Inhoudsopgave

EEN WOORD VAN DANK 2

VOORWOORD 3

INLEIDING 5

DEEL 1. NATIONAAL 7

1. Definiëring terrorisme 7

2. Totstandkoming van de Wet digitaal speurwerk 8

2.1. Historiek 9

3. Het begrip ‘IT-gerelateerde criminaliteit’ 11

4. Maatregelen inzake bewijsgaring door de Wet digitaal speurwerk 12

4.1. Open-bronnen-onderzoek 13

4.2. Online infiltratie: nieuw art. 46sexies Sv. 16

4.3. Vernieuwd regime IT-recherche 19

4.3.1. Niet-heimelijke/openlijke informatica- en netwerkzoekingen 20

4.3.2. Heimelijke IT-zoekingen 25

4.4. Databeslag – Behandeling van digitaal bewijs 28

4.4.1. Databeslag 28

4.4.2. Authenticiteit en integriteit van het digitaal bewijsmateriaal 28

4.4.2.1. Authenticiteit 29

4.4.2.2. Integriteit 29

4.4.2.3. Onvolkomen notificatieplicht 30

4.4.3. Afwezigheid van waarborgen voor de beslagene 32

5. Strafrechtelijk beleid inzake digitale recherche 33

5.1. Online onderzoek 33

5.2. IT-onderzoek 33

5.2.1. Computer Crime Units 34

5.2.2. Toezichtsrapport Comité P 34

5.2.2.1. Aanleiding 34

5.2.2.2. Bedreigende factoren voor een goede CCU-werking 35

5.2.2.3. Conclusie: risico’s voor de digitale bewijsvoering 37

6. Kritische bedenkingen door rechtspractici 38

DEEL 2. RAAD VAN EUROPA 40

1. Inleiding – EVRM en EHRM 40

2. Standpunten Raad van Europa inzake maatregelen van terrorismebestrijding en recente initiatieven 41

2.1. Raad van Europa en terrorismebestrijding: algemeen 41

2.2. Recente initiatieven inzake terrorismebestrijding 43

2.2.1. Algemeen 43

2.2.2. Aanbeveling speciale onderzoekstechnieken 43

2.2.2.1. Speciale onderzoekstechnieken 44

2.2.2.2. Cyberonderzoek 44

2.2.2.3. Algemene principes 44

2.2.2.4. Gebruiksvoorwaarden 45

3. Kwalificatie van de verschillende rechten en vrijheden 46

3.1. Artikel 6 EVRM 47

3.2. Artikel 8 EVRM 48

3.2.1. Reikwijdte 49

3.2.2. Beperkingen 50

DEEL 3. Maatregelen Wet digitaal speurwerk in het licht van de artikelen 6 en 8 EVRM 53

1. Artikel 8 EVRM 54

1.1. Szabó en Vissy/Hongarije. 54

1.1.1. Rechterlijke controle 54

1.1.2. Kennisgeving 55

1.2. Weber en Saravia/Duitsland 55

1.3. P.G. en J.H./Verenigd Koninkrijk 56

1.4. Prezhdarovi/Bulgarije 57

2. Artikel 6 EVRM 57

3. Gebruik van (digitaal) bewijs verkregen in strijd met artt. 6 en 8 EVRM 58

CONCLUSIE 60

# EEN WOORD VAN DANK

Deze masterproef werd geschreven als eindwerk teneinde het diploma Master in de Rechten aan de Vrije Universiteit Brussel te kunnen behalen.

Vooraleer wordt overgegaan tot de orde van de dag, zou ik graag enkele mensen willen bedanken.

In de eerste plaats dank ik mijn promotor, Prof. Dr. Paul De Hert voor het aanvaarden van het onderwerp van deze masterproef. Binnen het door hem aangeboden kader heb ik veel ruimte gekregen voor de verdere afbakening en invulling van mijn onderwerp. Dit heeft me de kans gegeven een onderzoek te voeren binnen mijn persoonlijk interesseveld.

Daarnaast ben ik aan verschillende personen in mijn leefomgeving een uitgebreid dankwoord verschuldigd.

Daarbij denk ik in de eerste plaats aan mijn ouders en mijn broer, Jasper Deltour. Zij hebben mij gedurende de voorbije vijf jaar aan de VUB steeds gesteund. Bij de verschillende hindernissen die rechtenstudies kunnen kenmerken, stonden zij voor me klaar, zo ook bij het schrijven van deze masterproef.

Ook dank ik de rest van mijn familie voor hun oprechte interesse in mijn studies en hun aanmoedigingen wanneer ik die nodig had.

Tot slot valt uiteraard het belang van een standvastige vriendenkring niet te ontkennen. Wanneer de twijfel of vermoeidheid toesloeg, hebben mijn vrienden me steeds met een bijzonder grote overtuigingskracht herinnerd aan mijn eigen willen en kunnen. Hun aanzienlijk vertrouwen in mij motiveerde me om verder te blijven gaan.

Feia Deltour

 Wemmel, augustus 2018

# VOORWOORD

Terrorisme is geen nieuw fenomeen. Al zeer lang wordt getracht geloofsovertuigingen en nieuwe maatschappijvisies door te drukken buiten de bestaande -al dan niet democratische- besluitvorming. De inhoud ervan veranderde wel regelmatig door de jaren heen, doordat er ook verschillende impulsen aan ten grondslag liggen. Na de Tweede Wereldoorlog concentreerde het terrorisme zich meestal in landen waar zelfverklaarde onafhankelijkheidsstrijders afscheuring van het moederland beoogden of politieke eisen wilden doordrukken, men denke aan de ETA in Spanje en het IRA-verzet in Noord-Ierland en Groot-Brittannië. Daarna kreeg het terrorisme echter stilaan een meer globale aard.

De aanslagen van 9/11 in de Verenigde Staten zorgden ervoor dat het moslimfundamentalisme het nieuwe symbool werd van terreur. In de jaren die erop volgden, werden talrijke aanslagen met gelijkaardige onderliggende beweegredenen in het collectieve (Europese) geheugen gegrift.

In de nasleep hiervan werden talrijke maatregelen getroffen om het straf(proces)rechtelijk arsenaal in de talrijke getroffen regimes uit te breiden. Hiervan getuigt ook de reeks Belgische initiatieven die na de aanslagen van 22 maart 2016 het licht zag.

Terreurdreiging valt in dat kader als een aanzet te beschouwen voor talrijke -en steeds verder reikende- maatregelen die zowel administratief als repressief van aard kunnen zijn. De Belgische *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* (hierna: Wet digitaal speurwerk) is hiervan een goed voorbeeld en vormt het centrale onderwerp van deze masterproef.

Er kan niet omheen dat terreur vandaag vooral gebruik maakt van de buitengewone digitalisering die onze hedendaagse samenleving kenmerkt. Recente ontwikkelingen hebben in termen van communicatie en netwerking namelijk gezorgd voor de creatie van een wereld waarin elke offline speler ook online vertegenwoordigd is. Dit heeft bewerkstelligd dat we vandaag kunnen spreken van een interactief ‘Web 2.0’, getypeerd door de mogelijkheid van de talrijke internetgebruikers om ook zelf de inhoud van dat internet mee te bepalen.

Dergelijke wereld, gedreven door internet en ICT, biedt uiteraard veel ruimte voor criminelen bij het uitoefenen van hun criminele activiteiten. Het internet fungeert bijvoorbeeld als facilitator voor het aanbieden van criminele producten en diensten en de verspreiding ervan. Ook wordt via de verschillende sociale media de mogelijkheid geboden tot gemeenschapsvorming voor criminele doeleinden, zo bijvoorbeeld in het kader van terrorisme. ICT-gerelateerde criminaliteit dient dan ook tijdig te worden aangepakt.

Daartegenover staat dat de recente digitale evolutie een aanzienlijke invloed heeft gehad op de mogelijkheden waarmee criminaliteit kan worden opgespoord en vervolgd. Het internet en verwante informatica-ontwikkelingen zijn in die zin dus tevens een opportuniteit voor de criminaliteitsbestrijding en de veiligheidshandhaving. Meer bepaald kunnen ze in hoofdzaak dienen voor het vergaren van bewijs. Het belang van digitale tegenmaatregelen valt dus niet te ontkennen.

# INLEIDING

De Belgische strijd tegen het terrorisme heeft de voorbije jaren geresulteerd in een brede verzameling van initiatieven, met als belangrijkste doel de verschillende justitiële actoren in de sfeer van het Belgisch strafprocesrecht te voorzien van een uitgebreid arsenaal aan middelen.

Daarnaast werd een (medewerkings)verplichting gecreëerd in hoofde van de telecomoperatoren en de aanbieders van telefonie- en internetdiensten om bepaalde gegevens m.b.t. de elektronische communicatie te bewaren.

Maar daar bleef het niet bij: met de Wet digitaal speurwerk, ook genoemd de derde BOM-wet, vond een verdere aanvulling plaats van de middelen waarvan justitie zich kan bedienen in de steeds evoluerende strijd tegen de georganiseerde criminaliteit en (het verband met) het terrorisme. Op deze strijd legde het wetsontwerp dat de Wet digitaal speurwerk voorafging sterk de nadruk.

Bij velen leeft de overtuiging dat de wetgever er de voorbije jaren in geslaagd is om de balans tussen efficiëntie langs de ene kant, en respect voor de grondrechten langs de andere kant, in evenwicht te houden. Toch kan er niet omheen dat die mening niet door iedereen gedeeld wordt. In onze democratische samenleving, waar justitie, handhavingsorganen, advocaten en talrijke andere rechtspractici hun eigen (professionele) waarden verdedigen, is dat verschil in opvattingen logisch. Zo werd her en der ook geopperd dat door de Wet digitaal speurwerk te verregaande inmengingen in de persoonlijke levenssfeer en in andere grondrechten gefaciliteerd worden.

**Doelstelling**

Deze masterproef heeft tot doel de maatregelen van de Wet digitaal speurwerk aan een grondrechtelijke analyse te onderwerpen, waarbij zowel een Belgische als Europeesrechtelijke benadering van de materie aan bod komt.

Om enige duidelijkheid te verschaffen, werd ervoor gekozen om dit werk in drie grote delen op te splitsen.

In het eerste deel wordt gefocust op de nieuwe Belgische mogelijkheden van internet- en informaticarecherche met als doel digitaal bewijs te bekomen, al dan niet met het oog op terrorismebestrijding. De maatregelen die geboden worden door de Wet digitaal speurwerk worden in dit eerste deel dus geanalyseerd. Ook wordt aandacht besteed aan kritische bedenkingen van rechtspractici. Verder wordt de wet gesitueerd in het Belgische strafrechtelijke beleid. In deze beleidscontext vindt de wet namelijk haar toepassing. Wetgeving die dikwijls op gespannen voet komt te staan met de grondrechten –bijvoorbeeld deze vervat in de artt. 6 en 8 EVRM- vergt namelijk een duidelijke beleidssetting. In dat kader zijn duidelijke regels, knowhow en een streng deontologisch kader van het gehele juridische apparaat onontbeerlijk. Tussen wet en regelgeving enerzijds, en correcte toepassing ervan anderzijds, staan nu eenmaal mensen die moeten beschikken over een degelijke opleiding en een duidelijk referentiekader.

In het tweede deel wordt de materie vanuit het standpunt van de Raad van Europa geanalyseerd. Hierbij worden de constante wisselwerking en kruisbestuiving tussen visies, initiatieven en controlemechanismen van de Raad en zijn Verdragsstaten in het achterhoofd gehouden. In eerste instantie zal worden stilgestaan bij de algemene visie van de Raad op nieuwe maatregelen die een diepgaande inmenging (kunnen) inhouden op grondrechten, en die verantwoord worden door het oogmerk van een efficiënte terrorismebestrijding. Daarna wordt de aandacht gevestigd op een aantal recente initiatieven binnen de Raad inzake terrorismebestrijding, die aanleunen bij de materie van deze masterproef. Het sturende belang van de Raad van Europa voor nationale maatregelen door toedoen van recente aanbevelingen en initiatieven inzake de materie is namelijk groot. Daarop volgt in algemene zin een bespreking van de betekenis en de inhoud van de artikelen 6 en 8 EVRM.

Het laatste deel besteedt concreter aandacht aan de specifieke (rechtspraak inzake de) artt. 6 en 8 EVRM, die in de materie relevant is. Hierdoor wordt een toetsing van de nieuwe maatregelen inzake internet- en informaticarecherche, geregeld in de Belgische Wet digitaal speurwerk, mogelijk gemaakt.

# **DEEL 1. NATIONAAL**

## Definiëring terrorisme

Vandaag bestaat er op het internationale en Europese toneel geen uniforme definitie van het begrip terrorisme.[[1]](#footnote-1) Wel krijgt het begrip over het algemeen een steeds bredere invulling. Dit kan uiteraard leiden tot misbruik door nationale autoriteiten. Een breder wordend terrorismebegrip is namelijk een steeds groter wordende aanzet voor het wettigen van verregaande inmengingen in grondrechten.

Ook op Belgisch vlak worden momenteel vrij ruime –en door toedoen van wetswijzigingen: steeds ruimere- omschrijvingen van het begrip gehanteerd.

Terrorisme wordt enerzijds gedefinieerd in de Wet houdende de regeling van de inlichtingen- en veiligheidsdiensten: “*het gebruik van geweld tegen personen of materiële belangen om ideologische of politieke redenen met het doel zijn doelstellingen door middel van terreur, intimidatie of dreigingen te bereiken. Hieronder wordt ook het radicaliseringsproces begrepen’’.[[2]](#footnote-2)*

In het Belgische Strafwetboek wordt terrorisme gedefinieerd aan de hand van een limitatieve opsomming van ernstige misdrijven. Een misdrijf uit deze lijst wordt gekwalificeerd als terroristisch misdrijf wanneer het “*door zijn aard of context een land of een internationale organisatie ernstig kan schaden en opzettelijk gepleegd is met het oogmerk om:*

*-een bevolking ernstige vrees aan te jagen; of*

*-een overheid of een internationale organisatie op onrechtmatige wijze te dwingen tot het verrichten of het zich onthouden van een handeling; of*

*-de politie, constitutionele, economische of sociale basisstructuren van een land of een internationale organisatie ernstig te ontwrichten of te vernietigen’’.[[3]](#footnote-3)*

## Totstandkoming van de Wet digitaal speurwerk

Binnen de Federale Overheidsdienst Justitie werd in april 2015 een werkgroep opgericht, die werk moest maken van van “een meer aangepast juridisch kader voor de zoeking in een informaticasysteem en het onderscheppen en kennisnemen van elektronische communicatie’’.[[4]](#footnote-4)

Het daaruit voortvloeiende wetsontwerp ligt in dezelfde lijn als de Kadernota Integrale Veiligheid (KIV), die als het moederdocument van ons veiligheidsbeleid kan worden bestempeld.[[5]](#footnote-5) Daarnaast sluit het naadloos aan bij het bijhorend Nationaal Veiligheidsplan (NVP), dat de opdrachten en de belangrijkste doelstellingen van de federale politie bepaalt.[[6]](#footnote-6) In beide beleidsdocumenten werd opgeroepen tot een aanpassing van de bijzondere opsporingsmethoden -zowel in de reële als in de virtuele wereld- en tot een betere regeling voor de toegang op afstand, al dan niet heimelijk, tot een informaticasysteem. Alle pijlen werden dus gericht op een bijwerking van de desbetreffende wetgeving, waardoor de strafprocedure aan de snel digitaliserende samenleving aangepast kon worden.

Aandacht werd tevens gevraagd voor de effectieve uitbouw van internetpatrouilles en internetrecherche, en de bijhorende ‘online-agenten’, die niet enkel in staat moeten zijn om zeer efficiënt misdrijven op te sporen, maar ook om op een correcte en volledige manier de noodzakelijke vaststellingen te doen zodat deze kunnen gebruikt worden bij de voortzetting van onderzoeken.

Bij dit alles werd gewezen op de noodzaak van een globaal evenwicht tussen de efficiëntie van de opsporing en vervolging enerzijds en de bescherming van de persoonlijke levenssfeer en de rechten van verdediging anderzijds.[[7]](#footnote-7)

### 2.1. Historiek

In 2000 deed de Belgische wetgever een eerste inspanning om de strafprocedure aan de vlug digitaliserende samenleving aan te passen: de Wet van 28 november 2000 inzake informaticacriminaliteit[[8]](#footnote-8) zorgde voor de toevoeging van een aantal nieuwe procedurele instrumenten[[9]](#footnote-9) aan het Wetboek van Strafvordering, waarvan de belangrijkste het databeslag en de netwerkzoeking waren.[[10]](#footnote-10) Met deze wet werd inhoudelijk de Cybercrimeconventie van de Raad van Europa van 23 november 2001[[11]](#footnote-11) omgezet. Sindsdien werden de onderzoeksmaatregelen in de technologieomgeving echter niet meer aangepast, hoewel het gebruik van ICT door criminelen in buitengewone mate toenam.[[12]](#footnote-12)

Daarom werden in het wetsontwerp van de Wet digitaal speurwerk de artikelen m.b.t. het databeslag (art. 39bis Sv.), de netwerkzoeking (art. 88ter Sv.) en de medewerkingsplicht (art. 88quater Sv.) aangepast.[[13]](#footnote-13)

Daarnaast zorgde de Wet van 6 januari 2003[[14]](#footnote-14) voor een wettelijke regeling van het gebruik van bepaalde bijzondere opsporingsmethoden, of BOM. De belangrijkste BOM zijn de observatie, de infiltratie en de informantenwerking. Tevens introduceerde de wet een aantal onderzoeksmethoden die nauw aanleunen bij de BOM, maar daar niet als dusdanig onder vallen. Voorbeelden daarvan zijn de inkijkoperatie en het direct afluisteren.[[15]](#footnote-15) Deze wet werd grondig hervormd door de Wet van 27 december 2005[[16]](#footnote-16) nadat het Grondwettelijk Hof een aanzienlijk aantal bepalingen had vernietigd.[[17]](#footnote-17) Ook met een volgend arrest van het Grondwettelijk Hof werden enkele artikelen vernietigd, maar herstelwetgeving bleef uit.[[18]](#footnote-18)

Ten tijde van de introductie van het wetsontwerp was het dus sinds 2005 geleden dat de BOM herzien waren. Daarom werd gestreefd naar een verbetering van deze bestaande BOM sensu stricto.[[19]](#footnote-19) Ook werden nieuwe bepalingen toegevoegd over de interacties en infiltraties op het internet, die als “cyber-onderzoeksmethoden” gecatalogeerd kunnen worden.[[20]](#footnote-20)

Ten slotte bracht het wetsontwerp het achterhaald karakter van de Wet ter bescherming van de persoonlijke levenssfeer[[21]](#footnote-21) onder de aandacht, die indertijd werd geschreven met uitsluitend de klassieke telefonie voor ogen. De genoemde wet zorgde voor de invoering van de artikelen 90ter e.v. betreffende de telefoontap in het Wetboek van Strafvordering. Deze artikelen waren uitsluitend van toepassing op communicatie en telecommunicatie tijdens de overbrenging ervan en voldeden volgens het wetsontwerp dus niet meer aan de “eigen realiteit van het internet, waar elektronische gegevens het voorwerp uitmaken van communicatie op de elektronische snelweg’’.[[22]](#footnote-22)

Onduidelijkheid heerste dan ook over het statuut van deze gegevens en de rechtsgrond om ze in beslag te nemen of te intercepteren. Dat leidde in de strafrechtelijke praktijk herhaaldelijk tot moeilijkheden.[[23]](#footnote-23)

Dit alles zorgde voor een zogenaamde onhoudbare situatie die tot herziening van de eerder besproken maatregelen verplichtte, waarbij rekening diende te worden gehouden met de verbanden tussen de drie eerder besproken wetgevingen.[[24]](#footnote-24)

Binnen het geldende strafprocesrecht heerste een gebrek aan effectiviteit van de opsporing en de bewijsvoering, meer bepaald bij elke vorm van criminaliteit die in meer of mindere mate gerelateerd is aan informatietechnologie.[[25]](#footnote-25) Om politie en magistratuur over dezelfde middelen te laten beschikken als criminelen, werd daarom een actualisering noodzakelijk bevonden. Aangepaste middelen dienden ter beschikking te worden gesteld van gerechtelijke autoriteiten om bewijzen te verzamelen in informaticasystemen. Het uitgangspunt was een meer aangepast juridisch kader voor de zoeking in een informaticasysteem en het onderscheppen en kennisnemen van elektronische communicatie.[[26]](#footnote-26)

De evoluerende strijd tegen de georganiseerde criminaliteit – en in verband daarmee het terrorisme – stond in dit wetsontwerp centraal.

Het wetsontwerp waarborgde tevens een stijgende bescherming naarmate de gerechtelijke autoriteiten verder kunnen binnendringen in de persoonlijke levenssfeer van individuen.[[27]](#footnote-27) Echter dient opgemerkt dat verschillende actoren de mening toegedaan zijn dat, hoewel deze wet zeer duidelijk een stap zet in de richting van een efficiëntere criminaliteitsbestrijding, het evenwicht met de bescherming van de fundamentele rechten al te veel uit het oog verloren wordt.[[28]](#footnote-28)

Op 27 januari traden de wetswijzigingen in werking.

## Het begrip ‘IT-gerelateerde criminaliteit’

Onder informaticacriminaliteit in strikte zin worden verschillende in het Strafwetboek opgesomde misdrijven begrepen.[[29]](#footnote-29) In ruimere zin is informaticacriminaliteit (Engels: “cybercrime”) de verzamelnaam voor elke vorm van criminaliteit waarbij ICT (informatie- en communicatietechnologie) betrokken is, als doel (bijv. een externe hacking) of als middel. In dit laatste geval kan ICT ook in zeer algemene zin worden aangewend bij het voorbereiden of helpen plegen van misdrijven. Dit gebeurt bijvoorbeeld wanneer communicatie in de voorbereiding van een misdrijf door middel van ICT plaatsvindt.[[30]](#footnote-30)

Hieruit volgt dat deze masterproef, die het forensisch onderzoek in een geïnformatiseerde omgeving behandelt, niet de bestrijding van informaticacriminaliteit in strikte zin betreft. Ook betreft ze tot op een zekere hoogte niet de bestrijding van informaticacriminaliteit in ruime zin. Echter dient in dat kader opgemerkt te worden dat de bestrijding van de informaticacriminaliteit in ruime zin niet losstaat van het forensisch onderzoek in een geïnformatiseerde omgeving. Zo vervaagt onophoudelijk de grens tussen dergelijke informaticacriminaliteit en klassieke misdrijven waarbij ook informatietechnologie wordt aangewend, doordat de ‘gewone’ crimineel steeds vaker informatietechnologie gebruikt om zijn ‘gewone’ misdrijven te plegen.[[31]](#footnote-31)

Daarnaast kan ook opgemerkt worden dat de bestrijding van informaticacriminaliteit enerzijds en het forensisch onderzoek in een geïnformatiseerde omgeving als steunopdracht anderzijds traditioneel opdrachten zijn die worden uitgevoerd door de Computer Crime Units van de federale politie.[[32]](#footnote-32)

## Maatregelen inzake bewijsgaring door de Wet digitaal speurwerk

Hier bespreken we de belangrijkste **zelfstandige opsporingsmethoden** die door de Wet digitaal speurwerk werden ingevoerd. Het betreft maatregelen waartoe de opsporingsinstanties zélf het initiatief kunnen nemen, en waarbij er geen sprake is van samenwerking met andere (telecom)diensten.

We bekijken achtereenvolgens:

1. Het **open-bronnen-onderzoek** (4.1.)
2. De **online infiltratie** (4.2)
3. Het **vernieuwde regime voor het open en heimelijk IT-onderzoek** (4.3.)
4. Het **databeslag en de behandeling van digitaal bewijs in het algemeen** (4.4.)In dit onderdeel bespreken we de manier waarop verzamelde gegevens dienen te worden vastgelegd en gebruikt. Ook wordt de aandacht gevestigd op waarborgen die (dienen te) bestaan voor de persoon in kwestie en de gegevens zelf wanneer deze al dan niet in een gerechtelijk dossier gebruikt worden.

Hoewel niet uitdrukkelijk in de Wet digitaal speurwerk vermeld, valt er bij de zelfstandige opsporingsmethoden wel degelijk een onderscheid te maken tussen het open-bronnen-onderzoek (‘open source’) enerzijds, dat niet expliciet in de wet vervat is, en het vernieuwde regime voor het open en heimelijk IT-onderzoek anderzijds, dat wel expliciet in de wet geregeld wordt.

Hieronder volgt vooreerst een bespreking van het open-bronnen-onderzoek. Daarna komt het vernieuwd regime inzake IT-recherche aan bod.

### 4.1. Open-bronnen-onderzoek

De middelen die bij het open-bronnen-onderzoek gebruikt worden, zijn vrij beschikbaar op het internet. Dit heeft als gevolg dat iedereen deze zou kunnen gebruiken. In de praktijk worden de vrij beschikbare middelen veelvuldig door politiediensten gebruikt wanneer deze aan internetpatrouille/internetrecherche doen.

Diensten als Google, Creepy, Strava, Dead Drop en Echosec zijn voorbeelden van dergelijke hulpmiddelen.

**Het internet** in zijn breedste vorm beslaat veel meer dan wat vaak gedacht wordt. Binnen het internet dient namelijk een onderscheid gemaakt te worden tussen

- het *surface web* of *visible web*, dat via een simpele zoekmachine als Google bereikt kan worden;

- het *deep web*, dat alles omvat wat een zoekmachine niet kan vinden;

- en het *dark web*, dat slechts via anonimiserende software bereikbaar wordt. Dit *dark web* vertegenwoordigt een kleiner deel van het *deep web.[[33]](#footnote-33)*

Cybercriminaliteit is groot op het *dark web*: voorbeelden zijn de levendige handel in illegale goederen en diensten of de organisatie van terroristische acties. Welbekende cryptocurrencies zoals de bitcoin en blockchain-technologieën werden ontwikkeld op het *dark web* om anonieme betalingen mogelijk te maken.[[34]](#footnote-34)

Bij dit *dark web* gaat het dus om een werkelijk verstopt deel van het *web* waartoe enkel toegang verkregen kan worden via anonimiserende tools, die zorgen voor een afscherming van het IP-adres. Een voorbeeld van een forum dat zich op het *dark web* bevindt, is het Agoraforum: een online zwarte markt. Het hoeft geen betoog dat zowel de anonimiserende tools als de diverse fora op het *dark web* veel gebruikt worden voor criminele doeleinden, maar natuurlijk ook (en steeds meer) door politie-instanties. Een zeer belangrijke *anonymizer* is de TOR-browser, waarbij TOR staat voor “The Onion Router”. Deze laat toe om zich anoniem op het internet te kunnen begeven.[[35]](#footnote-35)

**Artikel 26 WPA**[[36]](#footnote-36) werd in 1992 voor de reële wereld geschreven en voorziet dat politieambtenaren, voor het uitvoeren van hun opdrachten –zowel van bestuurlijke, als van gerechtelijke politie- steeds de voor het publiek toegankelijke plaatsen en verlaten onroerende goederen kunnen betreden.[[37]](#footnote-37) Het artikel lijkt vandaag echter ook de wettelijke basis te vormen voor het autonoom surveilleren/patrouilleren op het internet door de politie, en dus ook voor het kunnen kennisnemen van de zogenaamde *publieke privacy* (zie verder) aldaar.[[38]](#footnote-38)

Onlangs werd dit door het Hof van Cassatie bevestigd.[[39]](#footnote-39) In casu begaf de politie zich op het *dark web* zonder bijzondere machtiging. Meer bepaald verschafte ze zich toegang tot de online zwarte markt van het voormelde Agoraforum. Met het oog op het verkrijgen van deze toegang werd anonimiserende software (TOR) gebruikt. Daarnaast kreeg de politie de vereiste uitnodigingslink van een lid van het Agoraforum. Tot slot werd een fictieve identiteit aangemaakt.

In cassatie werd beslist dat de politie wel degelijk toegang had kunnen nemen tot het Agoraforum. Ten eerste omdat het ging om een automatisch gegenereerde uitnodigingslink, die daardoor niet voldeed aan de redelijke privacyverwachting.[[40]](#footnote-40) De persoon in kwestie mocht met andere woorden niet redelijkerwijs verwachten dat diens privacy werd beschermd.[[41]](#footnote-41) Ten tweede ging het volgens het Hof om een publiek toegankelijke plaats, waardoor art. 26 WPA toepassing vond. Tot slot kon volgens de mening van het Hof een alias gebruikt worden, zolang er geen geloofwaardige identiteit wordt aangenomen, noch sprake is van provocatie.

Bijgevolg was er volgens de cassatie-uitspraak geen netwerkzoeking, gekenmerkt door bijkomende grondrechtelijke garanties, vereist. Ook was er geen sprake van enig hackingprocédé in hoofde van de politie.

Deze uitspraak leidde echter ook tot verontwaardiging. CONINGS stelt zich in dat verband de vraag waar precies de grens ligt tussen deze open-source-waarnemingen, waarbij online geobserveerd wordt, en de stelselmatige observatie. In dat kader wijst ze ook op de noodzaak van een beter artikel voor de online observatie. Vandaag worden de open-source-waarnemingen op het internet immers nog niet op een duidelijke manier onttrokken aan de observatie, die in art. 47sexies Sv. geregeld wordt. Discussies over de kwalificatie van de desbetreffende onderzoekshandeling zijn dan ook een logisch gevolg.[[42]](#footnote-42)

Ten slotte brengt CONINGS in herinnering dat ook in publiek toegankelijke plaatsen volgens het EHRM een redelijke privacyverwachting kan bestaan. Het vergaren van gegevens op het internet kan dus een inbreuk uitmaken op het recht op privacy zoals vastgelegd in art. 8 EVRM. Hiervan getuigen de verschillende EHRM-arresten[[43]](#footnote-43) waarin het privéleven als een zeer breed begrip wordt opgevat, dat niet het voorwerp kan zijn van een exhaustieve definitie. Aangezien art. 8 EVRM onder andere het recht beschermt om relaties met andere mensen en de buitenwereld op te bouwen en te ontwikkelen, is er volgens het Hof sprake van een ruimte voor interactie van een persoon met anderen. Die ruimte voor interactie kan zelfs in een openbare context onder de reikwijdte van “privéleven” vallen. Ook indien bepaalde gebeurtenissen of contacten met anderen plaatsvinden in de publiek te achten gedeelten van het internet, kunnen ze dus beschermd worden door art. 8 EVRM.[[44]](#footnote-44) Het vergaren van gegevens op het internet kan dan ook een inbreuk uitmaken op het recht op privacy zoals vastgelegd in art. 8 EVRM.

Art. 26 WPA wordt vandaag aldus in de praktijk als wettelijke basis beschouwd voor het autonoom surveilleren/patrouilleren op het internet door de politie –hiervan getuigt de voormelde cassatierechtspraak. Echter werd vooralsnog geen aanpassing van art. 26 WPA doorgevoerd. In dat kader bestaat nog enige onduidelijkheid omtrent de uitbreiding van art. 26 WPA van de reële wereld naar de voor het publiek toegankelijke plaatsen op het internet. Meer bepaald gaat het over de omlijning, de toegangsformaliteiten en het gebruik van een fictieve identiteit.[[45]](#footnote-45)

Naast het College van procureurs-generaal en het Openbaar Ministerie was ook de Commissie voor de Bescherming van de Persoonlijke Levenssfeer (CBPL)[[46]](#footnote-46) voorstander van een modernisering van art. 26 WPA door het toelaten van open-source-waarnemingen op het internet door de politie.[[47]](#footnote-47) De CBPL adviseerde[[48]](#footnote-48) echter wel een strengere omlijning van de grenzen van deze internetpatrouille. In elk ander geval bestond volgens de Commissie een risico op *de facto* strafvorderlijke observatie en/of infiltratie. Ook werd geijverd voor een zuiver formeel karakter van eventuele toegangsformaliteiten (registratie), en werd gesteld dat een fictieve identiteit van de politie nooit geloofwaardig mag zijn. Er mag dus geen misbruik gemaakt worden van de redelijke en geloofwaardige schijn van een (bestaande) naam.[[49]](#footnote-49) Daarnaast herinnerde de CBPL aan het uitgangspunt dat er nooit geprovoceerd mag worden.[[50]](#footnote-50) De provocatie van misdrijven wordt namelijk principieel verboden en leidt tot een onontvankelijke strafvordering.[[51]](#footnote-51)

In de Belgische praktijk ligt het open-bronnen-onderzoek in handen van de recentelijk ingevoerde **Internet Referral Unit** (IRU) bij de federale politie, die zich aldus met internetrecherche bezighoudt. Deze internetpolitie maakt deel uit van de Algemene Directie Gerechtelijke Politie - Directie van de bestrijding van de zware en georganiseerde criminaliteit, ofwel de DJSOC. Haar taak is het detecteren van de informatie en de publicaties op internet m.b.t. tot de propaganda, het terrorisme, het radicalisme, het gewelddadige extremisme, de haatmisdrijven/haatmisdaden online, en/of de mensenhandel, alsook het verwijderen van de desbetreffende inhoud en het nemen van maatregelen om de toegankelijkheid ervan te blokkeren. De IRU patrouilleert aldus op het internet; daartoe doorzoekt en verzamelt ze de gegevens die vrij teruggevonden kunnen worden op het internet of in sociale media.[[52]](#footnote-52)

Daarnaast werd in de nasleep van de aanslagen een tool voor internetonderzoek (*Open Source Intelligence Techniques*, of **OSINT**) geïntroduceerd. Met deze open-source-onderzoekstool is toegang tot het *dark web* mogelijk, in de eerste plaats in het kader van de strijd tegen terrorisme en gewelddadig radicalisme.

### Online infiltratie: nieuw art. 46sexies Sv.

De nieuwe regeling rond infiltratie of interactie op het internet werd, in tegenstelling tot het open-bronnen-onderzoek, expliciet in de Wet digitaal speurwerk opgenomen.

Deze bijkomende regeling wordt ook de ‘infiltratie light’ genoemd en is thans in het nieuwe art. 46sexies Sv. terug te vinden. Ze staat daarmee naast de volwaardige infiltratie in de reële wereld, die het voorwerp van art. 47octies en 47novies Sv. vormt. Met de infiltratie-light werd een efficiëntere aanpak beoogd van misdrijven als oplichting via het internet, handel in drugs en wapens, en cybercrime waarbij verdachten malware aanbieden via het *dark web*.[[53]](#footnote-53)

De maatregel houdt in dat het Openbaar Ministerie (OM) de politie schriftelijk kan machtigen om (desgevallend) onder fictieve identiteit op het internet (begrepen in ruime zin) contact te onderhouden met één of meerdere personen. Het gaat dus niet om een interactie énkel met het oog op arrestatie of verificatie, die daarentegen eenmalig zou zijn.

In dit kader blijft het verbod van een niet-expliciet, misleidend of provocatief optreden door de politie onverminderd gelden. De politiemensen in kwestie kunnen specialisten zijn in de materies van terrorisme, wapenhandel, mensenhandel of zedendelicten, maar in uitzonderlijke omstandigheden en indien strikt noodzakelijk kan ook een beroep worden gedaan op een burgerdeskundige.[[54]](#footnote-54)

Opdat de maatregel getroffen kan worden, dienen ernstige aanwijzingen te bestaan dat de betrokken persoon of personen misdrijven plegen of zouden plegen die een hoofdgevangenisstraf van 1 jaar of meer tot gevolg kunnen hebben (proportionaliteitseis) *en* dat het onderzoek de maatregel vereist en de overige onderzoeksmiddelen niet lijken te volstaan om de waarheid aan het licht te brengen (subsidiariteitseis).[[55]](#footnote-55)

De machtiging geldt voor een termijn van drie maanden, en kan hernieuwd worden.[[56]](#footnote-56)

Enkel in de mate dat het plegen van misdrijven wordt gemachtigd en/of er een beroep wordt gedaan op een burgerdeskundige, zal een vertrouwelijk ‘infiltratie-light’-dossier worden aangelegd. Controle op de infiltratie-light gebeurt door de kamer van inbeschuldigingstelling, doch enkel in het geval een vertrouwelijk dossier werd aangelegd.[[57]](#footnote-57)

Art. 46sexies, § 1, vierde lid Sv. bepaalt dat het artikel geen toepassing vindt (en er dus geen voorafgaande machtiging van het OM nodig is) bij *“de persoonlijke interactie op het internet van politieambtenaren, bij de uitvoering van hun opdrachten van gerechtelijke politie, met één 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”.* *A contrario* kan de politie dus *autonoom* op het internet, onder een *ongeloofwaardige* fictieve identiteit (of zonder vermelding van een identiteit), met personen contacten onderhouden met als rechtstreekse finaliteit een ‘gerichte verificatie’ of een ‘arrestatie’. Evenwel is het begrip “gerichte verificatie” daarbij niet duidelijk.[[58]](#footnote-58)

De politie heeft dan ook geen echte autonome surveillance- en opsporingsfunctie in de virtuele wereld. Magistratelijke machtiging is steeds nodig wanneer ze middels een *geloofwaardige* fictieve identiteit binnen de gerechtelijke politiefunctie wil opereren op het internet en ageren met een bepaalde target.[[59]](#footnote-59)

Processen-verbaal worden opgesteld door de OGP van de verschillende fasen in de uitvoering van de infiltratie, samen met de relevante contacten. Deze PV’s worden bij het dossier gevoegd. De contacten op het internet worden met “*de passende technische middelen*” geregistreerd en eveneens bij het dossier gevoegd of ter griffie neergelegd.[[60]](#footnote-60) Deze zinsnede komt tevens op verschillende andere plaatsen in de Wet digitaal speurwerk naar voren en schept onduidelijkheid (zie verder).

Het soepeler regime van deze infiltratie-light wordt verantwoord door het feit dat deze interactie op het internet minder indringend is dan de infiltraties in de fysieke wereld, maar ook omdat alle contacten, in tegenstelling tot bij deze gewone fysieke infiltratie, geregistreerd en in het strafdossier gevoegd worden. Op die manier wordt een garantie van transparantie geboden. Volgens de parlementaire voorbereiding is dit namelijk enkel mogelijk op het internet, en niet in de reële wereld.[[61]](#footnote-61) De drempel van 1 jaar voor deze maatregel is minder zwaar dan de klassieke infiltratie, waar het om een criminele organisatie dan wel de misdrijven van de taplijst van art 90ter Sv. dient te gaan.[[62]](#footnote-62)

### 4.3. Vernieuwd regime IT-recherche

Daarnaast regelt de Wet digitaal speurwerk het vernieuwde regime inzake IT-recherche.

In de nieuwe regeling wordt een onderscheid gemaakt tussen de al dan niet heimelijkheid van de *doelstelling* van de onderzoekshandeling. Het criterium daarbij is of deze mét, dan wel buiten medeweten van de verdachte gebeurt. ‘Heimelijk’ is in dat verband geen synoniem van ‘geheim’ of ‘buiten medeweten van’. Wanneer bijvoorbeeld een smartphone doorzocht wordt, die op achterbank van een verlaten voertuig werd aangetroffen, heeft men niet steeds de bedoeling om heimelijk te zijn.

Het nieuwe onderscheidingscriterium verving het volledig achterhaalde onderscheid van de al dan niet in transitie zijnde data/communicatie.

Ten gevolge van het nieuwe onderscheid zijn er enerzijds openlijke (niet-heimelijke) onderzoekshandelingen, en anderzijds heimelijke onderzoekshandelingen.

Ter herinnering: in principe vinden in het kader van het opsporingsonderzoek dat geleid wordt door de procureur des Konings (PK) geen dwangmaatregelen of schendingen van individuele rechten en vrijheden plaats.[[63]](#footnote-63) Zijn dergelijke maatregelen wel noodzakelijk of wenselijk, dan zal in beginsel een gerechtelijk onderzoek[[64]](#footnote-64) moeten worden gevorderd. Per uitzondering zijn in het opsporingsonderzoek wel dwangmaatregelen mogelijk wanneer de wet dit toelaat, via de mini-instructie of bij de heterdaadsituatie.[[65]](#footnote-65) Voor het uitvoeren van opsporingshandelingen in de praktijk doet de PK een beroep op de politiediensten.[[66]](#footnote-66)

Bij niet-heimelijke onderzoeken speelt hoofdzakelijk de bevoegdheid van het Openbaar Ministerie (OM). Deze onderzoeken gebeuren onder de ogen van de verdachte. Deze heeft vanaf het begin de bijstand van een advocaat, zoals in hoofdzaak geregeld door art. 39bis Sv.[[67]](#footnote-67)

De heimelijke onderzoeken daarentegen, die hoofdzakelijk geregeld worden door art. 90ter Sv., gebeuren per definitie buiten medeweten van de verdachte. Daarom gebeuren ze in principe onder het toezicht van de onderzoeksrechter (OR).[[68]](#footnote-68) Voor het uitvoeren van heimelijke onderzoekshandelingen zal doorgaans de machtiging van een OR nodig zijn.

#### Niet-heimelijke/openlijke informatica- en netwerkzoekingen

Met ‘informaticasystemen’ worden “*alle systemen voor de opslag, verwerking of overdracht van data*” bedoeld, waarbij “*vooral wordt gedacht aan computers, chipkaarten en dergelijke, maar ook aan netwerken en delen daarvan, evenals aan telecommunicatiesystemen of onderdelen daarvan die een beroep doen op IT’’.*[[69]](#footnote-69)

Voor niet-heimelijke zoekingen is art. 39bis Sv. sinds de Wet digitaal speurwerk het referentieartikel geworden. Dit artikel regelt, naast het informaticabeslag, drie verschillende bevoegdheden voor openlijke zoekingen in een informaticasysteem, zijnde de informaticazoeking, de netwerkzoeking (voorheen opgenomen in art. 88ter Sv.) en elke andere openlijke zoeking.[[70]](#footnote-70)

Sinds de Wet digitaal speurwerk bestaan er **4 niveaus** van zoeking, gekoppeld aan de bevoegde instantie. Het gaat dus om een getrapte bevoegdheid.

1. **Bevoegdheid officier van gerechtelijke politie (OGP).**

Wanneer door de opsporingsinstanties tijdens zoekingen in bepaalde plaatsen of tijdens fouilleringen informaticasystemen aangetroffen worden, is het mogelijk dat deze systemen relevante gegevens kunnen bevatten voor het strafrechtelijk onderzoek.[[71]](#footnote-71) Dan kan tot een informaticazoeking besloten worden, waarbij de zoeking beperkt wordt tot de gegevens die in het systeem zelf zijn opgeslagen.[[72]](#footnote-72)

De geldende regel in dit kader is dat, wanneer een OGP een gegevensdrager *in beslag heeft genomen*, hij deze ook mag uitlezen. De OGP kan dus autonoom een informaticazoeking doen van een systeem dat wettelijk door hem in beslag werd genomen.[[73]](#footnote-73) Op die manier kan de OGP bijvoorbeeld een gsm/smartphone uitlezen van een op heterdaad betrapte drugsdealer.[[74]](#footnote-74)

Alvorens met de zoeking wordt begonnen, zal de politie (of de parketmagistraat) het toestel op vliegtuigmodus moeten zetten, waardoor de wifi of 4G-connectie verhinderd wordt. Elke externe verbinding van het informaticasysteem dient namelijk te worden uitgeschakeld. Daardoor kan de informaticazoeking zich enkel uitstrekken tot gegevens die staan opgeslagen op het informaticasysteem zelf.[[75]](#footnote-75)

Voor het kraken van paswoorden met het oog op het verrichten van deze informaticazoeking, daarentegen, heeft de OGP het fiat van het OM nodig.[[76]](#footnote-76)

1. **Bevoegdheid Openbaar Ministerie (OM)**

Met het OM worden bedoeld de procureur des Konings, de arbeidsauditeur, de federale procureur en de procureur-generaal.[[77]](#footnote-77)

Wanneer door de OGP een informaticasysteem in beslag *kan* worden genomen, maar dit niet daadwerkelijk wordt gedaan, moet het OM het bevel geven aan de OGP om de zoeking in het informaticasysteem te doen.[[78]](#footnote-78) Zo zal bijvoorbeeld een bevel nodig zijn om een zoeking te doen in een computer die door een verdachte gebruikt werd in een internetcafé. Het zal namelijk niet wenselijk/noodzakelijk zijn deze computer in beslag te nemen.[[79]](#footnote-79)

Dit onderscheid, waardoor op basis van de toepassing van het beslag wordt bepaald welke instantie de zoeking kan uitvoeren, is volgens CONINGS bedenkelijk. Wanneer een OGP een systeem ter plaatse wil uitlezen, naar aanleiding van een fouillering, zal de machtiging van het OM nodig zijn. Indien hij daarentegen het systeem meeneemt, is deze machtiging niet vereist.[[80]](#footnote-80)

Ook in dit geval is de zoeking in beginsel beperkt tot de gegevens die in het informaticasysteem zijn opgeslagen.[[81]](#footnote-81) Het informaticasysteem kan dus enkel op zich onderzocht worden, nadat alle netwerkverbindingen worden uitgeschakeld. Eens dit is gebeurd, kan de OGP alle applicaties openen die geïnstalleerd zijn op het toestel, zoals de Facebook app, mailing apps als Gmail of Hotmail, en Messenger apps zoals Whatsapp.[[82]](#footnote-82)

Bij deze informaticazoeking kan wél gebruik worden gemaakt van vasle sleutels teneinde in het IT-systeem in te breken. Zo zal men bijvoorbeeld een gekraakt paswoord of een vingerafdruk als valse sleutel aanwenden met als doel het omzeilen of kraken van de beveiliging van het systeem in kwestie.[[83]](#footnote-83)

Het nieuwe art. 39bis § 5, zesde en laatste lid Sv. biedt het OM de mogelijkheid om aan de OGP op te dragen “*alle passende technische middelen*” aan te wenden om de gegevens, voorwerp van het misdrijf of uit het misdrijf voortgekomen en die strijdig zijn met de openbare orde en de goede zeden, ontoegankelijk te maken. Deze maatregel is mogelijk ten aanzien van de dreiging van het plegen van terroristische misdrijven of het aanzetten daartoe.[[84]](#footnote-84)

1. **Bevoegdheid OM: netwerkzoeking**/**uitgebreide informaticazoeking**

De bevoegdheid tot het uitvoeren van een netwerkzoeking bestond voor de onderzoeksrechter reeds in toepassing van art. 88ter Sv., maar kon toen ook via mini-onderzoek.[[85]](#footnote-85) Art. 88ter Sv. werd ingevoegd door de Wet informaticacriminaliteit als omzetting van het Cybercrimeverdrag en gaf aan de onderzoeksrechter de bevoegdheid om onder bepaalde voorwaarden te bevelen dat een zoeking in een informaticasysteem wordt uitgebreid naar systemen die zich op een andere plaats bevinden dan waar de zoeking fysisch plaatsvindt.[[86]](#footnote-86) Door de Wet digitaal speurwerk werd de bevoegdheid tot het uitvoeren van een netwerkzoeking overgeheveld naar het OM, wat wordt verantwoord door het niet-heimelijke karakter van de zoeking.

Hierdoor wordt vandaag door toedoen van de netwerkzoeking de mogelijkheid gegeven aan het OM om de zoeking van de eerder besproken niveaus 1 en 2 schriftelijk uit te breiden naar (een deel van) een informaticasysteem dat zich op een andere plaats bevindt dan het ‘basissysteem’.[[87]](#footnote-87)

Door CONINGS en ROYER worden enkele sprekende voorbeelden gegeven van dergelijke netwerkzoeking. Zo zal men toegang kunnen krijgen tot een facebook- of hotmailaccount van een inbeslaggenomen smartphone, of zal men zich toegang kunnen verschaffen tot een bankrekening van de persoon wiens informaticasysteem doorzocht wordt in het kader van een informaticazoeking.[[88]](#footnote-88)

De algemene voorwaarden voor netwerkzoeking zijn dat ze noodzakelijk is voor de waarheidsvinding enerzijds, *en* dat anderzijds andere maatregelen disproportioneel zijn *of* dat er zonder netwerkzoeking een risico is dat de bewijselementen verloren zouden gaan.[[89]](#footnote-89)

Het gaat om twee cumulatieve voorwaarden.

In dit verband wordt er door CONINGS en ROYER op gewezen dat er bijna altijd een risico op verlies van bewijsmateriaal zal zijn, aangezien informaticagegevens getypeerd worden door hun vluchtigheid. Daarnaast zal doorgaans heel snel de disproportionaliteit van andere maatregelen kunnen worden aangetoond, gezien het tijds- en arbeidsintensieve karakter van de alternatieve huiszoeking. Hieruit kan worden afgeleid dat de netwerkzoeking steeds een mogelijkheid zal zijn wanneer de maatregel noodzakelijk wordt geacht voor de waarheidsvinding.[[90]](#footnote-90)

Zolang er ter uitvoering van de netwerkzoeking geen paswoorden gekraakt dienen te worden van het inbeslaggenomen systeem, blijft het OM bevoegd. In het omgekeerde geval, wanneer er voor de netwerkzoeking een nieuwe poging tot decodering of ‘hacking’ nodig is, bovenop deze die nodig was om binnen te dringen in het IT-systeem van niveau 2, zal het nodig zijn zich tot de onderzoeksrechter te wenden.[[91]](#footnote-91)

Het volgende praktische voorbeeld[[92]](#footnote-92) verduidelijkt dit. De politie heeft een smartphone in beslag genomen en begint deze uit te lezen, eventueel, na toestemming van het OM, met gebruik van een paswoord. Wanneer het doel van de zoeking is om een Gmail account in de ‘cloud’ te raadplegen (netwerkzoeking), is er geen machtiging van de onderzoeksrechter nodig indien die account vrij toegankelijk is (bijvoorbeeld omdat het wachtwoord ‘onthouden’ werd door het systeem), en de politie dus geen nieuw wachtwoord dient in te geven. Echter, indien wél een nieuw paswoord vereist is, dient er een machtiging van de onderzoeksrechter te zijn. De beslissing van het OM volstaat dan niet.

CONINGS wijst in dit verband op de problematiek dat in de praktijk maar zelden een wachtwoord zal moeten worden ingegeven om vanop een iPhone toegang te krijgen tot de emailaccount. Er zal in dergelijk geval dus geen machtiging van de onderzoeksrechter nodig zijn.

De overheveling van de bevoegdheid tot het uitvoeren van een netwerkzoeking naar het OM is dan ook al meermaals kritisch onthaald.[[93]](#footnote-93) De netwerkzoeking geeft namelijk vaak toegang tot een zeer grote hoeveelheid aan privé-informatie.

1. **Bevoegdheid onderzoeksrechter**

De onderzoeksrechter is als enige bijkomend bevoegd voor elke andere zoeking dan deze van de drie vorige niveaus; het gaat dus om een ‘restcategorie’. De OR kan deze andere zoekingen doen onder dezelfde algemene voorwaarden als deze die gelden voor de netwerkzoeking.[[94]](#footnote-94)

Deze restcategorie biedt in de praktijk de mogelijkheid van hacken op afstand. De noodzaak hiervoor dringt zich bijvoorbeeld op in het volgende sprekende geval, waarbij er geen ‘basissysteem’ ter beschikking is van waaruit de zoeking kan verricht worden: de verdachte gooit zijn/haar smartphone in een rivier, maar de speurders hebben tegelijkertijd een Hotmail-account op het oog via een observatie; men heeft dus wél de login en het wachtwoord ter beschikking. Deze account zal dan doorzocht kunnen worden via hacken op afstand.[[95]](#footnote-95)

Een **notificatieplicht** dient het openlijk karakter van de besproken zoekingen in IT-systemen uit art. 39bis Sv. te verzekeren (zie verder).

#### Heimelijke IT-zoekingen

Door de Wet digitaal speurwerk werden twee varianten van heimelijke zoekingen in informaticasystemen ingevoerd, die het effectieve onderzoek van de opsporingsdiensten willen vergemakkelijken. Deze diensten kunnen namelijk uitdagingen ondervinden door het gebruik van elektronische communicatiediensten, in combinatie met het wijdverspreide gebruik van encryptie.

De eerste variant is de inkijkoperatie in een informaticasysteem, geregeld in art.89ter Sv.

De tweede variant is de werkelijke heimelijke doorzoeking van een informaticasysteem, geregeld in art. 90ter Sv.

1. **Inkijkoperatie in een informaticasysteem (art. 89ter Sv.)**

De inkijkoperatie in een informaticasysteem werd geïncorporeerd in de reeds bestaande regeling van de klassieke inkijkoperatie die toelaat private plaatsen te betreden, en waarbij het de bedoeling is “zoekend rond te kijken”.[[96]](#footnote-96)

Door de inschrijving van de inkijkoperatie in informaticasystemen in art. 89ter Sv., werd deze gelijkgeschakeld met een inkijkoperatie in een woning. Daardoor is enkel de onderzoeksrechter bevoegd. Tevens kan de onderzoekshandeling niet in het kader van een mini-onderzoek plaatsvinden.[[97]](#footnote-97) Door CONINGS wordt er dan ook op gewezen dat bij deze bevoegdheid de privacygevoeligheid wél erkend wordt, in tegenstelling tot bij de andere nieuwe bevoegdheden sinds de Wet digitaal speurwerk.

De inkijkoperatie kan enkel uitgevoerd worden wanneer de onderzoeksrechter ernstige aanwijzingen heeft dat de feiten een misdrijf uitmaken uit de taplijst[[98]](#footnote-98) of dat het om een misdrijf gaat in het kader van een criminele organisatie.[[99]](#footnote-99) Ook geldt de vereiste van subsidiariteit.[[100]](#footnote-100)

Men kan zich heimelijk toegang verschaffen tot private informaticasystemen, met hetzelfde doel als bij de klassieke inkijkoperatie: zich vergewissen van bepaalde gegevens en bewijzen verzamelen van de aanwezigheid van deze gegevens.[[101]](#footnote-101)

Het verschil tussen deze inkijkoperatie en de nieuwe werkelijke heimelijke doorzoekingsbevoegdheid van art. 90ter Sv. (zie hierna) lijkt voornamelijk in de beperkte doelstelling van de eerste te liggen: de inkijkoperatie zou slechts dienen als ‘oriënterend instrument’. Volgens CONINGS en ROYER is er evenwel nauwelijks nog een verschil tussen beide bevoegdheden:[[102]](#footnote-102) de inkijkoperatie in een informaticasysteem lijkt niet meer beperkt tot het louter zoekend rondkijken. Daarenboven voorziet de wet niet in een vertrouwelijk dossier, dat er nochtans voor zou moeten zorgen dat het gebrek aan controle door de verdediging wordt opvangen.[[103]](#footnote-103)

1. **Werkelijke heimelijke doorzoeking van informaticasystemen (art. 90ter Sv.)**

De intussen achterhaalde tapwetgeving van art. 90ter Sv. e.v. dateert van 1994 en had de klassieke telefonie voor ogen. Ze werd geschreven in een wereld die nog ver af stond van de hedendaagse digitale wereld.[[104]](#footnote-104) Het artikel was exclusief van toepassing op (tele)communicatie tijdens de overbrenging ervan. Door de nieuwe ontwikkelingen op informaticagebied was het vaak onmogelijk geworden om uit te maken of een communicatie nog in overbrenging was of reeds afgeleverd was. Daarom werd de zinsnede *‘tijdens de overbrenging ervan’* in art. 90ter, § 1 Sv. geschrapt. Nu kunnen in het kader van een heimelijke zoeking in een informaticasysteem data gekopieerd worden, ongeacht in welke doorsturingsfase de data zich bevinden.[[105]](#footnote-105)

De Wet digitaal speurwerk heeft de tapmaatregel van art. 90ter Sv. hervormd, waardoor een overgang werd gemaakt van ‘telefoontap’ naar ‘informaticatap/communicatietap’. De onderzoeksrechter kan krachtens de herschreven eerste paragraaf van art. 90 ter Sv. “*met een heimelijk oogmerk de 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 zoeking in een informaticasysteem of een deel ervan uitbreiden”*.[[106]](#footnote-106) Onder deze ‘niet voor het publiek toegankelijke communicatie’ vallen nog steeds de termen privé-communicatie of telecommunicatie van het oude art. 90ter Sv.[[107]](#footnote-107)

De vroegere tapbevoegdheid werd aldus sterk uitgebreid. Voortaan omvat art. 90ter Sv. de bevoegdheid om heimelijk informaticasystemen binnen te dringen met het oog op een doorzoeking en/of het in *real time* volgen van ontwikkelingen op het toestel.[[108]](#footnote-108) Toch een bedenking: ondanks het feit dat deze wijziging slechts als een modernisering van de tapmaatregel werd voorgesteld, lijkt de nieuwe bevoegdheid ook hacken toe te laten, waardoor ze veel indringender blijkt te zijn dan de klassieke tapbevoegdheid.[[109]](#footnote-109)

De onderzoekshandeling kan in de eerste plaats bevolen worden ten aanzien van personen die er op grond van precieze aanwijzingen van verdacht worden een misdrijf te hebben gepleegd uit de taplijst.[[110]](#footnote-110) Daarnaast kan de zoeking ook worden bevolen ten aanzien van personen van wie op grond van precieze feiten wordt vermoed dat ze regelmatig in verbinding staan met de verdachte persoon.[[111]](#footnote-111) Voor dat laatste geval werd evenwel geen bijkomende garantie voorzien dat de zoeking voldoende gericht zou zijn op gegevens van de verdachte, en niet van deze derde persoon.[[112]](#footnote-112)

De maatregel komt toe aan de onderzoeksrechter. Weliswaar kan, bij heterdaad en zolang die duurt, de PK de maatregel bevelen voor enkele strafbare feiten, waaronder terrorisme.[[113]](#footnote-113) Bovendien kan hij het bevel in dergelijk geval verlenen tot 72 uur na de ontdekking ervan. Dit maakt dat het OM 72 uur heeft (en eventueel langer indien de heterdaad langer duurt) om autonoom te tappen. Men kan dus spreken van een ruimere heterdaadbevoegdheid in het geval van terroristische misdrijven.[[114]](#footnote-114)

### 4.4. Databeslag – Behandeling van digitaal bewijs

#### 4.4.1. Databeslag

Na het eerder besproken open of heimelijk IT-onderzoek kunnen gevonden stukken en/of informatie in beslag genomen en bewaard worden. In 2000 werd de mogelijkheid ingevoerd in art. 39bis Sv. om deze gegevens op grond van het databeslag in beslag te nemen, naast de reeds bestaande mogelijkheid om dat ook op grond van het klassieke beslag met hun materiële drager (art. 35 e.v. Sv.) te doen.[[115]](#footnote-115)

Door het beslag onttrekt de bevoegde overheid één of meerdere zaken aan de vrije beschikking van een persoon. Het databeslag, meer specifiek, omvat het kopiëren en ontoegankelijk maken van gegevens en heeft tot doel de bewaring van de gegevens en hun integriteit voor de procedure ten gronde, waar ze als bewijs kunnen worden aangewend of eventueel kunnen worden verbeurdverklaard.[[116]](#footnote-116)

#### 4.4.2. Authenticiteit en integriteit van het digitaal bewijsmateriaal

Hoewel art. 39bis Sv. reeds veel onduidelijkheden in zich droeg, heeft de nieuwe Wet digitaal speurwerk de bestaande voorwaarden grotendeels bevestigd. Het artikel maakt niet veel woorden vuil aan de manier waarop het databeslag dient te gebeuren. De Raad van State adviseerde[[117]](#footnote-117) nochtans om, ter verzekering van de integriteit van het bewijs, preciezere bewoordingen te gebruiken. Echter stelt art. 39bis, § 8 Sv. nog steeds het volgende:

*“De procureur des Konings wendt de passende technische middelen aan om de integriteit en de vertrouwelijkheid van deze gegevens te waarborgen.”*

Ook op andere plaatsen in art. 39bis Sv. wordt van “passende technische middelen” gesproken. Hoewel deze bepaling een duidelijke flexibiliteitswens van de wetgever veruitwendigt, vormt deze bepaling het zeer logische voorwerp van discussie.[[118]](#footnote-118)

Digitale gegevens zijn immers zeer gemakkelijk manipuleerbaar; daardoor worden ook de de authenticiteit en integriteit van de in beslag genomen gegevens al snel bedreigd. Deze zijn nochtans cruciaal voor het verdere gebruik als bewijsmateriaal voor de vonnisrechter en voor het garanderen van het recht op een eerlijk proces.[[119]](#footnote-119) Het is dan ook zeer belangrijk om in de praktijk de authenticiteit en de integriteit van het digitaal bewijs te waarborgen.

##### 4.4.2.1. Authenticiteit

Voor het kunnen vrijwaren van de authenticiteit zal men moeten kunnen aantonen waar de oorsprong ligt van het aangedragen elektronisch bewijsmateriaal -dat meestal door de politie vergaard werd- en of het kan worden toegeschreven aan de verdachte in kwestie. Daarbij is het belangrijk dat de politie nauwkeurig beschrijft wat haar handelingen zijn geweest met het oog op de inbeslagneming van het bewijsmateriaal.[[120]](#footnote-120)

Echter is het bewijzen van de authenticiteit niet altijd even vanzelfsprekend, aangezien cybercriminelen maar al te graag gebruik maken van “anonymizers” zoals TOR, die hen toelaten zich anoniem te maken- juist met de bedoeling niet te kunnen worden gelinkt met het belastend bewijsmateriaal.[[121]](#footnote-121)

##### 4.4.2.2. Integriteit

Daarnaast is het van fundamenteel belang om de integriteit van de gegevens te vrijwaren. Deze wordt gevrijwaard wanneer vaststaat dat het bewijsmateriaal niet werd aangetast na de inbeslagname en dus geen voorwerp is geworden van wijzigingen. Het verworven bewijsmateriaal moet onaangetast blijven tot aan de behandeling ten gronde. Deze integriteit kan zowel tijdens de inbeslagneming zelf, als tijdens het verdere onderzoek en tijdens de bewaring in het gedrang komen.[[122]](#footnote-122)

In afwachting van een betere invulling van de “passende technische middelen” probeert men vandaag in de praktijk op verschillende manieren te garanderen dat gegevens die ten gronde worden voorgelegd, dezelfde zijn als deze die in beslag genomen werden. Zo kan bij de zoekingen en inbeslagnames gebruik gemaakt worden van blanco harde schijven, of forensische kopieën waarbij elk digitaal gegeven (elke bit) mee gekopieerd wordt.[[123]](#footnote-123) Nochtans worden dergelijke mogelijkheden nergens in art. 39bis Sv. vermeld.

Vandaag bestaat bij gebrek aan verdere invulling van de “passende technische middelen” dus nog steeds een situatie die vragen oproept m.b.t. de daadwerkelijke garantie van de integriteit van digitale gegevens. Er heerst dan ook een grote bezorgdheid over de manier waarop de vertaling - met een volledige garantie voor de integriteit - van digitale vaststellingen naar het niet-digitale dossier gebeurt.

Immers: de garantie van het recht op een eerlijk proces (art. 6 EVRM) kan door een gebrek aan waarborgen voor de integriteit van het digitaal materiaal ernstig gehypothekeerd worden. Men denke vooral aan de onderling verweven rechten op wapengelijkheid, tegenspraak en interne openbaarheid die onder druk komen te staan bij een gebrek aan integriteitswaarborg. Voor het garanderen van elk van deze rechten is het dus van uitermate belang dat de integriteit (en authenticiteit) van het digitaal bewijsmateriaal gewaarborgd worden.

##### 4.4.2.3. Onvolkomen notificatieplicht

Ook de onvolkomen notificatieplicht van art. 39bis Sv. bedreigt de authenticiteit en de integriteit van het digitaal bewijsmateriaal.

De zoekingen in IT-systemen uit art. 39bis Sv. zijn typisch openlijk. De notificatieplicht moet dit openlijk karakter verzekeren.[[124]](#footnote-124) Paragraaf 7 van art. 39bis Sv. bepaalt dan ook dat de verantwoordelijke van het IT-systeem op de hoogte gebracht dient te worden van de zoeking of de uitbreiding ervan.[[125]](#footnote-125)

Deze kennisgeving dient echter slechts te gebeuren *“tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden”.* Een vraag die terecht gesteld wordt door menig rechtspractici, is hoe het begrip ‘redelijkerwijs’ ingevuld moet worden, en of een digitale notificatie dergelijk probleem niet kan opvangen.[[126]](#footnote-126) Ook zal de identiteit van de verantwoordelijke van het IT-systeem zelden achterhaald kunnen worden, aangezien regelmatig technische instrumenten gebruikt worden met oog op het zich afschermen voor de buitenwereld; men denke aan het verstoppen van IP-adressen.[[127]](#footnote-127)

Verder werd de mededelingsverplichting niet op straffe van nietigheid voorgeschreven, en werd werd ze niet aan enige termijn onderworpen.[[128]](#footnote-128)

Nochtans kan het gebrekkig oflaattijdig informeren van de beslagene niet alleen de bewijswaarde, maar tevens de authenticiteit en de integriteit van het bewijsmateriaal in het gedrang brengen, aangezien het recht op een eerlijk proces in haar geheel beoordeeld wordt.[[129]](#footnote-129)

In België wordt de (digitale) bewijsvoering, waaronder de bruikbaarheid van eventueel onrechtmatig bekomen bewijsmateriaal voor de rechter ten gronde, geregeld door de Antigoonrechtpraak van het Hof van Cassatie. Hieraan werd een wettelijke grondslag gegeven in de Voorafgaande Titel van het Wetboek van Strafvordering.[[130]](#footnote-130)De rechtspraak bepaalt dat onrechtmatig verkregen bewijs enkel nog in drie hypothesen buiten beschouwing gelaten wordt, meer bepaald

1. wanneer de geschonden regel is voorgeschreven op straffe van nietigheid
2. wanneer door de schending de betrouwbaarheid van het bewijs is aangetast – dit is essentieel in de materie, meer bepaald omdat de authenticiteit en integriteit van in beslag genomen digitaal bewijsmateriaal aangetast kunnen zijn.
3. wanneer de rechten van verdediging werden geschonden – ook dit is essentieel in de materie. Door het Hof van Cassatie werd bovendien verduidelijkt dat de rechter de elementen van de zaak in haar geheel in overweging mag nemen.[[131]](#footnote-131)

Het is dus van uitermate belang dat de authenticiteit en integriteit van het bewijsmateriaal gewaarborgd worden.

#### 4.4.3. Afwezigheid van waarborgen voor de beslagene

Naast de gebreken die inzake het waarborgen van de authenticiteit en vooral de integriteit van het bewijsmateriaal blijken te bestaan, brengen CONINGS EN ROYER de verdere afwezigheid van waarborgen voor de beslagene zelf onder de aandacht.

Door de graduele stijging van gegevens als gevolg van de technologische evoluties, worden speurders vaak genoopt tot het in beslag nemen van gegevens of gegevensdragers om slechts naderhand een selectie van het strafrechtelijk relevante bewijsmateriaal door te voeren.[[132]](#footnote-132) In de praktijk kan het databeslag dan ook problemen opleveren in het licht van het proportionaliteitsbeginsel. Hoewel in principe de in beslag genomen gegevens steeds een verband moeten tonen met het onderzochte misdrijf, worden vandaag (te) grote hoeveelheden – en dus tevens irrelevante gegevens - in beslag genomen.[[133]](#footnote-133) Reeds ten tijde van het wetsontwerp inzake informaticacriminaliteit werd door de Privacycommissie de nodige aandacht gevestigd op dergelijke problematiek.[[134]](#footnote-134)

Het belang van deze proportionele inbeslagneming werd reeds door Hof van Cassatie bevestigd.[[135]](#footnote-135) In casu werd in Cassatie (en voorafgaand in hoger beroep) bepaald dat zogenaamde *fishing expeditions*, waarbij buitensporige hoeveelheden gegevens in beslag genomen worden, strijdig zijn met het recht op een eerlijk proces en het recht op privéleven.

Daarnaast bestaat er een gevaar in de combinatie en verwerking van persoonsgegevens die door de justitiële autoriteiten bij de opsporing en berechting van misdrijven in enorme hoeveelheden worden verzameld met het oog op een latere doorzoeking. Art. 39bis Sv. voorziet nochtans niets omtrent het lot van (ir)relevante persoonsgegevens die in het strafdossier verzameld zijn. Zo heerst onduidelijkheid over hoe lang dergelijke gegevens na een definitieve uitspraak nog bewaard mogen blijven en wanneer ze eventueel dienen te worden vernietigd. Hoewel de Privacycommissie in die zin adviseerde, bevat art. 39bis Sv. geen verwijzing naar de Wet Verwerking Persoonsgegevens[[136]](#footnote-136) die in België de geautomatiseerde verwerking van persoonsgegevens regelt.[[137]](#footnote-137)

## Strafrechtelijk beleid inzake digitale recherche

In de Belgische praktijk zijn vandaag verschillende actoren verantwoordelijk voor de digitale recherche.

### 5.1. Online onderzoek

Het open-bronnen-onderzoek enerzijds ligt in handen van de eerder aangehaalde **Internet Referral Unit** (IRU) bij de federale politie. Deze internetpolitie is verantwoordelijk voor internetrecherche en maakt deel uit van de DJSOC. Zoals eerder besproken, richt zij haar pijlen op informatie m.b.t. tot de propaganda, het terrorisme, het radicalisme, het gewelddadige extremisme, de haatmisdrijven en/of de mensenhandel. De IRU patrouilleert aldus op het internet; daartoe doorzoekt en verzamelt ze de gegevens die daarop vrij teruggevonden kunnen worden.[[138]](#footnote-138) Wat betreft de opleiding van deze online agenten blijkt het personeel een interne opleiding gekregen te hebben, die essentieel gericht is op “materie gelinkt aan het internet in het algemeen”.[[139]](#footnote-139) Verdere specificaties omtrent deze opleiding, de controle op verrichte werkzaamheden en een toepasselijk regelgevend kader lijken momenteel uit te blijven.

Daarnaast richt de recent geïntroduceerde *Open Source Intelligence* of **OSINT** zich als open-source-onderzoekstool prioritair op de strijd tegen het terrorisme en gewelddadig radicalisme. Het gaat om een interdepartementaal project van de federale politie, de Staatsveiligheid en de militaire inlichtingendienst ADIV. Het heeft tot doel het verkrijgen van een geïntegreerde informatica-toepassing voor OSINT-opzoekingen op het internet, het *deep web* en het *dark web*.[[140]](#footnote-140)

### 5.2. IT-onderzoek

#### 5.2.1. Computer Crime Units

Het IT-onderzoek wordt vandaag in de praktijk door de Computer Crime Units (CCU’s) van de federale gerechtelijke politie uitgevoerd. Naast de bestrijding van informaticacriminaliteit verlenen zij namelijk ook steun in de vorm van forensisch onderzoek in een geïnformatiseerde omgeving. Dit doen ze zowel ten behoeve van de eigen recherchediensten als van de lokale politiezones. Deze steun wordt verleend in het kader van de bestrijding van traditionele vormen van criminaliteit en betreft o.m. het kopiëren van digitale data, bijstand bij huiszoekingen in geïnformatiseerde omgevingen, de forensische analyse van ICT-systemen of de bijstand bij technische verhoren. Het betreft opdrachten van gerechtelijke politie.[[141]](#footnote-141)

De CCU’s zijn in principe uitgebouwd op twee niveaus, te weten de Federal Computer Crime Unit (FCCU) op nationaal niveau, die ondergebracht werd in de Centrale directie van de bestrijding van de zware en georganiseerde criminaliteit, en de regionale CCU's (RCCU’s) binnen elke gerechtelijke directie in de arrondissementen.[[142]](#footnote-142) Echter worden sinds kort ook Local Computer Crime Units (LCCU’s) opgericht bij lokale politiezones.

Deze CCU's moeten garant staan voor een efficiënte en tijdige bijstand aan de politiediensten.[[143]](#footnote-143) Ze dienen alle relevante informatie in ICT-omgevingen op te sporen, te vrijwaren en in leesbare vorm ter beschikking te stellen van de rechercheurs. De bruikbaarheid van de onderzoeksresultaten door onderzoekers en magistraten moet daarbij voorop staan.[[144]](#footnote-144)

#### 5.2.2. Toezichtsrapport Comité P

#### 5.2.2.1. Aanleiding

Een recent toezichtsrapport[[145]](#footnote-145) van het Vast Comité van Toezicht op de politiediensten (Comité P) legt echter op duidelijke wijze verschillende gebreken bloot in de praktijk van deze steunverlening. Aanleiding voor het onderzoek vormde de -soms zeer grote- achterstand van verschillende RCCU’s bij het uitlezen van in beslag genomen gegevensdragers zoals computerapparaten. Dergelijke achterstand kan een gepaste afhandeling van strafonderzoeken ernstig schaden, en creëert het gevaar op verlies van informatie. Ook de ontwikkeling van de Local Computer Crime Units (LCCU’s) bij lokale politiezones liet vermoeden dat de steunverlening onder druk staat.

Daarom werd tot een toezichtsonderzoek beslist dat het forensisch onderzoek in een geïnformatiseerde omgeving betrof en resulteerde in een recent tussentijds verslag.

#### 5.2.2.2. Bedreigende factoren voor een goede CCU-werking

Verschillende factoren bleken een goede CCU-werking bij de federale politie te bedreigen. Hierdoor bestaat ook een risico voor de basisprincipes van de politiewerking[[146]](#footnote-146), te weten de geïntegreerde werking, de gelijkwaardige dienstverlening en een kwaliteitsvolle dienstverlening.

###### 5.2.2.2.1. Gebrek aan eenduidige visie en functionering

In de eerste plaats is er bij de federale politie momenteel geen goedgekeurd intern functioneringsmodel dat de werking van de FCCU en de RCCU’s op elkaar afstemt; voor bepaalde opdrachten is dus onduidelijk door wie deze opgenomen moeten worden. Hierdoor ontbreekt het ook aan een geïntegreerde werking.

Daarnaast bestaan binnen de federale gerechtelijke politie verschillen in visie over de wenselijkheid van LCCU-initiatieven bij de lokale politie. De oprichting ervan kan immers verschillende risico’s inhouden, temeer doordat ook een grote diversiteit inzake de lokale initiatieven zélf bestaat: waar sommige politiezones geen initiatieven ontwikkelen en verder beroep wensen te doen op de RCCU’s van de federale gerechtelijke politie, hebben andere zones (vooral in Vlaanderen) een eigen LCCU opgericht. Dit creërt het risico dat een politie met twee snelheden ontstaat. Daardoor kan een gelijkwaardige dienstverlening gevaar lopen.

###### 5.2.2.2.2. Capaciteitsgebrek

Hoewel bij de FCCU en de RCCU’s in 2015 een personeelskader werd voorzien van 280 FTE’S,[[147]](#footnote-147) bestond in maart 2017 een tekort van 60 FTE’s. Verschillende oorzaken liggen aan de basis van dit capaciteitsgebrek, waaronder problemen inzake het rekruteren van nieuwe medewerkers. Ook de oprichting van LCCU’s blijkt een bijkomend probleem om de capaciteit op peil te houden, doordat bij de oprichting van LCCU’s gerekruteerd wordt uit de RCCU’s.

###### 5.2.2.2.3. Gebrekkig kennisbeheer

Het behoeft geen betoog datde huidige technologische ontwikkelingen - en de toenemende complexiteit van de forensische onderzoeken - medewerkers noodzaken met gespecialiseerde kennisniveaus. Toch bestaat er momenteel bij de F/RCCU’s slechts één profiel van onderzoeker, gekoppeld aan één enkele basisopleiding. Deze basisopleiding omvat een zestal weken en werd tot op heden georganiseerd bij de FCCU met ondersteuning van één RCCU-medewerker. Dit beantwoordt uiteraard niet meer aan de operationele realiteit. Daarom bestaat de noodzaak aan een differentiatie in onderzoeksprofielen, een afgestemd rekruteringsbeleid en een aangepast opleidingsbeleid.

Deze noodzaak blijkt des te meer wil men bij de forensische onderzoeken de *chain of custody[[148]](#footnote-148)*, de bewijsintegriteit en de authenticiteit van het digitaal bewijs kunnen garanderen. De inzet van medewerkers die voldoende opgeleid zijn om deze garanties te kunnen bieden, is onontbeerlijk. Zeker in het kader van de oprichting van LCCU’s doet deze problematiek zich voor, *“waar een aantal zones immers verschillende tools bezitten om digitale gegevensdragers forensisch uit te lezen, maar niet de knowhow hebben om de resultaten daarvan voldoende grondig te interpreteren(…).”[[149]](#footnote-149)*

Tevens bestaat momenteel geen instrument dat de uitwisseling van goede praktijken en ervaringen toelaat tussen de R/FCCU’s onderling, evenals met de andere partners, de lokale politiezones en de parketten. Initiatieven tot expertise-uitwisseling beperken zich momenteel tot de CCU-diensten van de federale politie. Nochtans is een expertise-coördinatie een noodzaak in een snel evoluerende technologische omgeving, waarin het onmogelijk wordt dat iedereen voor alles de nodige expertise kan hebben.

###### 5.2.2.2.4. Ontoereikende budgettaire en materiële middelen

Het belang van evoluerende budgettaire en materiële middelen ter beschikking van de F/RCCU’s is groot in een ICT-wereld die zelf constant evolueert; zeker omdat de onderzoeksresultaten worden aangewend in strafonderzoeken waarbij de *chain of custody*, de bewijsintegriteit en de authenticiteit van het digitaal bewijs gegarandeerd moeten worden. Evenwel bestaan in de dagdagelijkse werking van de F/RCCU’s verschillende problemen die verband houden met de begrensde middelen. Ook hier blijkt de oprichting van lokale initiatieven een bijkomend gevaar in te houden, meer bepaald een versnippering een een niet-efficiënte aanwending van aangekochte en ingezette middelen.

###### 5.2.2.2.5. Gebrekkige functionering

Er bestaan verschillende gebreken inzake functionering op niveau van de federale politie. Het belang van een goede afstemming tussen de reguliere onderzoeker en de CCU-onderzoeker tijdens het strafonderzoek is zeer groot; de reguliere onderzoeker moet weten wat hij kan verwachten van de CCU-diensten. Dit blijkt momenteel echter niet steeds het geval. Daarnaast bestaat er binnen de federale gerechtelijke politie momenteel geen uniform dossierbeheersysteem inzake de CCU-werking. Het ontbreekt dan ook aan eenvormigheid of standaardisatie wat het recherchemanagement betreft: elke CCU-eenheid van de federale gerechtelijke politie heeft zijn eigen methode om gegevens bij te houden en de CCU-werking op te volgen. Er bestaan geen algemene evaluatiemethodieken/toezichtsinstanties om verricht werk te beoordelen of controleren en eventueel bij te sturen. Een gelijkwaardige dienstverlening loopt dan ook gevaar.

Tot slot bestaat binnen de VCLP nog geen uitgewerkte visie inzake de CCU-werking, ondanks de enorme verschuiving van taken van de federale naar de lokale politie.

#### 5.2.2.3. Conclusie: risico’s voor de digitale bewijsvoering

De bestaande steunverlening volstaat duidelijk niet meer opdat door de geïntegreerde politie voldoende resultaten kunnen worden geboekt bij de uitvoering van het forensisch onderzoek in een geïnformatiseerde omgeving.

De verschillende genoemde risico’s vormen niet alleen een bedreiging voor een geïntegreerde werking en een gelijkwaardige en kwaliteitsvolle dienstverlening, maar daarnaast loopt ook de legaliteit van de bewijsvoering in het kader van het strafonderzoek gevaar. Meer bepaald worden de integriteit en authenticiteit van verzamelde data, evenals een correcte en transparante analyse erdoor bedreigd.

Om overal een kwaliteitsvolle bewijsvoering te kunnen garanderen, werd aan het Openbaar Ministerie daarom aanbevolen om zo snel mogelijk een uniform beleid te ontwikkelen.

## Kritische bedenkingen door rechtspractici

Naast de kritiekpunten die her en der reeds vermeld werden doorheen de bespreking van haar nieuwe maatregelen, is de Wet digitaal speurwerk in algemene zin vooral het voorwerp van kritiek omwille van het feit dat ze het evenwicht met de bescherming van de fundamentele rechten te veel uit het oog zou verliezen. Men denke vooral aan de het recht op een eerlijk proces en de privacyrechten, gewaarborgd door respectievelijk art. 6 en art. 8 EVRM.

CONINGS wijst op het feit dat de nieuwe, door de wet gehanteerde, onderscheidingscriteria niet relevant zijn: het criterium heimelijk/niet-heimelijk toont volgens haar geen verband met de al dan niet bestaande privacygevoeligheid. Ze herinnert aan de extreme privacygevoeligheid van de zoeking in een informaticasysteem, die volgens haar verder gaat dan een huiszoeking. In dit kader brengt ze de uitspraak van het US Supreme Court[[150]](#footnote-150) in herinnering, waarin het volgende werd gesteld: *“A cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form.”*

Bovendien zijn de onvolkomen plicht tot notificatie die op verschillende plaatsen in de wet vervat is, en de onzekere toekomstige jurisprudentiële invulling van de vage begrippen “redelijkerwijs” en “met passende technische middelen” volgens CONINGS en ROYER bronnen van rechtsonzekerheid en niet-afdoende rechtsbescherming.[[151]](#footnote-151)

Tevens wordt door velen gewezen op de onterechte verdere uitholling van de figuur van de onderzoeksrechter in de materie. De EHRM-rechtspraak vereist nochtans een (voorafgaande) rechterlijke machtiging vanaf het moment dat een indringende bevoegdheid wordt uitgeoefend (zie verder).[[152]](#footnote-152) Zo stelden de Ligue des Droits de l’Homme en haar tegenhanger, de Liga voor Mensenrechten, bij het Grondwettelijk Hof een beroep tot vernietiging in van de artt. 2 en 7 van de Wet digitaal speurwerk.[[153]](#footnote-153) Meer bepaald werd door beide vzw’s gepleit voor de tussenkomst van een onafhankelijke en onpartijdige rechter telkens wanneer een zoeking in een informaticasysteem wordt verricht. Daarnaast werd het nieuwe regime van infiltraties op het internet bekritiseerd, aangezien dit te weinig waarborgen en controlemechanismen biedt en daardoor te weinig bescherming wordt geboden aan zowel zij die moeten infiltreren als zij die het voorwerp uitmaken van dergelijke infiltraties.[[154]](#footnote-154)

Ten slotte heeft ook de Orde van Vlaamse Balies (hierna: Orde) ernstige bedenkingen bij de aanhoudende trend van overheveling van kernbevoegdheden naar het OM en de politie. Dergelijke overheveling gaat ten koste van de rechterlijke macht, en gebeurt zonder evenredige uitbreiding van de rechten van verdediging. De Orde dringt daarom aan op een betere grondrechtenbescherming voor alle betrokken personen. Ze haalt tevens aan dat een zoeking in een informaticasysteem volgens de EHRM-rechtspraak doelgericht moet gebeuren, hoewel zulke vereiste ontbreekt in art. 39bis Sv.[[155]](#footnote-155) Ten slotte pleit de Orde voor een wettelijk bepaalde nietigheidssanctie ingeval de regels omtrent de ingrijpende onderzoekshandelingen geschonden worden.

Deze kritische bedenkingen zullen in het derde deel uitgebreider geanalyseerd worden in het licht van EHRM-rechtspraak die in de materie relevant is.

# DEEL 2. RAAD VAN EUROPA

## Inleiding – EVRM en EHRM

Binnen de Raad van Europa, hoedster over de mensenrechten op het Europese continent, werd het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM) opgesteld.[[156]](#footnote-156) De meeste artikels van het EVRM hebben directe werking in de Belgische rechtsorde.[[157]](#footnote-157)

De Verdragsstaten zijn verplicht om ten aanzien van iedere persoon onder hun rechtsmacht de rechten en vrijheden van de eerste titel van het EVRM en de aanvullende protocollen, te verzekeren.[[158]](#footnote-158) Toezicht op de naleving van de verdragsbepalingen wordt door het Europees Hof voor de Rechten van de Mens (EHRM) voorzien.[[159]](#footnote-159)

De te verzekeren rechten en vrijheden zijn klassieke burgerlijke en politieke rechten.[[160]](#footnote-160) Ze zijn daarnaast bijna allemaal expliciet geformuleerd. Daarnaast bestaan echter ook bepaalde expliciete rechten waarvan de effectiviteit slechts gegarandeerd kan worden doordat er enkele inherente rechten aan gekoppeld worden. Het recht op een eerlijk proces is daarvan een goed voorbeeld (zie verder).

Het EHRM legt sinds enige tijd de verplichting op aan de Verdragsstaten om positieve inspanningen te leveren ter voorkoming van schendingen van het Verdrag[[161]](#footnote-161) en ter bescherming van het leven en welzijn van de personen onder hun jurisdictie.[[162]](#footnote-162) De Verdragsstaten dienen dus de nodige stappen te nemen om de betrokken rechten en vrijheden te vrijwaren.[[163]](#footnote-163) Zo dienen de Verdragsstaten er alles aan te doen om terroristische aanvallen te voorkomen. Een snelle bewijsgaring wordt daarom steeds belangrijker met het oog op een goede bescherming van de bevolking. De vraag stelt zich dan ook in welke mate er soepeler met de bewijsgaring omgegaan kan worden, gezien deze positieve verplichting.

## Standpunten Raad van Europa inzake maatregelen van terrorismebestrijding en recente initiatieven

### Raad van Europa en terrorismebestrijding: algemeen

Meermaals werd i.h.k.v. de Raad van Europa op het belang gewezen van de bescherming van mensenrechten in tijden van terrorisme.[[164]](#footnote-164)

Juridische initiatieven in de strijd tegen terrorisme zijn de laatste jaren vliegensvlug toegenomen, zowel op nationaal als op Europees vlak.[[165]](#footnote-165) Verscheidene wetgevers denken na over een modernisering van een “strafprocedure 2.0” als tegenhanger van het “web 2.0” die onze hedendaasge samenleving kenmerkt.[[166]](#footnote-166)

In eerste instantie wordt daarbij uiteraard erkend dat de terroristische aanslagen en dreigementen van de afgelopen jaren een directe aanval zijn op de fundamentele waarden van mensenrechten, democratie en rechtsstaat. Terrorisme heeft namelijk verwoestende gevolgen (gehad) voor het recht op leven, vrijheid en fysieke integriteit van onschuldige slachtoffers.[[167]](#footnote-167) Het EHRM brengt dan ook veel begrip op voor de specificiteit van de bestrijding van terrorisme en de daarmee samenhangende georganiseerde criminaliteit.

Wanneer het Hof zich uitspreekt over maatregelen in de strijd tegen het terrorisme, stelt het daarom zich bewust te zijn van de uitdagingen waarmee staten geconfronteerd worden. Dit wordt in verschillende van haar arresten[[168]](#footnote-168) bevestigd: *“The Court is acutely conscious of the difficulties faced by States in protecting their populations from terrorist violence.”*

Gezien de positieve verplichting van de Verdragsstaten om terroristische aanslagen te voorkomen of op zijn minst de daders efficiënt te vervolgen en streng te bestraffen, aanvaardt het Hof dat een Staat bepaalde grenzen stelt aan het genot van de mensenrechten.[[169]](#footnote-169) De druk op politieke verantwoordelijken, veiligheidshandhavers, politie en gerecht om bewijzen te verzamelen is namelijk zeer groot. Het EHRM aanvaardt principieel dat de strijd tegen het terrorisme één van de legitieme belangen is waardoor staten het genot van individuele rechten kunnen beperken.[[170]](#footnote-170) De legitimiteit van de strijd tegen het terrorisme als zodanig wordt dus niet door het Hof in twijfel getrokken.[[171]](#footnote-171)

Echter zijn de Verdragsstaten bij de uitvoering van hun verplichtingen ter bestrijding/voorkoming van het terrorisme niet vrijgesteld van de verplichting tot nakoming van hun parallelle verbintenissen tot bescherming van de grondrechten.[[172]](#footnote-172) Er wordt dan ook steeds gewezen op het belang van respect voor mensenrechten, dat volgens de algemene opvatting binnen de Raad in crisistijden van terrorisme belangrijker is dan ooit. Elke andere keuze zou de doelstellingen van terroristen namelijk begunstigen, en zou de fundamenten van onze democratische samenlevingen ondermijnen.

Ook werd er meermaals op gewezen dat de noodzaak om mensenrechten te respecteren geen belemmering dient te vormen voor de effectieve bestrijding van terrorisme; het stelt er hoogstens een grens aan. Door het Comité van Ministers wordt dan ook sinds enige tijd opgeroepen[[173]](#footnote-173) om beide vereisten te verzoenen: de samenleving verdedigen en de fundamentele rechten en vrijheden beschermen.

Samenvattend kan worden gesteld dat alle maatregelen die door staten worden genomen om terrorisme te bestrijden, de mensenrechten en het beginsel van de rechtsstaat moeten respecteren, met uitsluiting van elke vorm van willekeur, evenals elke vorm van discriminerende of racistische behandeling. Daarenboven moeten de maatregelen aan een passend toezicht worden onderworpen.

De basisinstrumenten van de Raad van Europa inzake terrorismebestrijding zijn het Verdrag van de Raad van Europa ter voorkoming van terrorisme[[174]](#footnote-174) en haar aanvullend Protocol.[[175]](#footnote-175)

### Recente initiatieven inzake terrorismebestrijding

#### Algemeen

Sinds 2018 werd het CODEXTER (Committee of Experts on Terrorism) opgevolgd door het CDCT, oftewel “Council of Europe Counter-Terrorism Committee”, dat de initiatieven van de Raad van Europa tegen het terrorisme coördineert. Zo richt het comité zich op de vraagstukken van terrorisme en het internet, maar ook op de materie van speciale onderzoekstechnieken.

Voor 2018 en 2019 zijn enkele hoofdprioriteiten het analyseren van de haalbaarheid van een pan-Europese wettelijke definitie van het begrip terrorisme, en het werken aan een Counter-Terrorismstrategie van de Raad van Europa voor de periode 2018-2022. Een andere hoofdprioriteit is de aanpak van het gebruik en misbruik van het internet door terroristen.

#### Aanbeveling speciale onderzoekstechnieken

Een nieuwe aanbeveling over speciale onderzoekstechnieken (hierna: SOT) met betrekking tot ernstige strafbare feiten, met inbegrip van terroristische daden, werd op 5 juli 2017 aangenomen.[[176]](#footnote-176) De aanbeveling behandelt de toepassing van SOT in een juridische context, inclusief ten behoeve van cyberonderzoeken.

De grote vooruitgang van computer- en internettechnologie, en de parallelle nieuwe mogelijkheden voor zowel criminelen als voor de rechtshandhaving, werden als de belangrijkste redenen gezien voor de introductie van deze nieuwe aanbeveling. Het gebruik van SOT kan namelijk een vitaal instrument zijn voor het voorkomen, onderdrukken en vervolgen van terreurdaden.

Evenwel wordt in de aanbeveling vooral herinnerd aan het belang van regulering van dergelijke technieken om de eerbiediging van de mensenrechten te waarborgen zowel voor verdachten als voor slachtoffers en derden. Speciale onderzoekstechnieken kenmerken zich namelijk doordat ze talrijk, gevarieerd en voortdurend in ontwikkeling zijn, maar ook door hun verborgen/geheime karakter en het feit dat hun toepassing de fundamentele rechten en vrijheden zou kunnen aantasten.

Aan de verschillende regeringen van de Verdragsstaten wordt daarom aanbeveeld om bij het formuleren van hun interne wetgeving, bij de herziening van hun strafrechtelijk beleid en bij het gebruik zelf van SOT, rekening te houden met de principes en maatregelen die in de aanbeveling naar voren geschoven worden.

Deze aanbeveling is natuurlijk niet bindend, maar toont wel aan welke randvoorwaarden noodzakelijk zijn om bijzondere opsporingstechnieken - zoals de nieuwe maatregelen door toedoen van de Wet digitaal speurwerk - op een legitieme manier toe te passen.

##### Speciale onderzoekstechnieken

In de aanbeveling worden speciale onderzoekstechnieken gedefinieerd als technieken die door de bevoegde autoriteiten worden toegepast in het kader van strafrechtelijk onderzoek met het oog op het voorkomen, opsporen, onderzoeken, vervolgen en onderdrukken van ernstige misdrijven, gericht op het verzamelen van informatie op een wijze die de betrokkene niet waarschuwt.

##### Cyberonderzoek

Een cyberonderzoek is volgens de aanbeveling gericht op het vervolgen en onderdrukken van ernstige delicten, met inbegrip van terreurdaden, alsmede elk strafbaar feit dat is vastgelegd in het Verdrag van de Raad van Europa ter voorkoming van terrorisme en haar aanvullend protocol gepleegd via internet en elke onwettige inmenging in informatie, computersystemen, computerprogramma's en gegevens, die opzettelijk zijn gepleegd met het doel ernstige misdaden te plegen; inclusief terreurdaden in het kader van strafrechtelijke onderzoeken.

##### Algemene principes

In de eerste plaats moeten de omstandigheden waarbinnen, en de voorwaarden waaronder, de bevoegde autoriteiten gemachtigd zijn gebruik te maken van SOT, bij wet voorzien en voldoende helder zijn. Nationale wetgeving moet adequate en effectieve garanties bieden tegen willekeurige en onrechtmatige praktijken, vooral met betrekking tot het recht op een eerlijk proces en het recht op eerbiediging van het privéleven.

Daarnaast dienen de wetgevende maatregelen met het oog op gebruik van SOT noodzakelijk te zijn in een democratische samenleving, en onmisbaar voor een efficiënt strafrechtelijk onderzoek en vervolging.

Ook wordt aan het belang herinnerd van een evaluatie van de SOT-toepassing door justitiële autoriteiten of andere bevoegde autoriteiten door middel van voorafgaande toestemming, toezicht tijdens het onderzoek of achteraf (post facto).

Tot slot dienen de Verdragsstaten te voorzien dat een persoon, beweerlijk slachtoffer van een inbreuk op zijn rechten als gevolg van het misbruik van SOT, toegang heeft tot een effectief rechtsmiddel (effective remedy) voor een bevoegde autoriteit.

##### Gebruiksvoorwaarden

De SOT mogen alleen worden aangewend als er voldoende redenen voorhanden zijn om aan te nemen dat een ernstig misdrijf is gepleegd of (wordt) voorbereid.Daarnaast dient evenredigheid te bestaan tussen de gebruikte SOT en de nagestreefde legitieme doelstellingen.

Tevens wordt de Verdragsstaten aanbevolen om passende wetgevende maatregelen te nemen om het produceren van bewijsmateriaal -verkregen door het wettige gebruik van SOT- voor de rechtbanken mogelijk te maken. Procedurevoorschriften die de productie en toelaatbaarheid van dergelijk bewijs regelen, waarborgen het recht van de beschuldigde op een eerlijk proces, geregeld door art. 6 EVRM.

Tot slot wordt herinnerd aan het belang van een adequate opleiding van de autoriteiten die belast zijn met de SOT. Een dergelijke opleiding moet de technische en operationele aspecten van SOT, de relevante strafrechtelijke procedurele wetgeving, en relevante mensenrechten omhelzen.

## Kwalificatie van de verschillende rechten en vrijheden

Overeenkomstig art. 15 EVRM (de “afwijkingsclausule”) kunnen de verschillende rechten en vrijheden van het EVRM en de bijhorende protocollen onderverdeeld worden in **notstandsfeste rechten en niet-notstandsfeste rechten**.

De niet-notstandsfeste rechten kunnen in geval van oorlog of een andere algemene noodtoestand tijdelijk of voorlopig opgeschort worden door de overheid. De Verdragsstaten hebben nochtans een ruime appreciatiemarge bij het bepalen of er sprake is van een noodtoestand en bij het vastleggen van de nodige maatregelen in dergelijk geval.[[177]](#footnote-177) Notstandsfeste rechten kunnen daarentegen nooit opgeschort worden. Deze rechten worden door art. 15, § 2 EVRM bepaald.[[178]](#footnote-178) Voorbeelden zijn het recht op leven en het verbod op foltering en onmenselijke of vernederende behandeling of bestraffing.[[179]](#footnote-179) Zo werd in *Trabelsi/België[[180]](#footnote-180)* m.b.t. de strijd tegen het terrorisme bevestigd dat het verbod op foltering absoluut is, en werd verklaard dat de positieve verplichting om de bevolking te beschermen het absolute karakter van art. 3 EVRM niet in twijfel kan trekken.

Daarnaast is het van belang de absolute van de relatieve rechten te onderscheiden.

Een absoluut recht is in principe niet onderworpen aan beperkingen of inmengingen. Er gebeurt in principe geen afweging van het verdragsrecht ten opzichte van andere verdragsrechten of belangen teneinde de juiste draagwijdte van het recht te bepalen. Uitzonderingen zijn mogelijk, maar enkel als ze zijn opgenomen bij de inhoudelijke omschrijving van de draag- of reikwijdte van het recht.[[181]](#footnote-181) Een relatief recht daarentegen kan in principe wél onderworpen worden aan beperkingen of inmengingen. Aangezien de bescherming van een ander belang of recht de toepassing ervan kan verhinderen, zal bescherming in een bepaalde situatie mogelijk niet van toepassing zijn.[[182]](#footnote-182) Een inmenging of beperking vereist wel steeds een afzonderlijke rechtvaardiging.[[183]](#footnote-183)

### Artikel 6 EVRM

Artikel 6 EVRM, dat het recht op een eerlijk proces regelt, valt onder de niet-notstandsfeste rechten. Met uitzondering van de deelbepaling over de openbaarheid van terechtzitting, dat relatief is, is het artikel tevens absoluut.[[184]](#footnote-184)

Art. 6 EVRM biedt de bescherming van het recht op een eerlijk proces in burgerlijke en strafrechtelijke procedures. Art. 6 EVRM bevat meerdere ‘samengestelde’ rechten, waarvan sommige uitdrukkelijk in het EVRM zijn opgenomen, en andere door het Hof als impliciet in de tekst worden erkend. Een expliciet vermeld recht is bijvoorbeeld het recht op een eerlijke en openbare hoorzitting binnen een redelijke termijn door een onafhankelijk en onpartijdig gerecht dat bij wet is ingesteld. Voorbeelden van impliciete/inherente rechten zijn het recht om te zwijgen en zichzelf niet te beschuldigen,[[185]](#footnote-185) en het recht op openbaarmaking van relevante bewijsstukken aan de verwerende strafprocespartij[[186]](#footnote-186).

Het belang van art. 6 EVRM voor de strafprocedure is groot, aangezien daarbinnen een evenwicht tussen de maatschappelijke finaliteit van die procedure enerzijds, en de individuele rechtsbescherming anderzijds, nagestreefd wordt.[[187]](#footnote-187) De maatschappelijke finaliteit van de strafprocedure wordt bereikt wanneer de strafwet effectief gehandhaafd wordt. Daarentegen vertrekt het aspect van de individuele rechtsbescherming vanuit de idee dat de burger in een rechtsstaat bescherming nodig heeft tegen overheidsmacht. Het is de overheid niet toegelaten om bij de waarheidsvinding (disproportionele) inbreuken te maken op fundamentele rechten van de burgers, zoals het recht op het privéleven (art. 8 EVRM).[[188]](#footnote-188) Bovendien dienen de betrokkenen in de loop van de strafprocedure voldoende formele procedurele middelen ter beschikking te hebben, wat dan weer tot uiting komt in art. 6 EVRM.[[189]](#footnote-189)

De verschillende door art. 6 EVRM gewaarborgde rechten van verdediging moeten voorzien in de middelen en de mogelijkheden voor het actief en onderbouwd opbouwen en voeren van de verdediging. Het gaat onder andere om de onderling verweven rechten op wapengelijkheid,[[190]](#footnote-190) tegenspraak[[191]](#footnote-191) en interne openbaarheid.

**Het recht op wapengelijkheid**[[192]](#footnote-192)betreft de mogelijkheid tot het aanbrengen van een stelling, inclusief een verdediging, in omstandigheden die niet minder nadelig zijn dan deze van de tegenpartij in de procedure. Deze procedurele gelijkheid draagt ​​bij tot het bereiken van een correcte uitkomst van het onderzoek.[[193]](#footnote-193)

Ook de verplichting om een ​​**tegensprekelijk debat** te respecteren, neemt een prominente plaats in in de organisatie en in het voeren van een eerlijk proces. Het behartigt de belangen van de partijen voor zover het hun de mogelijkheid biedt om hun respectieve standpunten te laten gelden. Het behartigt ook de belangen van een goede rechtsbedeling.[[194]](#footnote-194) De loyauteit van de procedure wordt in essentie geconcretiseerd door het recht op een tegensprekelijke procedure.[[195]](#footnote-195)

**Het recht op interne openbaarheid** ten slotte[[196]](#footnote-196) waarborgt de toegang van de procespartijen tot de relevante (dossier)gegevens voor de behandeling van de zaak. Meer bepaald geldt de noodzaak van betrouwbaarheid van het strafdossier enerzijds, en de toegang ertoe anderzijds.[[197]](#footnote-197) Alle aspecten van het onderzoek moeten dan ook op een volledige en correcte manier in het strafdossier worden opgenomen; ook informatie met betrekking tot de bewijswaardering van de in het dossier vervatte elementen.[[198]](#footnote-198) Het Hof hanteert als uitgangspunt[[199]](#footnote-199) de volledige interne openbaarheid.

### Artikel 8 EVRM

Artikel 8 EVRM, dat het recht op eerbiediging van privéleven, gezinsleven, woning en briefwisseling regelt, valt tevens onder de niet-notstandsfeste rechten. In tegenstelling tot (het grootste deel van) art. 6 EVRM, is het relatief.[[200]](#footnote-200)

Art. 8 EVRM primeert op de bepalingen van intern recht, en dus ook op art. 22 Gw., dat op Belgisch vlak het recht op het privéleven waarborgt. [[201]](#footnote-201)

#### Reikwijdte

Art. 8 EVRM is een open bepaling, en omhelst bijvoorbeeld ook het recht om met anderen relaties aan te gaan.[[202]](#footnote-202) Tot op heden werd de definitie van het recht op privacy bewust niet gegeven door het EHRM,[[203]](#footnote-203) en het Hof hanteert dan ook een zeer ruime invulling van het privacybegrip. De algemene formulering van art. 8 EVRM zorgt ervoor dat een soepele toepassing op nieuwe probleemgevallen wordt toegelaten en dat het begrip privéleven openstaat voor interpretatie. [[204]](#footnote-204)

Zo kan ook in de publieke sfeer bijvoorbeeld een beroep gedaan worden op de bescherming van art. 8 EVRM. Dit concept van publieke privacy werd principieel erkend in het arrest *Rotaru/Roemenië*.[[205]](#footnote-205)

Uiteraard neemt het belang van een degelijke privacybescherming exponentieel toe in een informatiemaatschappij als de onze.[[206]](#footnote-206) Private IT-systemen bevatten immers een enorme hoeveelheid private gegevens.[[207]](#footnote-207) Door het internet wordt toegelaten dat wereldwijd – en tegen relatief lage kosten - grote hoeveelheden informatie worden gedeeld.[[208]](#footnote-208) Vooral de gebruikers zelf zijn vandaag de drijvende kracht achter het internet: zij genereren namelijk een groot deel van de inhoud (de zgn. *user-generated content*).[[209]](#footnote-209) De bescherming van de integriteit van de gebruikte communicatietechnologie is dan ook steeds meer een fundamenteel aspect van de bescherming van het recht op privéleven (aan het worden). Zo heeft het Duitse Grondwettelijk Hof uit het algemeen persoonlijkheidsrecht een nieuw ICT-grondrecht afgeleid, nadat het geoordeeld had dat de bescherming van het privéleven onvoldoende weerwerk biedt tegen heimelijke intrusies van de overheid in informaticasystemen van de burger.[[210]](#footnote-210)

#### Beperkingen

Zoals ook bij art. 6 EVRM het geval is, wordt bij de toepassing van art. 8 EVRM een afweging gemaakt tussen de rechten van het individu en die van de gemeenschap.[[211]](#footnote-211) Telkens dient een evenwicht te worden gezocht tussen het individuele grondrecht op privacy en eventuele rechtmatige belangen van derden.[[212]](#footnote-212) Aangezien dit evenwicht in sterke mate gestuurd wordt door concrete omstandigheden, zal een precieze afweging steeds noodzakelijk zijn.[[213]](#footnote-213)

Meer bepaald moet een eventuele inmenging in het privéleven in het licht van de vereisten van de tweede paragraaf van art. 8 EVRM beoordeeld worden.[[214]](#footnote-214) Om in overeenstemming te zijn met art. 8(2) moet de beperking van het recht aan de drie aldaar vermelde voorwaarden[[215]](#footnote-215) voldoen:

1. Er moet een wettelijke basis voor de beperking zijn: wanneer de inbreuk niet steunt op of strijdig is met een nationale wet, leidt dit automatisch tot een schending van het EVRM (vereiste van legaliteit)
2. De beperking moet beantwoorden aan één van de doeleinden die in art. 8(2) vermeld zijn (vereiste van legitimiteit)
3. De beperking moet ten slotte noodzakelijk zijn in een democratische samenleving/in verhouding staan tot het nagestreede doel (vereiste van proportionaliteit).[[216]](#footnote-216)

De wettigheidsvereiste/legaliteitsvereiste houdt tevens in dat de Verdragsstaten zich dienen te baseren op een voldoende voorzienbare rechtsgrondslag. Staten mogen dus niet handelen op basis van wettelijke bepalingen die te vaag zijn.[[217]](#footnote-217) De zogenaamde kwaliteitscriteria stellen namelijk dat een inmenging slechts bij wet voorzien is indien ze voldoende toegankelijk is voor de rechtsonderhorige. Daarnaast dienen het toepassingsgebied en de inhoud van de norm voldoende precies te zijn, zodat de gevolgen ervan met redelijke voorspelbaarheid voorzienbaar (‘foreseeable’) zijn.

Dit is in het bijzonder van belang voor de zoeking.[[218]](#footnote-218) Een duidelijke gradatie blijkt uit de EHRM-rechtspraak: hoe ernstiger de inmenging in de privacy, hoe strenger het Hof is in zijn beoordeling van de kwaliteit van de rechtsgrond. De legaliteitsvoorwaarde zal dus streng geïnterpreteerd worden bij ernstige inbreuken op de privacy.[[219]](#footnote-219)

Wat betreft de toepassing van geheime dwangmiddelen zal het vaak zeer moeilijk zijn om een concrete inbreuk te bewijzen in het grondrecht van art. 8 EVRM. Daarom zal ook mestal niet meer resten dan een controle van de wetgeving in kwestie.[[220]](#footnote-220)

Door de evenredigheidstest/noodzakelijkheidstoets wordt verzekerd dat het belang dat de staat nastreeft, de inmenging in het betrokken individuele recht rechtvaardigt. Afhankelijk van het geval kan de strijd tegen het terrorisme daarom bepaalde beperkingen van individuele rechten perfect rechtvaardigen. Echter, de Verdragsstaten mogen in naam van de strijd tegen terrorisme niet zomaar elke maatregel nemen die zij passend achten.[[221]](#footnote-221) Het concrete resultaat zal afhangen van de beoordeling van alle omstandigheden van de zaak en de afweging van de verschillende betrokken belangen.[[222]](#footnote-222)

Hoe dan ook moet, telkens wanneer via de nationale bevoegdheden een inbreuk gemaakt wordt op basis van de tweede paragraaf van art. 8 EVRM, deze inbreuk eng worden geïnterpreteerd. Aangezien het EVRM normenhiërarchisch zo hoog staat aangeschreven, moeten de rechten van art. 8 EVRM in een afweging namelijk zwaar doorwegen.[[223]](#footnote-223)

Zo werd in het arrest *Klass*[[224]](#footnote-224) en het recentere *Szabó en Vissy*[[225]](#footnote-225) gesteld m.b.t. de tweede paragraaf van art. 8 EVRM: *“since it provides for an exception to a right guaranteed by the Convention, is to be* ***narrowly interpreted****.”*

in *Buck/Duitsland*[[226]](#footnote-226) wordt op een goede manier aangetoond op welke (strenge) manier het Hof een inmenging zal analyseren (eigen onderlijning):

“*§44. (…) the notion of “necessity” implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate**aim pursued. In determining whether an interference is “necessary in a democratic society”****,*** *the Court will take into account that a certain margin of appreciation is left to the Contracting States. However, the exceptions provided for in paragraph 2 of Article 8 are to be interpreted narrowly, and the need for them in a given case must be convincingly established”*

*“§45. As regards, in particular, searches of premises and seizures, the Court has consistently held that the Contracting States may consider it necessary to resort to such measures in order to obtain physical evidence of certain offences. The Court will assess whether the reasons adduced to justify such measures were relevant and sufficient and whether the aforementioned proportionality principle has been adhered to****.*** *As regards the latter point, the Court must first ensure that the relevant legislation and practice afford individuals adequate and effective safeguards against abuse. Secondly, the Court must consider the specific circumstances of each case in order to determine whether, in the particular case, the interference in question was proportionate to the aim pursued(…).”*

Dergelijke enge interpratie van een inbreuk geldt overigens in meer algemene zin voor alle artikelen van het EVRM die in een uitzondering voorzien: *“those paragraphs of Articles of the Convention which provide for an exception to a right guaranteed are to be narrowly interpreted”.* [[227]](#footnote-227)

# DEEL 3. Maatregelen Wet digitaal speurwerk in het licht van de artikelen 6 en 8 EVRM

Het EHRM heeft, geconfonteerd met rechtsgeschillen die een verband tonen met de strijd tegen het terrorisme, reeds in veel gevallen een schending van het Verdrag geconstateerd.[[228]](#footnote-228) Terrorisme is namelijk een terugkerend probleem waarmee het Hof sinds het begin van haar bestaan ​​te maken heeft: haar allereerste uitspraak ooit deed het in een terrorismezaak.[[229]](#footnote-229)

Doorheen de verschillende geschillen die de traditionele vrijheden van de artt. 8 tot en met 11 EVRM tot voorwerp hebben, heeft het Hof aangetoond veel belang te hechten aan de traditionele beginselen van haar jurisprudentie, ondanks de terroristische context.[[230]](#footnote-230) Het Hof weigert in dit verband het ‘valse dilemma van vrijheid of veiligheid’ te accepteren, en stuurt daarentegen de boodschap dat deze twee belangrijke waarden van onze democratische samenlevingen naast elkaar dienen te blijven bestaan.[[231]](#footnote-231)

In veel lidstaten van de Raad van Europa is de bestrijding van het terrorisme, zoals eerder vermeld, één van de hoofdpunten van het nationaal beleid geworden, met als gevolg dat verregaande wijzigingen in de desbetreffende regelgeving schering en inslag zijn geworden. Echter, maatregelen ter bestrijding van terrorisme kunnen tot een beperking van grondrechten van (beweerde) terreurverdachten leiden, waaronder het recht op privacy en het recht op een eerlijk proces. Daarom is het niet alleen nuttig, maar ook noodzakelijk om (via relevante case law van het EHRM) de huidige Belgische situatie inzake digitale bewijsgaring, en meerbepaald de methoden van internet- en informaticarecherche, te toetsen aan de artt. 6 en 8 EVRM.

Immers, bijzondere opsporingsmethoden en enige andere onderzoeksmethoden werden sinds het ontstaan van de wet in 2003 al vaker het voorwerp van commotie. Het toepassen van de methoden kan namelijk de fundamentele rechten en vrijheden aantasten.[[232]](#footnote-232)

## Artikel 8 EVRM

Autoriteiten moeten zich bij de bewijsgaring in het vooronderzoek onthouden van technieken in strijd met het recht op de bescherming van het privéleven. Veel onderzoekshandelingen kunnen namelijk een inbreuk uitmaken op art. 8 EVRM. Aangezien het om een gekwalificeerd recht gaat, maakt echter niet elk gebruik van bewijs verkregen in strijd met art. 8 EVRM automatisch een schendig uit van de rechten van verdediging.[[233]](#footnote-233) Bijna elke onderzoeksmaatregel raakt namelijk in meerdere of mindere mate het privéleven van de verdachte.[[234]](#footnote-234)

### Szabó en Vissy/Hongarije.

Het recente *Szabó en Vissy*[[235]](#footnote-235) geeft een duidelijk beeld van de eisen die het Hof stelt aan wetgeving die vergelijkbaar is met de Wet digitaal speurwerk. In casu betrof het Hongaarse wetgeving inzake geheime antiterreurbewaking, op grond waarvan de TEK (de Hongaarse antiterrorisme-eenheid) het recht kreeg om in het geheim huizen te doorzoeken en te bewaken (surveilleren), post en pakjes te controleren, elektronische communicatie en gegevensoverdrachten van computers te volgen en opnamen te maken van alle gegevens die met behulp van deze methoden werden verkregen.

Het Hof besloot in casu dat de wetgeving in kwestie art. 8 EVRM schond.

#### Rechterlijke controle

Vooral relevant is de herbevestiging van het belang dat door het Hof gehecht wordt aan een *a priori controle door een rechter-magistraat* bij een zoeking of een andere aanzienlijke inmenging in de persoonlijke levenssfeer.[[236]](#footnote-236) Indien een dergelijke inmenging zonder tussenkomst van een rechter wordt verricht, dient de procedure die de inmenging vormgeeft minstens voldoende waarborgen te bevatten om misbruiken te voorkomen.[[237]](#footnote-237)

De wetgeving bevatte geen dergelijke vereiste van voorafgaande rechterlijke toestemming. Het Hof beklemtoonde dat, in gevallen van extreme spoedeisendheid, toezichtmaatregelen die vooraf door een niet-rechterlijke autoriteit waren toegestaan, onderworpen moeten worden aan een post factum rechterlijk toezicht.

Door de Wet digitaal speurwerk werd een verdere overheveling van kernbevoegdheden van de onderzoeksrechter naar het Openbaar Ministerie en de politie bewerkstelligd. Een steeds grotere discretionaire bevoegdheid wordt aan hen verleend om zonder voorafgaande instemming van een rechter informaticasystemen uit te lezen. Deze uitholling staat dan ook op gespannen voet met de eisen die het Hof stelt aan een rechterlijke machtiging telkens er sprake is van een indringende bevoegdheid in het privéleven.

Daarenboven blijkt in de Belgische praktijk de uitvoering van het forensisch onderzoek in een geïnformatiseerde omgeving -uitgevoerd door de politiediensten - onder druk te staan. De verschillende eerder besproken risico’s vormen niet alleen een bedreiging voor een geïntegreerde werking en een gelijkwaardige en kwaliteitsvolle dienstverlening, maar bedreigen daarnaast ook de legaliteit van de bewijsvoering in het kader van het strafonderzoek. Meer bepaald worden de integriteit en authenticiteit van verzamelde data, evenals een correcte en transparante analyse erdoor bedreigd.

#### Kennisgeving

In casu werd niet voorzien in enige vorm van *latere kennisgeving* van de surveillancemaatregelen aan de burgers die daaraan waren onderworpen. Het Hof liet in dat verband opmerken dat ze nochtans een grote waarde hecht aan een notificatie aan de onderworpen persoon.

Ook in de Wet digitaal speurwerk is er echter slechts sprake van een onvolkomen notificatieplicht.

### Weber en Saravia/Duitsland

De *Weber*-uitspraak[[238]](#footnote-238) toont aan dat het enkele bestaan van wetgeving die een systeem van geheim toezicht op communicatie mogelijk maakt, een dreiging inhoudt van toezicht voor iedereen op wie de wetgeving kan worden toegepast. Deze dreiging komt op zichzelf neer op een inbreuk op de uitoefening van de rechten van art. 8 EVRM. Daarbovenop is er sprake van een verdere afzonderlijke inmenging in de rechten op grond van art. 8 EVRM, indien onderschepte persoonsgegevens worden doorgegeven aan andere autoriteiten, en eventueel door hen gebruikt worden. Het Hof bevestigde in de zaak dan ook het belang van adequate en effectieve waarborgen tegen misbruik.

De uitspraak bevestigt daarnaast het belang van een regeling omtrent de vernietiging van persoonsgegevens die door toedoen van de monitoring verkregen waren. *In casu* bestond een aanvaardbare procedure.

Hoewel er in de Belgische context een gevaar bestaat in de combinatie en verwerking van persoonsgegevens die door de justitiële autoriteiten bij de opsporing en berechting van misdrijven in enorme hoeveelheden worden verzameld met het oog op een latere doorzoeking, voorziet art. 39bis Sv. niets omtrent het lot van (ir)relevante persoonsgegevens die in het strafdossier verzameld zijn. Zo heerst onduidelijkheid over hoe lang dergelijke gegevens na een definitieve uitspraak nog bewaard mogen blijven en wanneer ze eventueel dienen te worden vernietigd.

Ten slotte werd opnieuw het belang van een kennisgeving aan personen, onderworpen aan de inmengende maatregelen, aangetoond. *In casu* moest dit zo spoedig mogelijk worden gedaan; regels verhinderden dat de meldingsplicht werd omzeild, behalve in gevallen waarin de gegevens binnen drie maanden werden vernietigd zonder ooit te zijn gebruikt.

### P.G. en J.H./Verenigd Koninkrijk

Door de zaak *P.G. en J.H.*[[239]](#footnote-239) oordeelde het Hof dat er een interactiezone van een persoon met anderen is, zelfs in een openbare context, die binnen de reikwijdte van het privéleven kan vallen. Ook in de publieke sfeer kan dus een beroep gedaan worden op de bescherming van art. 8 EVRM. Dit concept van publieke privacy werd echter reeds eerder principieel erkend in het arrest *Rotaru/Roemenië*.[[240]](#footnote-240)

In de Belgische context staat dit concept van publieke privacy dan ook op gespannen voet met de zeer uitgebreide digitale recherche die zich momenteel op het internet in haar breedste vorm afspeelt.

### Prezhdarovi/Bulgarije

Volgens deze uitspraak[[241]](#footnote-241) lijkt een zoeking in een informaticasysteem doelgericht te moeten gebeuren.

Zulke vereiste ontbreekt echter in art. 39bis Sv. van de Wet digitaal speurwerk. In de praktijk worden speurders heden vaak genoopt tot het digitaal in beslag nemen van gegevens of gegevensdragers om slechts naderhand een selectie van het strafrechtelijk relevante bewijsmateriaal door te voeren.[[242]](#footnote-242) Vandaag worden dus vandaag (te) grote hoeveelheden – en dus tevens irrelevante gegevens - in beslag genomen en doorzocht.[[243]](#footnote-243)

## Artikel 6 EVRM

Zowel bij de bewijsgaring als bij het gebruik van het bewijs moeten de rechten van verdediging van art. 6 EVRM gerespecteerd worden. De wijze van bewijsgaring, en het gebruik ervan, zullen beoordeeld worden in het licht van de procedure in haar geheel.[[244]](#footnote-244) In *Lee Davies*[[245]](#footnote-245) heeft het EHRM namelijk verklaard dat moet worden onderzocht of de procedure in haar geheel eerlijk is geweest.

Het EHRM hanteert dus de ‘holistische’ lezing[[246]](#footnote-246) van art. 6 EVRM, dat de zaak in haar geheel omvat.[[247]](#footnote-247)

Daarom bepaalt het EHRM dat de autoriteiten de rechten van verdediging van art. 6 EVRM ook moeten respecteren tijdens de fase van het onderzoek. Immers, bewijs dat vergaard werd tijdens het onderzoek, is zeer bepalend voor het verloop van de procedure ten gronde en een eventuele inbreuk in de onderzoeksfase kan een impact hebben op het vervolg van de procedure, die altijd eerlijk dient te zijn.[[248]](#footnote-248)

Er zal dus rekening moeten worden gehouden met de onderzoeksfase voor het beoordelen of de procedure in haar geheel de in art. 6 EVRM vervatte rechten heeft gerespecteerd.[[249]](#footnote-249)

Speciale technieken met het oog op bewijsgaring zullen op zich geen inbreuk uitmaken op art. 6 EVRM; de rechter ten gronde zal echter wel dienen na te gaan of de toepassing ervan de rechten van de beklaagde niet heeft ondermijnd.[[250]](#footnote-250)

Zoals eerder vermeld, is het in deze holistische visie dan ook van uitermate belang dat de onderling verweven rechten op wapengelijkheid, tegenspraak en interne openbaarheid gegarandeerd worden. Echter worden deze rechten bedreigd door een gebrek aan waarborg van authenticiteit en integriteit van digitaal bewijsmateriaal. De grote onduidelijkheid die nog heerst over de manier waarop in het Belgische strafrecht de vertaling van digitale vaststellingen naar het niet-digitale dossier gebeurt, roept daarom bezorgdheid op.

In de strijd tegen het terrorisme wordt door het EHRM de waarborg van een onpartijdige en onafhankelijke instantie die de maatregelen controleert duidelijk naar voren geschoven. De controle dient te gebeuren door een onafhankelijke magistraat die niet verbonden was aan het onderzoek.[[251]](#footnote-251) Ook deze waarborg ontbreekt momenteel grotendeels in de Belgische Wet digitaal speurwerk.

## Gebruik van (digitaal) bewijs verkregen in strijd met artt. 6 en 8 EVRM

Ten slotte is het nog nuttig om de wettelijk verankerde Antigoonrechtspraak van het Hof van Cassatie aan te halen. Deze bepaalt dat onrechtmatig verkregen bewijs enkel nog in drie hypothesen buiten beschouwing gelaten wordt, meer bepaald

1. wanneer de geschonden regel is voorgeschreven op straffe van nietigheid
2. wanneer door de schending de betrouwbaarheid van het bewijs is aangetast – dit is essentieel in de materie, meer bepaald omdat de authenticiteit en integriteit van in beslag genomen digitaal bewijsmateriaal aangetast kunnen zijn.
3. wanneer de rechten van verdediging werden geschonden – dit is logisch aangezien art. 6 EVRM directe werking heeft. Ook dit is essentieel in de materie. Door het Hof van Cassatie werd bovendien verduidelijkt dat de rechter de elementen van de zaak in haar geheel in overweging mag nemen.[[252]](#footnote-252)

Hieruit wordt afgeleid dat de schending van het recht op respect voor de privacy niet automatisch tot een uitsluiting van het verkregen bewijsmateriaal leidt.[[253]](#footnote-253) Het EHRM heeft er herhaaldelijk op gewezen dat bewijsmateriaal dat is verzameld *"in strijd met het recht op eerbiediging van het privéleven niet noodzakelijk onverenigbaar is met het recht op een eerlijk proces"*.[[254]](#footnote-254) De rechtspraak is dus eerder geneigd om het in strijd met het recht op privacy verzamelde bewijsmateriaal ontvankelijk te verklaren.[[255]](#footnote-255)

Wel geeft het Hof aan dat bewijs verkregen met een inbreuk op art. 8 enkel toelaatbaar is in zoverre het recht op een eerlijk proces, in het bijzonder de rechten van verdediging, erdoor niet geschonden worden of de betrouwbaarheid van het bewijs niet aangetast wordt. Daar wordt de vereiste (rechterlijke) controle vooropgesteld.[[256]](#footnote-256)

Art. 6 EVRM is dus van groot belang voor de fase van het onderzoek, voor zowel de bewijsgaring als de bewijsuitsluiting.[[257]](#footnote-257)

#  CONCLUSIE

Mede onder impuls van recente terreuraanslagen in België en Europa kwam er een uitbreiding van de BOM-bevoegdheden. Hierdoor kregen de politie en het Openbaar Ministerie uitgebreide bevoegdheden om zelfs zonder toestemming binnen te dringen in het digitale leven van verdachten zonder evenwel een evenredige uitbreiding van de rechten van verdediging. Door toedoen van deze nieuwe bevoegdheden stoot men vaak op uiterst intieme en privacygevoelige informatie.

Bijna iedereen beschikt tegenwoordig over een smartphone of een computer en maakt gebruik van sociale media. Vaak worden diezelfde informaticasystemen bovendien door verschillende personen gebruikt. De politie die op eigen houtje informaticasystemen in beslag neemt en uitleest krijgt dan ook toegang tot diverse persoonlijke gegevens die niet enkel de verdachte gebruiker maar ook derden betreffen. Deze laatsten zullen zich vaak niet bewust zijn van de “collateral damage” die hun privacy oploopt.

De onlogische en incoherente regeling van de wet, waarbij het al dan niet in beslag nemen van een informaticasysteem bepaalt of de politie of het Openbaar Ministerie het initiatief kan nemen voor de uitlezing van de gegevens, is niet van aard om een duidelijke wettelijk kader te creëren. Het Europees Hof voor de Rechten van de Mens vereist nochtans een wettelijk voorzienbaar kader.

In de nieuwe Wet digitaal speurwerk wordt bovendien nergens expliciet vermeld dat de zoeking doelgericht moet gebeuren waardoor er mogelijk geen enkele rem staat op de ijver van de speurders die enorme hoeveelheden informatie uitpluizen ongeacht de relevantie voor het onderzoek. Ook dit is in weerwil van het EHRM dat een doelgerichte zoeking in informaticasystemen lijkt te vereisen. Daarnaast lijkt de wet niet tegemoet te komen aan de eis van het Hof om steeds een (voorafgaande) rechterlijke machtiging te voorzien bij een indringende bevoegdheid.

Een recent onderzoeksrapport van het Vast Comité van toezicht op de politiediensten toonde bovendien aan dat de digitale recherche in handen is van diverse politiediensten die tot op heden zo goed als niet beschikken over duidelijk afgelijnde en geprofileerde vaardigheden, taakstelling en kunde in de materie. Daarom kan men zich uiteraard vragen stellen bij de te waarborgen integriteit in dit soort onderzoeken. In een materie waar de discretionaire marge van de onderzoekers ruim is, is dit onrustwekkend. Authenticiteit en integriteit van digitaal bewijsmateriaal lopen dan ook gevaar.

Verder valt het te betreuren dat in de Wet digitaal speurwerk zelf geen periodiek evaluatiemechanisme door een onpartijdige instantie werd ingeschreven. Dit zou zeker nuttig zijn om desgevallend de wet zo snel mogelijk bij te sturen bij eventuele misbruiken.

Ten slotte zijn loutere wetsaanpassingen alleen niet zaligmakend. Een wet op zich is immers geen garantie voor een behoorlijk beleid. In deze delicatie, privacygebonden materie is het dan ook belangrijk om de actoren van Justitie een duidelijk deontologisch kader bij te brengen dat de verregaande bevoegdheden die zij krijgen afbakent. Opleiding en vorming zullen dus ook een cruciale rol moeten spelen in dit domein.

1. P. DE HERT, K. WEIS, J. VAN CAENEGHEM en M. HOLVOET, *Handboek internationaal en Europees strafrecht*, Antwerpen, Intersentia, 2014, 434. [↑](#footnote-ref-1)
2. Art. 8 Wet 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, *BS* 18 december 1998, 40.312. [↑](#footnote-ref-2)
3. Art. 137 Sw. [↑](#footnote-ref-3)
4. MvT bij het wetsontwerp 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, *Parl.St*. Kamer 2015-16, nr. 54K1966/001, 8. (hierna: ‘wetsontwerp wet 25 december 2016’). [↑](#footnote-ref-4)
5. B. DE RUYVER, “Bestuurlijke handhaving van radicalisme, gewelddadig extremisme en terrorisme” in P. TRAEST, A. VERHAGE en G. VERMEULEN (eds.), *Strafrecht en strafprocesrecht: doel of middel in een veranderende samenleving?*, Mechelen, Kluwer, 2017, 649. [↑](#footnote-ref-5)
6. R. VERSTRAETEN, *Handboek strafvordering*, Antwerpen, Maklu, 2012, 245. [↑](#footnote-ref-6)
7. Kadernota Intergrale Veiligheid 2016-2019, <https://www.politie.be/5998/nl/over-ons/geintegreerde-politie/het-nationaal-veiligheidsplan>. [↑](#footnote-ref-7)
8. Wet 28 november 2000 inzake informaticacriminaliteit, *BS* 3 februari 2001, 2909. [↑](#footnote-ref-8)
9. Art. 39bis Sv., art. 88ter Sv. en art. 88quater Sv. samen met een aanpassing van de artt. 90ter en 90quater Sv. [↑](#footnote-ref-9)
10. MvT bij het wetsontwerp wet 25 december 2016, *Parl.St*. Kamer 2015-16, nr. 54K1966/001, 5. [↑](#footnote-ref-10)
11. Verdrag van de Raad van Europa inzake informaticacriminaliteit van 23 november 2001, *ETS*, nr. 185. [↑](#footnote-ref-11)
12. P. Van Linthout en J. Kerkhofs, “Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel’’, *T. Strafr*. 2008, 79. [↑](#footnote-ref-12)
13. MvT bij het wetsontwerp wet 25 december 2016, *Parl.St*. Kamer 2015-16, nr. 54K1966/001, 6. [↑](#footnote-ref-13)
14. Wet 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *BS* 12 mei 2003, 25351. [↑](#footnote-ref-14)
15. MvT bij het wetsontwerp wet 25 december 2016, *Parl.St*. Kamer 2015-16, nr. 54K1966/001, 4. [↑](#footnote-ref-15)
16. Wet 27 december 2005 houdende diverse wijzigingen van het Wetboek van strafvordering en van het Gerechtelijk Wetboek met het oog op de verbetering van de onderzoeksmethoden in de strijd tegen het terrorisme en de zware en georganiseerde criminaliteit, *BS* 30 december 2005, 57397. [↑](#footnote-ref-16)
17. GwH 21 december 2004, nr. 202/2004. [↑](#footnote-ref-17)
18. GwH 19 juli 2007, nr. 105/2007. [↑](#footnote-ref-18)
19. F. Schuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in Verhage, a. en Vermeulen, G. (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 15. [↑](#footnote-ref-19)
20. F. Schuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in Verhage, a. en Vermeulen, G. (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 15. [↑](#footnote-ref-20)
21. Wet 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en openen van privé-communicatie en –telecommunicatie, *BS* 24 januari 1995, 1542. [↑](#footnote-ref-21)
22. MvT bij het wetsontwerp wet 25 december 2016, *Parl.St*. Kamer 2015-16, nr. 54K1966/001, 6. [↑](#footnote-ref-22)
23. P. Van Linthout en J. Kerkhofs, J., “Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel’’, *T. Strafr*. 2008, 79. [↑](#footnote-ref-23)
24. MvT bij het wetsontwerp wet 25 december 2016, *Parl.St*. Kamer 2015-16, nr. 54K1966/001, 7. [↑](#footnote-ref-24)
25. MvT bij het wetsontwerp wet 25 december 2016, *Parl.St*. Kamer 2015-16, nr. 54K1966/001, 7. [↑](#footnote-ref-25)
26. MvT bij het wetsontwerp wet 25 december 2016, *Parl.St*. Kamer 2015-16, nr. 54K1966/001, 7. [↑](#footnote-ref-26)
27. MvT bij het wetsontwerp wet 25 december 2016, *Parl.St*. Kamer 2015-16, nr. 54K1966/001, 8. [↑](#footnote-ref-27)
28. C. Conings en S. Royer, “Verzamelen en vastleggen van digitaal bewijs in strafzaken’’, *NC* 2017, 338. [↑](#footnote-ref-28)
29. Het betreft de misdrijven valsheid in informatica (art. 210bis Sw.), informaticabedrog (art. 504quater Sw.) en hacking (art. 550bis Sw.) en informaticasabotage (art. 550ter Sw.). [↑](#footnote-ref-29)
30. J. Kerkhofs en P. Van Linthout, *Cybercrime*, Brussel, Politeia, 2013, 35. [↑](#footnote-ref-30)
31. COMITE P, *Tussentijds verslag 2018: De geïntegreerde politie en het forensisch onderzoek in een geïnformatiseerde omgeving*, <http://www.comitep.be/AdditionalReports/2018-06-21%20Forensisch%20onderzoek.pdf>. [↑](#footnote-ref-31)
32. COMITE P, *Tussentijds verslag 2018: De geïntegreerde politie en het forensisch onderzoek in een geïnformatiseerde omgeving*, <http://www.comitep.be/AdditionalReports/2018-06-21%20Forensisch%20onderzoek.pdf>. [↑](#footnote-ref-32)
33. J. STEVENSON, *All you need to know about Darkweb – How to access and what to look out for*, London, John Stevenson, 24. [↑](#footnote-ref-33)
34. C. SENKER, *Cybercrime & the Dark Net: Revealing the hidden underworld of the internet*, Londen, Arcturus Publishing, 2016, 3. [↑](#footnote-ref-34)
35. J. Kerkhofs en P. Van Linthout, *Cybercrime*, Brussel, Politeia, 2013, 181. [↑](#footnote-ref-35)
36. Art. 26 Wet 5 augustus 1992 op het politieambt, *BS* 22 december 1992, 27.124. [↑](#footnote-ref-36)
37. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 21. [↑](#footnote-ref-37)
38. J. Kerkhofs en P. Van Linthout, *Cybercrime*, Brussel, Politeia, 2013, 220. [↑](#footnote-ref-38)
39. Cass. 28 maart 2017, AR P.16.1245.N. [↑](#footnote-ref-39)
40. Cass. 9 september 2008, AR P.08.0276.N. [↑](#footnote-ref-40)
41. A. MICHEL, “L’utilisation des contenus postés sur les réseaux sociaux comme éléments de preuve d’un dommage”, *RDTI* 2016, afl. 4, 106. [↑](#footnote-ref-41)
42. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 24. [↑](#footnote-ref-42)
43. EHRM 2 september 2010, nr. 35623/05, Uzun/Duitsland, § 43. In de zaak wordt geen uitspraak gedaan over het surveilleren op het internet, maar gaat het over het gebruik van een GPS om de verplaatsingen, in publieke ruimte, van een persoon onder systematisch toezicht te kunnen stellen; in dat arrest wordt tevens naar verschillende eerdere uitspraken verwezen. [↑](#footnote-ref-43)
44. J. Kerkhofs en P. Van Linthout, *Cybercrime*, Brussel, Politeia, 2013, 219. [↑](#footnote-ref-44)
45. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 21. [↑](#footnote-ref-45)
46. Sinds 25 mei 2018: Gegevensbeschermingsautoriteit [↑](#footnote-ref-46)
47. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 21. [↑](#footnote-ref-47)
48. COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER (CBPL), Advies over 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, 13 mei 2015, nr. 13/2015, <https://www.privacycommission.be/sites/privacycommission/files/documents/advies_13_2015.pdf>. [↑](#footnote-ref-48)
49. J. Kerkhofs en P. Van Linthout, *Cybercrime*, Brussel, Politeia, 2013, 232. [↑](#footnote-ref-49)
50. Art. 30 V.T. Sv. [↑](#footnote-ref-50)
51. F. DERUYCK, *Overzicht van het Belgisch strafprocesrecht*, Brugge, Die Keure, 2017, 101. [↑](#footnote-ref-51)
52. *Vr. en Antw*. Kamer, 27 juni 2017, nr. 54/127, 2314 (Vr. nr. 1 en 2 K. JADIN). [↑](#footnote-ref-52)
53. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 24. [↑](#footnote-ref-53)
54. Art. 46sexies, § 1, derde lid Sv. [↑](#footnote-ref-54)
55. F. DERUYCK, *Overzicht van het Belgisch strafprocesrecht*, Brugge, Die Keure, 2017, 106. [↑](#footnote-ref-55)
56. Art. 46sexies, § 2 Sv. [↑](#footnote-ref-56)
57. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 26. [↑](#footnote-ref-57)
58. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 27. [↑](#footnote-ref-58)
59. *Ibid.* [↑](#footnote-ref-59)
60. Art. 46sexies, § 4, tweede lid Sv. [↑](#footnote-ref-60)
61. MvT bij het wetsontwerp wet 25 december 2016, *Parl.St*. Kamer 2015-16, nr. 54K1966/001, 9. [↑](#footnote-ref-61)
62. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 28. [↑](#footnote-ref-62)
63. Art. 28bis, § 3, eerste lid Sv. [↑](#footnote-ref-63)
64. Art. 55 Sv. [↑](#footnote-ref-64)
65. R. VERSTRAETEN, *Handboek strafvordering*, Antwerpen, Maklu, 2012, 279. [↑](#footnote-ref-65)
66. Art. 28ter, § 3 Sv. [↑](#footnote-ref-66)
67. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 20. [↑](#footnote-ref-67)
68. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 21. [↑](#footnote-ref-68)
69. MvT, *Parl. St.* Kamer 1999-2000, nr. 50K0213/001, 12. [↑](#footnote-ref-69)
70. R. VERSTRAETEN en F. VERBRUGGEN, *Strafrecht en Strafprocesrecht voor bachelors*, I, Antwerpen, Maklu, 2017, 194. [↑](#footnote-ref-70)
71. C. CONINGS en S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken”, *NC* 2017, 313. [↑](#footnote-ref-71)
72. Art. 39bis, § 2, derde lid Sv. [↑](#footnote-ref-72)
73. Art. 39bis, § 2, eerste lid Sv. [↑](#footnote-ref-73)
74. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 16. [↑](#footnote-ref-74)
75. R. VERSTRAETEN en F. VERBRUGGEN, *Strafrecht en Strafprocesrecht voor bachelors*, I, Antwerpen, Maklu, 2017, 194. [↑](#footnote-ref-75)
76. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 16. [↑](#footnote-ref-76)
77. *Ibid.* [↑](#footnote-ref-77)
78. Art. 39bis, § 2, tweede lid Sv. [↑](#footnote-ref-78)
79. C. FORGET, “Les nouvelles méthodes d’enquête dans hun contexte informatique: vers un encadrement (plus) strict?”, *RDTI* 2017, afl. 1-2, 31. [↑](#footnote-ref-79)
80. C. CONINGS en S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken”, *NC* 2017, 314. [↑](#footnote-ref-80)
81. Art. 39bis, § 2, derde lid Sv. [↑](#footnote-ref-81)
82. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 18. [↑](#footnote-ref-82)
83. C. FORGET, “Les nouvelles méthodes d’enquête dans hun contexte informatique: vers un encadrement (plus) strict?”, *RDTI* 2017, afl. 1-2, 36. [↑](#footnote-ref-83)
84. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 16. [↑](#footnote-ref-84)
85. *Ibid*., 18. [↑](#footnote-ref-85)
86. P. DE HERT en G. LICHTENSTEIN, “De betekenis van het Europees Verdrag Cybercriminaliteit voor het vooronderzoek en de internationale samenwerking”, *Vigiles: tijdschrift voor politierecht* 2004, 163. [↑](#footnote-ref-86)
87. Art. 39bis, § 3, eerste lid Sv. [↑](#footnote-ref-87)
88. C. CONINGS en S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken”, *NC* 2017, 314. [↑](#footnote-ref-88)
89. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 18. [↑](#footnote-ref-89)
90. C. CONINGS en S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken”, *NC* 2017, 315. [↑](#footnote-ref-90)
91. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 19. [↑](#footnote-ref-91)
92. Parl. St. *Kamer*, 2016-2017, 1966/001, 19-20. [↑](#footnote-ref-92)
93. C. CONINGS en S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken”, *NC* 2017, 315. [↑](#footnote-ref-93)
94. Art. 39bis, § 4, eerste lid Sv. [↑](#footnote-ref-94)
95. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 20. [↑](#footnote-ref-95)
96. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 20. [↑](#footnote-ref-96)
97. *Ibid.* [↑](#footnote-ref-97)
98. Art. 90ter Sv., waarin onder andere Boek II, Titel Iter Sw. (terrorisme) is opgenomen. [↑](#footnote-ref-98)
99. Art. 324bis Sw. [↑](#footnote-ref-99)
100. De inkijkoperate is dus slecht toegelaten indien de overige middelen van onderzoek niet lijken te volstaan om de waarheid aan het licht te brengen. [↑](#footnote-ref-100)
101. Deze voorwaarden worden in art. 46quinquies Sv. opgesomd. [↑](#footnote-ref-101)
102. C. CONINGS en S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken”, *NC* 2017, 317. [↑](#footnote-ref-102)
103. *Ibid.,* 318. [↑](#footnote-ref-103)
104. P. Van Linthout en J. Kerkhofs, “Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel’’, *T. Strafr*. 2008, 85. [↑](#footnote-ref-104)
105. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 30. [↑](#footnote-ref-105)
106. Art. 90ter, § 1 Sv. [↑](#footnote-ref-106)
107. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 30. [↑](#footnote-ref-107)
108. C. CONINGS en S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken”, *NC* 2017, 318. [↑](#footnote-ref-108)
109. *Ibid.* [↑](#footnote-ref-109)
110. Art. 90ter, § 1, eerste lid Sv. [↑](#footnote-ref-110)
111. Art. 90ter, § 1, vierde lid Sv. [↑](#footnote-ref-111)
112. C. CONINGS en S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken”, *NC* 2017, 318. [↑](#footnote-ref-112)
113. Art. 90ter, § 5 Sv. [↑](#footnote-ref-113)
114. F. SChuermans, “Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden” in A. Verhage en G. Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie*, Antwerpen, Maklu, 2017, 30. [↑](#footnote-ref-114)
115. C. CONINGS en S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken”, *NC* 2017, 328. [↑](#footnote-ref-115)
116. *Ibid*., 329. [↑](#footnote-ref-116)
117. MvT bij het wetsontwerp wet 25 december 2016, *Parl.St*. Kamer 2015-16, nr. 54K1966/001, 23. [↑](#footnote-ref-117)
118. J. Kerkhofs en P. Van Linthout, *Cybercrime*, Brussel, Politeia, 2013, 183. [↑](#footnote-ref-118)
119. *Ibid.*, 334. [↑](#footnote-ref-119)
120. *Ibid.,* 187. [↑](#footnote-ref-120)
121. *Ibid*., 188. [↑](#footnote-ref-121)
122. C. CONINGS en S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken”, *NC* 2017, 334. [↑](#footnote-ref-122)
123. J. Kerkhofs en P. Van Linthout, *Cybercrime*, Brussel, Politeia, 2013, 190. [↑](#footnote-ref-123)
124. C. CONINGS, *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Antwerpen, Intersentia, 2017, 128. [↑](#footnote-ref-124)
125. Deze notificatieplicht geldt ook ten aanzien van de persoon die onderworpen werd aan de maatregel van art. 90ter Sv. (werkelijke heimelijke doorzoeking van informaticasystemen). [↑](#footnote-ref-125)
126. C. CONINGS en S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken”, *NC* 2017, 320. [↑](#footnote-ref-126)
127. J. Kerkhofs en P. Van Linthout, *Cybercrime*, Brussel, Politeia, 2013, 267. [↑](#footnote-ref-127)
128. *Ibid*., 335. [↑](#footnote-ref-128)
129. *Ibid*., 176. [↑](#footnote-ref-129)
130. Art. 32 wet 17 april 1878 houdende de voorafgaande titel van het wetboek van strafvordering, *BS* 25 april 1878, 1.265. [↑](#footnote-ref-130)
131. Cass. 23 maart 2004, AR P.04.0012.N. [↑](#footnote-ref-131)
132. C. CONINGS en S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken”, *NC* 2017, 329. [↑](#footnote-ref-132)
133. *Ibid*., 334. [↑](#footnote-ref-133)
134. COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, Advies over de wetsontwerpen inzake informaticacriminaliteit, 13 december 1999, nr. 33/1999, [https://www.privacycommission.be/sites/privacycommission/files/documents/advies\_33\_1999\_0.pdf.)](https://www.privacycommission.be/sites/privacycommission/files/documents/advies_33_1999_0.pdf.%29) [↑](#footnote-ref-134)
135. Cass. 22 januari 2015, AR C.13.0532.F. [↑](#footnote-ref-135)
136. Wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *BS* 18 maart 1993, 5.801 [↑](#footnote-ref-136)
137. C. CONINGS en S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken”, *NC* 2017, 337. [↑](#footnote-ref-137)
138. *Vr. en Antw*. Kamer, 27 juni 2017, nr. 54/127, 2314 (Vr. nr. 1 en 2 K. JADIN). [↑](#footnote-ref-138)
139. *Vr. en Antw*. Kamer, 11 juli 2016, nr. 54/86, 1532 (Vr. nr. 1 en 2 F. DEMON). [↑](#footnote-ref-139)
140. *Vr. en Antw.* Kamer, 8 november 2017, nr. 54/140, 2716 (Vr. nr.1 V. SCOURNEAU). [↑](#footnote-ref-140)
141. *Vr. en Antw.* Kamer, 8 oktober 2015, nr. 54/51, 699 (Vr. nr. 4 R. DESEYN). [↑](#footnote-ref-141)
142. Bron: [website Federale Politie](https://www.police.be/5998/nl/over-ons/centrale-directies/federal-computer-crime-unit) [↑](#footnote-ref-142)
143. L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, Orde dag 2010, 61. [↑](#footnote-ref-143)
144. Bron: [website Federale Politie](https://www.police.be/5998/nl/over-ons/centrale-directies/federal-computer-crime-unit) [↑](#footnote-ref-144)
145. COMITE P, Tussentijds verslag 2018: De geïntegreerde politie en het forensisch onderzoek in een geïnformatiseerde omgeving, <http://www.comitep.be/AdditionalReports/2018-06-21%20Forensisch%20onderzoek.pdf>. [↑](#footnote-ref-145)
146. Art. 3 Wet 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, *BS* 5 januari 1999, 132. [↑](#footnote-ref-146)
147. KB 27 oktober 2015 tot vaststelling van de personeelsformatie van de federale politie, *BS* 30 oktober 2015, 66.439. FTE’s zijn voltijdse werknemers. [↑](#footnote-ref-147)
148. Het behoud van de bewijsketen. Deze geeft aan welke personen opeenvolgend gedurende het onderzoek in aanraking zijn geweest met de data, welke handelingen ze daarbij eventueel hebben gesteld en met welke middelen. [↑](#footnote-ref-148)
149. Federale Gerechtelijke Politie, Eindrapport van de werkgroep ‘Samenwerking tussen de federale en de lokale politie in kader van forensische analyse in IT’, 15 oktober 2017, 6. [↑](#footnote-ref-149)
150. US Supreme Court 25 juni 2014, Riley/California. [↑](#footnote-ref-150)
151. C. CONINGS en S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken”, *NC* 2017, 312. [↑](#footnote-ref-151)
152. EHRM 30 maart 1989, Ian Chappell/Verenigd Koninkrijk en EHRM 25 februari 1993, Miailhe/Frankrijk en EHRM 12 januari 2016, nr. 37138/14, Szabó en Vissy/Hongarije. [↑](#footnote-ref-152)
153. Ber. GwH voorgeschreven bij art. 74 van de bijzondere wet van 6 januari 1989, *BS* 4 september 2017, 81.975. [↑](#footnote-ref-153)
154. Liga, “De Liga voor Mensenrechten vecht BOM-wet aan bij Grondwettelijk Hof”, 2017, <https://mensenrechten.be/nieuwsberichten/de_liga_voor_mensenrechten_vecht_bom_wet_aan_bij_grondwettelijk_hof_om>. [↑](#footnote-ref-154)
155. EHRM 30 september 2014, nr. 8429/05, Prezhdarovi/Bulgarije. [↑](#footnote-ref-155)
156. Y. Haeck, *Procederen voor het Europees Hof voor de Rechten van de Mens.* Antwerpen, Intersentia, 2009, 1. [↑](#footnote-ref-156)
157. J. Vande Lanotte, J. en Y. Haeck, *Handboek EVRM*, I, Antwerpen, Intersentia, 2005, 95. [↑](#footnote-ref-157)
158. P. DE HERT, K. WEIS, J. VAN CAENEGHEM en M. HOLVOET, *Handboek internationaal en Europees strafrecht*, Antwerpen, Intersentia, 2014, 44. [↑](#footnote-ref-158)
159. *Ibid.* [↑](#footnote-ref-159)
160. J. Vande Lanotte, J. en Y. Haeck, *Handboek EVRM*, I, Antwerpen, Intersentia, 2005, 33. [↑](#footnote-ref-160)
161. B. RAINEY, *Human Rights Law Concentrate: Law Revision and Study Guide*, Oxford, Oxford University Press, 2017, 31. [↑](#footnote-ref-161)
162. EHRM 13 juni 1979, nr. 6833/74, Marckx/België, § 31 “*in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective "respect" for family life”* (Art. 8 (1) – right to respect for family life) en EHRM 28 oktober 1998, nr. 23452/94, Osman/Verenigd Koninkrijk, § 115: “*The Court notes that the first sentence of Article 2 § 1 enjoins the State not only to refrain from the intentional and unlawful taking of life, but also to take appropriate steps to safeguard the lives of those within its jurisdiction” (Article 2 – right to life)* [↑](#footnote-ref-162)
163. J. VANDE LANOTTE en Y. HAECK, *Handboek EVRM*, I, Antwerpen, Intersentia, 2005, 99 en recent: EHRM 13 april 2017, nr. 26562/07, Tagayeva e.a./Rusland, § 482: “*Turning to the question of positive obligation, the Court reiterates that Article 2 of the Convention may imply a positive obligation on the authorities to take preventive operational measures to protect an individual whose life is at risk from the criminal acts of another individual”.* [↑](#footnote-ref-163)
164. Council of Europe Guidelines on human rights and the fight against terrorism, Directorate General of Human Rights, March 2005, 72 p. [↑](#footnote-ref-164)
165. G. FOUREZ, “Chronique de criminologie. Victimes et terrorisme au XXIe siècle: une production spécifique”, *RDPC* 2018, afl. 4, 414. [↑](#footnote-ref-165)
166. V. FRANSSEN, “Droit pénal et numérique: vers un nouveau paradigme?”, *Rev.dr.ULg* 2018, afl. 1, 199. [↑](#footnote-ref-166)
167. J. VELAERS, “La lutte contre le terrorisme et les droits de l’homme: développements récents en Belgique” in P. D’ARGENT, D. RENDERS en M. VERDUSSEN (eds.), *Les visages de l’État. Liber Amicorum Yves Lejeune*, Brussel, Bruylant, 2017, 775. [↑](#footnote-ref-167)
168. Bijv. EHRM 3 december 2009, 19576/08, Daoudi/Frankrijk (§ 65) en EHRM 19 februari 2009, nr. 3455/05, A. en anderen/Verenigd Koninkrijk (§ 126). [↑](#footnote-ref-168)
169. J. VELAERS, “La lutte contre le terrorisme et les droits de l’homme: développements récents en Belgique” in P. D’ARGENT, D. RENDERS en M. VERDUSSEN (eds.), *Les visages de l’État. Liber Amicorum Yves Lejeune*, Brussel, Bruylant, 2017, 775. [↑](#footnote-ref-169)
170. EHRM 14 november 1960, nr. 332/57, Lawless/Ierland (§ 23-30). [↑](#footnote-ref-170)
171. F. Bernard, “La Cour européenne des droits de l’homme et la lutte contre le terrorisme’’, *RTDH* 2016, 54. [↑](#footnote-ref-171)
172. J. VELAERS, “La lutte contre le terrorisme et les droits de l’homme: développements récents en Belgique” in P. D’ARGENT, D. RENDERS en M. VERDUSSEN (eds.), *Les visages de l’État. Liber Amicorum Yves Lejeune*, Brussel, Bruylant, 2017, 776. [↑](#footnote-ref-172)
173. *Guidelines on human rights and the fight against terrorism* adopted on 11 July 2002 en *Guidelines on the protection of victims of terrorist acts* on 2 March 2005 (revised guidelines adopted on 19 May 2017). [↑](#footnote-ref-173)
174. Verdrag van de Raad van Europa ter voorkoming van terrorisme van 16 mei 2005, *CETS*, nr. 196. [↑](#footnote-ref-174)
175. Aanvullend Prot. bij het Verdrag van de Raad van Europa ter voorkoming van terrorisme van 22 oktober 2015, *CETS*, nr. 217. [↑](#footnote-ref-175)
176. Aanbev. CM/Rec(2017)6 van het Comité van Ministers aan de lidstaten over “speciale onderzoekstechnieken” met betrekking tot ernstige strafbare feiten, met inbegrip van terroristische daden. [↑](#footnote-ref-176)
177. J. Vande Lanotte en Y. Haeck, *Handboek EVRM*, I, Antwerpen, Intersentia, 2005, 91. [↑](#footnote-ref-177)
178. *Ibid*., 92. [↑](#footnote-ref-178)
179. Council of Europe Factsheet “Derogation in time of emergency”, april 2018, <https://www.echr.coe.int/Pages/home.aspx?p=press/factsheets&c#n1347890855564_pointer>. [↑](#footnote-ref-179)
180. EHRM 4 september 2014, nr. 140/10, Trabelsi/België. [↑](#footnote-ref-180)
181. J. Vande Lanotte en Y. Haeck, *Handboek EVRM*, I, Antwerpen, Intersentia, 2005, 92. [↑](#footnote-ref-181)
182. *Ibid*. [↑](#footnote-ref-182)
183. *Ibid*., 93. [↑](#footnote-ref-183)
184. J. VANDE LANOTTE en Y. HAECK, *Handboek EVRM*, II, Antwerpen, Intersentia, 2005, 646. [↑](#footnote-ref-184)
185. R. GOSS, *Criminal Fair Trial Rights: Article 6 of the European Convention on Human Rights*, Londen, Bloomsbury Publishing, 2014, 1. [↑](#footnote-ref-185)
186. EHRM 16 februari 2000, Rowe en Davis/Verenigd Koninkrijk, § 60 en EHRM 24 juli 2003, Dowsett/Verenigd Koninkrijk, § 41. [↑](#footnote-ref-186)
187. J. HUYSMANS, *Legitieme verdediging. Gebruik en misbruik van de procedurele rechten door de verdediging in strafzaken*, Antwerpen, Intersentia, 2017, 747. [↑](#footnote-ref-187)
188. *Ibid*., 748. [↑](#footnote-ref-188)
189. *Ibid.*, 749. [↑](#footnote-ref-189)
190. Bijv. EHRM nr. 16913/04, 19 juli 2011, Jelcovas/Letland, § 106. [↑](#footnote-ref-190)
191. Bijv. EHRM 8 augustus 2006, nr. 43803/98, Eskelinen e.a./Finland, § 31. [↑](#footnote-ref-191)
192. T. DECAIGNY, *Tegenspraak in het vooronderzoek. Een onderzoek naar de meerwaarde van een vroege participatie van de verdachte in de Belgische strafprocedure*, Antwerpen, Intersentia, 2013, 98. [↑](#footnote-ref-192)
193. O. SIDHU, *The Concept of Equality of Arms in Criminal Proceedings under Article 6 of the European Convention on Human Rights*, Antwerpen, Intersentia, 2017, 63, 75. [↑](#footnote-ref-193)
194. P. GILLIAUX, *Droit(s) européen(s) à un procès équitable*, Brussel, Bruylant, 2012, 574. [↑](#footnote-ref-194)
195. *Ibid*, 573. [↑](#footnote-ref-195)
196. T. DECAIGNY, *Tegenspraak in het vooronderzoek. Een onderzoek naar de meerwaarde van een vroege participatie van de verdachte in de Belgische strafprocedure*, Antwerpen, Intersentia, 2013*.,* 153. [↑](#footnote-ref-196)
197. *Ibid.,* 117. [↑](#footnote-ref-197)
198. *Ibid.*, 207. [↑](#footnote-ref-198)
199. EHRM 16 december 1992, Edwards/Verenigd Koninkrijk, § 36. [↑](#footnote-ref-199)
200. J. VANDE LANOTTE en Y. HAECK, *Handboek EVRM*, II, Antwerpen, Intersentia, 2005, 646 en 782. [↑](#footnote-ref-200)
201. P. DE HERT, “Artikel 8. Recht op privacy” in J. VANDE LANOTTE en Y. HAECK (eds.), *Handboek EVRM,* II*,* Antwerpen, Intersentia, 2004, 710. [↑](#footnote-ref-201)
202. P. DE HERT, “Artikel 8. Recht op privacy” in J. VANDE LANOTTE en Y. HAECK (eds.), *Handboek EVRM,* II*,* Antwerpen, Intersentia, 2004, 722. [↑](#footnote-ref-202)
203. P. DE HERT, J. NOUWT, I. VOETS en J. VAN DER WEES, “Sms, opsporing en privacy”, *Computerr.* 2008, 155. [↑](#footnote-ref-203)
204. A. W. HERINGA en L. ZWAAK, “Right to respect for privacy (Article 8)” in P. VAN DIJK, F. VAN HOOF, A. VAN RIJN en L. ZWAAK (eds.), *Theory and Practice of the European Convention on Human Rights*, Antwerpen, Intersentia, 2006, 664. [↑](#footnote-ref-204)
205. EHRM 4 mei 2000, nr. 28341/95, Rotaru/Roemenië en P. DE HERT, “Het Europees Hof Rechten van de Mens erkent publieke privacy”, *NJW* 2002, 116. [↑](#footnote-ref-205)
206. H. GRAUX en J. DUMORTIER, *Privacywetgeving in de praktijk*, Heule, UGA, 2009, 16. [↑](#footnote-ref-206)
207. C. CONINGS, *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Antwerpen, Intersentia, 2017, 116. [↑](#footnote-ref-207)
208. P. DE HERT, “Grondrechten die bijna niet verdedigd kunnen worden. De bescherming van persoonlijke gegevens op het Internet” in K. RAES, P. DE HERT, P. VAN EECKE, J. DUMORTIER, P. VALCKE, D. VOORHOOF en P. THOMAS (eds.), *De rechten van de mens op het Internet*, Antwerpen, Maklu, 2000, 24. [↑](#footnote-ref-208)
209. *Ibid.,* 25. [↑](#footnote-ref-209)
210. P. DE HERT en R. SAELENS, “Digitale procesvoering en informatieveiligheid: integriteit van het systeem grondrechtelijk beschermd?” (noot onder RvS 9 februari 2016), *RW* 2016-2017, 588. [↑](#footnote-ref-210)
211. B. RAINEY, *Human Rights Law Concentrate: Law Revision and Study Guide*, Oxford, Oxford University Press, 2017, 33. [↑](#footnote-ref-211)
212. H. GRAUX en J. DUMORTIER, *Privacywetgeving in de praktijk*, Heule, UGA, 2009, 17. [↑](#footnote-ref-212)
213. *Ibid.,* 16. [↑](#footnote-ref-213)
214. G. VERMEULEN, *Privacy en strafrecht:* *nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu, 2007, 200. [↑](#footnote-ref-214)
215. EHRM 12 januari 2010, nr. 4158/05, Gillann en Quinton/Verenigd Koninkrijk (§ 65). [↑](#footnote-ref-215)
216. C. VAN DEN WYNGAERT, P. TRAEST en S. VANDROMME, *Strafrecht en Strafprocesrecht in Hoofdlijnen*, Antwerpen, Maklu, 2017, 931. [↑](#footnote-ref-216)
217. EHRM 12 januari 2010, nr. 4158/05, Gillann en Quinton/Verenigd Koninkrijk (§ 85). [↑](#footnote-ref-217)
218. C. CONINGS, *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Antwerpen, Intersentia, 2017, 14. [↑](#footnote-ref-218)
219. *Ibid.*, 33. [↑](#footnote-ref-219)
220. P. DE HERT, “Artikel 8. Recht op privacy” in J. VANDE LANOTTE en Y. HAECK (eds.), *Handboek EVRM,* II*,* Antwerpen, Intersentia, 2004, 717. [↑](#footnote-ref-220)
221. EHRM 6 september 1978, nr. 5029/71, Klass e.a./Duitsland, § 49. [↑](#footnote-ref-221)
222. *Ibid*., § 59. [↑](#footnote-ref-222)
223. P. DE HERT, “Artikel 8. Recht op privacy” in J. VANDE LANOTTE en Y. HAECK (eds.), *Handboek EVRM,* II*,* Antwerpen, Intersentia, 2004, 712. [↑](#footnote-ref-223)
224. EHRM 6 september 1978, nr. 5029/71, Klass e.a./Duitsland, § 42. [↑](#footnote-ref-224)
225. EHRM 12 januari 2016, nr. 37138/14, Szabó en Vissy/Hongarije, § 54. [↑](#footnote-ref-225)
226. EHRM 28 april 2005, nr. 41604/98, Buck/Duitsland, §§ 44-45. [↑](#footnote-ref-226)
227. EHRM 25 maart 1983, nr. 7136/75, Silver e.a./Verenigd Koninkrijk, § 97. [↑](#footnote-ref-227)
228. F. Bernard, “La Cour européenne des droits de l’homme et la lutte contre le terrorisme’’, *RTDH* 2016, 58. [↑](#footnote-ref-228)
229. EHRM 14 november 1960, nr. 332/57, Lawless/Ierland. [↑](#footnote-ref-229)
230. L. Sicilianos, “La Cour européenne des droits de l’homme face à l’Europe en crise’’, *RTDH* 2016, 25. [↑](#footnote-ref-230)
231. *Ibid*., 26. [↑](#footnote-ref-231)
232. A. DE NAUW en F. SCHUERMANS, “De wet betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden’’, *RW* 2004, 929. [↑](#footnote-ref-232)
233. P. WAETERINCKX en C. VAN DE HEYNING, “Rechten van verdediging tijdens het strafonderzoek en de regeling van de rechtspleging – Capita selecta” in C. DAELMAN e.a., *Mensenrechten in de praktijk. Toegepast in uw juridische dossiers*, Antwerpen, Intersentia, 2016, 228. [↑](#footnote-ref-233)
234. *Ibid*., 230. [↑](#footnote-ref-234)
235. EHRM 12 januari 2016, nr. 37138/14, Szabó en Vissy/Hongarije. [↑](#footnote-ref-235)
236. EHRM 30 maart 1989, Ian Chappell/Verenigd Koninkrijk en EHRM 25 februari 1993, Miailhe/Frankrijk. [↑](#footnote-ref-236)
237. EHRM 16 december 1997, Camenzind/Zwitserland. [↑](#footnote-ref-237)
238. EHRM 29 juni 2006, nr. 54934/00, Weber en Saravia/Duitsland. [↑](#footnote-ref-238)
239. EHRM 25 september 2001, nr. 44787/98, P.G. en J.H./Verenigd Koninkrijk, § 56. [↑](#footnote-ref-239)
240. EHRM 4 mei 2000, nr. 28341/95, Rotaru/Roemenië. [↑](#footnote-ref-240)
241. EHRM 30 september 2014, nr. 8429/05, Prezhdarovi/Bulgarije. [↑](#footnote-ref-241)
242. C. CONINGS en S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken”, *NC* 2017, 329. [↑](#footnote-ref-242)
243. *Ibid*., 334. [↑](#footnote-ref-243)
244. *Ibid*., 225. [↑](#footnote-ref-244)
245. EHRM 28 juli 2009, nr. 18704/06, Lee Davies/België. [↑](#footnote-ref-245)
246. P. WAETERINCKX en C. VAN DE HEYNING, “Rechten van verdediging tijdens het strafonderzoek en de regeling van de rechtspleging – Capita selecta” in C. DAELMAN e.a., *Mensenrechten in de praktijk. Toegepast in uw juridische dossiers*, Antwerpen, Intersentia, 2016, 220. [↑](#footnote-ref-246)
247. A. MICHEL, “L’utilisation des contenus postés sur les réseaux sociaux comme éléments de preuve d’un dommage”, *RDTI* 2016, afl. 4, 110. [↑](#footnote-ref-247)
248. P. WAETERINCKX en C. VAN DE HEYNING, “Rechten van verdediging tijdens het strafonderzoek en de regeling van de rechtspleging – Capita selecta” in C. DAELMAN e.a., *Mensenrechten in de praktijk. Toegepast in uw juridische dossiers*, Antwerpen, Intersentia, 2016, 220. [↑](#footnote-ref-248)
249. EHRM 20 oktober 2015, Dvorski/Kroatië, § 81. [↑](#footnote-ref-249)
250. bijv. EHRM 9 juni 1998, Teixeira De Castro/Portugal, § 34. [↑](#footnote-ref-250)
251. Vanneste, F., “Het Europese Hof voor de Rechten van de Mens en de overheden die terrorisme bestrijden: brothers in arms?’’, *RW* 2004, 1676. [↑](#footnote-ref-251)
252. Cass. 23 maart 2004, AR P.04.0012.N. [↑](#footnote-ref-252)
253. A. MICHEL, “L’utilisation des contenus postés sur les réseaux sociaux comme éléments de preuve d’un dommage”, *RDTI* 2016, afl. 4, 109. [↑](#footnote-ref-253)
254. *Ibid.,* 110. [↑](#footnote-ref-254)
255. *Ibid.,* 112. [↑](#footnote-ref-255)
256. P. WAETERINCKX en C. VAN DE HEYNING, “Rechten van verdediging tijdens het strafonderzoek en de regeling van de rechtspleging – Capita selecta” in C. DAELMAN e.a., *Mensenrechten in de praktijk. Toegepast in uw juridische dossiers*, Antwerpen, Intersentia, 2016, 231. [↑](#footnote-ref-256)
257. *Ibid.*, 246. [↑](#footnote-ref-257)