratie wettigt, de redenen waarom de infiltratie onontbeerlijk is om de waarheid aan het licht te brengen, de naam of anders een zo nauwkeurig mogelijke beschrijving van de persoon of de personen waarvan er ernstige aanwijzingen zijn, dat zij strafbare feiten die deze operatie rechtvaardigen plegen of zouden plegen indien deze gegevens bekend zijn, de wijze waarop aan de infiltratie ten uitvoer zal worden gebracht, de periode tijdens welke de infiltratie kan worden uitgevoerd en de naam en de hoedanigheid van de officier van gerechtelijke politie, die de leiding heeft over de uitvoering van de infiltratie, vermelden.\(^\text{287}\)

De machtiging mag niet worden verleend voor een periode langer dan drie maanden te rekenen van de datum van de machtiging\(^\text{288}\) en kan zowel aangewend worden in het kader van een reactieve als een proactief onderzoek, zoals omschreven in artikel 28bis, §2 Sv. In dit laatste geval moet de machtiging van de procureur des Konings “het redelijk vermoeden van te plegen of reeds gepleegde maar nog niet aan het licht gebrachte strafbare feiten, en de bijzondere aanwijzingen met betrekking tot de elementen omschreven in deze laatste bepaling, die de infiltratie wettigen” vermelden.\(^\text{289}\)

In bepaalde gevallen zal het nochtans niet mogelijk zijn om een voorafgaandelijke schriftelijke machtiging van de procureur des Konings te verkrijgen. In zulke spoedeisende gevallen heeft de wetgever toegelaten dat de procureur des Konings een mondelinge machtiging tot infiltratie verstrekt. Deze zal achteraf wel zo vlug mogelijk moeten worden bevestigd in een schriftelijke vorm.\(^\text{290}\)

---

287 Artikel 47octies, §3 Sv.
288 Artikel 47octies, §3, 5° Sv.
289 Artikel 47octies, §3, 1° Sv.
290 Artikel 47octies, §5 Sv.
In het kader van een gerechtelijk onderzoek is het de onderzoeksrechter die de machtiging tot infiltratie verleent overeenkomstig artikel 56bis Sv. De procureur des Konings zal daarentegen belast zijn met de tenuitvoerlegging van de machtiging.291

2.2. Latere wijziging, aanvulling of verlenging van de machtiging

De machtiging kan nog steeds achteraf, wanneer het op gemotiveerde wijze gebeurt, worden gewijzigd, aangevuld of verlengd door de procureur des Konings. Infiltratieoperaties kunnen dus zowel voor een lange periode als een korte periode worden aangewend. In de memorie van toelichting wordt er nadruk gelegd op het feit dat de risicograad van een infiltratie niet vanzelfsprekend proportioneel is aan de tijdsduur van de infiltratie. De parlementaire tekst wijst er ons op dat andere factoren en feiten zoals “het gebrek aan duidelijke doelstellingen en richtlijnen voor de infiltrant, zowel uitgaande van de politonale hiërarchie, als van de magistraat, die de leiding, het gezag en de controle over de aanwending van de infiltratie heeft” de infiltratie uiteraard ook gevaarlijk maken.292 In ieder geval moet er nog aan de voorwaarden van de drie eerste paragrafen van het artikel worden voldaan voordat de procureur des Konings gebruik kan maken van deze mogelijkheden. Daarnaast, blijft het ook te allen tijde mogelijk voor de procureur des Konings om zijn machtiging in te trekken.293

2.3. Politionele onderzoekstechnieken

De procureur des Konings kan ook “de politiediensten machtigen om, binnen het wettelijk kader van een infiltratie en met inachtneming van de finaliteit ervan, bepaalde politonale onderzoekstechnieken aan te wenden. De Koning bepaalt bij een in de Ministerraad overlegd besluit, op voordracht van de minister van Justitie en na advies van het College van procureurs-generaal, deze politonale onderzoekstechnieken”.294 De memorie van toelichting wijst op het feit dat deze onderzoekstechnieken niet dezelfde zijn als de bijzondere opsporingsmethoden, maar slechts als ondersteuning van de bijzondere opsporingsmethoden mogen worden beschouwd, en dus in dit geval toegepast kunnen worden om de doelen van de infiltratieoperatie helpen te verwezenlijken, zodat ze in hetzelfde wettelijk kader als de infiltratie operatie worden aangewend en dat de toepassing van de beginselen die

291 Artikel 47octies, §7 Sv.
292 Memorie van Toelichting, Wetsontwerp betreffende de bijzondere opsporingsmethode en enige andere onderzoeksmethoden, Parl.St., Kamer, 2001-2002, nr. 50-1688/001, p. 34.
293 Artikel 47octies, §6 Sv.
294 Artikel 47octies, §2 tweede lid Sv.
gelden voor de infiltratie, zoals de proportionaliteits-, subsidiariteits-, loyauteits- en legaliteitsbeginsel, hier ook kunnen toegepast worden. Artikel 2 van de wet van 29 december 2010 heeft daarenboven in de tweede paragraaf van artikel 47octies Sv. toegevoegd dat “deze politionele onderzoekstechnieken kunnen slechts worden aangewend door leden van de directie van de speciale eenheden van de federale politie en, desgevallend, mits bijkomend voorafgaand akkoord van de federale procureur, in samenwerking met buitenlandse speciaal daartoe opgeleide en bevoegde ambtenaren”. De Koning heeft uiteindelijk deze politionele onderzoekstechnieken vastgelegd met de koninklijke besluit van 9 april 2003 betreffende de politionele onderzoekstechnieken. Deze technieken betreffen namelijk de pseudo-koop, de vertrouwenskoop, de testkoop, de pseudo-verkoop, de gecontroleerde aflevering, de gecontroleerde doorlevering en de frontstore. Er werd bewust gekozen om deze niet op een exhaustieve manier in de wet te regelen, gezien het evolutief karakter van hun inhoud. Inderdaad, het crimineel milieu stemt zeer snel zijn tactieken af op de technieken en tactieken die aangewend worden door de politiediensten, zodat het wettelijk kader vlug aangepast moet kunnen worden, wat gemakkelijker te verwezenlijken is bij K.B. dan bij wet.

3. Bevoegde infiltranten

3.1. Politionele infiltratie

Zoals we het uit de definitie van de eerste paragraaf kunnen afleiden, moet de infiltrant een politieambtenaar zijn die onder de dekmantel van een aangenomen fictieve identiteit werkt. In de memorie van toelichting wordt er verder uitgelegd dat in de praktijk de infiltraties altijd door speciaal daartoe opgeleide en getrainde politieambtenaren moeten worden uitgevoerd. Dit wordt als een absolute vereiste gezien ten aanzien van het delicaat karakter van deze maatregel en de noodzaak van een juiste sturing en strikte controle van de infiltranten vanuit hun eigen politionele hiërarchie. Daarom zijn het, in het kader van de geïntegreerde politiedienst, de leden van de directie van de speciale eenheden van de

---

296 Wet van 29 december 2010 houdende wijziging van artikel 47octies van het Wetboek van strafvordering betreffende de samenwerking met buitenlandse infiltranten, B.S. 20 januari 2011.
algemene directie van de operationele ondersteuning van de federale politie, die als infiltrant kunnen optreden.\footnote{Memorie van Toelichting, Wetsontwerp betreffende de bijzondere opsporingsmethode en enige andere onderzoeksmethoden, \textit{Parl.St.}, Kamer, 2001-2002, nr. 50-1688/001, p. 33.}

Niettemin, kan de procureur des Konings, in uitzonderlijke omstandigheden, aan de infiltrant toelaten om “bij een welbepaalde operatie kortstondig een beroep [te] doen op de deskundigheid van een persoon die niet tot de politiediensten behoort, indien dit strikt noodzakelijk voorkomt voor het welslagen van zijn opdracht”.\footnote{Artikel 47\textit{octies}, §1 tweede lid Sv.} Dit zou namelijk van nut kunnen zijn om de geloofwaardigheid van de infiltrant te handhaven of “zijn vermoedens bevestigd te zien”.\footnote{A. DE NAUW en F. SCHUERMANS, “De wet betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden”, \textit{R.W.} 2003-04, afl. 1, p. 940.} Meerdere voorbeelden van dergelijke bijstand worden gegeven in de memorie van toelichting waaronder onder meer het voorbeeld van een politie ambtenaar die geïnfiltrreerd is in een criminele organisatie gespecialiseerd in namaakdiamanten en die bijgestaan wordt door een diamantair. De magistraat zal deze burgerdeskundige voor ogen moeten houden en liefst zo veel mogelijk burgers met een crimineel verleden uitsluiten.\footnote{Wetsontwerp betreffende de bijzondere opsporingsmethode en enige andere onderzoeksmethoden, \textit{Parl.St.}, Kamer, 2001-2002, nr. 50-1688/001, p. 35.} Deze deskundigen beschikken nochtans niet over een initiatiefrecht. Hun bijstand is slechts kortstondig en ze zijn geacht om de instructies van de politieambtenaar, die als infiltrant optreedt te volgen. De regeling van deze burgerdeskundige is complex omdat, zoals we kunnen opmerken, de grens tussen de burgerdeskundigen en de burgerinfiltranten zeer dun is. Het is bijgevolg niet zeer duidelijk in welke mate de burgers als deskundigen kunnen worden beschouwd.\footnote{A. DE NAUW en F. SCHUERMANS, “De wet betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden”, \textit{R.W.} 2003-04, afl. 1, p. 940.}

3.2. Burgerinfiltratie

Er bestaat momenteel een wetsvoorstel van 19 februari 2018\footnote{Wetsontwerp tot wijziging van het Wetboek van strafvordering met het oog op het invoeren van de bijzondere opsporingsmethode burgerinfiltratie, \textit{Parl.St.}, Kamer, 2017-2018, nr. 54-2940/001.} dat het gebruik van burgerinfiltranten, die voordien uitgesloten waren, wil invoeren als vierde bijzondere opsporingsmethode naast de observatie, de infiltratie en de informantenwerking in de nieuwe artikelen 47\textit{novies}/1 tot 47\textit{novies}/3 Sv. Terwijl er vroeger ervoor gekozen werd om dit niet toe te laten, omdat burgerinfiltranten en zeker criminele infiltranten, moeilijk controleerbaar zijn, vaak opereren met een “\textit{dubbele agenda}” en gedreven kunnen worden door persoonlijke
belangen, zodat de infiltratie dan een hoge risicograad inhoudt, is de wetgever op zijn besluit teruggekomen ten gevolge van de toenemende terroristische dreiging. Het is volgens het wetsvoorstel bijzonder moeilijk voor de politiediensten om de terroristische milieus te infiltreren, “gelet op het bijzonder gesloten karakter (...) en de zware controle die terroristische organisaties als Da’esh uitvoeren op nieuwelingen”. Er zal daarom beroep kunnen worden gedaan op burgerinfiltranten in het kader van de opsporing en vervolging van de georganiseerde criminaliteit en het terrorisme “indien het onderzoek zulks vereist en indien de overige middelen van het onderzoek niet lijken te volstaan om de waarheid aan het licht te brengen”. In tegenstelling tot de politionele infiltratie, zal het hier niet verplicht zijn dat de burgerinfiltrant onder een fictieve identiteit opereert. Het kan inderdaad wenselijk zijn dat hij onder zijn werkelijke naam handelt, wanneer hij ingezet wordt in een milieu waar hij reeds gekend is.

4. Bescherming van de infiltranten

Verder is het absoluut noodzakelijk, volgens de memorie van toelichting, dat de infiltranten onder een fictieve identiteit handelen. De afscherming van hun werkelijke identiteit zou ervoor zorgen dat ze niet in gevaarlijke situaties terecht komen, zoals resorities en vergeldingsmaatregelen ten aanzien van hun persoon of hun familie wanneer ze in het criminele milieu ontdekt worden. Het is ook een noodzakelijke tactiek voor het slagen van de maatregel.

Om de veiligheid van de infiltranten en hun fysieke, psychische en morele integriteit te vrijwaren, kan de procureur des Konings tevens, wanneer er daartoe grond bestaat, een toelating verlenen tot het uitvoeren van maatregelen die daarvoor noodzakelijk zijn. Deze delicate en zeer belangrijke bevoegdheid van het Openbaar Ministerie verantwoordt zich ten

305 Memorie van Toelichting, Wetsontwerp betreffende de bijzondere opsporingsmethode en enige andere onderzoeksmethoden, Parl.St., Kamer, 2001-2002, nr. 50-1688/001, p. 34.
309 Artikel 47 octies, §2 derde lid Sv.
310 Artikelen 47 octies, §2 derde lid Sv.
aanzien van het feit dat de infiltranten werkelijk in levensgevaar kunnen verkeren door zich binnen het criminele milieu te bewegen, zonder enige directe politoniele hulp. Het Openbaar Ministerie kan er in zulke gevallen dan voor zorgen, dat het contact met de infiltranten altijd behouden wordt, door gebruik te maken van technische middelen die verzekeren dat men altijd vlug kan ingrijpen om hulp te verlenen aan de infiltranten in noodsituaties. De tussenkomst van de leidinggevende politieambtenaren en magistraten wordt volgens de memorie van toelichting soms ook verplicht “wanneer de infiltratie een dermate impact op de persoonlijkheid van de infiltrant heeft, dat zijn psychische of morele integriteit in het gedrang dreigt te komen”. De infiltrant kan inderdaad door het crimineel milieu besmet worden ten gevolge van een te grote betrokkenheid bij de door hem geïnfiltrerde criminele organisatie. Zelfs in het geval waarin er aanwijsbare redenen bestaan, die het voortzetten van de operatie bemoeilijken en de infiltrant in een gevaarlijke situatie zouden kunnen brengen, is het soms geboden dat de leidinggevende magistraat, al dan niet samen met de leidinggevende politieambtenaren, hun verantwoordelijkheid nemen om “de infiltratie te beëindigen of fundamenteel bij te sturen”. In de parlementaire tekst wordt namelijk het voorbeeld gegeven van het hanteren van microfoons om de gesprekken te beluisteren die plaatsvinden tussen de infiltrant en het doelwit, om ervoor te zorgen dat er tijdig kan worden tussen gekomen wanneer de infiltrant zich in een gevaarlijke situatie zou bevinden. Niettemin zullen de registreerde gesprekken in geen enkel geval tijdens de strafprocedure kunnen worden aangewend en zullen ze na de operatie vernietigd moeten worden, wanneer ze niet voldoen aan de voorwaarden van de informatietap van artikelen 90ter e.v. Sv. Er is dus een machtiging van de onderzoeksrechter vereist om deze te kunnen gebruiken in het kader van de bewijsvoering van de strafprocedure.

Ook tijdens de zitting kunnen er beschermingsmaatregelen worden genomen ten aanzien van de infiltranten. De memorie van toelichting van de BOM-wet verwijst namelijk naar het arrest van het Hof van Beroep Bergen van 4 mei 1990, waarin werd beslist “dat de officier van gerechtelijke politie, tijdens een verhoor in rechte, het recht heeft de identiteit van een informant geheim te houden en dat deze regel ook geldt ten aanzien van de leden van de rijkswacht die, niet als verbalisanten, maar als pseudo-kopers zijn opgetreden”. Hetzelfde

Hof heeft in 1993\textsuperscript{315} eveneens geoordeeld dat de rechter niet verplicht is om de geïnfiltrerde rijkswachter als getuige tijdens de terechtzitting te horen, om de rechten van verdediging en het recht op een eerlijk proces van de EVRM, zoals het beginsel van de gelijkheid der wapens, te eerbiedigen. Volgens deze rechtspraak volstaat het dat hij de onderzoeksrechter en de officier die het bevel over deze rijkswachter voert, hoort.\textsuperscript{316}

Daarnaast bepaalt artikel 47\textit{quinquies} Sv. nog dat de minister van Justitie en de minister van Binnenlandse Zaken “\textit{op gezamenlijk voorstel van de federale procureur en de procureur-generaal belast met specifieke taken inzake het terrorisme en het groothanditisme, de bijzondere maatregelen [nemen], die strikt noodzakelijk zijn om de afscherming van de identiteit en de veiligheid van de politieambtenaren, belast met de uitvoering van de bijzondere opsporingsmethoden, bij de voorbereiding en de uitvoering van hun opdrachten te allen tijde te vrijwaren}”.\textsuperscript{317} Overeenkomstig de vierde paragraaf van het artikel bestaat er een strafuitsluitende rechtvaardigingsgrond ten aanzien van de feiten die daarvoor worden gepleegd, omdat deze niet als misdrijven kunnen worden beschouwd.\textsuperscript{318}

5. Het plegen van misdrijven door de infiltranten

5.1. De strafuitsluitende verschoningsgrond

Het kan zijn dat het in sommige gevallen noodzakelijk is voor het welslagen van de operatie, dat de infiltranten sommige misdrijven plegen. Op basis van de tweede paragraaf van artikel 47\textit{quinquies} Sv., geldt er een strafuitsluitende verschoningsgrond voor “\textit{de politieambtenaren die, in het kader van hun opdracht en met het oog op het welslagen ervan of ter verzekering van hun eigen veiligheid of deze van andere bij de operatie betrokken personen, strikt noodzakelijke strafbare feiten plegen}”. Deze strafuitsluitende verschoningsgrond is overigens ook van toepassing op de magistraat, die machtiging verleent aan een politieambtenaar en aan de personen die aan de uitvoering van de infiltratie noodzakelijke en rechtstreekse hulp of bijstand hebben verleend en aan de burgerdeskundigen van artikel 47\textit{octies}, §1, tweede lid Sv.\textsuperscript{319} De procureur des Konings moet echter zijn

\begin{itemize}
\item 317 Artikel 47\textit{quinquies}, §4 Sv.
\item 319 Artikel 47\textit{quinquies}, §2 derde en vierde lid Sv.
\end{itemize}
uitdrukkelijk akkoord daarvoor verlenen.\textsuperscript{320} Verder bepaalt artikel 47\textit{quinquies} Sv. dat de feiten die gepleegd worden niet ernstiger mogen zijn dan de strafbare feiten waarvoor de methode, hier de infiltratie, aangewend wordt “en moeten noodzakelijkerwijs evenredig zijn met het nagestreefde doel”.\textsuperscript{321}

Deze strafuitsluitende verschoningsgrond betreft niettemin enkel de bestraffing, zodat de toepassing ervan niet op de schuldvraag slaat en dat de strafbare feiten als zodanig hun onwettig karakter blijven behouden. De keuze van de wetgever voor een strafuitsluitende verschoningsgrond moeten wij toejichten omdat het steeds toelaat aan de eventuele slachtoffers om een vordering tot schadevergoeding in te stellen.\textsuperscript{322}

Daarnaast heeft de wetgever door de wet van 25 april 2014\textsuperscript{323} een gelijkaardige strafuitsluitende verschoningsgrond voor de “politieambtenaren van de directie van de speciale eenheden van de federale politie die, in het kader van hun opleiding en met het oog op het kunnen uitvoeren van de bijzondere opsporingsmethoden van de observatie en van de infiltratie, strikt noodzakelijke strafbare feiten plegen bedoeld in” de wegcode\textsuperscript{324}, die we verder niet gaan bekijken, in artikel 47\textit{quinquies} Sv. ingevoerd.\textsuperscript{325}

5.2. De voorafgaandelijke toestemming

In paragraaf drie van artikel 47\textit{quinquies} Sv. wordt bepaald dat de politieambtenaren voor de uitvoering van de infiltratie, schriftelijk aan de procureur des Konings moeten melden welke misdrijven, zij, de personen die aan de uitvoering van de infiltratie noodzakelijke en rechtstreekse hulp of bijstaan gaan verlenen en de eventuele burgerdeskundigen, voornemens zijn te plegen.\textsuperscript{326} Soms is zulke voorafgaande vermelding echter niet mogelijk, zodat de wetgever de mogelijkheid geeft aan de politieambtenaren om de procureur des Konings onverwijld in kennis te stellen van de misdrijven die zij hebben gepleegd, of de andere personen zoals hoger vermeld en deze nadien schriftelijk te bevestigen.\textsuperscript{327} De procureur des Konings moet daarna in een afzonderlijke en schriftelijke beslissing de misdrijven vermelden.

\textsuperscript{320} Artikel 47\textit{quinquies}, §2 eerste lid Sv.
\textsuperscript{321} Artikel 47\textit{quinquies}, §2 tweede lid Sv.
\textsuperscript{322} A. DE NAUW en F. SCHUERMANS, “De wet betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden”, \textit{R.W.} 2003-04, afl. 1, p. 925.
\textsuperscript{323} Wet van 25 april 2014 houdende diverse bepalingen betreffende Justitie, \textit{B.S.} 14 mei 2014.
\textsuperscript{324} Koninklijke besluit van 1 december 1975 houdende algemeen reglement op de politie van het wegverkeer en van het gebruik van de openbare weg, \textit{B.S.} 9 december 1975.
\textsuperscript{325} Artikel 47\textit{quinquies}, §5 Sv.
\textsuperscript{326} Artikel 47\textit{quinquies}, §3 eerste lid Sv.
\textsuperscript{327} Artikel 47\textit{quinquies}, §3 tweede lid Sv.
die door deze verscheidene actoren in het kader van de uitvoering van de operatie mogen worden gepleegd.\textsuperscript{328} Deze regeling geldt ook voor het gerechtelijk onderzoek.\textsuperscript{329}

6. Het proces-verbaal en het vertrouwelijk dossier

De wet van 27 december 2005\textsuperscript{330} heeft een tweede specifiek artikel voor de infiltratie naast artikel 47\textit{octies} in het Wetboek van Strafvordering ingevoerd. Dit artikel 47\textit{novies} Sv. bevat de regeling van het proces-verbaal van de uitvoering van de infiltratie en het vertrouwelijk dossier.

In de eerste paragraaf van dit artikel wordt er bepaald dat de officier van gerechtelijke politie, die de leiding heeft over de uitvoering van de operatie, een nauwgezet, volledig en waarheidsgetrouw schriftelijk verslag over elke fase in de uitvoering van de operatie aan de procureur des Konings moet overmaken. Deze verslagen bestaan uit de processen-verbaal die de officiers van gerechtelijke politie opstellen van de verschillende fasen van de uitvoering van de infiltratie. Hierin worden echter “geen elementen die de afscherming van de gebruikte technische hulpmiddelen en de politionele onderzoekstechnieken of de vrijwaring van de veiligheid en de afscherming van de identiteit van de informant, de politieambtenaren, belast met de uitvoering van de infiltratie” en de burgerdeskundigen, in het gedrang kunnen brengen.\textsuperscript{331} Deze verslagen worden bewaard in een vertrouwelijk dossier. Dit wil zeggen dat slechts de procureur des Konings, de onderzoeksrechter en de Kamer van inbeschuldigingstelling in het kader van hun inzagerecht toegang tot het dossier hebben, dat tevens onder het beroepsgeheim valt.\textsuperscript{332} Deze processen-verbaal, zoals de schriftelijke bevestiging door de procureur des Konings of de onderzoeksrechter van het bestaan van de verleende machtiging tot infiltratie worden “uiterlijk na het beëindigen van de infiltratie bij het strafdossier gevoegd”.\textsuperscript{333}

Het vertrouwelijk dossier bevat onder meer de machtiging tot infiltratie, de beslissingen tot wijzigingen, aanvulling of verlenging\textsuperscript{334} en de beslissing van de procureur des

\begin{itemize}
\item \textsuperscript{328} Artikel 47\textit{octies}, §4 Sv.
\item \textsuperscript{329} Artikel 47\textit{octies}, §7 tweede lid Sv.
\item \textsuperscript{330} Die we reeds supra besproken hebben in deel II, hoofdstuk 1, afdeling 2.
\item \textsuperscript{331} Artikel 47\textit{novies}, §2 eerste lid Sv.
\item \textsuperscript{332} Artikel 47\textit{novies}, §2 eerste lid Sv.
\item \textsuperscript{333} Artikel 47\textit{novies}, §2 laatste lid Sv.
\item \textsuperscript{334} Artikel 47\textit{novies}, §2 eerste lid Sv.
\end{itemize}
Konings van de misdrijven die gepleegd kunnen worden in het kader van de uitvoering van de infiltratie.\textsuperscript{335}

\textsuperscript{335} Artikel 47\textit{octies},§4 en §7 tweede lid Sv.
Hoofdstuk 4. Vergelijking tussen de online en de offline infiltratie

Eerst en vooral is het belangrijk om aandacht te besteden aan gemeenschappelijke kenmerken van de twee operaties die deze van andere opsporingsmiddelen onderscheiden voordat we sommige belangrijke verschillen tussen de twee soorten infiltraties nader bekijken.

Afdeling 1. Gemeenschappelijke kenmerken

1. Heimelijk karakter van de operatie

Bij beide soorten infiltraties blijft het politiekaracter van de operatie geheim. Zowel op het internet als in de fysieke wereld vermijden de undercoveragenten hun werkelijke identiteit en hun functie te onthullen. Het gebruik van een fictieve identiteit wordt daarom vereist bij de offline infiltratie, terwijl het slechts als een mogelijkheid wordt bedongen in artikel 46sexies Sv. Dit is te verklaren door het feit dat de infiltranten fysieke contacten hebben met de doelwitten van de operatie, zodat ze mogelijks een groter risico lopen voor hun leven. De politieambtenaren die als infiltranten optreden, spelen ook altijd een zekere rol, zoals die van crimineel of van koper van een bepaald verboden goed, om actief de doelwitten van de operatie te misleiden. In de cyberwereld gebeurt deze misleiding ook op de chatfora. De undercoveragenten nemen contact op met de doelwitten van de operatie door hun te laten geloven dat ze bijvoorbeeld een klant zijn of dat ze ook een activiteit uitoefenen in dit crimineel milieu, om de nodige informatie en bewijsstukken voor het onderzoek te kunnen verzamelen.

2. Deelname van de politie aan de strafbare feiten

Een andere gemeenschappelijke kenmerk van beide soorten infiltraties, die deze onderscheiden van de andere opsporingsmethoden, is dat de politieambtenaren tijdens de uitvoering van de infiltratie vaak zullen moeten deelnemen aan de misdrijven die ze aan het onderzoeken zijn. We kunnen hier bijvoorbeeld denken aan de undercoveragent die via het dark web of gewoon in de reële wereld cocaïne koopt aan een drugshandelaar of die wapens koopt.336 Het plegen van strafbare feiten kan noodzakelijk zijn voor de uitvoering van het onderzoek en om de geloofwaardigheid van de infiltrant te vrijwaren. Deze toelating om strafbare feiten te plegen wordt op een gelijkaardige manier in de derde paragraaf van artikel

46sexies Sv. voor wat de online infiltratie betreft en in de vijfde paragraaf van artikel 47octies Sv. en artikel 47quinques Sv. voor wat de offline infiltratie betreft, geregeld. Dit kan als eigenaardig worden gezien, omdat de online infiltratie normaal gezien een lichte versie van de offline infiltratie, met minder strenge voorwaarden, moet uitmaken. We zouden dus kunnen verwachten dat er in het kader van de uitvoering van de infiltratie minder verregaande maatregelen zouden kunnen worden genomen door de politieambtenaren dan bij de klassieke infiltratie, die aan striktere voorwaarden is onderworpen. Zoals we het supra337 hebben gezien, laken de vertegenwoordiger van de Liga voor Mensenrechten en de Raad van State in hun advies van 9 mei 2016338, dat er in het nieuwe artikel 46sexies Sv. geen limitatieve opsomming wordt gegeven van de strafbare feiten die mogen worden begaan in het kader van de uitvoering van de operatie. Hun bezwaren zijn inderdaad legitiem, wanneer we weten dat de strafbare feiten die de politiediensten mogen plegen, niet ernstiger mogen zijn dan de feiten waarvoor de maatregel wordt aangewend, terwijl de online infiltratie volgens de voorwaarden kan worden toegepast op een groot aantal misdrijven. Er bestaat dus een grote marge van strafbare feiten, die gepleegd kunnen worden in functie van de misdrijven, waarvoor de infiltratie wordt aangewend, wat de bepaling misschien te soepel maakt ten aanzien van de verregaande gevolgen die de operatie teweeg kan brengen. Maar van een andere kant kunnen we onderlijnen dat het zeer moeilijk is voor de magistraten om op voorhand te kunnen bepalen welke misdrijven toegelaten zijn. Voor het welslagen van de operatie is het inderdaad cruciaal dat de politieambtenaren over een grote vrijheid van handeling beschikken om zich te kunnen aanpassen aan het milieu dat ze infiltreren. Een exhaustieve lijst in de wet van alle misdrijven die gepleegd kunnen worden onder bepaalde voorwaarden is ook niet wenselijk, aangezien het de criminele organisaties of terroristische groepen zou toelaten om hun leden te testen door te bevelen om misdrijven van die lijst te plegen.339

Afdeling 2. Verschillen tussen de twee soorten infiltraties

1. Fysieke contacten

Het grootste verschil tussen de twee operaties is dat er geen fysieke contacten tussen de infiltranten en de doelwitten van de operatie plaatsvinden tijdens de online infiltratie, terwijl

337 Zie deel II, hoofdstuk 2, afdeling 2.
dat wel het geval is bij de klassieke infiltratie. In de regeling van de bijzondere opsporingsmethode van infiltratie, vinden wij daarom meerdere maatregelen die gericht zijn op de bescherming van de infiltranten, zoals de verplichting om een fictieve identiteit aan te nemen en de mogelijkheid, voor de procureur des Konings, overeenkomstig paragraaf twee van artikel 47octies Sv., en de minister van Justitie en de minister van Binnenlandse Zaken, overeenkomstig paragraaf vier van artikel 47quinquies Sv., om maatregelen te nemen die noodzakelijk zijn voor de bescherming van de politieambtenaren die als infiltranten optreden. Zulke beschermingsmaatregelen vinden we niet terug in artikel 46sexies Sv. Dit verschil tussen de twee operaties is één van de redenen die ervoor hebben gezorgd dat de wetgever de online infiltratie slechts als een lichte versie beschouwt van de offline infiltratie en dat er daarom een soepeler regime voor de uitvoering ervan van toepassing moet zijn.

2. **Opname van de communicaties**

Een andere eigenheid van de online infiltratie, die al vermeld werd en die het soepeler regime rechtvaardigt, is dat alle contacten tussen de infiltranten en de doelwitten van de operatie in het kader van de online infiltratie, in tegenstelling tot de offline infiltratie, geregistreerd worden volgens het tweede lid van paragraaf vier van artikel 46sexies Sv. Dit is tevens een zeer belangrijke afwijking van artikel 47octies Sv. omdat het de hele operatie transparanter maakt dan de offline infiltratie. Deze regeling biedt een aangepast antwoord ten aanzien van de technologische evolutie, omdat de politiediensten genieten van de voordelen die de technologie hen toestaat om misbruiken te voorkomen. De uitvoering van de operatie wordt dus gemakkelijker te verantwoorden, omdat ze minder aan de willekeur van de infiltranten wordt overgelaten en het dus eenvoudiger wordt om na te kijken als er aan de rechten van verdediging wordt voldaan.

3. **Duurzaam contact**

Terwijl de politieambtenaar in het kader van de klassieke infiltratie een duurzaam contact moet onderhouden met de doelwitten van de operatie, is er geen vereiste van duurzaam contact bij de online infiltratie. Dit zou willen zeggen dat een eenmalig contact van een politieambtenaar met een verdachte op het internet, al een online infiltratie zou kunnen uitmaken, wanneer de andere toepassingsvoorwaarden vervuld worden. Er kan dus vlugger sprake zijn van een online infiltratie dan een offline infiltratie, wat kan worden verklaard door de eigenaardigheden van de cyberwereld. Transacties kunnen inderdaad zeer snel
plaatsvinden op het internet, zodat het niet altijd vereist is om meerdere contacten te onderhouden met verdachten om misdrijven op te sporen. Zeker op het dark web kan het voor de partijen van belang zijn om de contacten zo kortstondig mogelijk te houden om te vermijden dat er gevoelige informatie wordt gedeeld en dat er dus verdenkingen zouden kunnen ontstaan over de toepassing van de infiltratie, zodat de operatie gesaboteerd zou kunnen worden.

4. **Toepassingsgebied**

Het grootste verschil situeert zich nochtans op het vlak van de strafbare feiten die de operatie kunnen rechtvaardigen. Terwijl de drempel zeer laag ligt bij de online infiltratie, is het toepassingsgebied van de klassieke infiltratie veel geringer. De offline infiltratie is inderdaad, gezien de verregaande inbreuk op de individuele rechten en vrijheden die het veroorzaakt, onderworpen aan een proportionaliteitsbeginsel, zodat het slechts ten aanzien van de zwaardere misdrijven, die ook een proactief onderzoek rechtvaardigen, mag worden aangewend. Artikel 46sexies Sv. breidt bovendien aanzienlijk het toepassingsgebied van het proactief onderzoek van artikel 28bis Sv uit. Dit zou ertoe kunnen leiden dat de politiediensten veel vlugger de infiltratie zullen aanwenden in het kader van onderzoeken naar misdrijven in de cyberwereld dan voor onderzoeken naar misdrijven in de fysieke wereld, wanneer de overige middelen van onderzoek niet lijken te volstaan. Dit blijkt een goede maatregel te zijn, gezien de constant toenemende ruimte die het internet in ons dagelijkse leven inneemt. Politiediensten moeten dus de mogelijkheid krijgen, zelfs bij minder ernstige misdrijven, om via het internet in contact te kunnen komen met verdachten om het onderzoek vooruit te bevorderen. De organisatie en veel andere aspecten van de criminaliteit geschieden steeds meer via de numerieke wereld, zodat de rechtshandhavingsdiensten met de tijd moeten meegaan.

5. **Tijdsduur van de operatie**

Terwijl we de regeling van artikel 47octies Sv. omtrent de tijdsduur van de machtiging tot infiltratie ongeschikt beschouwen voor de infiltratie in de cyberwereld, merken we dat de wetgever een gelijkaardige regeling heeft ingevoerd in artikel 46sexies Sv. Er geldt dus ook bij de online infiltratie een beperking van de tijdsduur van de operatie voor een periode van drie maanden, die niettemin verlengbaar is. De formulering van de regeling in de twee artikelen is echter verschillend, omdat er voor de offline infiltratie wordt bepaald dat de
periode tijdens welke de infiltratie kan worden uitgevoerd niet langer mag zijn dan “drie maanden te rekenen van de datum van de machtiging” terwijl er voor de cyberinfiltratie in de tweede paragraaf van artikel 46sexies Sv. wordt bepaald dat de machtiging geldig is voor een termijn van drie maanden, onverminderd eventuele hernieuwingen. De infiltratie geldt dus sowieso voor een periode van drie maanden, die hernieuwbaar is, terwijl voor de klassieke infiltratie de oorspronkelijke machtiging maximum drie maanden duurt, maar onderhevig is aan een eventuele verlenging door de procureur des Konings. Los van het feit dat er wordt bepaald dat het mogelijk is om de termijn van drie maanden te hernieuwen, wordt er niets over de voorwaarden van deze hernieuwing in het nieuw artikel bepaald. Dit onderscheidt de regeling van de online infiltratie van de regeling van artikel 46octies Sv. waar er in de zesde paragraaf wordt bepaald dat de procureur des Konings op gemotiveerde wijze zijn machtiging kan verlengen, maar dat deze aan de voorwaarden van de drie eerste paragrafen van het artikel moet voldoen en dat hij daarvoor opnieuw een schriftelijke machtiging tot infiltratie moet verlenen overeenkomstig de voorschriften van de derde paragraaf. Terwijl we hier dus niet meer te maken kunnen hebben met termijnen die korter mogen zijn dan drie maanden, biedt de nieuwe regeling van artikel 46sexies Sv. geen grote aanpassingen van de regeling van de klassieke infiltratie aan de cyberwereld op dit vlak.

6. Vormvereisten van de machtiging tot infiltratie

Wat de vormvereisten van de machtiging betreft, kunnen we opmerken dat er nauwelijks iets wordt vermeld over de inhoud van de schriftelijke vermelding in artikel 46sexies Sv. in vergelijking met artikel 47octies Sv. We kunnen eruit afleiden dat het gemakkelijker is om de online infiltratie toe te passen, omdat het bijvoorbeeld niet noodzakelijk is om de redenen op te geven waarom de infiltratie onontbeerlijk is om de waarheid aan het licht te brengen, noch de wijze waarop de infiltratie zal gebeuren. Alle details van de operatie moeten dus niet al op voorhand vastliggen, zodat de bevoegde infiltranten met meer vrijheid met de omstandigheden kunnen omgaan. Hier wordt er dus duidelijk gekozen om de efficiëntie van het onderzoek te bevorderen door minder procedurele vereisten in te voeren die een snelle uitvoering van de operatie zouden kunnen belemmeren. De keuze van de wetgever om de vormvereisten van de machtiging eenvoudiger te maken, is dus aangepast aan de kenmerkende snelheid van de cyberwereld.

340 Artikel 47octies, §3, 5° Sv.
7. **Politieke onderzoekstechnieken**

Een ander verschil tussen beide soorten infiltraties, is dat de procureur des Konings in het kader van de offline infiltratie de leden van de directie van de speciale eenheden van de federale politie kan machtigen om bepaalde politieke onderzoekstechnieken te gebruiken, terwijl er niets over deze mogelijkheid wordt bepaald in artikel 46sexies Svb. De wetgever heeft dus beoogd dat deze niet nodig waren om de online infiltratie te ondersteunen.

8. **Bevoegde infiltranten**

Ten aanzien van de politieambtenaren die als infiltranten kunnen optreden, is de regeling van de online infiltratie minder strikt dan de regeling van de offline infiltratie. Inderdaad, de online infiltratie wordt in tegenstelling tot de offline infiltratie, niet voorbehouden voor de speciale eenheden van de algemene directie van de operationele ondersteuning van de federale politie, maar kan tevens uitgevoerd worden door speciaal opgeleide speurders gespecialiseerd in het onderzoek. Dit kan namelijk een aangepaste oplossing bieden ten aanzien van de zeer technische en complexe cyberwereld. Verder is de regeling bij de online infiltratie tevens soepeler omdat het de Koning is die de voorwaarden en de nadere regels voor de aanwijzing van de bevoegde politiediensten bepaalt. Omdat deze bevoegdheid niet wordt vastgesteld in de wet, maar eerder in een koninklijk besluit, kunnen de voorwaarden voor de aanwijzing van de bevoegde infiltranten snel worden gewijzigd, zodat er altijd gekwalificeerde politiediensten ten aanzien van de situatie ingezet kunnen worden.

Daarnaast is het tot nu toe voor beide soorten infiltraties niet toegelaten om beroep te doen op burgerinfiltranten, terwijl het voor beide soorten infiltraties wel toegelaten is om een kortstondig beroep te doen op burgerdeskundigen. De grens tussen beide is wel dun, zodat we zeer voorzichtig met deze bepalingen moeten omgaan. Dit is niettemin onderhevig aan veranderingen door het wetsontwerp van 19 februari 2018. In het wetsontwerp wordt er niettemin niet verwezen naar de mogelijkheid om burgerinfiltranten te gebruiken voor onderzoeken in de online wereld. Dit wordt verantwoord door het feit dat de politieambtenaren zelf plaats kunnen nemen achter een computer en dat ze daarenboven in geval van technische moeilijkheden tevens beroep kunnen doen op de expertise van burgerdeskundigen. Niettemin zou de mogelijkheid om beroep te doen op burgerinfiltranten voor de opsporing van misdrijven in de cyberwereld in bepaalde gevallen een meerwaarde
kunnen vertonen. Inderdaad, omdat het van belang is voor het onderzoek dat de infiltrant zijn positie behoudt in de groep, moet deze laatste ook geloofwaardig blijven, wat moeilijker kan blijken wanneer we te maken hebben met complexere vormen van cybercriminaliteit. De beperking van de rol van de burger tot een loutere kortstondige technische ondersteuning tijdens de binnendringing van de infiltrant in een bepaalde groep, kan dus niet altijd als efficiënt worden beschouwd. Een voortdurende deskundigheid doorheen de hele operatie kan dus in sommige gevallen noodzakelijk en wenselijk zijn voor het onderzoek, zeker omdat de risico’s die verbonden kunnen zijn aan de burgerinfiltratie kunnen worden gehouden door de controlemogelijkheden die het internet biedt.

341 Met name dat de burgerinfiltranten moeilijk controleerbaar kunnen zijn omdat ze gedreven kunnen zijn door persoonlijke belangen of omdat ze vaak opereren met een dubbele agenda. Memorie van Toelichting, Wetsontwerp betreffende de bijzondere opsporingsmethode en enige andere onderzoeksmethoden, Parl.St., Kamer, 2001-2002, nr. 50-1688/001, p. 34.
Hoofdstuk 5. De online infiltratie in naburige landen

In dit hoofdstuk gaan we in grote lijnen bekijken hoe de cyberinfiltratie wordt geregeld in naburige landen, met name Frankrijk en Nederland, en wat sommige nadelen en voordelen van hun regelingen zijn. Een vergelijking van bepaalde aspecten van de buitenlandse regelingen met de huidige Belgische regeling kan namelijk bepaalde wenselijke wijzigingen van de Belgische regeling van de operatie aanwijzen om die effectiever te maken.

Afdeling 1. Frankrijk

In Frankrijk heeft de wetgever sneller dan in België ingegrepen om de cyberinfiltratie mogelijk te maken voor de politiediensten, door met het artikel 35 van de wet no2007-297 van 5 maart 2007 “relative à la prévention de la délinquance” een nieuw artikel 706-35-1 in de Franse Code de procédure pénale (hierna CPP) in te voeren. Dit artikel bevindt zich in de titel XVII “De la poursuite, de l’instruction et du jugement des infractions en matière de traite des êtres humains, de proxénétisme ou de recours à la prostitution des mineurs” van het vierde boek van het Code de Procédure Pénale. Er bestaat dus geen algemene regeling van de online infiltratie in de Franse Code de Procédure Pénale in tegenstelling tot in het Belgische Wetboek van Strafvordering, waar er niet wordt bepaald voor welke misdrijven het kan worden aangewend behalve dat de misdrijven een bepaalde straf tot gevolg moeten kunnen hebben. De online infiltratie wordt hier dus per categorieën van misdrijven geregeld.

Daarentegen werd de klassieke offline infiltratie later dan in België door de Franse wetgever ingevoerd, omdat ze door de wet van 9 maart 2004 “portant adaptation de la justice aux évolutions de la criminalité” in artikelen 706-81 tot 706-87 CPP werd ingevoerd. Het toepassingsgebied van deze operatie wijkt niettemin af van het toepassingsgebied van de online infiltratie, omdat de operatie hier kan worden aangewend in het kader van het onderzoek van ernstige misdrijven, die in artikelen 706-73 en 706-73-1 CPP zijn opgesomd, zoals moord, foltering of wreedheden in het kader van georganiseerde criminaliteit en de misdrijven van mensenhandel, sekshandel en terroristische daden onder andere. Het toepassingsgebied van de offline infiltratie werd echter later met de wet van 6 december 2004 ingevoerd.

344 Code de procédure pénale (FR).
uitgebreid tot verscheidene financiële en economische delicten, die opgesomd zijn in de artikelen 706-1-1 en 706-1-2 CPP, zoals de delicten van corruptie, machtsmisbruik of fiscale fraude.

1. Toepassingsgebied

Door de invoering van “l’enquête sous pseudonyme”, die als een soort lichte infiltratie of cyberpatrouille kan worden omschreven, in 2007 heeft de wetgever de aanwending van telecommunicatienetwerken mogelijk gemaakt in het kader van de uitvoering van de infiltratie. Deze kan echter wel slechts worden aangewend in het kader van een onderzoek naar ernstige misdrijven zoals mensenhandel, prostitutie van minderjarigen en het sekshandel en de misdrijven die eruit voortvloeien, en bovendien slechts wanneer deze misdrijven worden gepleegd door middel van elektronische communicatie. Overeenkomstig het artikel 706-35-1 CPP, mogen de officieren of de agenten van de gerechtelijke politie, wanneer deze werden toegewezen aan een gespecialiseerde dienst die voor deze doeleinden gerechtigd is, onder pseudoniem deelnemen aan de elektronische uitwisselingen en dus in contact komen via deze middelen met de verdachte daders van deze misdrijven. Ze kunnen dan tevens illegale inhoud downloaden, doorsturen als antwoord op een dringende aanvraag, verwerven of bewaren zonder daarvoor strafrechtelijk verantwoord te worden gesteld. De voorwaarden van deze verschillende acties is in het besluit van 21 oktober 2015 “relatif à l’habilitation au sein de services spécialisés d’officiers ou agents de police judiciaire pouvant procéder aux enquêtes sous pseudonyme” vastgelegd. Dit besluit bepaalt namelijk de diensten waartoe de officieren en de agenten van de gerechtelijke politie moeten behoren om gerechtigd te zijn om aan cyberinfiltratie te kunnen doen. Verder wordt er bepaald, dat op straffe van nietigheid, deze verschillende acties geen uitlokking om misdrijven te plegen mogen veroorzaken.

Daarnaast werden er gelijkaardige regelingen van “l’enquête sous pseudonyme” in andere delen van het Frans wetboek en dus voor andere misdrijven ingevoerd. We denken hier namelijk aan het artikel 706-87-1 CPP dat door de wet van 13 november 2014 “renforçant les
Dispositions de la lutte contre le terrorisme"350 werd ingevoerd en die een kopie van het artikel 706-35-1 CPP is, behalve dat het hier van toepassing is op de georganiseerde criminaliteit, zoals voor de klassieke infiltratie van artikel 706-81 CP, en de misdrijven in verband met de schending van de systemen van geautomatiseerde gegevensverwerking. Het toepassingsgebied van artikelen 706-87-1 CPP en 706-81 CPP werd achteraf uitgebreid naar de cyberaanvallen, de hulp op illegaal verblijf in Frankrijk, de niet-rechtvaardiging van inkomstenbronnen, de georganiseerde oplichterij en de illegale arbeid, onder andere door de wet van 17 augustus 2015 “portant adaptation de la procédure pénale au droit de l’Union européenne”351.352 Ook voor sommige seksuele misdrijven die door middel van elektronische communicaties worden gepleegd, bestaat er een gelijkaardige regeling van de online infiltratie of cyberpatrouilles, in het artikel 706-47-3 CPP, en voor misdrijven die worden gepleegd ter gelegenheid van weddenschappen of online geldspelen en kansspelen in artikel 59 van de wet van 12 mei 2010 “relative à l’ouverture à la concurrence et à la régulation du secteur des jeux d’argent et de hasard en ligne”353.354 Omdat deze artikelen slechts een paar nuances of verschillen ten aanzien van het artikel 706-35-1 CPP bevatten om de infiltratie aan te passen aan de eigenaardigheden van de misdrijven, gaan we deze niet verder bekijken.

2. Vergelijking met de Belgische regeling van de online infiltratie

2.1. Toepassingsgebied

Als we de regeling van de “enquête sous pseudonyme” in artikelen 706-35-1 CPP vergelijken met de Belgische regeling van de cyberinfiltratie van artikel 46sexies Sv. merken we dat het toepassingsgebied van de operatie geringer is in de Franse regeling. Niet alleen kan het slechts worden aangewend voor ernstige misdrijven, waarnaar wordt verwezen in de artikelen, het kan tevens slechts worden aangewend wanneer die misdrijven door middel van een elektronisch communicatiemiddel werden gepleegd. Het betreft dus namelijk enkel de specifieke en de niet-specifieke criminaliteit355. In tegenstelling daarmee wordt er in artikel

355 Zie begripsomschrijving supra in deel I, hoofdstuk 1, afdeling 3.
46sexies Sv. niet vermeld dat de misdrijven waarvoor de infiltratie wordt uitgevoerd, door middel van een elektronisch communicatiemiddel moeten worden gepleegd. Politiediensten kunnen in België dus genieten van de mogelijkheden die het internet hen biedt om in contact te komen met verdachten, wanneer er ernstige aanwijzingen tegen hen bestaan voor tal van misdrijven die misschien niets te maken hebben met de informaticacriminaliteit. Natuurlijk moet er wel een zekere link met de informatie-technologieën bestaan om in contact te kunnen komen met de verdachten, maar de misdrijven moeten niet via dit middel worden gepleegd. Daarnaast kan de maatregel in België ook van toepassing zijn op misdrijven die minder erg zijn voor zover deze “een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben”356, zoals een diefstal bijvoorbeeld, wanneer er aan alle voorwaarden van artikel 46sexies Sv. wordt voldaan.

We kunnen nochtans de Belgische regeling niet laken omdat ze een breder toepassingsgebied heeft dan de Franse regeling, aangezien ze namelijk de politiediensten toestaat gebruik te maken van de voordelen die de cyberwereld biedt op het vlak van contacten te leggen met het criminele milieu op een minder gevaarlijke manier dan in de fysieke wereld. Omdat de ICT steeds een belangrijkere plaats neemt in onze interactie met andere burgers, blijkt het dus opportuun om het onderzoek te kunnen richten naar de numerieke communicatienetwerken, zelfs wanneer misdrijven niet via deze middelen werden gepleegd.

Daartegenover kunnen we ook zeggen dat het toepassingsgebied van de Franse regeling minder streng is, omdat in tegenstelling tot de Belgische regeling, de cyberinfiltratie in Frankrijk niet uitsluitend kan worden aangewend om contact te onderhouden met personen waarvan er ernstige aanwijzingen bestaan dat zij strafbare feiten waarvoor de online infiltratie kan worden aangewend, hebben gepleegd of zouden plegen en wanneer “de overige middelen van onderzoek niet lijken te volstaan om de waarheid aan de dag te brengen”.357 Volgens de Franse regeling van de cyberinfiltratie moet er, met andere woorden, niet aan subsidiariteitsvoorwaarden worden voldaan en het volstaat dat de personen de daders kunnen zijn. Dit is te verklaaren door het feit dat het onderzoek onder pseudoniem slechts kan worden toegepast in het kader van limitatief opgesomde en zeer ernstige misdrifsen. Deze verantwoorden sowieso, zeker omdat ze via numerieke communicatiemiddelen moeten worden gepleegd, de aanwending van de cyberinfiltratie. Het Belgisch artikel 46sexies Sv.

356 Artikel 46sexies, §1 eerste lid Sv.
357 Artikel 46sexies, §1 eerste lid Sv.
moet dus niet als te beperkend worden beschouwd, want zonder deze voorwaarden zou de online infiltratie in een groot aantal onderzoeken kunnen worden toegepast, terwijl de infiltratie niettemin een verregaande maatregel kan zijn ten aanzien van bepaalde fundamentele rechten, zoals het recht op een privéleven.

2.2. Mogelijkheid om strafbare feiten te plegen tijdens de uitvoering van de infiltratie

Een ander verschil tussen de Belgische en de Franse regeling betreft de mogelijkheid voor de infiltranten om strafbare feiten te plegen tijdens de uitvoering van de operatie. Terwijl de regeling in paragraaf drie van het artikel 46sexies Sv. zeer vaag blijft over de strafbare feiten die gepleegd kunnen worden, wordt er in artikel 706-35-1 CPP verduidelijkt over welke strafbare feiten het kan gaan. Er wordt namelijk bepaald dat de infiltranten illegale inhoud kunnen downloaden en doorsturen in antwoord op een dringende aanvraag en die kunnen verwerven of bewaren zonder strafrechtelijk verantwoordelijk te worden gesteld, volgens de voorwaarden vastgesteld in een decreet. Het blijft dus nog steeds onnauwkeurig ten aanzien van de illegale inhou, maar men weet dat het slechts gaat over strafbare feiten die zich op het internet gaan voordoen. Een dergelijke formulering van de regeling gecombineerd met de voorwaarden voor het plegen van strafbare feiten van de derde paragraaf van artikel 46sexies Sv., zou tegemoet kunnen komen aan de kritiek van de Raad van State en de vertegenwoordiger van de Liga voor Mensenrechten ten aanzien van de onnauwkeurigheid van de bepaling. Niettemin zou een gelijkaardige regeling zoals de Franse niet wenselijk zijn, omdat zelfs als het verregaande gevolgen kan hebben, het de bevoegde infiltranten soms kan brengen tot het plegen van strafbare feiten, die zich niet in de cyberwereld voordoen, met het ogen op het welslagen van hun opdracht of om hun veiligheid en die van de andere betrokken personen, te verzekeren. De Belgische regeling lijkt dus soepeler en biedt een meer adequaat antwoord aan de complexiteit van sommige onderzoeken. Verder bevatten de Franse en de Belgische bepalingen, een gelijkaardig provocatieverbod.

2.3. Beroep op de expertise van burgerdeskundigen

Als laatste verschil dat hier behandeld wordt, kunnen wij erop wijzen dat er in de artikelen 706-35-1 en 706-87-1 CPP niet wordt vermeld, in tegenstelling tot in artikel 46sexies Sv., dat de officieren of agenten van de gerechtelijke politie onder bepaalde voorwaarden beroep kunnen doen op burgerdeskundigen. Zoals reeds gezien, is de cyberwereld zeer complex, zodat het meer dan noodzakelijk is, dat de infiltranten genoeg getraind en gevormd zijn voor de effectiviteit van de operatie. De mogelijkheid om beroep te
doen op burgerdeskundigen in België zorgt ervoor, dat zelfs in zeer specifieke en complexe situaties de infiltranten over de nodige expertise beschikken.

Afdeling 2. Nederland

De infiltratie heeft in Nederland sedert het jaar 2000 een wettelijke basis gekregen door de Wet bijzondere opsporingsbevoegdheden (Wet BOB) in artikel 126h en 126p van het Wetboek van Strafvoering (hierna WS). De wet heeft ook andere undercover opsporingsmethoden in het Wetboek ingevoerd, namelijk de pseudo-koop of de pseudo-dienstverlening in artikel 126i WS en de stelselmatige inwinning van informatie in artikel 126j WS. Wat eigenaardig is aan de Nederlandse regeling, is dat de wetgever sinds de invoering van deze artikelen in het Wetboek van Strafvoering al de keuze had gemaakt om deze ook toepasbaar te maken voor de cyberwereld. Inderdaad, er wordt in de memorie van toelichting van de Wet computercriminaliteit II verklaard dat bepaalde opsporingsbevoegdheden op een netwerk relevant kunnen zijn, onder meer de bijzondere opsporingsbevoegdheden van infiltratie en observatie. Deze bevoegdheden moeten dus naast hun “normale” toepassing in de fysieke wereld, ook onder dezelfde voorwaarden, “tenzij de specifieke aard van het onderzoek in een geautomatiseerde omgeving om specifieke voorzieningen vraagt”, kunnen toegepast worden in de online wereld.

1. De undercover opsporingsmethoden

Terwijl de online infiltratie op één enkele manier wordt geregeld in het Belgische Wetboek van Strafvoering, bestaan er drie varianten van de cyberinfiltratie of undercover opsporingsmethoden in het Nederlandse Wetboek van Strafvoering, die elk hun eigen regeling hebben.

---

359 Wetboek van Strafvoering (NL).
361 Memorie van Toelichting, Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvoering en de Telecommunicatiewet in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II), Kamerstuk 1998-1999, 26 671, nr. 3, p. 36.
1.1. De pseudo-koop of pseudo-dienstverlening

De pseudo-koop of pseudo-dienstverlening van artikel 126i WS kan slechts worden aangewend ten aanzien van verdenkingen van misdrijven waarvoor een bevel tot voorlopige hechtenis kan worden gerechtvaardigd. Deze operatie wordt ook geregeld in artikel 126q WS, voor het geval dat er vermoedens bestaan van georganiseerde criminaliteit. Beide artikelen bevatten een gelijkwaardige regeling van de pseudo-koop of de pseudo-dienstverlening, zodat we slechts de regeling van artikel 126i WS hier verder gaan bespreken.

In tegenstelling tot de twee andere undercoveroperaties die we hierna gaan bekijken, was de oorspronkelijke regeling van de pseudo-koop of pseudo-dienstverlening niet geschikt voor de cyberwereld. Daarom werd het eerste lid van het artikel gewijzigd door de wet van 1 juni 2006\(^\text{362}\), om de overdracht of de afname van gegevens in de cyberwereld ook onder deze regeling te kunnen brengen. Voor de uitvoering van deze operatie gaat de undercoveragent zich voordoen “als potentiële koper van een illegaal via internet aangeboden goed of dienst” en wordt hij in geen enkel geval gerechtvaardigd om andere strafbare feiten te plegen dan goederen af te nemen of diensten te verlenen aan de verdachten.\(^\text{363}\) De undercoveragenten kunnen dus hier bijvoorbeeld op basis van artikel 126i WS wapens of illegale drugs op het dark web kopen of verkopen, voor zover dat ze de verdachte “niet brengen tot andere strafbare feiten dan waarop diens opzet reeds tevoren was gericht”.\(^\text{364}\) Deze operatie wordt los van de infiltratie geregeld, omdat zoals we gaan zien, de infiltratie slechts binnen een criminele groep wordt toegepast, terwijl het hier ook mogelijk is om de operatie buiten een criminele groep uit te voeren. Voor deze operatie wordt er ook geen subsidiariteitsvereiste opgelegd. Er kan dus snel worden overgegaan tot de uitvoering van deze operatie omdat het volstaat, volgens het eerste lid van artikel 126i WS, dat de officier van justitie deze maatregel in het belang van het onderzoek acht, om deze te kunnen bevelen.

1.2. De stelselmatige inwinning van informatie

Daarnaast kunnen de opsporingsambtenaren, op basis van artikel 126j WS, wanneer er verdenkingen bestaan van een misdrijf, stelselmatig informatie inwinnen over de verdachten. De operatie van online undercover interacties met individuen betreft hier dus, het actief

\(^{362}\) Wet van 1 juni 2006 tot wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie, Stb 13 juli 2006.

\(^{363}\) J.-J. OERLEMANS, Normering van digitale opsporingsmethoden, Breda, Nederlandse Defensie Academie, 2017, p. 27.

\(^{364}\) Artikel 126i, tweede lid van het Nederlandse Wetboek van Strafvordering.
deelnemen van de opsporingsambtenaren aan een chatkanaal, zonder dat de doelwitten van de operatie op de hoogte worden gebracht, dat ze met politieambtenaren aan het communiceren zijn, door zelfs berichten te posten om informatie te verkrijgen, zodat het verder gaat dan het louter observeren. Het slechts rondkijken en lezen van wat er voor iedereen toegankelijk is, is niet onderworpen aan de voorwaarden van dit artikel. Verder moet er sprake zijn van een stelselmatig onderzoek en dus een inbreuk op de persoonlijke levenssfeer van de verdachte, om het onderzoek te moeten onderwerpen aan de voorwaarden van artikel 126j WS. Hier is de maatregel niet beperkt tot bepaalde misdrijven, zoals wat er geregeld is voor de pseudo-coop of pseudo-dienstverlening, omdat de opsporingsambtenaren hier geen enkel strafbaar feit gaan plegen, maar enkel het vertrouwen van de doelwitten van de operatie schenden. Hier, zoals voor artikel 126i WS, geldt er ook geen subsidiariteitsvoorwaarde en zijn de voorwaarden minder streng dan voor de infiltratie, omdat er minder risico's zijn verbonden aan deze operatie.

1.3. De infiltratie

Ten laatste, is de infiltratie geregeld in artikel 126h WS, voor wat de ernstige misdrijven betreft, en in artikel 126p WS, voor wat de georganiseerde criminaliteit betreft. De regeling van de operatie is gelijkaardig in beide artikels, zodat we slechts artikel 126h verder zullen bespreken.

In de memorie van toelichting bij het wetsvoorstel dat heeft geleid tot de Wet bijzondere opsporingsbevoegdheden, wordt bepaald dat de infiltratie ook een andere vorm kan aannemen op het internet, zodat de opsporingsambtenaren in een niet-fysieke zin kunnen betrokken worden in een groep. Deze maatregel is vergelijkbaar met de twee vorige undercover interacties, maar onderscheidt zich door het feit dat ze verregaander is, omdat de opsporingsambtenaren hier tot op een zekere hoogte strafbare feiten mogen plegen, wanneer het noodzakelijk is “om hun denkmantel te behouden en het vertrouwen te winnen van leden

---

367 Memorie van Toelichting, Wetsvoorstel tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden), Kamerstukken II 1996-1997, 25 403, nr. 3, p. 29.
368 Memorie van Toelichting, Wetsvoorstel tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden), Kamerstukken II 1996-1997, 25 403, nr. 3, p. 29.
van een criminele organisatie”. De strafbare feiten die voor het welslagen van de operatie gepleegd kunnen worden, zijn dus minder beperkt dan in het kader van de uitvoering van een pseudo-koop of een pseudo-dienstverlening zodat de politiediensten hier over een grotere handelingsvrijheid beschikken. Daarnaast, in tegenstelling tot het stelselmatig undercover inwinnen van informatie, neemt de opsporingsambtenaar hier deel aan een criminele groep. Dit verschil verklaart waarom er slechts beroep kan worden gedaan op de infiltratie wanneer het onderzoek het dringend vordert voor dezelfde misdrijven als bij de pseudo-koop, maar die gezien hun aard “of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde” opleveren. De voorwaarden voor de toepassing van de infiltratie zijn dus strenger dan voor de twee andere undercoveroperaties omdat er hier, zoals in België, een subsidiariteitsbeginsel van toepassing is.

2. Vergelijking met de Belgische regeling van de online infiltratie

2.1. Machtiging in spoedeisende gevallen

In tegenstelling tot wat in artikel 46sexies Sv. wordt bepaald, bestaat er geen mogelijkheid in de Nederlandse regeling van de infiltratie om in spoedeisende gevallen de machtiging tot infiltratie mondeling te verstrekken om die daarna zo snel mogelijk schriftelijk te bevestigen. Dit is wel mogelijk voor de pseudo-koop of pseudo-dienstverlening en de stelselmatige inwinning van informatie. Zelfs als de infiltratie verregaandere gevolgen inhoudt dan de twee operaties, lijkt een soepelere regeling voor spoedeisende gevallen wel wenselijk, gezien de vluchtigheid die het internet kenmerkt. Inderdaad, er wordt een snelle reactie verwacht om tegenmoet te komen aan de snelheid van de informatie-uitwisseling die in de cyberwereld plaatsvindt. Het ontbreken van mondelinge machtiging kan dus in bepaalde gevallen de politieonderzoeken belemmeren.

---

369 J.-J. OERLEMANS, Normering van digitale opsporingsmethoden, Breda, Nederlandse Defensie Academie, 2017, p. 27.
370 Memorie van Toelichting, Wetsvoorstel tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden), Kamerstukken II 1996-1997, 25 403, nr. 3, p. 29.
371 Het gaat namelijk over de misdrijven die omschreven zijn in het eerste lid van artikel 67 van het Wetboek van Strafvordering.
372 Artikel 126h, eerste lid van het Nederlandse Wetboek van Strafvordering.
2.2. Tijdsduur van de infiltratie

Een ander verschil tussen de Nederlandse en Belgische regeling van de online infiltratie, is dat er behalve voor de stelselmatige inwinning van informatie van artikel 126j WS, niets over een bepaalde maximum tijdsduur van de operatie wordt gezegd in de Nederlandse regeling. Het Nederlandse wettelijk kader biedt dus de basis voor zowel kortstondige als langdurige infiltratieacties.\textsuperscript{374} Inderdaad, zowel bij de infiltratie van het artikel 126h WS, als bij de pseudo-koop of pseudo-dienstverlening van artikel 126i WS, wordt er in het derde lid van het artikel bepaald dat het bevel tot de operatie de geldigheidsduur van de operatie of de periode waarbinnen aan het bevel uitvoering wordt gegeven, moet vermelden. Volgens de vijfde paragraaf van beide artikelen kan dit bevel achteraf nog schriftelijk en met opgave van redenen verlengd worden. Voor het stelselmatig inwinnen van informatie geldt daarentegen wel een maximale tijdsduur van drie maanden, die “telkens voor een periode van ten hoogste drie maanden worden verlengd”.\textsuperscript{375} Dit kan als eigenaardig worden beschouwd, zeker gezien het feit dat de infiltratie als een meer verregaande maatregel, dan de online undercover interacties wordt beschouwd, omdat bij de infiltratie de opsporingsambtenaren daadwerkelijk participeren in een criminale organisatie.\textsuperscript{376} De afwezigheid van een maximale tijdsduur voor de geldigheid van de bevelen, kan als een goede regeling worden beschouwd, aangezien we de beperking van de geldigheidsduur van de machtigingen in de Belgische regeling als ongeschikt beschouwen. Zelfs als het steeds mogelijk is, volgens de Belgische regeling, om deze tijdsduur te verlengen, kan het ontbreken van een wettelijke tijdslimiet als meer aangepast aan de cyberwereld worden beschouwd. Het is inderdaad een zeer complexe wereld, waarin de online infiltratie in bepaalde gevallen op een zeer korte periode moet plaatsvinden, maar die zich in andere gevallen ook over een zeer lange periode kan dienen te spreiden om het vertrouwen van de doelwitten van de operatie in te winnen. Daarom zou een grotere vrijheid ten aanzien van de tijdsduur van de machtiging tot de operatie wenselijk zijn om te vermijden dat de procedurele voorschriften in de weg zitten van een effectief onderzoek. De Belgische wetgever zou zich kunnen laten inspireren door de Nederlandse regeling, door bijvoorbeeld extra voorwaarden te stellen voor de selectie en opleiding van de infiltranten, en de organisatie van de operatie wanneer het gaat over van

\textsuperscript{374} Memorie van Toelichting, Wetsvoorstel tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden), Kamerstukken II 1996-1997, 25 403, nr. 3, p. 31.
\textsuperscript{375} Artikel 126j, tweede lid van het Nederlandse Wetboek van Strafvordering.
\textsuperscript{376} J.-J. OERLEMANS, Normering van digitale opsporingsmethoden, Breda, Nederlandse Defensie Academie, 2017, p. 27.
een lange termijninfiltratie. Verder is het niet zomaar mogelijk voor de opsporingsambtenaren om de operatie onbeperkt en nutteloos te laten duren. In de vijfde paragraaf van de artikelen over de infiltratie en de pseudo-koop of pseudo-dienstverlening wordt immers verwezen naar het zevende lid van artikel 126g WS, waar er bepaald wordt dat wanneer er niet meer wordt voldaan aan de voorwaarden van het eerste lid van artikel 126h en 126i het bevel door de officier van justitie wordt beëindigd. De regeling omtrent de tijdsduur van de operatie van de artikelen 126h en 126i WS lijken daarvoor meer aangepast te zijn aan de complexiteit van de onderzoeken die plaatsvinden op het internet.

2.3. De online pseudo-koop en pseudo-dienstverlening

In België, worden de pseudo-koop en de gecontroleerde aflevering en doorlevering beschouwd als politonelle onderzoekstechnieken die als ondersteuning voor de bijzondere opsporingsmethoden aangewend kunnen worden volgens het koninklijke besluit van 9 april 2003. In tegenstelling tot wat er in artikel 47octies Sv. voor de offline infiltratie wordt bepaald, heeft de Belgische wetgever geen verwijzingen naar deze onderzoekstechnieken gedaan in artikel 46sexies Sv. omdat de online infiltratie niet als een bijzondere opsporingsmethode wordt beschouwd, zodat het niet mogelijk is om beroep te doen op de pseudo-koop of pseudo-dienstverlening in het kader van de online infiltratie in tegenstelling tot in Nederland. Het zou nochtans wenselijk kunnen zijn om de toepassing van zulke onderzoekstechnieken mogelijk te maken, aangezien het door het in principe eenmalige karakter van de operatie, als een minder ingrijpende maatregel dan de infiltratie moet worden beschouwd.

2.4. Gelijke regeling van de online en de offline infiltratie

Zoals we het hebben kunnen opmerken is de Nederlandse regeling van de infiltratie zeer verschillend van de Belgische regeling. In Nederland wordt de infiltratie in drie verschillende undercoveroperaties ingedeeld, die zowel in de fysieke wereld als de cyberwereld van toepassing kunnen zijn, met verschillende voorwaarden in functie van de graad van inmenging in het privéleven, de verregaande gevolgen die ze kan hebben ten

---

aanzien van de verdachten en de risico’s die de operatie meebrengt, terwijl er een onderscheid wordt gemaakt tussen de online en offline wereld in België. We kunnen ons dus afvragen welke wettelijke regeling het meest geschikt is om effectieve middelen in te zetten die voldoende aangepast zijn aan de technologische evolutie. Zoals we het in het eerste deel hebben gezien, bestaan er fundamentele verschillen tussen de online en offline wereld. Het feit dat sinds het jaar 2000 de Nederlandse wetgever de keuze heeft gemaakt om de verschillende bijzondere opsporingsbevoegdheden ook toepasbaar te verklaren voor onderzoeken op het internet, kan dus als verrassend worden beschouwd. De risico’s die de undercoveragenten lopen, zijn inderdaad veel hoger bij een fysieke infiltratie in een crimineel milieu dan in de cyberwereld. Het is juist omdat politieambtenaren aan dergelijke bijzondere risico’s kunnen blootstaan en dat de maatregel veel indringender is ten aanzien van fundamentele rechten, dat het toepassingsgebied van de offline infiltratie beperkt wordt tot de opsporing van ernstige misdrijven.\textsuperscript{380} De infiltratie die uitsluitend plaatsvindt op het internet zal wellicht sneller goedgekeurd worden in Nederland dan de infiltratie in de fysieke wereld door de Centrale Toetsingscommissie (CTC), die een adviesorgaan van het College van Procureurs-Generaal is, maar dit volstaat niet omdat de rechters niet door deze adviezen gebonden zijn.\textsuperscript{381} Het is bovendien niet enkel het bijzonder hoog risico die de infiltranten tijdens de uitvoering van de operaties lopen, die het strikt toepassingsgebied kan rechtvaardigen, maar ook het feit dat het vertrouwen van de verdachte door de opsporingsambtenaar kan worden geschonden.\textsuperscript{382} Daarom is er een subsidiariteitsvoorwaarde van toepassing op de Nederlandse infiltratie, in tegenstelling tot de twee andere undercoveroperaties, zoals in de Belgische regeling van beide soorten infiltraties. Het feit dat dezelfde voorwaarden verbonden zijn aan de online infiltratie die minder indringend is, maakt de Nederlandse regeling van de online infiltratie te voorzichtig en te beperkend ten aanzien van de meerwaarde die een online infiltratie voor het onderzoek van tal van misdrijven zou kunnen brengen.

De keuze van de Belgische wetgever om een onderscheid te maken tussen de twee werelden blijkt dus gerechtvaardigd te zijn en is meer aangepast aan de voordelen die de

\textsuperscript{380} Memorie van Toelichting, Wetsvoorstel tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden), Kamerstukken II 1996-1997, 25 403, nr. 3, p. 29.
\textsuperscript{382} Memorie van Toelichting, Wetsvoorstel tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden), Kamerstukken II 1996-1997, 25 403, nr. 3, p. 30.
technologische evolutie aan het onderzoek kan bieden. Zelfs als er een gradatie is in de toepassingsvoorwaarden van drie verschillende vormen van undercoveroperaties, blijft de Nederlandse regeling blind aan de bijzonderheden en de kenmerken van de cyberwereld. Zoals Siemerink het doet opmerken is een aparte regeling van de cyberinfiltratie ook steeds aan te raden, omdat het in de cyberwereld gemakkelijker is om een andere identiteit te nemen. Daarnaast zou een aparte regeling, ook kunnen voorkomen dat er misbruik wordt gemaakt van de infiltratie, omdat het de CTC in staat zou stellen om specifieke toetsingscriteria te ontwikkelen voor de operaties die op het internet geschieden en dat er veel meer controlemogelijkheden zijn bij de online infiltratie.\textsuperscript{383}

2.5. De bijstand aan de opsporing door burgers

Een ander verschil tussen de Belgische regeling en de Nederlandse regeling, is dat de burgerinfiltratie wel mogelijk is in Nederland, terwijl het nog strikt verboden is in België om beroep te doen op burgerinfiltranten.\textsuperscript{384} De bijstand aan de opsporing door burgers heeft een wettelijke basis gekregen met de Wet BOB in de artikelen 126v tot 126z WS. Zowel de burgerinfiltratie van artikelen 126w en 126x WS dan de burgerpseudo-koop of burgerdienstverlening van artikelen 126ij en 126z WS zijn allebei onderworpen aan een bijkomende subsidiariteitsvereiste omdat er slechts toepassing kan worden gemaakt van deze bijstand door burgers wanneer de politiële infiltratie of de politiële pseudo-koop of pseudo-dienstverlening niet mogelijk zijn. We moeten dit verschil met de Belgische regeling wel relativeren aangezien de politiediensten overeenkomstig de eerste paragraaf van artikel 46sexies Sv. in bepaalde situaties een kortstondig beroep kunnen doen op burgerdeskundigen en dat deze mogelijkheid vanuit een zeker oogpunt minder noodzakelijk is voor de online infiltratie dan de offline infiltratie, omdat de politiediensten zich hier achter hun scherm kunnen laten bijstaan door burgerdeskundigen wanneer ze een complex milieu infiltreren zonder dat ze daarmee hun geloofwaardigheid verliezen.

\textsuperscript{384} Dit is niettemin onderhevig aan veranderingen met het wetsontwerp van 19 februari 2018.
Hoofdstuk 6. Effectiviteit van de online infiltratie

Het is nog te vroeg om daadwerkelijk de impact van de online infiltratie op de opsporing van misdrijven die via het internet als facilator worden gepleegd, te kunnen waarnemen. In een tijdsduur van amper meer dan één jaar hebben de politiediensten deze operatie nog onvoldoende kunnen aanwenden, gezien de strikte toepassingsvoorwaarden die eraan verbonden zijn, om de effectiviteit van de operatie op de bestrijding van de cybercriminaliteit te kunnen meten. Niettemin de bestudering van de wettelijke regeling van de online infiltratie in de vorige hoofdstukken, geeft ons de gelegenheid om te beoordelen of deze op een optimale manier beantwoordt aan de nood aan efficiënte middelen die voldoende aangepast zijn aan de technologische evolutie.

Eerst en vooral kunnen we vaststellen dat de wetgever met de wet van 25 december 2016 klaarblijkelijk rekening heeft gehouden met de noodzaak van een betere aanwending van de technologische middelen voor het onderzoek. Hiermee heeft hij voldoening gegeven aan de eis van de Kadernota Integrale Veiligheid om de wetgeving betreffende de bijzondere opsporingsmethoden en de maatregelen die verband houden met internet en telecommunicatie aan te passen aan de technologische evolutie.385 De versoepeling van de toepassingsvoorwaarden van de infiltratie, wanneer ze uitsluitend op het internet plaatsvindt, is een eerste belangrijke stap om te beantwoorden aan de nood aan efficiënte middelen die voldoende aangepast zijn aan de technologische evolutie. Het feit dat de online infiltratie niet beperkt is tot het onderzoek van informaticacriminaliteit, zowel specifieke en niet-specifieke, maar kan worden uitgevoerd voor het onderzoek van eender welke strafbare feiten die een correctionele hoofdgevangenisstraf van een jaar tot gevolg kunnen hebben, was een goed keuze van de wetgever. Hedendaags neemt de ICT steeds een belangrijkere plaats in onze dagelijkse leven, zodat zelfs als de misdrijven niet door middel van de informatietechnologie wordt gepleegd, deze toch vaak een link vertonen met de ICT. Het is onderdaad soms gemakkelijker om in contact te komen met verdachten in de online wereld dan in de offline wereld, omdat ze daar over meer mogelijkheden beschikken om hun identiteit en die van hun omgeving beter af te schermen. Daarnaast heeft de wetgever bepaalde procedurele vereisten en voorschriften van de offline infiltratie, namelijk omtrent de machtiging die door de procureur des Konings moet worden verleend, niet overgenomen in de regeling van de online

infiltratie. Deze keuze van de wetgever speelt ook in het voordeel van de effectiviteit van de operatie omdat het de aanwending ervan vergemakkelijkt.

Voor een efficiënte en daadwerkelijke aanpak van het fenomeen criminaliteit dient tevens de nodige gespecialiseerde kennis opgebouwd en in standgehouden te worden. In het wetsontwerp inzake informaticacriminaliteit van 3 november 1999 werd er al vastgesteld dat de opsporing en de bewijsvoering “als het voornaamste probleem worden ervaren bij de bestrijding van de criminaliteit op de informatiesnelweg” en dat het grotendeels te verklaren is door “de techniciteit van de materie en de nood aan specialisatie bij de politie en gerechtelijke diensten”. Het is inderdaad van cruciaal belang voor het welslagen van de uitvoering van de online infiltratie, dat de politieambtenaren die als infiltrant optreden over voldoende kennis over het milieu dat ze gaan infiltreren, beschikken. Omdat relevante gegevens voor het onderzoek zeer snel vernietigd kunnen worden, is het meer dan nodig dat politiediensten goed getraind en opgeleid zijn. Deze vereiste van investering in de opleiding en in een voortdurende uitwisseling van expertise en kennis tussen de verschillende schakels van de veiligheidsketen werd tevens ook al geuit in de Kadernota Integrale Veiligheid. Zoals reeds gezien, moeten de voorwaarden van de opleiding en de nadere regels van de aanwijzing van de bevoegde politiediensten nog in een koninklijke besluit worden vastgelegd. Dit zal dus in grote mate de effectiviteit van de operatie bepalen. We kunnen niettemin de keuze van de wetgever om de kring van de bevoegde infiltranten te vergroten, en dus niet enkel meer te beperken tot de leden van het undercoverteam bij de DSU zoals het geval is voor de offline infiltratie, met speciaal opgeleide speurders die gespecialiseerd zijn in een bepaald criminaliteitsdomein, goedkeuren. Zoals we het reeds in hoofdstuk 2 van dit deel hebben gezien, zou het meer armslag geven om op een gerichtere manier vooruitgang te boeken in het onderzoek. We kunnen dus hier te maken hebben met politiediensten die over een grotere deskundigheid beschikken over het milieu dat ze infiltreren. Bovendien, kunnen de infiltranten overeenkomstig de eerste paragraaf van het artikel 46sexies Sv. in uitzonderlijke omstandigheden en mits uitdrukkelijke machtiging van de procureur des

388 Artikel 46sexies, §1 eerste lid Sv.
390 Zie deel II, hoofdstuk 2, afdeling 2.
Konings, kortstondig beroep kunnen doen op burgerdeskundigen. Dit zorgt ervoor dat ze dan over voldoende expertise kunnen beschikken, zeker in complexere situaties. Zelfs als we hier in principe te maken zullen hebben met meer gespecialiseerde speurders in een bepaald criminaliteitsdomein dan bij de offline infiltratie, kunnen we niettemin het feit dat de infiltranten zich slechts kortstondig kunnen beroepen op de expertise van de burgerdeskundigen betrekken. Het zou inderdaad in bepaalde situaties wenselijk kunnen zijn voor het welslagen van de operatie dat ze voortdurend over dezelfde expertise beschikken om de hele operatie niet te doen verraden.

Een verlenging van de tijdsduur van de operatie of de mogelijkheid om politionele onderzoekstechnieken te gebruiken tijdens de uitvoering van de online infiltratie, zou deze nog toestaan om effectiever te zijn. We kunnen inderdaad betreuren dat de wetgever hier dezelfde keuze voor de tijdsduur als bij de offline infiltratie heeft gemaakt, terwijl de maatregel als minder indringend moet worden beschouwd. Zelfs als het nog steeds mogelijk is om deze tijdsduur te hernieuwen, zouden de procedurele voorschriften in de weg kunnen staan van een effectief onderzoek. Zoals we het al hebben gezegd, is de cyberwereld een complexe wereld waar de transacties soms zeer snel plaatsvinden, terwijl het in andere situaties veel tijd kan vergen voordat de infiltranten het vertrouwen van de doelwitten winnen om belangrijke bewijsstukken te verzamelen, zodat het wenselijk zou zijn om de tijdsduur niet meer te beperken, maar ervoor zorgen dat de machtiging wordt beëindigd van zodra er aan de toepassingsvoorwaarden niet meer wordt voldaan, zoals het geregeld is in Nederland. De voorzichtigheid van de wetgever ten aanzien van de tijdsduur van de operatie valt nog minder te begrijpen door het feit dat er al in het wetsontwerp van de BOM-wet werd verklaard dat de risicograad van de infiltratie niet vanzelfsprekend proportioneel is aan de tijdsduur ervan.392 Het betreft bovendien de offline infiltratie die meer risicovol wordt beschouwd.

In het algemeen kunnen we vaststellen dat de wetgever met de invoering van de online infiltratie, een belangrijk instrument heeft gegeven aan de politiediensten om niet alleen de informaticacriminaliteit te bestrijden maar ook om bewijsstukken te verzamelen voor een groot aantal misdrijven. De versoepeling van de toepassingsvoorwaarden die voor de offline infiltratie gelden, is hier gerechtvaardigd ten aanzien van de waarborgen dat de ICT kan brengen. De opnames van alle contacten tussen de infiltranten en de doelwitten van de operatie zowel als de afwezigheid van fysieke contacten, zorgen er inderdaad voor dat men

392 Zie deel II, hoofdstuk 3; Memorie van Toelichting, Wetsontwerp betreffende de bijzondere opsporingsmethode en enige andere onderzoeksmethoden, Parl.St., Kamer, 2001-2002, nr. 50-1688/001, p. 34.
minder bezwaren kan hebben tegenover de toepassing van deze operatie voor minder ernstige misdrijven.
In dit deel gaan we ons afvragen tot waar de online infiltratie mogelijk en toelaatbaar is om de fundamentele rechten van de burgers niet op een ongeoorloofde manier te schenden. Deze vraag is zeer relevant in de huidige context, omdat er in Europa en in de hele wereld een belangrijke kloof bestaat tussen enerzijds het wettelijk fundamenteel recht van vrijheid van meningsuiting en anderzijds de verzameling van gegevens om niet-democratische, immorele en illegale activiteiten te bestrijden en dus de veiligheid te verzekeren. Er zijn steeds twee belangrijke belangen die tegenover elkaar op het spel staan, namelijk de effectiviteit en de vooruitgang van het onderzoek tegenover de ethische principes en fundamentele rechten van de burgers.

Deze vragen zijn zeer belangrijk bij de toepassing van bijzondere opsporingsmethoden en andere zeer indringende maatregelen omdat de overheid, hier soms afstand gaat doen van belangrijke principes zoals het vertrouwen en de loyauteit, die het moet tonen ten aanzien van de burgers, door verschuilen te handelen om bepaalde strafbare feiten effectief te onderzoeken en dus de criminaliteit te bestrijden. Er bestaat dus een belangrijk moreel conflict wanneer het toegelaten is aan de politiediensten om bepaalde strafbare feiten voor het welslagen van het onderzoek te plegen of wanneer het plegen van bepaalde strafbare feiten door misdadigers verdragen en aanvaard wordt door de politiediensten om het onderzoek te doen opschieten. Met de invoering van de online “light” infiltratie, is het dus belangrijk om na te kijken als de versoepeling van de toepassingsvoorwaarden de waarborgen van de fundamentele rechten niet in het gedrang heeft gebracht.


Hoofdstuk 1. Recht op eerbiediging van het privéleven

Afdeling 1. Evenwicht tussen het recht op privéleven en de veiligheid

Door de technologische evolutie die plaatsvindt en de dataficatie van bijna alles door de regeringen en het bedrijfsleven, wordt het recht op privéleven van de burgers volgens artikel 22 van de Belgische Grondwet en artikel 8 EVRM steeds meer en meer aangetast. Dit laatste artikel bevat tevens een positieve verplichting voor de lidstaten “om de schendingen van dit recht op privacy ook daadwerkelijk te kunnen onderzoeken, de daders te kunnen identificeren en te vervolgen”. We kunnen ons dus afvragen hoe ver de politiediensten mogen gaan in het gebruik van de mogelijkheden die het internet en de infomarticatechnologieën hen bieden om de cybercriminaliteit effectief te bestrijden, zonder dat het recht op privéleven te veel wordt aangetast. In zijn advies over het wetsontwerp van de wet van 25 december 2016 had de Commissie voor de bescherming van de persoonlijke levenssfeer tevens verklaard dat ze van mening was “dat interacties op het internet een impact kunnen hebben op de privacy van de betrokkene”. Het is dus hier relevant om na te kijken of de wetgever er in is geslaagd om maatregelen te nemen die zowel de veiligheid als de privacy effectief nastreven en beschermen. Wat is de gewenste grens die niet mag worden overschreden om toch een juist evenwicht te bewaren tussen de effectiviteit van het onderzoek en de eerbiediging van fundamentele rechten? Is het nog mogelijk om de cybercriminaliteit effectief te bestrijden door middel van de online infiltratie zonder het recht op eerbiediging van het privéleven op een ongeoorloofde manier aan te tasten?

Een belangrijk verschil met de offline wereld is dat de anonimiteit een zeer belangrijke plaats heeft ingenomen op het internet. Veel internetgebruikers verschuilen zich echter achter een fictieve identiteit om hun recht op vrije meningsuiting, privéleven en privécommunicatie te beschermen. Het gebruik van sociale netwerken door de politiediensten tijdens het onderzoek werpt geen nieuwe vragen op, maar is slechts een vernieuwde uiting in de huidige

context van oude fenomenen zoals veiligheidsmanagement, privacy en informatie-uitwisseling. Politiemediensten moeten dus leren omgaan met platformen zoals Facebook of Twitter en duidelijk weten wat de grenzen zijn tussen het privé en het publiek gebruik van sociale media in het kader van de beoefening van hun professionele activiteiten. Dit kan het vertrouwen in de politiediensten onder druk zetten omdat burgers terughoudend zijn ten aanzien van inmenging van de overheid in hun privéleven. De politiediensten moeten dus het juiste evenwicht vinden in de aanwending van sociale netwerken voor het onderzoek, want hoewel het de communicatie met de burgers en de informatieverbreiding door de burgers kan bevorderen, kan het ook de fundamentele rechten van de burgers inperken en dus wantrouwen opwekken in de bevolking ten aanzien van de politie, wat contraproducentief voor het onderzoek zou zijn. Het juiste evenwicht vinden is een zeer moeilijke zaak omdat de bestrijding van de cybercriminaliteit zich voordoet in een vluchtig context, waar de informatietechnologie op een hoog tempo evolueert, zodat de noodzakelijke maatregelen voor de bestrijding van de criminaliteit vlug kunnen veranderen.

**Afdeling 2. Toegelaten beperking van het recht op privéleven**

Het recht op eerbiediging van het privéleven is echter niet absoluut. Volgens artikel 8 EVRM zijn inmengingen in het recht op eerbiediging van het privéleven toegestaan wanneer deze bij de wet zijn voorzien en in een democratische samenleving noodzakelijk zijn “in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen”. Om na te kijken als een inmenging in het recht toegelaten is, moeten wij dus niet alleen de beoogde veiligheid, die door de geadopteerde maatregel zal worden bereikt, afwegen tegenover de aantasting van het recht op privéleven, maar moeten wij eerder de daadwerkelijke impact die de geadopteerde maatregel zal hebben op de verbetering van de veiligheid beoordelen tegenover de vereiste van proportionaliteit en subsidiariteit. Meer veiligheid betekent dus niet per se, dat het recht op privéleven proportioneel daardoor kan worden aangetast. De confrontatie tussen het recht op eerbiediging van het privéleven en de

---

400 W. BRUGGEMAN, “Politie, justitie en (nieuwe) sociale media. De sporen gelegd, (te) weinig reizigers, de trein gemist, de trein ontspoord?”, *Panopticon* 2012, afl. 3, p. 204.
402 Artikel 8§2 EVRM.
veiligheid is bovendien te simplistisch en niet wenselijk omdat beide belangen niet op dezelfde manier kunnen worden overwogen. Beide zijn inderdaad mogelijk te combineren.

De schending van het recht op het privéleven die de online infiltratie mogelijk kan teweegbrengen zou hier door een legitiem doel verantwoord worden, namelijk de opsporing van strafbare feiten en de identificatie en vervolging van de daders om zo de informaticacriminaliteit te bestrijden. Het Europees Hof voor de Rechten van de Mens (EHRM) heeft trouwens Finland in een arrest van 2008 veroordeeld omdat daar voorrang werd gegeven aan het recht op privéleven en privacy van internetgebruikers tegenover het recht van een kind dat slachtoffer was van identiteitsmisbruik.

1. Offline infiltratie

Eerst moeten wij ons afvragen of de online infiltratie op zich als een schending op het recht op privéleven moet worden beschouwd, om te bepalen waar de wenselijke grens voor de politiediensten moet liggen. De maatregel zou een inmenging in het recht op eerbiediging van het privéleven in de zin van artikel 8 EVRM kunnen uitmaken, door het feit dat de politieambtenaren in het kader van de uitoefening van de maatregel onder een fictieve identiteit contact kunnen nemen met de doelwitten van de operatie en zich dus binnendringen in het leven van deze personen. Het EHRM heeft tot nu toe nog niet geoordeeld dat de infiltratie op zich als een inmenging in het recht op privéleven wordt beschouwd. We kunnen hier namelijk denken aan het arrest Lüdi tegen Zwitserland van 15 juni 1992 waar het Hof vond dat er geen inmenging was.

De situatie is echter wel anders wanneer er list wordt gebruikt bij de uitvoering van de operatie, wanneer het huis van het doelwit van de operatie wordt binnengedrongen door de infiltrant of dat de communicaties door de infiltrant worden opgenomen. De situatie is hier


2. **Online infiltratie**

De rechtsspraak van het Hof van Cassatie en het EHRM, die we hierboven hebben gezien, betreft desondanks slechts de klassieke offline infiltratie, zodat we niet weten als we deze rechtsspraak ook per analogie kunnen toepassen op de online infiltratie. In meerdere opzichten kunnen wij niettemin vaststellen dat de online infiltratie minder indringend is, zodat deze maatregel op zich sowieso ook niet als een schending op het recht op privéleven moet worden beschouwd.

Een belangrijk verschil tussen de online en de offline infiltratie is dat bij de toepassing van de online infiltratie alle contacten dat de infiltranten met de doelwitten van de operatie onderhouden door de passende technische middelen sowieso worden geregistreerd en bij het dossier worden gevoegd of ter griffie.\footnote{Artikel 46sexies, §4 tweede lid Sv.} Dit lijkt verder te gaan dan bij de offline infiltratie, maar men moet niet vergeten dat de twee werelden fundamenteel verschillend zijn. Terwijl het moeilijk is om veel aspecten van zijn leven te verbergen in de fysische wereld, zal de infiltrant vaak geconfronteerd worden met mensen die onder een anonieme identiteit handelen.
op het internet. Het is mogelijk maar wel veel moeilijker, en niet altijd toegestaan, om de reële identiteit van internetgebruikers in het kader van een onderzoek te onthullen. De registratie van de contacten tussen de infiltranten en de doelwitten moet dus niet als een disproportionele maatregel worden beschouwd, omdat deze registratie vooral voor een eventuele controle a posteriori van de uitvoering van de operatie wordt aangewend, en dus in het voordeel van het recht op een eerlijk proces van artikel 6 EVRM wordt toegepast.

Zoals we het al hebben gezien\(^{413}\) kan de online infiltratie voor de opsporing van een grotere verscheidenheid van misdrijven worden aangewend. Het zou dus kunnen betekenen dat de operatie een minder grote aantasting van het recht op eerbiediging van het privéleven inhoudt dan de offline infiltratie, aangezien het ook voor minder ernstige misdrijven kan worden aangewend. De maatregel moet inderdaad proportioneel zijn aan het nagestreefde doel, zodat normaal gezien de operatie minder verregaande negatieve gevolgen voor de burgers mag behalen, wanneer het ook in het kader van de opsporing en het onderzoek van minder ernstige misdrijven kan worden uitgevoerd. Het privéleven van de doelwitten van de operatie en hun omgeving moet dus minder aangetast worden dan in het kader van de opsporing van de ernstiger misdrijven die een offline infiltratie rechtvaardigen. Daarnaast is de online infiltratie, zoals de offline infiltratie, onderworpen aan een subsidiariteitsvoorwaarde, die ervoor zorgt dat de eventuele aantasting van het recht op privacy die deze maatregel kan teweegbrengen door de EVRM, kan gerechtvaardigd worden aangezien de politiediensten slechts voor deze operatie zullen kunnen opteren, wanneer ze het onderzoek niet kunnen oplossen door andere middelen van onderzoek.

Met de invoering van de nieuwe maatregel van online infiltratie in het Wetboek van strafvordering, is het dus belangrijk om stil te staan bij de verscheidene keuzes die gemaakt werden door de wetgever om het privéleven en de persoonsgegevens van de internetgebruikers zo weinig mogelijk aan te tasten. De infiltratie kan zeer indringend zijn en veel nefaste gevolgen teweegbrengen voor mensen die zich in de omgeving bevinden van de doelwitten van de operatie. In artikel 46sexies Sv. heeft de wetgever ervoor gekozen om niet op te leggen dat de contact tussen de infiltrant en het doelwit van de operatie duurzaam moet zijn. Dit verschil tussen de twee soorten infiltratie, verklaart zich door de kenmerkende vluchtigheid van de cyberwereld, waar interacties en strafbare activiteiten ook op een ogenblik kunnen geschieden, maar zorgt er ook voor dat er zo weinig mogelijk wordt

\(^{413}\) Zie deel II, hoofdstuk 2, afdeling 2.
binnengedrongen in het privéleven van niet-verdachten die ook in contact kunnen zijn met het doelwit van de operatie. Dus zelfs als er voor een grotere verscheidenheid van misdrijven kan worden gegaan tot de aanwending van de cyberinfiltratie, tegenover de offline infiltratie, kan de operatie effectief blijven zonder het recht op privéleven te veel aan te tasten omdat de contacten tussen de infiltranten en het milieu die ze binnendringen hier dus minder intens en minder crimineel is in een zekere zin dan bij een offline infiltratie.\textsuperscript{414} Daarnaast, zoals wat ongeveer van toepassing is voor de offline infiltratie, is de online infiltratie ook in de tijd beperkt, wat bevorderlijk kan zijn om de fundamentele rechten niet op een ongeoorloofde manier te schenden.

Omdat er bij de uitvoering van de operatie altijd sprake zal zijn van misleiding, vermits de politiediensten hiervoor een vals opgewekt en opgebouwd vertrouwen tot stand brengen en onderhouden, kunnen wij niet beweren dat er geen sprake is van afwezigheid van aantasting van de redelijke privacyverwachting van de doelwitten van de operatie.\textsuperscript{415} Om te beoordelen of de maatregel toch gerechtvaardigd kan worden, moet er dan worden gekeken naar de voorzienbaarheid van de bepaling van de online infiltratie en naar de privacyverwachting van de doelwitten van deze operatie.\textsuperscript{416} Eerst kunnen we vaststellen dat de maatregel een hogere voorzienbaarheid heeft dan de acties van de internetpatrouilles die slechts mogelijk zijn op de voor het publiek toegankelijke plaatsen overeenkomstig 26 WPA, maar die door het Hof van Cassatie ook een extensieve interpretatie heeft gekregen naar algemeen toegankelijke plaatsen op het internet.\textsuperscript{417} In dit opzicht is de online infiltratie dus voorspelbaar omdat men weet dat de politiediensten “plaatsen” in de cyberwereld mogen infiltreren, inclusief het dark web, zelfs door middel van een geloofwaardige fictieve identiteit, omdat aan deze maatregel striktere voorwaarden verbonden zijn om de fundamentele rechten van de burgers niet op een ongeoorloofde manier te schenden. Zoals we het supra hebben gezien\textsuperscript{418}, wordt er in de memorie van toelichting verduidelijkt dat het begrip “internet” dat we in het artikel 46sexies Sv. terugvinden, in de ruime zin wordt begrepen en dat zowel het niet-verborgen deel van het


\textsuperscript{417} Zie deel I, hoofdstuk 2, afdeling 2.

\textsuperscript{418} Zie deel II, hoofdstuk 2, afdeling 2.
internet als het dark web omvat.\textsuperscript{419} Daarnaast kunnen we vaststellen dat de toepassing van de online infiltratie moeilijker te rechtvaardigen is ten aanzien van de eerbiediging van het recht op privéleven, wanneer ze aangewend wordt in het kader van een proactief onderzoek naar minder ernstige misdrijven. Daartoe zouden we kunnen stellen dat het wenselijk zou zijn om de mogelijkheid om de online infiltratie in het kader van een proactief onderzoek te beperken tot ernstige misdrijven, net zoals dat geregeld is voor de offline infiltratie. Dit zou niettemin de effectiviteit van de maatregel in zekere mate kunnen aantasten, maar zou ervoor zorgen dat een evenwicht wordt bewaard tussen de bescherming van de recht op privéleven en de bestrijding van de criminaliteit.

Er dienen niettemin minder waarborgen voor het recht op privéleven aan de online infiltratie dan aan de regeling van de observatie te worden ingesteld, omdat er in tegenstelling tot de observatie, die geregeld is in artikel 47sexies Sv., de doelwetten hier niet heimelijk bewaakt worden. Het is ook belangrijk voor het welslagen van het onderzoek dat de politieambtenaren over genoeg vrijheden beschikken om zich goed te kunnen integreren in het milieu dat ze infiltreren.\textsuperscript{420} Strenge voorwaarden die het recht op eerbiediging van het privéleven van de burgers waarborgen zoals bij de regeling van de observatie zijn dus hier niet wenselijk voor de effectiviteit van de maatregel. Bovendien zijn de infiltranten slechts op basis van artikel 46sexies Sv. gemachtigd om contacten te onderhouden met de doelwetten van de operatie. Deze contacten worden echter niet gedwongen door de infiltranten, zodat de doelwetten enkel communiceren wat ze wensen te communiceren aan de infiltranten. Deze communicatie zou niettemin niet plaatsvinden wanneer de doelwetten niet misleid waren geweest over de identiteit van de personen met wie ze communiceren. De verhouding tussen het recht op privéleven en de vrijheid waarover infiltranten dienen te beschikken, is dus een complexe verhouding.

Bovendien moeten wij ook voor ogen houden dat zelfs als de politiediensten onder een fictieve hoedanigheid contact opnemen met de verdachten, de rechtstreekske omgeving van het doelwit van de operatie blijft vaak anoniem en zeker wanneer de infiltratie zich voordoet in een georganiseerd crimineel milieu.

\textsuperscript{419} Memorie van Toelichting, Wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, \textit{Parl.St.}, Kamer, 2015-2016, nr. 54-1966/001, p. 36.
Afdeling 3. Conclusie

In het algemeen kunnen wij stellen dat de Belgische regeling van de online infiltratie een juist evenwicht bewaart tussen de veiligheid en de fundamentele rechten van de burgers. De soepelere regeling van de online infiltratie ten aanzien van de klassieke infiltratie is gerechtvaardigd aangezien deze minder indringend is. De kenmerkende anonimiteit van de online wereld zorgt er inderdaad voor dat de politiediensten het recht op privéleven van de doelwitten van de operatie en hun omgeving minder vlug aantasten. Bovendien kan de operatie slechts worden aangewend wanneer er geen minder indringende maatregel toegepast kan worden voor het onderzoek. De wetgever heeft dus voldoende waarborgen voor het recht op privéleven aan de toepassing van de online infiltratie verbonden, zonder dat de effectiviteit van het onderzoek daarvoor naar de achtergrond werd verdrongen.
Hoofdstuk 2. Het provocatieverbod

Afdeling 1. Het algemeen provocatieverbod

Eén van de grootste gevaren tijdens de uitvoering van de online infiltratie, is dat de politieambtenaren die als infiltranten optreden zich schuldig maken aan uitlokking. Dit gevaar is des te groter bij de infiltratie, omdat de operatie ook aangewend kan worden in het kader van het proactief onderzoek, wanneer er ernstige aanwijzingen bestaan dat strafbare feiten gepleegd gaan worden. Politiediensten anticiperen hier de voorkoming van een bepaald misdrijf, waardoor ze misschien de neiging zouden hebben om dit misdrijf uit te lokken om het onderzoek sneller te kunnen afronden.421

Volgens het artikel 30 van de Wet houdende de voorafgaande titel van het Wetboek van Strafvordering is een strafvordering onontvankelijk wanneer de politieambtenaren, “of een derde handelend op het uitdrukkelijk verzoek van deze ambtenaar”, het voornemen om een misdrijf te plegen heeft doen ontstaan, verstrekt, of heeft bevestigd terwijl de dader dit wilde beëindigen. Dit algemeen provocatieverbod vormt dus een belangrijke beperking van de bevoegdheden van de politieambtenaren naast alle voorwaarden die al opgelegd worden in artikel 46sexies Sv. Dit verbod overschrijden zou de effectiviteit van de opsporing kunnen doen toenemen, door de politieambtenaar geloofwaardiger te maken, maar zou het onderzoek in conflict brengen met ethische en morele principes. Het zou inderdaad willen zeggen dat de overheid meer delinquentie toestaat, door de leden van een bepaald crimineel milieu uit te lokken, om de criminaliteit te bestrijden. We staan hier voor een belangrijk ethisch dilemma dat zich opdringt aan de overheid.422 Over het feit dat de uitlokking van misdrijven door de politieambtenaren verboden moet zijn, bestaat er een grote internationale consensus, maar de situatie is wel ingewikkelder ten aanzien van het waarom dat het verboden moet zijn en welke handelingen als een uitlokking kunnen worden beschouwd.423 We moeten ons dus hier afvragen waar de grenzen van de overheid liggen om het plegen van misdrijven niet uit te lokken, en dus om zijn ethische integriteit te behouden en het recht op een eerlijk proces van artikel 6 EVRM niet te schenden? De overheid kan inderdaad haar geloofwaardigheid en haar

moreel gezag op lange termijn verliezen door te veel gebruik te maken van dekmanteloperaties, omdat ze bewust gaan liegen en meedraait in de criminaliteit.\footnote{F. VERBRUGGEN, “Hoofdstuk II. De kat bij de melk. Strafrechtelijke grenzen aan praktijktests: het verbod op burgerinfiltratie en op de uitlokking van misdrijven”, in A. DE BOECK, B. KEIRSBILCK en R. VAN RANSBEECK. (eds.), Mystery shopping, Antwerpen, Intersentia, 1\textsuperscript{e} ed., 2017, p. 15.}

Het Hof van Cassatie heeft in meerdere arresten de politionele uitlokking tot het plegen van een misdrijf gedefinieerd. Er is namelijk geen sprake van provocatie “\textit{wanneer het opzet om het misdrijf te plegen is ontstaan buiten enig optreden van de politieambtenaar of van een derde handelend op het uitdrukkelijk verzoek van deze ambtenaar, deze zich heeft beperkt tot het scheppen van de gelegenheid om vrij een straftoepassing te plegen in zodanige omstandigheden dat hij de uitvoering ervan kan vaststellen en aan de dader ruimte wordt gelaten om vrij met zijn misdadig voornemen te breken}”.\footnote{M. DE RUE, “Les droits de l’homme et les méthodes modernes d’enquête policière”, J.T. 2000, afl. 5966, pp. 327-328.} De politionele provocatie moet dus noodzakelijk voorafgaand aan het plegen van het misdrijf en rechtstreeks verbonden zijn aan dit misdrijf. De lijn tussen het louter blootleggen van criminaliteit die legaal is en het aanzetten tot het plegen van misdrijven kan dus soms zeer dun zijn. Dit zal telkens \textit{in concreto} beoordeeld moeten worden aan het licht van de feiten van het dossier. Het zijn misschien slechts kleine handelingen van de politieambtenaren die op eerste gezicht niet als een uitlokking kunnen worden beschouwd, die de daders ertoe brengen om toch sommige misdrijven te plegen. Hoe kan de Openbaar Ministerie dan vaststellen dat het de infiltrant is die een situatie heeft gecreëerd die het doelwit ertoe heeft geleid om tot de daad over te gaan terwijl hij dat misschien zonder de tussenkomst van de infiltrant misschien ook had gedaan?\footnote{F. VERBRUGGEN, “Hoofdstuk II. De kat bij de melk. Strafrechtelijke grenzen aan praktijktests: het verbod op burgerinfiltratie en op de uitlokking van misdrijven”, in A. DE BOECK, B. KEIRSBILCK en R. VAN RANSBEECK. (eds.), Mystery shopping, Antwerpen, Intersentia, 1\textsuperscript{e} ed., 2017, p. 15.}

Bovendien wordt de online infiltratie als een indringende maatregel en als een laatste redmiddel beschouwd, zodat de infiltranten zich soms onder druk gezet voelen om bepaalde resultaten voor het onderzoek te bereiken. Er bestaat dus een werkelijke dreiging dat de politieambtenaren die als infiltranten optreden, zich als agent-provocateur gedragen.\footnote{F. VERBRUGGEN, “Hoofdstuk II. De kat bij de melk. Strafrechtelijke grenzen aan praktijktests: het verbod op burgerinfiltratie en op de uitlokking van misdrijven”, in A. DE BOECK, B. KEIRSBILCK en R. VAN RANSBEECK. (eds.), Mystery shopping, Antwerpen, Intersentia, 1\textsuperscript{e} ed., 2017, p. 15.}

\textbf{Afdeling 2. Rechtspraak van het EHRM}

Het Europees Hof voor de Rechten van de Mens heeft de vraag naar de wenselijke grens van de bevoegdheid van de infiltranten ten aanzien van het recht op een eerlijk proces van artikel 6 EVRM al meerdere keren bestudeerd. In het arrest Ramanauskas tegen Litouwen
van 5 februari 2008 stelt het Hof namelijk dat de verboden uitlokking gebeurt wanneer de politieambtenaren, of de mensen die onder hun leiding handelen, zich niet beperken tot het opsporen van misdrijven in een essentiële passieve manier, maar een werkelijke invloed uitoefenen op de doelwitten van de operatie, die ze aanzetten om strafbare feiten te plegen die ze anders niet zouden hebben gepleegd, ten einde het misdrijf vast te stellen en dus vervolgingen ten aanzien van deze personen te starten. De Belgische wetgeving stemt dus overeen met de Europese rechtspraak. Het gebruik maken van heimelijke opsporingsmethoden zoals de online infiltratie, en het listig optreden, zoals het aanwenden van een fictieve identiteit op het internet, zijn dus niet in strijd met het recht op een eerlijk proces. Het is slechts wanneer de politieambtenaar verder gaat dan slechts bewijzen te verzamelen en contacten te onderhouden met doelwitten van het onderzoek, maar deze in een zekere mate aanzet tot het plegen van bepaalde feiten dat de situatie ingewikkelder wordt.

Om te beoordelen of er sprake is van politionele uitlokking maakt het Hof gebruik van verscheidene kriptlijnen.

1. **Verdenkingen die tot de uitvoering van de online infiltratie hebben geleid**

Eerst en vooral moet er worden gekeken naar de verdenkingen die tot de uitvoering van de heimelijke operatie hebben geleid. In dit opzicht heeft het Hof verklaard in de arresten Constantin en Stoian tegen Roemenië van 29 september 2009 en Bannikova tegen Rusland van 4 november 2010 dat het strafrechtelijke verleden van het doelwit van de operatie op zich niet voldoende is om undercoveroperaties aan te wenden. In België wordt er daarvoor in de eerste paragraaf van artikel 46sexies Sv. verklaard dat de online infiltratie slechts kan worden toegepast ten aanzien van personen “waarvan er ernstige aanwijzingen zijn dat zij strafbare feiten die een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben, plegen of zouden plegen”. In de memorie van toelichting van de wet van 25 december 2016 vinden we geen verdere verklaring van wat er juist wordt bedoeld met de ernstige aanwijzingen. Omdat deze voorwaarde ervoor zorgt dat de politieambtenaren niet tot online infiltratie kunnen overgaan ten aanzien van personen waartegen de overheid niet veel aanwijzingen heeft dat deze strafbare feiten hebben gepleegd,

---

of voornemen te plegen, kunnen we stellen dat het Hof hiertegen geen bezwaren zou moeten hebben omdat er hier een kleine kans is dat de politieambtenaren de doelwitten zouden aanzetten tot het plegen van strafbare feiten die ze anders niet zouden hebben gepleegd.

2. **Kwaliteit van de rechterlijke machtiging en van het toezicht**

Daarnaast speelt de kwaliteit van de rechterlijke machtiging en van het toezicht volgens het Hof ook een belangrijke rol in het uitlokkingsrisico. De politieambtenaren die als infiltranten optreden op het internet, worden in België goed gevolgd. De machtiging tot infiltratie wordt slechts door de procureur des Konings verleend, wanneer er aan alle voorwaarden van proportionaliteit en subsidiariteit wordt voldaan. Politieambtenaren kunnen dus nooit op eigen houtje beslissen om tot een online infiltratie over te gaan. Een machtiging en een akkoord van de Openbaar Ministerie is altijd nodig; zelfs in spoedeisende gevallen moet er een machtiging worden gegeven, maar deze kan niettemin mondeling gebeuren. In tegenstelling tot artikel 47octies Sv., wordt er niettemin in artikel 46sexies Sv. niet bepaald dat de machtiging “de wijze waarop aan de infiltratie uitvoering zal worden gegeven” moet vermelden. Dit verschil moet genuanceerd worden aangezien de volledigheid van de contacten tussen de infiltranten en de doelwitten geregistreerd volgens de vierde paragraaf van artikel 46sexies Sv. Er worden dus weinig vrijheden gelaten aan de politiediensten, wat ervoor zorgt dat er zich minder snel schendingen van de fundamentele rechten voordoen.

**Afdeling 3. Transparantie van de online infiltratie**

Doordat de operatie transparanter is dan de offline infiltratie is het dan eenvoudiger voor de overheid om achteraf na te kijken als er sprake was van uitlokking in geval van twijfel. Omdat de provocatie niet wordt vermoed en dat de verdediging niet moet bewijzen dat er provocatie was, maar het slechts moet aanvoeren door bepaalde feiten, verschuift de bewijslast naar de overheid. Door deze registratieplicht van alle contacten is het dan gemakkelijker om na te kijken waar de overheid misschien de grenzen heeft overschreden.

---

434 Art. 46sexies, §2 Sv.
435 Art. 47octies, §3, 4° Sv.
De vraag naar de grenzen die de overheid niet mag overschrijden in het kader van de uitvoering van de online infiltratie is dus nog steeds gevoelig, maar gemakkelijker te controleren dan bij de offline infiltratie. In beide operaties pogen de infiltranten het vertrouwen te winnen van de doelwitten van de operatie en proberen zo persoonlijke relaties met hen te ontwikkelen, zeker wanneer ze meer dan één keer met hen een contact onderhouden. De infiltrant dient een normaal contact met de doelwitten van de operatie te onderhouden, zodat hij vermijdt om de aandacht op zich te vestigen. Dit zou de operatie in het gedrang kunnen brengen en de infiltranten kunnen bewegen tot het plegen van bepaalde misdrijven. Welke handelingen ze precies zouden moeten plegen is moeilijk voorspelbaar en hangt sterk af van het crimineel milieu dat gaan infiltreren en van de eigenaardigheid van elke situatie. We kunnen hier dus niet op voorhand vaststellen wat de precieze grenzen zijn die de politiediensten niet mogen overschrijden en moeten dit dus eerder a posteriori van geval tot geval beoordelen of sprake was van provocatie aan de hand van de registratie van de communicatie.

Afdeling 4. De fictieve identiteit van de infiltranten

Zoals we het al hebben gezien in het deel I, is de cyberwereld gekenmerkt door de anonimiteit. Het is een grote aantrekkingskracht van het internet voor misdadigers om misdrijven te plegen. Opsporing van misdrijven in de cyberwereld hebben daardoor een aangepast wettelijk kader nodig. We zouden ons in dit opzicht kunnen afvragen welke fictieve identiteit de politieambtenaren in het kader van de uitvoering van de maatregel kunnen aannemen? Het is natuurlijk wenselijk dat de infiltranten gebruik maken van een fictieve identiteit voor het welslagen van de operatie, gezien het belang van het recht op anonimiteit op het internet. Politieambtenaren zijn slechts gerechtigd om gebruik te maken van een geloofwaardige, fictieve identiteit mits ondersteuning door fictieve, ondersteunende documenten in het kader van de uitvoering van een bijzondere opsporingsmethode of van online infiltratie, die hoewel ze geen bijzondere opsporingsmethode uitmaakt, wel belangrijke aspecten en kenmerken met deze methoden deelt, in tegenstelling tot andere operaties zoals het politieoneel optreden in cyberspace of internetpatrouilles.437 De infiltranten gaan zich dus schuilhouden achter de identiteit van een potentiële klant of van iemand die tot hetzelfde crimineel milieu dan het doelwit behoort. Dit ontzeggen aan de politiediensten zou de effectiviteit van de operatie en dus de meerwaarde die het internet voor

opsporingsonderzoeken kan betekenen in het gevaar brengen.\textsuperscript{438} Het zou tevens ook verhinderen dat de weinige politieambtenaren die als infiltrant optreden, in andere operaties kunnen worden ingezet, omdat ze dan al zouden bekend zijn onder hun reële identiteit in het crimineel milieu.\textsuperscript{439}

Bij het kiezen van een fictieve identiteit moeten de politiediensten er toch voor zorgen dat deze nooit provocerend of te suggestief zijn. Vaak kan het niettemin als een provocatie worden beschouwd wanneer politieambtenaren de identiteit van een minderjarig meisje of jongen aannemen, een “lokpuber” zoals het in Nederland wordt genoemd, om misdrijven van kinderpornografie of van online grooming op te sporen. De grens is hier dus heel dun zodat opsporingsambtenaren hier niet over veel vrijheid beschikken voordat ze zich schuldig zouden kunnen maken aan uitlokking. Zoals in Nederland, kan het gebruik maken van een lokpuber voor de opsporing van het misdrijf van online grooming tot vrijpraak leiden, omdat er zoals in Nederland, in de Belgische bepaling van artikel 377\textit{quater} Sv. wordt verklaard dat het strafbaar is, wanneer de misdadiger met een minderjarige afspeelt, wat hier \textit{in casu} niet het geval is.\textsuperscript{440} Naast het feit dat het wenselijk zou zijn om de wetgeving hier aan te passen en dus tot de arrestatie van de daders te kunnen overgaan, zelfs als die met een meerderjarige infiltrant aan het communiceren waren, zou het ook bevorderlijk zijn voor de effectiviteit van de operatie om dit niet als een provocatie te beschouwen, wanneer het niet de infiltrant is die het eerste stap zet, maar dat deze gewoon op een niet-provocerende wijze antwoordt op de berichten van het doelwit.

\textbf{Afdeling 5. Conclusie}

Kortom kunnen we vaststellen dat het provocatieverbod niet te beperkend is, zodat het niet de effectiviteit van de aanwending van de online infiltratie voor het onderzoek in het gedrang brengt. Het is wel onmogelijk om op voorhand vast te stellen waar de grens van de handelingen die de politieambtenaren mogen stellen, moet liggen. Voor het welslagen van de operatie moeten de infiltranten zich zo veel mogelijk inpassen in het milieu dat ze infiltreren, zodat de vaststelling van die grens de effectiviteit van de operatie in het gedrang zou kunnen brengen. Er moet dus echter elke keer \textit{in concreto} worden beoordeeld wat als een provocatie

\textsuperscript{440} J.-J. OERLEMANS, \textit{Normering van digitale opsporingsmethoden}, Breda, Nederlandse Defensie Academie, 2017, p. 32.
zou kunnen worden beschouwd. De wetgever heeft hier dus een grote handelingsvrijheid gelaten aan de politiediensten, omdat deze zelf onder bepaalde voorwaarden gerechtvaardigd kunnen worden om misdrijven te plegen voor het welslagen van de operatie, zonder dat het als een provocatie moet worden beschouwd. Daarnaast bestaan er voldoende waarborgen in de regeling van artikel 46 sexies Sv. omdat alle contacten tussen de infiltranten en de doelwitten worden geregistreerd, zodat het altijd mogelijk is om achteraf na te kijken of de infiltrant zich schuldig heeft gemaakt aan uitlokking.
ALGEMENE CONCLUSIE

Zoals we het hebben kunnen opmerken, vormt de online wereld een parallelle wereld aan de offline wereld. De kenmerken van deze virtuele wereld zorgen voor tal van uitdagingen voor de wetgever om het wettelijk kader up-to-date te houden en aan de stand van de technologie. Aanpassingen waren snel nodig aangezien dat de wettelijke achterstand in het voordeel van misdadigers was. Deze konden inderdaad al beroep doen op de mogelijkheden die de ICT hun bood, om het plegen van misdrijven te vergemakkelijken en de opsporing te bemoeilijken en te verhinderen, terwijl de opsporingsdiensten slechts gerechtvaardigd waren om gebruik te maken van opsporingsmethoden die bedoeld waren voor de offline wereld. Het crimineel milieu was de Belgische rechtshandhavingsdiensten een grote stap voor, zodat de informaticacriminaliteit alleen maar aan het toenemen was de laatste jaren. Bepaalde aspecten van het internet, zoals de kenmerkende anonimiteit en de mogelijke grootschaligheid van de gevolgen van bepaalde acties, zorgen ervoor dat de cyberwereld een grote aantrekkingskracht heeft op criminalen. Met de wet inzake informaticacriminaliteit is de wetgever sinds 2000 bezig met de modernisering en de aanpassing van het Strafwetboek en de Wetboek van Strafvordering aan de technologische realiteit. Dit is een complex proces omdat de technologische realiteit voortdurend aan het evolueren is. In 2016 zijn nog grote wijzigingen aangebracht aan het Wetboek van Strafvordering om nieuwe middelen te geven aan de politiediensten om de informaticacriminaliteit in de brede zin te bestrijden. De doelstelling van deze masterproef was dan ook te beoordelen of de wetgever met de invoering van de online infiltratie een aangepaste methode ter beschikking heeft gesteld van de politiediensten om op een meer effectieve wijze het hoofd te bieden aan de informaticacriminaliteit.

Concluderend kunnen we vaststellen dat de wetgever met de wet van 25 december 2016 ervoor heeft gezorgd dat de politiediensten over nieuwe middelen beschikken om de toenemende cybercriminaliteit, die voortvloeit uit de exponentiële verbondenheid van de samenleving in netwerken en de technologische vooruitgang van de ICT, en tal van andere misdrijven, die misschien slechts van ver een link hebben met de ICT, effectief op te sporen. Zoals we hebben gezien, is het weliswaar nog te vroeg om de cijfers te kunnen gebruiken, die de impact van de invoering van de online infiltratie in het Belgische Wetboek van Strafvordering meten, maar door een grondige omschrijving en vergelijking van de regeling van de online infiltratie met de Belgische regeling van de offline infiltratie en de Franse en
Nederlandse regeling van de offline infiltratie, hebben we een paar opmerkingen of aanbevelingen kunnen doen over het artikel 46sexies Sv.

Eerst en vooral kunnen we de keuze van de wetgever om een aparte regeling voor de online infiltratie in te voeren, goedkeuren. De fysieke wereld en de virtuele wereld vertonen zoveel verschillen, dat de operaties in de twee werelden apart moeten worden geregeld om op een effectieve manier te kunnen worden uitgevoerd. De offline infiltratie van artikel 47octies Sv. is onder meer indringender dan de cyberinfiltratie en meer risicovol voor de infiltranten, zodat er meer waarborgen en strengere toepassingsvoorwaarden aan deze operaties moeten worden verbonden. In tegenstelling daaraan wordt de offline infiltratie niet als een bijzondere opsporingsmethode beschouwd en dient deze operaties dus soepeler te worden geregeld. De mogelijkheid om tot de online infiltratie over te gaan moet voor de politiediensten sneller toepasbaar zijn, aangezien de online infiltratie een belangrijke bron van informatie kan zijn voor het onderzoek, zonder dat ze daarvoor een groot risico nemen en fundamentele rechten schenden op een ongeoorloofde manier. Dit ontzeggen aan de politiediensten zou belemmerend kunnen zijn voor het onderzoek en er ook voor zorgen dat het crimineel milieu zijn voorsprong tegenover de politiediensten behoudt.

Daarnaast kunnen we bepaalde keuzes van de wetgever betreuren zoals de limitatieve tijdsduur van drie maanden zoals voor de offline infiltratie, zelfs als deze hernieuwbaar is en ze kortstondig een beroep kunnen doen op burgerdeskundigen. Voor het welslagen van de operatie moet gezorgd worden dat ze over de grootst mogelijke handelingsvrijheid beschikken, zonder dat ze fundamentele rechten op een ongeoorloofde manier schenden. Het is de bedoeling dat de infiltranten het vertrouwen van de leden van het crimineel milieu dat ze infiltreren inwinnen. Daarom moeten ze op dezelfde manier handelen als de mensen die ze trachten op te sporen door de toepassing van de online infiltratie. Dit kan dus belangrijke ethische vragen opwerpen, maar de wetgever moet ervoor zorgen dat er zo weinig mogelijk procedurele hindernissen de effectiviteit van de maatregel in de weg staan. Een minder beperkende regeling omtrent de tijdsduur en de mogelijkheid om langer beroep te doen op burgerdeskundigen, zeker omdat deze niet over een initiatiefrecht beschikken, zou dus wenselijk zijn. Aangezien dat er momenteel een wetsontwerp op tafel ligt omtrent de burgerinfiltratie in België is het mogelijk dat er wijzigingen daaromtrent aankomen. Burgerinfiltratie in de online wereld zou niettemin niet per se noodzakelijk zijn, aangezien de politiediensten zich perfect kunnen laten bijstaan door burgerdeskundigen vermits de operatie toch plaatsvindt achter de schermen.
Bovendien rust de effectiviteit van de operatie op de bestrijding van de criminaliteit in grote mate op de deskundigheid en de expertise van de infiltranten over de cyberwereld. We kunnen dit niettemin nuanceren met de mogelijkheid over dewelke de infiltranten beschikken om kortstondig beroep te doen op burgerdeskundigen. Ondertussen is het wachten op de koninklijk besluit die de voorwaarden van de opleiding en de nadere aanwijzing van de bevoegde politiediensten gaat bepalen.

In het algemeen kunnen we dus stellen dat de operatie een juist antwoord biedt op de derde maatregel van de Kadernota Integrale Veiligheid omtrent het transversale thema, de uitdaging van het internet en ICT als faciliterend instrument voor de criminaliteit, met name dat het wettelijk kader moet worden aangepast aan de technologische evolutie zonder dat er afbreek wordt gedaan aan het globale evenwicht tussen het juridisch kader voor de opsporing en vervolging enerzijds en de bescherming van de fundamentele rechten zoals het recht op eerbiediging van het privéleven en het recht op een eerlijk proces anderzijds.

De regeling van de online infiltratie blijkt, zoals we hebben kunnen vaststellen in deel III, een juist evenwicht te behouden tussen het welslagen en de effectiviteit van het onderzoek en de waarborgen van de fundamentele rechten. De wetgever heeft hier voordeel gehaald uit de mogelijkheden die de ICT kan bieden, om ervoor te zorgen dat misbruiken tijdens deze operaties vermeden kunnen worden. Inderdaad, het feit dat alle contacten tijdens de uitvoering van de cyberinfiltratie worden geregistreerd, zorgt ervoor dat het recht op een eerlijk proces van artikel 6 EVRM niet wordt geschonden, omdat er a posteriori kan worden nagekeken als de politiediensten zich schuldig hebben gedaan aan uitlokking. Daarnaast kunnen we ook besluiten dat de online infiltratie minder indringend is ten aanzien van het recht op privéleven dan de offline infiltratie en dat de uitvoering van deze operatie ten aanzien van minder ernstige misdrijven dan diegene die de offline infiltratie kunnen rechtvaardigen, dus als geoorloofd kan worden beschouwd.
1. **Wetgeving**

1.1. **Internationale en Europese wetgeving**


Aanbev. Raad, R (95) 13 van 11 september 1995 over problemen inzake strafrechtelijke procedures in verband met de informatietechnologie.

Aanbev. Raad, R (89) 9 van 13 september 1989 inzake computergerelateerde criminaliteit.

1.2. **Belgische wetgeving**


Wetboek van strafvordering van 17 november 1808, *B.S.* 27 november 1808, art. 46bis, 46sexies en 47octies.

Strafwetboek van 8 juni 1867, *B.S.* 9 juni 1867, art. 66, 377quater en 383bis.

Wet van 17 april 1878 houdende de voorafgaande titel van het Wetboek van Strafvoering, *B.S.* 25 april 1878, art. 30 en 32.


Wet 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren,


Wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten, B.S. 10 maart 2010.

Wet van 29 december 2010 houdende wijziging van artikel 47octies van het Wetboek van strafvordering betreffende de samenwerking met buitenlandse infiltranten, B.S. 20 januari 2011.


Wet van 10 april 2014 betreffende de bescherming van minderjarigen tegen benadering met als oogmerk het plegen van strafbare feiten van seksuele aard, B.S. 30 april 2014.


Wet van 5 februari 2016 tot wijziging van het strafrecht en de strafvordering en houdende diverse bepalingen inzake justitie (Potpourri II-wet), B.S. 19 februari 2016.

Wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, B.S. 18 juli 2016.

Koninklijke besluit van 1 december 1975 houdende algemeen reglement op de politie van het wegverkeer en van het gebruik van de openbare weg, B.S. 9 december 1975.


1.3. Belgische parlementaire stukken


Advies nr. 13/2015 van 13 mei 2015 van de Commissie voor de Bescherming van de Persoonlijke levenssfeer betreffende de voorontwerpen van wet houdende diverse bepalingen – wijzigingen aan de wet tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, aan de wet op het politieambt en aan de wet van 18 maart 2014 betreffende het politionele informatiebeheer.

Advies nr. 21/2016 van 18 mei 2016 van de Commissie voor de Bescherming van de Persoonlijke levenssfeer betreffende het voorontwerp van wet betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties, Parl.St., Kamer, 2015-2016, nr. 54-1966/002.


Wetsontwerp inzake informaticacriminaliteit, Parl.St., Kamer, 1999-2000, nr. 50-0213/001, 50-0214/001.

1.4. *Buitenlandse wetgeving*

1.4.1. *Franse wetgeving*

Code de procédure pénale (FR).


1.4.2. *Nederlandse wetgeving en parlementaire stukken*

Wetboek van Strafvordering (NL).


Wetsvoorstel tot wijziging van het Wetboek van Strafvordering in verband met de regeling
van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden), Kamerstukken II 1996-1997, 25 403, nr. 3.

Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en de Telecommunicatiewet in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II), Kamerstuk 1998-1999, 26 671, nr. 3.

2. **Rechtspraak**

2.1. Europese rechtspraak

**Europees Hof voor de Rechten van de Mens**


**Europees Hof van Justitie**


2.2. Belgische rechtspraak

**Hof van Cassatie**


Cass. 28 maart 2017, [www.cass.be](http://www.cass.be); *NC* 2017, afl. 4, p. 381.

**Grondwettelijk Hof**


GwH 11 juni 2015, nr. 84/2015.

**Hoven van Beroep**


### 3. Rechtsleer

#### 3.1. Boeken


3.2. Tijdschriften


DE PAUW, P., “Sociale controle in onlinegemeenschappen: een taak voor de overheid of volstaat zelfregulering?”, De orde van de dag 2010, afl. 49, pp. 5-68.


DE SCHEPPER, K. en VERBRUGGEN, F., “Ontsnappen space invaders aan onze pacmannen? De materiële en formele strafrechtsmacht van België bij strafbare weigering van
medewerking door elektronische dienstverleners”, T.strafr. 2013, pp. 143-166.


VAN DEN HEYNING, C., “Het gebruik van telecommunicatiegegevens in het strafrechtelijk


VAN ROY, B., “Wijzigingen aan de Belgische bepalingen inzake informaticacriminaliteit”, Computerr. 2006, p. 188.


3.3. Verzamelwerken


VAN LINTHOUT, P. en KERKHOFS, J., “Inleiding tot het materieel en strafprocedureel cyberstrafrecht: uitdagingen voor de advocatuur”, in B. DE MEULENAERE, Internet &/@ Recht, Gent, Larcier, 2013, pp. 1-44.


3.4. Proefschriften


3.5. Overige

BAERT, J. en DE SUTTER, B., “Veranderingen en aanpassingen – vanuit een rechtsstatelijk perspectief- van bestuur, regelgeving en rechtspraak, die noodzakelijk zijn als gevolg van


# BIJLAGE 2

**GEREGISTREERDE CRIMINALITEIT OP HET NATIONAAL NIVEAU**

## Informaticacriminaliteit

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hacking</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vol.</td>
<td>398</td>
<td>511</td>
<td>668</td>
<td>821</td>
<td>1.068</td>
<td>1.958</td>
<td>1.679</td>
<td>1.984</td>
<td>2.105</td>
<td>2.269</td>
<td>1.046</td>
</tr>
<tr>
<td>Pog.</td>
<td>9</td>
<td>13</td>
<td>10</td>
<td>15</td>
<td>20</td>
<td>57</td>
<td>66</td>
<td>71</td>
<td>65</td>
<td>69</td>
<td>34</td>
</tr>
<tr>
<td>Subtotaal:</td>
<td>407</td>
<td>524</td>
<td>678</td>
<td>836</td>
<td>1.088</td>
<td>2.015</td>
<td>1.745</td>
<td>2.055</td>
<td>2.170</td>
<td>2.338</td>
<td>1.080</td>
</tr>
</tbody>
</table>

| **Verval van informatie** | | | | | | | | | | | | |
| Vol. | 348 | 418 | 399 | 462 | 431 | 455 | 489 | 640 | 776 | 721 | 356 |
| Pog. | 8 | 3 | 9 | 10 | 3 | 17 | 6 | 6 | 14 | 20 | 10 |
| Subtotaal: | 356 | 421 | 408 | 472 | 434 | 472 | 495 | 646 | 790 | 741 | 366 |

| **Informaticabedrog** | | | | | | | | | | | | |
| Pog. | 478 | 443 | 507 | 570 | 703 | 1.235 | 1.376 | 1.187 | 1.328 | 1.369 | 515 |

| **Sabotage** | | | | | | | | | | | | |
| Vol. | 56 | 49 | 74 | 69 | 116 | 4.300 | 1.143 | 412 | 416 | 441 | 238 |
| Pog. | 1 | 1 | 1 | 2 | 3 | 79 | 43 | 19 | 10 | 39 | 7 |
| Subtotaal: | 57 | 50 | 75 | 71 | 119 | 4.379 | 1.186 | 431 | 426 | 480 | 245 |

| **Niet nader bepaald** | | | | | | | | | | | | |
| Vol. | 1 |
| Subtotaal: | 1 |

**Totaal:** 4

**Met de gegevens moet worden opgelet dat deze betrekking hebben op de hergeorganiseerde criminaliteitsstatistiek en niet op de politiesstatistiek.**

### Percentage of Individuals using the Internet

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Belgium</td>
<td>29.43</td>
<td>31.29</td>
<td>46.33</td>
<td>49.97</td>
<td>53.86</td>
<td>55.82</td>
<td>59.72</td>
<td>64.44</td>
<td>66.00</td>
<td>70.00</td>
<td>75.00</td>
<td>81.61</td>
<td>80.72</td>
<td>82.17</td>
<td>85.00</td>
<td>85.05</td>
</tr>
</tbody>
</table>

Artikel 46sexies Sv. luidt als volgt:

§ 1. Bij het opsporen van de misdaden en wanbedrijven, wanneer het onderzoek zulks vereist en de overige middelen van onderzoek niet lijken te volstaan om de waarheid aan de dag te brengen, kan de procureur des Konings de politiediensten bedoeld in het tweede lid machtigen om op het internet, desgevallend onder een fictieve identiteit, contact te onderhouden met een of meerdere personen waarvan er ernstige aanwijzingen zijn dat zij strafbare feiten die een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben, plegen of zouden plegen.

De Koning bepaalt de voorwaarden, onder meer voor wat de opleiding betreft, en de nadere regels voor de aanwijzing van de politiediensten die bevoegd zijn om de maatregel, bedoeld in dit artikel, ten uitvoer te leggen.

In uitzonderlijke omstandigheden en mits uitdrukkelijke machtiging van de procureur des Konings, kan de ambtenaar van de in het tweede lid bedoelde politiediensten bij een welbepaalde operatie kortstondig een beroep doen op de deskundigheid van een persoon die niet tot de politiediensten behoort, indien dit strikt noodzakelijk voorkomt voor het welslagen van zijn opdracht. De machtiging en de identiteit van deze persoon worden bewaard in het in paragraaf 3, zevende lid, bedoelde dossier.

Dit artikel is niet van toepassing op de persoonlijke interactie op het internet van politieambtenaren, bij de uitvoering van hun opdrachten van gerechtelijke politie, met een of meerdere personen, die enkel een gerichte verificatie of een arrestatie tot direct doel heeft, en dit zonder gebruik te maken van een geloofwaardige fictieve identiteit.

§ 2. De maatregel bedoeld in § 1 wordt door de procureur des Konings bevolen met een voorafgaandelijke en met redenen omklede schriftelijke machtiging. Deze machtiging is geldig voor een termijn van drie maanden, onverminderd hernieuwing.

In spoedeisende gevallen kan de machtiging mondeling worden verstrekt. De machtiging moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het eerste lid.

§ 3. Blijven vrij van straf de politieambtenaren die, in het kader van hun opdracht en met het oog op het welslagen ervan of ter verzekering van hun eigen veiligheid of deze van andere bij de maatregel betrokken personen, strikt noodzakelijke strafbare feiten plegen, mits uitdrukkelijk akkoord van de procureur des Konings.
Die strafbare feiten mogen niet ernstiger zijn dan die waarvoor de maatregel wordt aangewend en moeten noodzakelijkerwijze evenredig zijn met het nagestreefde doel.

Het eerste en het tweede lid zijn eveneens van toepassing op de personen die aan de uitvoering van deze opdracht noodzakelijke en rechtstreekse hulp of bijstand hebben verleend en op de personen, bedoeld in § 1, derde lid.

Blijft vrij van straf de magistraat die, met inachtneming van dit Wetboek, machtiging verleent aan een politieambtenaar en aan de persoon bedoeld in het derde lid tot het plegen van strafbare feiten in het kader van de uitvoering van de maatregel.

De politieambtenaren melden schriftelijk en voór de uitvoering van de maatregel aan de procureur des Konings, de misdrijven die zij of de personen bedoeld in het derde lid, voornemens zijn te plegen.

Indien deze voorafgaande kennisgeving niet kon gebeuren, stellen de politieambtenaren de procureur des Konings onverwijld in kennis van de misdrijven die zij of de personen bedoeld in het derde lid, hebben gepleegd en bevestigen dit nadien schriftelijk.

De procureur des Konings vermeldt in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld in het derde lid in het kader van deze door hem bevolen maatregel kunnen worden gepleegd. Deze beslissing wordt in een afzonderlijk en vertrouwelijk dossier bewaard. Hij heeft als enige toegang tot dit dossier, onverminderd het in artikel 56bis, respectievelijk de artikelen 235ter, § 3, en 235quater, § 3, bedoelde inzagerecht van de onderzoeksrechter en de kamer van inbeschuldigingstelling. De inhoud van dit dossier valt onder het beroepsgeheim.

§ 4. De met het onderzoek belaste officier van gerechtelijke politie stelt proces-verbaal op van de verschillende fasen in de uitvoering van deze maatregel, met inbegrip van de relevante contacten. Deze processen-verbaal worden uiterlijk na het beëindigen van de maatregel bij het dossier gevoegd.

De contacten bedoeld in paragraaf 1 worden met de passende technische middelen geregistreerd en uiterlijk na het beëindigen van de maatregel bij het dossier gevoegd of ter griffie, al dan niet in digitale vorm, neergelegd.

§ 5. De procureur des Konings staat in voor de tenuitvoerlegging van de machtigingen tot de maatregel bedoeld in § 1, eerste lid, die zijn verleend door de onderzoeksrechter in het kader van een gerechtelijk onderzoek overeenkomstig artikel 56bis.

De procureur des Konings vermeldt op dat ogenblik in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld § 3,
derde lid, in het kader van de door de onderzoeksrechter bevolen maatregel kunnen worden gepleegd. Deze beslissing wordt in het dossier bedoeld in § 3, zevende lid, bewaard.
Artikel 47octies Sv. luidt als volgt:

§ 1. Infiltratie in de zin van dit wetboek is het door een politieambtenaar, infiltrant genoemd, 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, zoals bedoeld in artikel 324bis van het Strafwetboek, of misdaden of wanbedrijven als bedoeld in artikel 90ter, §§ 2 tot 4 plegen of zouden plegen.

In uitzonderlijke omstandigheden en mits uitdrukkelijke machtiging van de bevoegde magistraat, kan de infiltrant bij een welbepaalde operatie kortstondig een beroep doen op de deskundigheid van een persoon die niet tot de politiediensten behoort, indien dit strikt noodzakelijk voorkomt voor het welslagen van zijn opdracht.

§ 2. De procureur des Konings kan in het kader van het opsporingsonderzoek een infiltratie machtigen wanneer het onderzoek zulks vereist en de overige middelen van onderzoek niet lijken te volstaan om de waarheid aan de dag te brengen.

Hij kan de politiedienst machtigen om, binnen het wettelijk kader van een infiltratie en met inachtneming van de finaliteit ervan, bepaalde politionele onderzoekstechnieken aan te wenden. De Koning bepaalt bij een in Ministerraad overlegd besluit, op voordracht van de minister van Justitie en na advies van het College van procureurs-generaal, deze politionele onderzoekstechnieken. Deze politionele onderzoekstechnieken kunnen slechts worden aangewend door leden van de directie van de speciale eenheden van de federale politie en, desgevallend, mits bijkomend voorafgaand akkoord van de federale procureur, in samenwerking met buitenlandse speciaal daartoe opgeleide en bevoegde ambtenaren.

De procureur des Konings kan tevens, indien daartoe grond bestaat, toelating verlenen om de noodzakelijke maatregelen te nemen ter vrijwaring van de veiligheid en de fysieke, psychische en morele integriteit van de infiltrant. Deze toelating wordt bewaard in het vertrouwelijk dossier bedoeld in artikel 47novies, § 1, tweede lid.

§ 3. De machtiging tot infiltratie is schriftelijk en vermeldt:

1° de ernstige aanwijzingen van het strafbaar feit die de infiltratie wettigen of, indien de infiltratie zich situeert in het proactieve onderzoek zoals omschreven in artikel 28bis, § 2, het redelijk vermoeden van te plegen of reeds gepleegde maar nog niet aan het licht gebrachte strafbare feiten, en de bijzondere aanwijzingen met betrekking tot de elementen omschreven in deze laatste bepaling, die de infiltratie wettigen;
2° de redenen waarom de infiltratie onontbeerlijk is om de waarheid aan de dag te brengen;

3° indien bekend, de naam of anders een zo nauwkeurig mogelijke beschrijving van de persoon of personen bedoeld in § 1;

4° de wijze waarop aan de infiltratie uitvoering zal worden gegeven, daaronder begrepen de toelating kortstondig een beroep te doen op de deskundigheid van een burger, zoals bepaald in § 1, tweede lid, en de toelating politionele onderzoekstechnieken, zoals bepaald in § 2, tweede lid, aan te wenden;

5° de periode tijdens welke de infiltratie kan worden uitgevoerd en die niet langer mag zijn dan drie maanden te rekenen van de datum van de machtiging;

6° de naam en de hoedanigheid van de officier van gerechtelijke politie, die de leiding heeft over de uitvoering van de infiltratie.

§ 4. De procureur des Konings vermeldt op dat ogenblik in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld in artikel 47quinquies, § 2, derde lid, in het kader van de infiltratie kunnen worden gepleegd. Deze beslissing wordt in het dossier bedoeld in artikel 47novies, § 1, tweede lid, bewaard.

§ 5. In spoedeisende gevallen kan de machtiging tot infiltratie mondeling worden verstrekt. De machtiging moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in paragraaf 3.


Hij gaat bij elkewijziging, aanvulling of verlenging van zijn machtiging na of de voorwaarden bepaald in §§ 1 tot 3 zijn vervuld en handelt daarbij overeenkomstig § 3, 1° tot 6°.

§ 7. De procureur des Konings staat in voor de tenuitvoerlegging van de machtigingen tot infiltratie die zijn verleend door de onderzoeksrechter in het kader van een gerechtelijk onderzoek overeenkomstig artikel 56bis.

De procureur des Konings vermeldt op dat ogenblik in een afzonderlijke en schriftelijke beslissing de misdrijven die door de politiediensten en de personen bedoeld in artikel 47quinquies, § 2, derde lid, in het kader van de door de onderzoeksrechter bevolen infiltratie kunnen worden gepleegd. Deze beslissing wordt in het dossier bedoeld in artikel 47novies, § 1, tweede lid, bewaard.