



Advies nr 21/2016 van 18 mei 2016

Betreft: Advies over het voorontwerp van wet betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties (CO-A-2016-021)

De Commissie voor de bescherming van de persoonlijke levenssfeer ;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 29;

Gelet op het verzoek om advies van de heer Koen Geens, Minister van Justitie ontvangen op 31/03/2016;

Gelet op het verslag van mevrouw Séverine Waterbley en de heer Frank Schuermans;

Brengt op 18 mei 2016 het volgend advies uit:

I. ONDERWERP VAN DE ADVIESAANVRAAG

1. De Commissie voor de bescherming van de persoonlijke levenssfeer (hierna "de Commissie"), ontving op 31 maart 2016 een adviesaanvraag van de heer Koen Geens, Minister van Justitie, over een voorontwerp van wet betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties
2. Dit voorontwerp van wet bevat een zeker aantal wijzigingen aan het Wetboek voor Strafvordering en het Strafwetboek en strekt er vooral toe om een aantal verbeteringen in te voeren in het opsporingsonderzoek en het gerechtelijk onderzoek, enerzijds bij de toepassing van de bijzondere onderzoeksmethoden en anderzijds bij bepaalde onderzoeksmethoden die in het bijzonder betrekking hebben op de internetrecherche en de elektronische- en telecommunicaties. Het is vooral dat laatste aspect dat de kern van het voorstel uitmaakt.
3. Criminelen en maken immers steeds vaker gebruik van de mogelijkheden die de informatietechnologie hen biedt. Het voorontwerp van wet wil hier dan ook een meer aangepast juridisch kader ontwerpen voor ondermeer de zoeking in een informaticasysteem, voor het actief zijn op het internet door de politiediensten en het onderscheppen en kennisnemen van elektronische communicaties.

II. ALGEMENE INLEIDING

4. Het recht op de bescherming van de persoonsgegevens is, in de loop van de jaren, naast het recht op de bescherming van de persoonlijke levenssfeer komen te staan als een zelfstandig en volwaardig grondrecht. Dit is het duidelijkst tot uiting gekomen in het "Handvest van de grondrechten van de Europese Unie van 12 december 2007" waar benevens het artikel 7 , "de eerbiediging van het privé-leven en van het familie-en gezinsleven" het daaropvolgende artikel 8 "de bescherming van persoonsgegevens" uitdrukkelijk verwoordt. Daarmee is het onderscheid tussen de "privacy" en de "dataprotectie" scherper gesteld dan klassiek uit het artikel 22 van de Belgische Grondwet of het artikel 8 van het EVRM kan worden afgeleid.¹
5. Deze beide grondrechten zijn niet enkel complementair maar behoren klassiek tot de "vrijheden" en moeten samenhangend met de andere rechten en vrijheden worden benaderd en toegepast worden. Het is niet toevallig dat onder de titel "Vrijheden" van het Handvest voornoemde artikelen 7 en 8 worden voorafgegaan door het artikel 6 dat onder de titel "het

¹ zie Dirk De Bot, "Gegevensverwerking in de publieke sector", Brussel 59, ASP/Politea, inzonderheid Deel I : "Privacyrecht en gegevensverwerking in de publieke sector" blz. 59-132.

recht op vrijheid en veiligheid” deze interferentie omschrijft “eenieder heeft recht op vrijheid en veiligheid van zijn persoon”. Overigens maakt ook de Wet Verwerking Persoonsgegevens of WVP² ook de binding met de andere grondrechten door in het artikel 2 het recht op gegevensbescherming te richten op het doel : de bescherming van de fundamentele rechten en vrijheden.

6. Het recht van elke burger op “veiligheid” en fysieke en morele “integriteit” is eveneens en evenzeer beschermingswaardig als het recht op de bescherming van de persoonsgegevens. Daarbij wordt veelal betoogt dat deze beide rechten en aanspraken tot een juist evenwicht moeten komen en dat is juist. Maar enkel ten dele : het is evenzeer zo dat deze rechten elkaar moeten aanvullen, versterken en schragen. Zo is het niet mogelijk een sluitende bescherming van de persoonsgegevens en de persoonlijke levenssfeer op te bouwen zonder te voorzien in een rechtshandhaving daarvan. En ook daarvoor zal het klassieke algemene en bijzondere strafrecht ook een belangrijke bijdrage moeten leveren. Niet voor niets sluit de huidige WVP af met een hoofdstuk “strafbepalingen”. Over enkele dagen, vanaf 24 mei, is de nieuwe “algemene verordening gegevensbescherming”³ van kracht die op deze rechtshandhavende taak inzet door bijkomende verplichtingen op te leggen aan de overheden in het algemeen en de “toezichthoudende autoriteit” (de vroegere privacycommissie) in het bijzonder. En ook hier wordt de band gelegd met de andere “grondrechten en fundamentele vrijheden” (artikel 1.2.) en worden beperkingen voorzien in artikel 23.

7. Ter bescherming van de fundamentele rechten en vrijheden is niet alleen het materiële recht nodig maar ook evenzeer het instrumentarium, de strafvordering. Strafrechtelijk onderzoek is bij uitstek privacyinvasief, ook wanneer de bescherming van de persoonlijke levenssfeer en de persoonsgegevens in het geding is. Wanneer zich nieuwe of zich wijzigende communicatievormen aandienen of wanneer wordt vastgesteld dat de nood tot ingrijpende inzicht en informatiegaring noodzakelijk is moeten deze onderzoeksmethodes ook aangepast of toegepast kunnen worden. En dit ter bescherming van diezelfde burger over wiens persoonsgegevens het gaat.

² de zogenaamde Belgische privacywet is eigenlijk een data protection wet van het zuiverste water en dit valt ook af te lezen uit de titel die het trefzeker heeft over de “wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens”

³ Verordening (EU) 2016/679 van het Europees parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG

III. ONDERZOEK TEN GRONDE

1. Voorafgaande opmerking

8. Zoals hoger gezegd, zal de inhoud en de draagwijdte van bepaalde wijzigingen aan het Wetboek voor Strafvordering en het Strafwetboek raken aan fundamentele rechten, zoals het grondrecht op privacy, beschermd door artikel 8, 1ste lid van het EVRM en artikel 22 van het Grondwet en het recht op onschendbaarheid van de woning, zoals beschermd door artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten en artikel 15 van de Grondwet.
9. Deze wijzigingen in het opsporingsonderzoek en het gerechtelijk onderzoek in het bijzonder bij het toepassen van de zogenaamde bijzondere onderzoeksmethoden (afgekort "BOM")⁴ en vooral bij bepaalde andere indringende (onderzoeks)methodes inzake internetrecherche en telecommunicaties, moeten de test van artikel 8, §2 van het EVRM kunnen doorstaan, dat niet alleen een wettelijke basis vereist maar ook bepaalt dat in een democratische samenleving een inmenging in de uitoefening van dit recht proportioneel en noodzakelijk moet zijn.
10. De jurisprudentie van het Europees Hof van de Rechten van Mens legt meestal het accent op de dringende noodzaak om willekeurige inmenging in de privacy van de betrokkenen te vermijden. Daaruit vloeit voort dat elke nationale bepaling ter zake voldoende helder en nader omschreven moet zijn zodat aan eenieder op een passende manier kan worden meegegeven onder welke voorwaarden deze bepalingen het openbaar gezag toelaat gebruik te maken van geheime onderzoeksmaatregelen. Naast deze gemeenschappelijke vereiste, vaardigde het Hof nog andere minimale garanties uit. De nationale wetgevingen moeten heel precies omschrijven welke misdrijven aanleiding kunnen geven tot een rechtmatig tapbevel, moeten de toepasselijke, subjectieve beperkingen van bepaalde categorieën personen aangeven, moeten de limieten bepalen van de duur van dat toezicht, moet de te volgen procedure(s) bij het onderzoek alsook het gebruik, het delen en het bewaren van de verkregen gegevens omschrijven, moeten de te nemen voorzorgsmaatregelen bij de mededeling van die informatie aan derden bevatten, moeten de omstandigheden waaronder de informatie mag gewist of vernietigd worden omschrijven⁵ en moeten voorzien in een onderzoek ex ante of ex post door een rechter of ieder andere daadwerkelijke (objectieve en subjectieve) onpartijdige deskundige, die feitelijk maar ook hiërarchisch onafhankelijk is van de instantie

⁴ Ter herinnering. Het Wetboek van Strafvordering kent drie soorten bijzondere opsporingsmethoden, met name de observatie, de infiltratie en de informantenwerking.

⁵ Weber et Saravia vs. Duitsland (dec.) ; Association for European Integration and Human Rights et Ekimdzhev vs. Bulgarije ; Liberty en andere organisatie vs. Groot-Brittannië.

die verantwoordelijk is voor het opleggen van dergelijke maatregelen en die gemachtigd is om de authenticiteit en de betrouwbaarheid van de registraties te waarborgen. Hoewel de nationale wetgeving nalaat om naar bepaalde van de bovenvermelde elementen te verwijzen, zal het Hof zijn onderzoek ook uitbreiden tot de nationale jurisprudentie die relevant is of kan zijn voor de bescherming van het individu.⁶

2. Analyse van artikel 2 van het voorontwerp - wijzigingen aan het artikel 39bis van het Wetboek van Strafvordering - niet-heimelijke zoeking in informaticasystemen

11. Dit artikel wijzigt artikel 39bis van het Wetboek van Strafvordering (Sv.) en betreft de niet-heimelijke zoeking in informaticasystemen. Dit artikel integreert de inhoud van artikel 88ter Sv. met betrekking tot de zoeking in informaticasystemen of van een gedeelte ervan in artikel 39bis van hetzelfde wetboek met de bedoeling een coherent artikel te bekomen over de niet-heimelijke zoeking en zijn uitbreiding in informaticasystemen. Omdat de inhoud van artikel 88ter Sv. geheel is overgenomen, heeft dit artikel geen bestaansreden meer en wordt het opgeheven.
12. Overigens, de wijzigingen aan artikel 39bis Sv. strekken ertoe de bevoegdheden op te helderen van de verschillende actoren inzake zoekingen in informaticasystemen of in een gedeelte daarvan. Het huidig artikel 39bis WSV is hierover inderdaad niet duidelijk genoeg.
13. Bijgevolg wordt voorzien in 4 niveau's.
14. Het eerst niveau is dat van de zoeking in een informaticasysteem dat in beslag werd genomen in het kader van een vooronderzoek in strafzaken (dat dus zowel ene opsporingsonderzoek als gerechtelijk onderzoek kan zijn). Deze zoeking kan worden verricht door een officier van de gerechtelijke politie zonder voorafgaande machtiging van de procureur des Koning of onderzoeksrechter (artikel 39bis, §2 Sv. in voorontwerp).
15. De Commissie stelt vast dat het Hof van Cassatie in zijn arrest van 11 februari 2015⁷ heeft gesteld dat het huidige recht de politieambtenaren nu al toestaat om kennis te nemen van de gegevens op een in beslag genomen gsm. Daarmee maakte het Hof een einde aan een jarenlange onduidelijkheid nopens de exacte politionele bevoegdheden tot "uitlezing" wanneer een gsm of smartphone in beslag werd genomen.

⁶ Ivana Roagna, La protection du droit au respect de la vie privée et familiale par la Convention européenne des droits de l'homme

⁷ Cass., 11 februari 2015 (AR P.14.1739.F), juridat.

16. Het tweede niveau betreft de zoeking in een informaticasysteem dat niet in beslag is genomen, maar waarvoor de voorwaarden voor een inbeslagneming zijn vervuld. In dit geval moet de zoeking gemachtigd worden door de procureur des Konings⁸. (art. 39bis, §2, 2^e lid en §3 Sv in voorontwerp).
17. De Commissie stelt vast dat daarin in wezen al is voorzien met het huidige artikel 39bis, §2 Sv.
18. Een derde niveau betreft de niet-heimelijke opzoeken en uitbreiding in informaticasystemen. Artikel 39bis, §4, SV bepaalt de grenzen van de uitbreiding van de niet-heimelijke zoeking in een informaticasysteem of in een deel daarvan, dat zich op een andere plaats bevindt dan waar de zoeking wordt verricht.
19. De uitbreiding van de zoeking in een informaticasysteem of in een deel daarvan kan worden bevolen door de procureur des Konings :
- als die uitbreiding noodzakelijk is om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp van de zoeking uitmaakt en
 - er geen andere maatregelen voorhanden zijn die minder indringend zijn en waarmee hetzelfde resultaat kan worden bereikt of dat er een risico bestaat dat zonder deze uitbreiding bewijselementen verloren gaan.
20. DHet ontwerp verantwoordt de tussenkomst van de procureur des Koning (zodat dit aldus geen exclusieve bevoegdheid is van de onderzoeksrechter) met het argument dat artikel 39bis Sv. zich beperkt tot de niet-heimelijke zoekingen. Er wordt dus op de privacy van personen en/of verdachten dus op geen enkele wijze heimelijk eeninbreuk gepleegd . Integendeel het openbaar ministerie moet de verantwoordelijke van het informaticasysteem op de hoogte brengen van de zoeking. Daarnaast is de overdracht van deze maatregel (namelijk de uitbreiding van de zoeking) van artikel 88ter Sv. naar artikel 39bis Sv., waardoor naast dede onderzoeksrechter ook de procureur des Konings deze bevoegdheid krijgt, gerechtvaardigd door het feit dat, wegens de ontwikkeling van nieuwe technologieën, het onderscheid tussen hetgeen zich op het toestel bevindt en hetgeen zich in de cloud bevindt (wat een uitbreiding van de zoeking noodzakelijk maakt) voor een deel artificieel geworden.
21. Hoewel de Commissie meent dat een tussenkomst van een rechter meer garanties biedt tegen een inmenging in het privéleven, verzet zij zich er niet tegen dat het openbaar ministerie

⁸ De Commissie gaat ervan uit dat telkens het ontwerp het heeft over "de procureur des Konings" daarmee ook worden bedoeld de federale procureur, de arbeidsauditeur en de procureur-generaal naar gelang van het geval.

bevoegd zou zijn voor alle niet-geheime zoekingen in informaticatoepassingen aangezien de parketmagistraat, zoals gesteld, "*de verantwoordelijke van het informaticasysteem op de hoogte (moet brengen) van de zoeking in het informaticasysteem of de uitbreiding ervan, tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden, en deelt hem in voorkomend geval een samenvatting mee van de gegevens die zijn gekopieerd, ontoegankelijk gemaakt of verwijderd*" (art. 39bis, §5, WSV in het voorontwerp). Meer algemeen herinnert de Commissie er overigens aan dat ook het openbaar ministerie onafhankelijk is in de individuele opsporing en vervolging (art. 151 Grondwet) en moet waken over de wettigheid van de bewijsmiddelen en de loyaliteit waarmee ze worden verzameld (art. 28bis §3, laatste lid Sv.). Dat loyaliteitsbeginsel houdt volgens het Hof van Cassatie in dat alle door het parket verzamelde gegevens bij het strafdossier worden gevoegd, inzonderheid de gegevens à décharge⁹. Daarmee sloot het Hof van Cassatie zich ook aan bij het Grondwettelijk Hof dat reeds herhaaldelijk het volgende heeft gesteld: "*Tussen het openbaar ministerie en de verdachte bestaat een fundamenteel verschil dat op een objectief criterium steunt: het openbaar ministerie vervult, in het belang van de gemeenschap, de opdrachten van openbare dienst met betrekking tot de opsporing en de vervolging van de misdrijven en vordert de toepassing van de strafwet; de verdachte verdedigt zijn persoonlijk belang*"¹⁰.

22. De Commissie stelt overigens vast dat een heimelijke indringing in een informaticasysteem en het toezicht erop, onderworpen blijven aan een tussenkomst van de onderzoeksrechter (art. 90 en volgende Sv.).
23. De Commissie stelt evenwel vast dat alleen de onderzoeksrechter het gebruik van "*valse sleutels*"¹¹ kan bevelen. In de toelichting bij het artikel 2 van het voorontwerp verduidelijkt de wetgever evenwel: *Dit is enkel het geval voor de gegevens die zich niet bevinden op het informaticasysteem dat in beslag genomen werd of dat in beslag genomen zou kunnen worden. Indien, naast de valse sleutels die nodig waren om toegang te krijgen tot de algemene inhoud van het informaticasysteem, het gebruik van bijkomende "valse sleutels" nodig is om toegang te krijgen tot welbepaalde specifieke delen van het intern geheugen van het informaticasysteem, blijft de procureur des Konings bevoegd om dergelijk gebruik van valse sleutels te bevelen*". De bevoegdheidsverdeling tussen parket en onderzoeksrechter in het kader van de niet heimelijke informaticazoeeking wordt daardoor in een snel evoluerende informatica-omgeving ongetwijfeld complex. Als de Commissie het goed begrepen heeft is

⁹ Zie o.a. Cass. 19 december 2012, n° P. 12.1310.F/1,

¹⁰ Zie o.a. Grondwettelijk Hof, 1 december 1994, n° 82/1994; zie ook de arresten n° 22/95, n° 43/95, n° 76/95, n° 49/97, n° 29/98, n° 58/98, n° 12/2000, n° 58/2001, n° 69/2001, n° 5/2002, n° 70/2005, n° 191/2005, n° 182/2008, www.grondwettelijkhof.be

¹¹ Installatie van technische apparatuur in de betrokken informaticasystemen voor het decrypteren en decoderen van de in dit systeem opgeslagen, verwerkte of doorgegeven gegevens.

het parket bevoegd tot een niet heimelijke informaticazoeking en uitbreiding ervan. Het parket kan zo nodig "valse sleutels" aanwenden om die niet heimelijke informaticazoeking te doen (ontworpen §4ter, 1^e lid), maar van zodra er sprake is van een uitbreiding (er dus m.a.w. netwerkverbindingen zijn, wat quasi steeds het geval zal zijn) dient een onderzoeksrechter gevorderd (ontworpen §4ter, 2^e lid) te worden.

24. De Commissie neemt hiervan akte.

25. Het vierde niveau betreft informaticasystemen die niet vatbaar zijn voor inbeslagneming. In dat geval is voor de zoeking de machtiging van een onderzoeksrechter nodig, in voorkomend geval in het kader van de mini-instructie.

26. De Commissie neemt hiervan akte.

3. Analyse van de artikelen 3 en 4 van het voorontwerp - invoeging van de artikelen 39ter en 39quater van het Wetboek van Strafvordering - snelle bewaring en onthulling van informaticagegevens

27. Het nieuwe artikel 39ter Sv. belichaamt de omzetting van de artikelen 16 en 17 van de Cybercrimeconventie¹² met betrekking tot de snelle bewaring en onthulling van nationale gegevens.

28. Het nieuwe artikel 39quater Sv. betreft de omzetting van de artikelen 29 en 30 van de Cybercrimeconventie met betrekking tot de snelle bewaring en onthulling van gegevens op nationaal niveau.

29. Deze artikelen bepalen dat aan meerdere natuurlijke personen of aan rechtspersonen bevolen kan worden om gegevens die in hun bezit zijn of waarover zij de controle hebben, te bewaren *"wanneer er redenen bestaan om aan te nemen dat gegevens die opgeslagen, verwerkt of overgedragen worden door middel van een informaticasysteem bijzonder kwetsbaar zijn voor verlies of voor wijziging ».*

30. De Commissie stelt vast dat op internationaal niveau deze maatregel kan genomen worden door de het openbaar ministerie. Ze neemt er akte van dat de maatregel op nationaal niveau

¹² STE 185 – Cybercriminalité (Convention), 23.XI.2001

zal kunnen bevolen worden "*door iedere officier van gerechtelijke politie*" en heeft daarbij geen bijzondere opmerkingen

4. Analyse van de artikelen 6 en 15 van het voorontwerp - wijzigingen aan de artikelen 46quinquies en 89 van het Wetboek van Strafvordering - inkijkoperaties

31. Naast het betreden van een private plaats wordt het mogelijk gemaakt tijdens een inkijkoperatie kennis te nemen van de inhoud van gesloten voorwerpen die zich daar bevinden, zoals bijvoorbeeld slotvaste kasten of safes.
32. De toelichting bij artikel 6 preciseert: "*met gesloten voorwerp wordt echter niet een informaticasysteem bedoeld. Om informaticasystemen (zoals laptops of smartphones) te kunnen doorzoeken, is er steeds een bevelschrift van de onderzoeksrechter nodig. Nochtans mogen de opsporingsdiensten binnendringen in een informaticasysteem indien dit enkel tot doel heeft een technisch hulpmiddel te plaatsen, te herstellen of terug te nemen in het kader van een observatie.*»
33. De Commissie merkt op dat een staalname nu al mogelijk is. De memorie van toelichting bij de wet van 6 januari 2003 geeft immers aan "*het kan aangewezen zijn dat de politieambtenaren die, naar aanleiding van een inkijkoperatie, een hoeveelheid wit poeder of een hoeveelheid verdachte liquide middelen aantreffen, daar een staal van nemen, teneinde met zekerheid te kunnen bepalen of het hier al dan niet om drugs of hormonenpreparaat gaat*¹³».
34. De nieuwe paragraaf 5 voorziet dat de onderzoekers een voorwerp gevonden op de plaats van de inkijkoperatie kunnen meenemen indien het onderzoek van het voorwerp niet ter plaatse kan gebeuren en indien de informatie niet op een andere manier kan worden verkregen. *In fine* wordt gesteld "*Het bewuste voorwerp wordt zo spoedig mogelijk teruggeplaatst, tenzij dit het goede verloop van het onderzoek in de weg staat* ».
35. De Commissie neemt hiervan akte.
36. Artikel 89ter Sv. voert ook de nieuwe mogelijkheid in van een heimelijke zoeking in een informaticasysteem maar uitsluitend voor de doeleinden als omschreven onder artikel 46quinquies, §2 Sv.

¹³ Doc. Parl. 50-1688/001, p. 59

37. Het doel van die maatregel is na te gaan of er bewijsmateriaal bestaat maar niet om het te verzamelen. Er mogen enkel stalen worden genomen. In het kader van een inkijkoperatie in een informaticasysteem betekent dit dat een gerichte kopie mag genomen worden van bepaalde gegevens.
38. Het onderscheid tussen de heimelijke zoeking in een informaticasysteem zoals ingevoerd in artikel 89ter Sv. en de heimelijke zoeking in een informaticasysteem zoals ingevoerd door artikel 90ter Sv., ligt voornamelijk in de finaliteit van de maatregel. De finaliteit van artikel 89ter Sv. is dat er kan gezocht worden naar bewijs van strafbare feiten, maar het gevonden bewijs mag niet verzameld en gebruikt worden; er mogen enkel stalen worden genomen. De inkijkoperatie in een informaticasysteem is met andere woorden een oriënterend instrument dat het mogelijk maakt om gradueel op de privacy in te breken en stalen te nemen die in voorkomend geval een nog verdergaande maatregel kunnen verantwoorden.
39. Er is voor geopteerd om de inkijkoperatie (voor ander doeleinden dan het louter plaatsen, herstellen of terugnemen van een hulpmiddel om een observatie te kunnen doen) in een informaticasysteem onder te brengen in artikel 89ter en niet in artikel 46quinquies, ook al zou in principe kunnen worden verdedigd dat een informaticasysteem - bijvoorbeeld een Hotmailaccount, een Facebook-account, een iCloud-account, ... - private plaatsen zijn die géén woning zijn. Gelet op het feit dat de privacy van personen online of in de 'cloud' dermate omvangrijk en gevoelig kan zijn, gecombineerd met het feit dat deze privacy bij een inkijkoperatie 'heimelijk' wordt benaderd, dient dit consequent onder de controle van de onderzoeksrechter te worden gesteld.
40. Na lezing van die bepalingen stelt de Commissie vast dat in het kader van een inkijkoperatie aan de informaticasystemen dezelfde bescherming wordt toegekend als aan de woning. Zij neemt hiervan akte.
- 5. Analyse van artikel 7 van het voorontwerp - Invoeging van artikel 46sexies in het Wetboek van Strafvordering - interacties en infiltraties die uitsluitend op het internet plaatsvinden**

41. Dit artikel voert de mogelijkheid in tot een infiltratie of een interactie op internet¹⁴ over te gaan die niet enkel een gerichte verificatie of arrestatie op het oog heeft. Men spreekt soms ook wel over een zgn. "infiltratie-light".
42. De Procureur des Konings kan dit machtigen "*indien het onderzoek zulks vereist*"; indien "*de overige middelen van onderzoek niet volstaan om de waarheid aan de dag te brengen*" en indien "*er ernstige aanwijzingen bestaan dat het een feit betreft dat aanleiding geeft tot een correctionele gevangenisstraf in hoofdzaak van een jaar of tot een zwaardere straf*".
43. De Commissie is van mening dat interacties op het internet een impact kunnen hebben op de privacy van de betrokkene. De Commissie noteert dat, artikel 46sexies, §4, 2de lid, Sv. bepaalt dat alle relevante contacten moeten geregistreerd worden. Dit maakt de maatregel veel transparanter a posteriori en vermijdt risico op misbruik. Daarnaast kunnen de beschuldigde, de beklaagde, de burgerlijke partij of hun raadsman van de procureur de Konings toestemming krijgen om alle of een deel van de geregistreerde contacten te raadplegen.
44. Na lezing van artikel 46sexies Sv in voorontwerp en het commentaar bij het artikel is het voor de Commissie niet duidelijk wat wordt bedoeld met "*infiltratie op internet of een interactie op internet die niet enkel een gerichte verificatie of een arrestatie tot doel heeft*". De uitsluiting van de toepassing van artikel 46sexies Sv. op "*de persoonlijke interactie op het internet van politieambtenaren met een of meerdere personen, die enkel een gerichte verificatie of een arrestatie tot direct doel heeft*" is op zijn minst raadselachtig gezien het feit dat de bedoelde maatregel onder artikel 46sexies Sv. überhaupt alleen kan bevolen worden door de procureur des Konings als er "*ernstige aanwijzingen zijn dat zij strafbare feiten die een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben, plegen of zouden plegen*." Het lijkt erop dat met de voorgenomen uitzonderingsbepaling het voor politieambtenaren mogelijk wordt gemaakt autonoom een interactie op het internet te ondernemen, met als doelstelling een doelgerichte verificatie of arrestatie van een persoon.
45. De Commissie vermoedt dus dat met deze passus zoals verwoord in §1, 3^e lid de politieambtenaren autonoom op internet moeten kunnen "patrouilleren". In dat geval moet artikel 46sexies Sv. evenwel duidelijker worden gelibelleerd. De vraag is immers of deze uitzonderingsbepaling op zich voldoende duidelijk is en of die voorgenomen autonome

¹⁴ Het begrip internet moet in brede zin worden begrepen en bevat meer bepaald het "dark web".

bevoegdheid van de politie niet op zich duidelijk dient ingeschreven te worden hetzij in het Wetboek van Strafvordering, hetzij in de Wet op het Politieambt.

46. De Commissie vestigt in dat verband de aandacht van de aanvrager op haar advies nr. 13/2015 van 13 mei 2015 betreffende de voorontwerpen van wet houdende diverse bepalingen – wijzigingen aan de wet tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, aan de wet op het politieambt en aan de wet van 18 maart 2014 betreffende het politionele informatiebeheer.
47. Een van de voorgenomen wijzigingen van de wet van 5 augustus 1992 op het politieambt strekte er precies toe om in artikel 26 nader te omschrijven dat *"voor het publiek toegankelijke plaatsen op het internet of op andere elektronische communicatienetwerken, ongeacht of er voor het nemen van de toegang daartoe bepaalde vormelijke toegangsformaliteiten moeten worden ondernomen, gelijkgesteld worden met publiek toegankelijke plaatsen. De politieambtenaren mogen deze plaatsen bezoeken, bestuderen en er kopieën van maken »*.
48. Gelet op een dergelijke definitie van "voor het publiek toegankelijke plaatsen", zouden de politieambtenaren mogen "patrouilleren" op internet teneinde ondermeer een gerichte verificatie of arrestatie te verrichten. Deze bevoegdheid moet echter duidelijk in een wet worden gegoten zodat het rechtmatigheidsbeginsel en voorzienbaarheidsbeginsel zijn geëerbiedigd. Het is de Commissie niet duidelijk waarom er blijkbaar geen sprake meer is van de voorgenomen wijziging van artikel 26 WPA in de zin zoals men kennelijk nu toch onrechtstreeks lijkt te willen doorvoeren via het ontworpen artikel 46sexies Sv.

6. Analyse van artikel 14 van het voorontwerp - wijzigingen aan artikel 88quater van het Wetboek van Strafvordering – Medewerkingsplicht

49. Artikel 14 legt strengere straffen op aan personen die niet meewerken aan de zoeking in een informaticasysteem of de uitbreiding ervan. In de memorie van toelichting wordt dit als volgt gemotiveerd: *"Deze strengere bestraffing moet een duidelijk signaal geven aan personen die hun medewerking niet verlenen of die het onderzoek dwarsbomen. (...) Gelet op de huidige stand van de technologie en de verdere evolutie die op dit domein nog mag worden verwacht, is het voor de opsporingsdiensten vaak bijzonder moeilijk of zelfs onmogelijk om toegang te verkrijgen tot gegevens op een informaticasysteem, zonder hulp van externen die op de hoogte zijn van de werking ervan, de gebruikte versleuteling etc."*

50. De Commissie merkt op dat deze medewerkingsplicht in sommige gevallen op gespannen voet kan komen te staan met wat artikel 48 van de wet *betreffende de elektronische communicatie van 13 juni 2015* (hierna "WEC") voorschrijft. Laatstgenoemde bepaling stelt met name dat het gebruik van versleuteling vrij is, waaruit ook kan afgeleid worden dat de gebruikers van versleutelingen niet verplicht zijn om de sleutels te bewaren. Gebruikers die de sleutels niet hebben bijgehouden kunnen in het kader van hun medewerkingsplicht zoals voorzien in artikel 88quater Sv evident weinig nuttige informatie verstrekken aan de opsporingsdiensten en het lijkt betwistbaar dat zij hiervoor zouden kunnen gesanctioneerd worden, juist gelet op voornoemd artikel 48 WEC.

7. Analyse van de artikelen 17 en volgende van het voorontwerp - wijzigingen aan artikel 90ter van het Wetboek van Strafvordering - heimelijke zoekingen in een informaticasysteem en heimelijke kennisname van communicatie

51. Artikel 90ter Sv. (betreffende het aftappen van telecommunicaties) is grondig herzien door:

- De introductie van de heimelijke zoeking in informaticasystemen;
- de heimelijke zoeking in informaticasystemen en de onderschepping van telecommunicaties¹⁵ samen te voegen tot één maatregel. Door de technologische evolutie kan vaak geen onderscheid meer worden gemaakt tussen de twee. Men spreekt nu beter van de heimelijke kennisname van communicatie en informatie;
- de lijst van misdrijven waarvoor de maatregel van artikel 90ter mogelijk is, uit te breiden

52. Het eerste lid, §1, van art. 90ter Sv beschrijft de maatregel die de onderzoeksrechter kan bevelen. Die bevat de onderschepping, de kennisname, onderzoek en registratie van de niet voor het publiek toegankelijke communicaties¹⁶ of gegevens van een informaticasysteem of een deel daarvan, evenals de uitbreiding van een zoeking in een informaticasysteem.

53. De Commissie herinnert eraan dat het Europees Hof voor Rechten van de Mens van mening is dat de telefoongesprekken vervat zitten in de begrippen "privéleven" en "correspondentie" als bedoeld in artikel 8 van EVRM¹⁷.

¹⁶ Uit de commentaren bij de artikelen moeten "niet voor het publiek toegankelijke communicaties" worden begrepen als communicaties of elektronische communicaties binnen de persoonlijke levenssfeer. Het betreft een globaal begrip dat ook de woorden "privécommunicaties of telecommunicaties" dekken van het oude artikel 90ter.

¹⁷ zie meer bepaald het bovenvermelde *Klass et autres, §41 Malone vs. Groot-Brittannië*, 2 augustus 1984, §64, Serie A nr. 82 en *Lambert vs. Frankrijk* 24 augustus 1988, §21 *Receuil des arrêts et décisions* 1998-V

54. De Commissie stelt vast dat die maatregel slechts in uitzonderlijke gevallen bevolen kan worden omdat het onderzoek zulks vereist, er ernstige aanwijzingen zijn dat het een welbepaald misdrijf betreft en de andere onderzoeksmiddelen niet volstaan om de waarheid aan het licht te brengen.
55. De Commissie stelt eveneens vast dat in het arrest nr. 202/2004 van 21 december 2004 van het Grondwettelijk Hof over de wet van 6 januari 2003 betreffende de bijzondere onderzoeksmethoden en en enige andere onderzoeksmethoden, van oordeel was dat een inijkoperatie (artikel 89ter WSV) en de observatie met gebruik van technische hulpmiddelen om zicht te verwerven in een woning (artikel 56bis, tweede lid WSV.) maatregelen zijn die, wat betreft de inmenging in het recht op eerbiediging van het privéleven, vergeleken kunnen worden met de huiszoeking en met het afluisteren en opnemen van privécommunicaties en -telecommunicatie. Deze maatregelen kunnen volgens het Hof dan ook enkel worden toegestaan onder dezelfde voorwaarden als deze die gelden voor de huiszoeking en het afluisteren van telefoongesprekken.
56. Om die reden moeten de inijkoperatie en de observatie met gebruik van technische hulpmiddelen om zicht te verwerven in een woning, worden uitgesloten van 'de toepassings sfeer van het mini-onderzoek.
57. Dezelfde uitsluiting geldt voor de onderzoeksmaatregel van de heimelijke zoeking en kennisname van communicatie. Om die reden wordt deze maatregel geïntegreerd in artikel 90ter, §1 Sv, dat dezelfde kenmerken vertoont. De wijziging heeft niet enkel tot gevolg dat, naast de reeds bestaande maatregel van de interceptie van communicatie, de heimelijke zoeking in een informaticasysteem wordt toegevoegd. Ze leidt er eerder toe dat de twee maatregelen verenigd worden in één maatregel, om zich aan te passen aan de technologische evoluties die het onmogelijk maken om het verschil te maken tussen, enerzijds, de heimelijke zoeking in een informaticasysteem, en anderzijds, de interceptie van communicatie.
58. De Commissie neemt akte van het feit dat de "toevallige" of "doorzoekende" zoekingen niet mogen worden verricht. Artikel 90ter, §1, 4de lid Sv., omschrijft immers het doeleinde van de maatregel: De maatregel zal uitsluitend kunnen worden bevolen om gegevens te zoeken die de waarheid aan het licht kunnen brengen.
59. De Commissie is evenwel van mening dat de maatregel de waaier aan domeinen aanzienlijk uitbreidt die van nature het voorwerp uitmaken van een heimelijke zoeking en wenst de aandacht van de wetgever te vestigen op het feit dat deze uitbreiding het voorwerp moet uitmaken van een grondig parlementair debat.

60. Voor de maatregelen die de veiligheid en de vertrouwelijkheid van de persoonsgegevens waarborgen, neemt de Commissie er akte van dat artikel 90septies Sv. bepaalt dat "*de passende middelen worden aangewend om de integriteit en de vertrouwelijkheid van de opgenomen niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem te waarborgen*" en dat artikel 90octies, §2 Sv. bepaalt dat "*Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek* ».
61. De Commissie neemt er akte van dat iedere persoon die het voorwerp uitmaakte van de maatregel bedoeld in artikel 90ter Sv, ingelicht wordt van de aard van de maatregel en de data waarop die werd uitgevoerd (behalve wanneer de identiteit of het adres van die persoon niet redelijkerwijze kan worden teruggevonden).
62. Die informatie aan de betrokkene is in overeenstemming met de jurisprudentie van het Europees Hof van de Rechten van de Mens dat stelt dat "*la question de la notification ultérieure de mesures de surveillance est indissolublement liée au caractère effectif des recours judiciaires et donc à l'existence de garanties effectives contre les abus des pouvoirs de surveillance ; si on ne l'avise pas des mesures prises à son insu, l'intéressé ne peut guère, en principe, en contester rétrospectivement la légalité en justice* »¹⁸.

8. Analyse van artikel 33 van het voorontwerp - oprichting van een gegevensbank van stemafdrukken

63. Artikel 33 van het voorontwerp richt een gegevensbank op voor stemafdrukken die er toe strekt om met behulp van software de stem te herkennen van verdachten en veroordeelde personen van wie de stemafdruk reeds geregistreerd is in het kader van dossiers waarvoor een telefoon –of communicatietap (thans of in het verleden) is goedgekeurd door de bevoegde magistraat.
64. De Commissie meent dat een dergelijke gegevensbank inderdaad bij wet moet worden voorzien.

¹⁸ Weber et Saravia vs. Duitsland; Klass et autres vs. Duitsland

65. De Commissie merkt op dat enkel de stemafdrukken mogen worden bewaard van personen die het voorwerp uitmaakten van een tapmaatregel en die bedoeld worden in artikel 44/5, §3, 1° van de wet op het politieambt¹⁹ (verdachten en veroordeelde personen). Stemafdrukken van andere personen wiens stem opgenomen zijn bij een telefoon- of communicatietap, zoals getuigen of geheel toevallige betrokkenen, mogen niet worden aangemaakt of bewaard.
66. De Commissie herinnert eraan dat het Europees Hof voor Rechten van de Mens in zijn jurisprudentie meermaals heeft vastgesteld dat "*l'interception secrète de conversations téléphoniques entraine dans le champ d'application de l'article 8 pour ce qui est du droit au respect tant de la vie privée que de la correspondance. Certes, les enregistrements sont en général effectués dans le but d'utiliser le contenu de conversations d'une manière ou d'une autre, mais la Cour n'est pas convaincue que des enregistrements destinés à servir d'échantillons de voix puissent passer pour échapper à la protection qu'offre l'article 8. La voix de la personne concernée a tout de même été enregistrée sur un support permanent et soumise à un processus d'analyse directement destiné à identifier cette personne à la lumière d'autres données personnelles. (...) l'enregistrement et l'analyse de leurs voix à cette occasion doivent cependant être considérés comme relevant des données personnelles les concernant*"²⁰.
67. De Commissie neemt akte van het feit dat deze gegevensbank van stemafdrukken deel uitmaakt van de Algemene Nationale Gegevensbank (ANG) waarvan de doeleinden zijn bepaald onder artikel 44/7 van de wet op het politieambt. De beheersregels van de ANG als bedoeld in de artikelen 44/7 tot 44/11/1 van de wet op het politieambt zijn dus van toepassing. Hier is eveneens in een bewaartermijn voorzien van 10 jaar. Daarnaast is meteen ook de controle door het Controleorgaan op de politonele Informatie op deze gegevensbank gegarandeerd.

¹⁹ Wet van 5 augustus 1992 op het politieambt, *BS*. 22 december 1992.

²⁰ P.G. en J.H. vs. Groot-Brittannië - 44787/98. Arrest 25.9.2001

**OM DEZE REDENEN,
De Commissie,**

brengt een *gunstig* advies uit over het voorontwerp van wet betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties op voorwaarde dat rekening wordt gehouden met haar opmerkingen onder de punten 44 tot 48, 50 en 59.

De wnd. Administrateur ,

De Voorzitter,

(get.) An Machtens

(get.) Willem Debeuckelaere