Vast Comité van Toezicht
op de inlichtingen- en veiligheidsdiensten

Advies over de in België geldende regels ter bescherming van de privacy ten aanzien van middelen die toelaten op grote schaal gegevens van België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België) te onderscheppen en te exploiteren

Annemie Schaus
Gewoon hooglerares
Vice-rector academisch beleid
Université libre de Bruxelles

I. Korte beschrijving van de bekende context van de massale onderschepping van persoonsgegevens[1]

Enorme hoeveelheden persoonsgegevens werden onderschept door het programma *PRISM* , dat inlichtingen verzamelt op een nooit geziene schaal en niveau en waarvan het doel veel verder reikt dan het bestrijden van terrorisme of economische spionage.
Hoewel er onduidelijkheid blijft bestaan over de precieze feiten en vooral de rol van bepaalde betrokkenen, lijkt iedereen het eens over de omvang van de onderschepping, monitoring en exploitatie van persoonsgegevens. Na de eerste onthullingen over *PRISM* bevestigde de directeur van het *NSA* namelijk dat de dienst zowel binnen als buiten de Verenigde Staten metagegevens over communicatie verzamelt bij alle grote operatoren en deze metagegevens gedurende vijf jaar opslaat in een database.[2]
Het is ook bewezen dat het *GCHQ* hetzelfde type intercepties heeft verricht en dat grote operatoren van communicatienetwerken of sociale netwerken [3] grote hoeveelheden persoonsgegevens hebben bezorgd aan het *NSA*.

II. Toepasselijke wetgeving

Eerst en vooral moet er op worden gewezen dat er niet wordt getwijfeld aan de verenigbaarheid van het bestaan van de inlichtingendiensten met het Europees Verdrag tot bescherming van de rechten van de mens[4]. Zoals het Europees Hof voor de Rechten van de Mens benadrukte, kan de bescherming van de mensenrechten het bestaan van inlichtingendiensten vereisen, op voorwaarde dat hun methodes de fundamentele beginselen inzake de bescherming van de mensenrechten in acht nemen:*"Quel que soit le système de surveillance retenu, la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus. Cette appréciation ne revêt qu'un caractère relatif : elle dépend de toutes les circonstances de la cause, par exemple la nature, l'étendue et la durée des*

---

1 Zie het verslag van Mathias Vermeulen, "De Snowden-revelaties, massale datacaptatie en politieke spionage. Open bronnenonderzoek", 25 november 2013.

2 *Le programme de surveillance des Etats-Unis et leurs effets sur les droits fondamentaux des citoyens de l'UE,* Nota van het Directoraat-generaal intern beleid, Beleidsondersteunende afdeling C: Rechten van de burger en constitutionele zaken, IPOL-LIBE_NT(2013)474405_FR; zie ook het verslag van Mathias Vermeulen.

3 Onder andere *Facebook, Twitter, Microsoft, Google, Yahoo!, PalTalk, YouTube, Skype, AOL* en*Apple;* zie het verslag van Mathias Vermeulen.

4 Hierna EVRM.

mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, exécuter et contrôler, le type de recours fourni par le droit interne".[5] [6]
Het Hof benadrukt dat de bewegingsruimte van de Verdragsluitende Staten niet onbeperkt is om personen binnen hun jurisdictie te onderwerpen aan maatregelen van geheime monitoring. In het besef dat de democratie dreigt te worden miskend of zelfs vernietigd in een poging haar te beschermen, wijst het Hof erop dat de Staten niet om het even welke maatregelen mogen nemen die ze geschikt achten in naam van de strijd tegen spionage en terrorisme.
Ter zake moeten de beginselen van legaliteit, finaliteit en proportionaliteit in acht worden genomen zodra het legitiem doel is vastgesteld[7]. Dit betekent dat het juridisch arsenaal om de privacy en de persoonsgegevens te beschermen in acht moet worden genomen (A), maar ook de soevereiniteit van de Staat op het grondgebied waarvan de persoonsgegevens worden verzameld, opgeslagen en verwerkt (B). Voor zover de feiten die ons zijn voorgelegd dat mogelijk maken, zullen we analyseren in hoeverre de regels toepasselijk zijn op het massaal verzamelen van persoonsgegevens waarvan wij kennis hebben gekregen. Tot slot geven we een overzicht van de eventuele rechtsmiddelen (C).

A. Naleving van het recht op eerbiediging van het privéleven en bescherming van persoonsgegevens

In deze zaak kunnen verschillende wetsbepalingen ter bescherming van het recht op eerbiediging van het privéleven van toepassing zijn; die bepalingen vullen elkaar aan. We zullen die bepalingen beknopt toelichten, gaande van de bepaling met de meest algemene draagwijdte tot de bepaling met een specifieker doel, i.e. artikel 17 van het Verdrag inzake burgerrechten en politieke rechten (1); artikel 8 van het EVRM (2); Verdrag nr. 108 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens (3) en het recht van de Europese Unie: artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie (4), Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens [8] (zoals aangevuld door Richtlijn 2002/58/EG van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie) (5) en Richtlijn 2006/24/EG betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG [9] (6). Tot slot moet verwezen

---

5 EHRM, *Klass en anderen tegen Duitsland* van 6 september 1978; EHRM, *Vereniging weekblad Bluf! tegen Nederland* van 9 februari 1995 (vrije vertaling).

6 "Welk monitoringsysteem er ook wordt gebruikt, het Hof moet zich vergewissen van het bestaan van passende en voldoende garanties tegen misbruiken. Deze beoordeling is slechts van relatieve aard: ze is afhankelijk van alle omstandigheden van de zaak, zoals de aard, de omvang en de duur van eventuele maatregelen, de vereiste redenen om daartoe het bevel te geven, de bevoegde overheden om toelating te geven voor die maatregelen, ze uit te voeren en te controleren, het type verhaal krachtens het intern recht" (vrije vertaling).

7 Terwijl de bestrijding van terrorisme een geldig doel kan vormen, geldt dat niet noodzakelijk voor de economische profilering van individuen.

8 Hierna "Richtlijn 95/46".

9 Hierna "Richtlijn 2006/24".

worden naar het territoriaal toepassingsgebied van de Belgische wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens [10] [11]; het is niet duidelijk of die voorwaarden in casu vervuld zijn. In het kader van deze studie kunnen we deze wetgeving dus niet specifiek analyseren. Voor zover ze aansluit bij de bepalingen van internationaal recht en het ter zake toepasselijk Europees recht uitvoert, zijn de onderstaande analyses ook van toepassing op de bewuste wetgeving.

Vervolgens bekijken we hoe de eerbiediging van de normen inzake de bescherming van persoonsgegevens het voorwerp is geweest van het *Safe Harbor*-akkoord tussen de EU en de Verenigde Staten (7).

Op het vlak van de doorgifte, de monitoring, de controle en de bewaring van persoonsgegevens door middel van nieuwe technologieën moet – zoals Cécile de Terwangne en Jean-Noël Colin benadrukken [12] – privacy niet worden geïnterpreteerd in de klassieke betekenis, namelijk in die van bescherming van de persoonlijke, intieme, familiale of vertrouwelijke levenssfeer. Overeenkomstig de evolutie van het recht en de technologieën moet privacy worden begrepen als de mogelijkheid tot zelfbeschikking en autonomie en het vermogen van het individu om existentiële of informatieve keuzes te maken.[13] In overeenstemming met het Handvest van de grondrechten van de Europese Unie[14] gaat het om informatieve zelfbeschikking, i.e. het recht van het individu om kennis te hebben van de gegevens die op hem betrekking hebben en die worden bijgehouden, de kanalen te beheersen via dewelke die gegevens worden gecommuniceerd en het ongepast of bedrieglijk gebruik ervan te beletten. Op dit gebied is persoonlijke levenssfeer dus niet beperkt tot een zoeken naar privacy, maar gaat het om de beheersing door elk individu van zijn 'informatiebeeld'.[15] Dit gezegd zijnde en zoals het EHRM benadrukt, *"la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention".* [16] [17] Het is in deze betekenis dat persoonlijke levenssfeer hier moet worden begrepen.

---

10 Hierna "WBPL".

11 De WBPL is van toepassing op de verwerking van persoonsgegevens wanneer de verwerking wordt verricht in het kader van de effectieve en daadwerkelijke activiteiten van een vaste vestiging van de verantwoordelijke voor de verwerking op het Belgisch grondgebied, zoals aangegeven door artikel 3bis, 1°.

12 *Défis pour la vie privée et la protection des données posés par la technologie,* Verslag, Namen FNDP, februari 2011.

13 Voor de expliciete erkenning van een recht op zelfbeschikking of persoonlijke autonomie zoals vervat in het recht op eerbiediging van het privéleven van artikel 8 EVRM, zie EHRM, *Evans tegen Verenigd Koninkrijk,* arrest van 7 maart 2006 (bevestigd door de Grote Kamer in zijn arrest van 10 april 2007); *Tysiac tegen Polen*, arrest van 20 maart 2007; *Daroczy tegen Hongarije*, arrest van 1 juli 2008.

14 Zie *infra* en de volgende voetnoot.

15 Paul De Hert, Katja de Vries en Serge Gutwirth, Observatienota over het arrest van het Duits federaal Grondwettelijk Hof van 27 februari 2008, *Revue du droit des technologies et de l'information,* 2009, p. 87. In dit arrest kent het Hof op basis van het algemeen recht van persoonlijkheid een volkomen nieuw fundamenteel recht toe op de bescherming van "de vertrouwelijkheid en de integriteit van de technologische informatiesystemen". Dit nieuw fundamenteel recht inzake informatietechnologie moet lacunes in de bestaande fundamentele rechten aanvullen.

16 EHRM, *S. en Marper tegen Verenigd Koninkrijk* van 4 december 2008.

17 "speelt de bescherming van persoonsgegevens een fundamentele rol voor de uitoefening van het recht op eerbiediging van het privéleven en het familie- en gezinsleven zoals bekrachtigd door artikel 8 van het Verdrag" (vrije vertaling).

1. Artikel 17 van het Internationaal verdrag inzake burgerrechten en politieke rechten[18]

Artikel 17 van het IVBPR is de enige internationale bepaling met universele draagwijdte die het recht op eerbiediging van het privéleven garandeert. Net als de zusterbepalingen van dit artikel 17, die van dezelfde periode dateren, verwijst dit artikel nergens naar persoonsgegevens als onderdeel van het recht op eerbiediging van het privéleven. Echter wordt die privacy, die beschermd wordt door Artikel 17, op de proef gesteld door nieuwe inmengingen die mogelijk gemaakt worden door nieuwe technologieën. Daarom spoort de 35ste internationale conferentie van commissarissen voor privacy en gegevensbescherming de Staten ertoe aan algemene opmerking nr. 16 van het IVBPR van 1988 aan te nemen, om zo de bescherming van het privéleven te versterken.[19] Die opmerking stimuleert de creatie van een wereldwijd rechtskader voor de bescherming van persoonsgegevens en van de persoonlijke levenssfeer. De Verenigde Staten hebben deze opmerking niet aangenomen en dat is de reden waarom tal van voorstellen tot doel hebben om artikel 17 van het IVBPR zelf aan te passen aan het digitale tijdperk[20], aangezien de Verenigde Staten dat Verdrag hebben getekend. Anderen stellen voor om een bijkomend protocol aan te nemen op basis van Algemene Opmerking nr. 16 zoals goedgekeurd door de Algemene Vergadering van de Verenigde Naties in 1996.[21]
Onlangs heeft de derde Commissie van de Algemene Vergadering van de Verenigde Naties een tekst aangenomen over het recht op eerbiediging van het privéleven in het digitale tijdperk.[22] Ze beveelt de bescherming van de persoonlijke levenssfeer aan van personen, zowel offline als online, en vraagt alle Lidstaten om "het recht op eerbiediging van het privéleven in acht te nemen en te beschermen, meer bepaald in de context van de digitale communicatie".[23] De interpretatie die vandaag aan artikel 17 van het IVBPR kan worden gegeven, is dat de bescherming van dit artikel betrekking heeft op persoonsgegevens.

2. Artikel 8 van het EVRM

Artikel 8 van het EVRM verzekert aan eenieder het recht op eerbiediging van het privéleven. Het Europees Hof voor de Rechten van de Mens heeft de draagwijdte van het concept 'privéleven' uitdrukkelijk uitgebreid tot de bescherming van persoonsgegevens. Voor het Hof speelt de bescherming van persoonsgegevens een fundamentele rol voor de uitoefening van het recht op eerbiediging van het privéleven zoals bekrachtigd door artikel 8[24]. Het Hof oordeelt dat *" la protection offerte par l'article 8 serait affaiblie de manière inacceptable si l'usage des techniques*

---

18 Hierna "IVBPR".
19 http://www.unhchr.ch/tbs/doc.nsf/0/7dc7e7821c5da97680256523004a423d?Opendocument
20 http://www.franceonu.org/IMG/pdf/Vie_privee_FR.pdf
21 http://droitdu.net/2013/10/35eme-conference-internationale-des-commissaires-a-la-protection-des-donnees-et-de-la-vie-privee-une-volonte-duniformiser-la-protection-des-donnees-personnelles/
22 http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1&Lang=F
23 Artikel 4 van de tekst van de derde Commissie van de Algemene Vergadering van de Verenigde Naties.
24 Zie document "Case law of the European Court of Human Rights concerning the protection of personal data", DP(2013)CASE LAW, 30 januari 2013 [niet beschikbaar in het Nederlands], http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/DP%202013%20Case%20Law_Eng %20%28final%29.pdf.

scientifiques modernes dans le système de la justice pénale était autorisé à n'importe quel prix et sans une mise en balance attentive des avantages pouvant résulter d'un large recours à ces techniques, d'une part, et des intérêts essentiels s'attachant à la protection de la vie privée, d'autre part. " [25] [26]

Volgens het Hof brengt artikel 8 de verplichting mee dat het intern recht voorziet in passende garanties om elk ongepast en onrechtmatig gebruik van persoonsgegevens te voorkomen. De nationale wetgeving moet ook verzekeren dat de gegevens relevant en niet excessief zijn ten opzichte van de doeleinden waarvoor ze zijn opgeslagen en dat ze slechts worden bewaard gedurende de periode die vereist is voor de doeleinden waarvoor ze zijn opgeslagen, in een vorm die de identificatie van personen mogelijk maakt.

Het Hof wijst erop dat "*dans ce contexte comme dans celui des écoutes téléphoniques, de la surveillance secrète et de la collecte secrète de renseignements, il est essentiel de fixer des règles claires et détaillées régissant la portée et l'application des mesures et imposant un minimum d'exigences concernant, notamment, la durée, le stockage, l'utilisation, l'accès des tiers, les procédures destinées à préserver l'intégrité et la confidentialité des données et les procédures de destruction de celles-ci, de manière à ce que les justiciables disposent de garanties suffisantes contre les risques d'abus et d'arbitraire [...]*" [27]

Aldus oordeelde het Hof dat de opslag door een overheidsinstantie van gegevens over de persoonlijke levenssfeer van een individu een inmenging vormde in het recht op eerbiediging van zijn privéleven zoals gewaarborgd door artikel 8, lid 1 van het EVRM, en verduidelijkte dat het gebruik van die gegevens er weinig toe doet, meer bepaald in de volgende bewoordingen:

"De opslag door een overheidsinstantie van gegevens over de persoonlijke levenssfeer van een individu vormt een inmenging in de betekenis van artikel 8. Het later gebruik van de opgeslagen informatie is van weinig tel." (vrije vertaling). [28]

De inzameling en de bewaring van gegevens moeten dus de garanties inhouden die noodzakelijk zijn om het recht op eerbiediging van het privéleven van de individuen te beschermen.[29]

Op 1 juli 2008 veroordeelde het Hof (in een zaak met gelijkaardige feiten) het Verenigd Koninkrijk wegens inbreuk op artikel 8 voor het illegaal onderscheppen van communicatie te land door de inlichtingendienst *GCHQ,* van 1990 tot 1998. Het *GCHQ* onderschepte alle communicatie te land

---

25 EHRM, *S. en Marper tegen Verenigd Koninkrijk* van 4 december 2008.

26 "de bescherming geboden door artikel 8 op onaanvaardbare wijze zou worden verzwakt indien het gebruik van moderne wetenschappelijke technieken in het systeem van het strafrecht zou worden toegelaten tegen gelijk welke prijs en zonder nauwgezette afweging van enerzijds de voordelen die kunnen voortvloeien uit een grootschalig gebruik van die technieken en anderzijds de essentiële belangen van de bescherming van het privéleven" (vrije vertaling).

27 "het in deze context, net als in die van het afluisteren van telefoongesprekken, het geheim toezicht en de geheime inzameling van inlichtingen, van wezenlijk belang is om duidelijke en gedetailleerde regels vast te leggen die de draagwijdte en de toepassing van de maatregelen vastleggen en een minimum aan vereisten opleggen betreffende meer bepaald de duur, de opslag, het gebruik, de toegang door derden, de procedures met het oog op het beschermen van de integriteit en de vertrouwelijkheid van de gegevens en de procedures tot vernietiging van die gegevens, zodat de rechtsonderhorigen voldoende garanties genieten tegen de risico's van misbruik en willekeur […]" (vrije vertaling).

28 EHRM, *Leander tegen Zweden* van 26 maart 1987; *Kopp tegen Zwitserland* van 25 maart 1998; *Amann tegen Zwitserland* van 16 februari 2000; *Association '21 Décembre 1989' en anderen tegen Roemenië* van 24 mei 2011.

29 EHRM, *Rotaru tegen Roemenië* van 4 mei 2000.

(fax, e-mail, telex en informatica) vanuit en naar de Ierse Republiek via de toren van *Capenhurst,* die binnen een kerncentrale ligt en 24 uur per dag operationeel is. De toren van *Capenhurst* diende niet alleen om informatie over terrorisme te verzamelen, maar werd ook gebruikt in het kader van economische spionage en voor het onderscheppen van diplomatieke communicatie van Ierland en persoonlijke communicatie van vooraanstaande Ieren, met behulp van specifieke lijsten van telefoonnummers of systemen van stemherkenning[30].

Het EHRM is ook van mening dat de Staten verplicht zijn om een doeltreffende procedure in te voeren die het de belanghebbenden mogelijk maakt toegang te hebben tot de documenten die de veiligheidsdiensten over hen verzamelen.[31]

De grootschaligheid van de interceptie, waarbij zonder onderscheid te werk wordt gegaan, de monitoring, het gebruik en de bewaring van persoonsgegevens waarvan in deze zaak sprake is, zijn in alle opzichten duidelijk strijdig met artikel 8; de gelaakte maatregelen hebben op onbepaalde wijze betrekking op private of publieke natuurlijke of rechtspersonen; de slachtoffers zijn meestal niet-identificeerbaar; deze maatregelen steunen op geen enkele geldige wettelijke basis en miskennen integendeel het recht dat van toepassing is op de doorgifte van persoonsgegevens; ze staan kennelijk niet in verhouding tot de beoogde doelstellingen, die zelf ook niet gedefinieerd zijn.

Omdat sommige actoren die aan dit systeem zouden hebben deelgenomen privépersonen zouden kunnen zijn, past het te benadrukken dat artikel 8 van het EVRM een horizontaal effect kan hebben.

Al in 1979 benadrukte het Europees Hof voor de Rechten van de Mens immers het volgende:

"Si l'article 8 a essentiellement pour objet de prémunir l'individu contre les ingérences arbitraires des pouvoirs publics, il ne se contente pas de commander à l'État de s'abstenir de pareilles ingérences : à cet engagement plutôt négatif s'ajoutent des obligations positives inhérentes à un respect effectif de la vie privée ou familiale. Elles peuvent impliquer l'adoption de mesures visant au respect de la vie privée jusque dans les relations des individus entre eux". [32] [33]

In het arrest *Soderman tegen Zweden* van 12 november 2013 wijst het Hof erop dat wanneer een bijzonder belangrijk aspect van het bestaan of de identiteit van een individu op het spel staat of de betrokken activiteiten betrekking hebben op een van de intiemste aspecten van het privéleven, de Staat nog minder bewegingsruimte heeft om de verplichting voor de particulieren te reglementeren.[34]

In hun activiteiten die afbreuk kunnen doen aan het recht op eerbiediging van het privéleven van individuen of publieke of private rechtspersonen vormt de eerbiediging van het privéleven duidelijk een verplichting voor providers van sociale netwerken, voor handelsondernemingen die actief zijn op het gebied van de nieuwe technologieën en voor andere verantwoordelijken voor de

---

30 EHRM, *Liberty en andere ngo's tegen het Verenigd Koninkrijk* van 1 juli 2008.

31 EHRM, *Joanna Szulc tegen Polen* van 13 november 2012.

32 EHRM, *Airey tegen Ierland* van 9 oktober 1979.

33 "Hoewel artikel 8 voornamelijk tot doel heeft het individu te beschermen tegen de willekeurige inmenging van het openbaar gezag, beperkt het zich er niet toe aan de Staat te bevelen zich te onthouden van dergelijke inmenging: deze veeleer negatieve verbintenis gaat gepaard met positieve verplichtingen die inherent zijn aan de daadwerkelijke eerbieding van het privé-, familie- en gezinsleven. Die verplichtingen kunnen impliceren dat er maatregelen worden getroffen met het oog op de eerbiediging van het privéleven tot in de onderlinge relaties tussen individuen" (vrije vertaling).

34 Zie ook o.a. EHRM, *I.B. tegen Griekenland* van 3 oktober 2013.

verwerking van persoonsgegevens, onder voorbehoud welteverstaan van een onderzoek in elk bijzonder geval van de territoriale werkingssfeer van de activiteit van die providers.[35]

3. Verdrag nr. 108 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens

Verdrag nr. 108 van de Raad van Europa tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens is het enige bindende specifieke rechtsinstrument voor alle Lidstaten van de Raad van Europa op dit gebied. De beginselen zijn de volgende:

- beginsel van eerlijkheid, rechtmatigheid en evenredigheid met het doel (gegevens opgeslagen voor expliciete en legitieme doeleinden die niet worden gebruikt op een manier die onverenigbaar is met die doeleinden)
- beginsel van kwaliteit van de gegevens (relevant, passend, actueel, bewaard voor beperkte duur)
- specifieke regeling voor gevoelige gegevens
- vereiste inzake veiligheid
- recht op toegang, rectificatie en beroep
- mogelijkheid tot afwijking in naam van doorslaggevende publieke of private belangen

In 2001 werd het Verdrag aangevuld met een bijkomend protocol betreffende de toezichthoudende autoriteiten en de grensoverschrijdende gegevensstromen. Het Verdrag nr. 108 is een van de beste rechtsinstrumenten om individuen te beschermen tegen de risico's die gepaard gaan met elektronische monitoring. Het verleent namelijk uitgebreide rechten, zoals een recht van toegang, verbetering of schrapping van persoonsgegevens.
Momenteel wordt het Verdrag gemoderniseerd[36] teneinde de leemtes te vullen die het jammer genoeg nog bevat ten opzichte van de technologische uitdagingen, meer bepaald met betrekking tot de extraterritoriale toepassing.[37]

4. Artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie

Artikel 7 waarborgt het recht op eerbiediging van het privéleven in aansluiting op de overige instrumenten die de mensenrechten beschermen. Artikel 8 heeft een meer originele draagwijdte en bepaalt dat eenieder recht heeft op bescherming van de hem betreffende persoonsgegevens

---

35 Voor Richtlijn 95/46, zie *infra.*

36 Voorstel tot modernisering van het Raadgevend comité van het Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens, 18 december 2012, STE nr. 108 (T-PD); zie ontwerpaanbeveling http://www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/T-PD%282013%295rev_fr_Projet%20de%20Rec.%20emploi.pdf; Over de herziening van *Verdrag nr. 108* Staat van de werkzaamheden in uitvoering: www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_fr.asp

37 *Rapport sur les lacunes de la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques,* Cécile de Terwangne, Jean-Philippe Moiny, Yves Poullet en Jean-Marc Van Gyzeghem, November 2010, Bureau van het Raadgevend Comité van het Verdrag nr. 108.

en dat deze gegevens eerlijk moeten worden verwerkt, voor bepaalde doeleinden en op basis van een gerechtvaardigde grondslag (toestemming of andere grondslag waarin de wet voorziet), alsook dat eenieder recht heeft op toegang tot en rectificatie van de over hem verzamelde gegevens. Artikel 7 bekrachtigt dus een autonoom recht op bescherming van persoonsgegevens.
Zoals advocaat-generaal Pedro Cruz Villalon onderstreept in zijn conclusies van 12 december ll.[38], bekrachtigt artikel 8 van het Handvest het recht op bescherming van persoonsgegevens als een recht dat zich onderscheidt van het recht op eerbiediging van het privéleven. Terwijl de bescherming van persoonsgegevens ertoe strekt de eerbiediging van het privéleven te waarborgen, is ze vooral onderworpen aan een autonome regeling die voornamelijk wordt gedefinieerd door Richtlijn 95/46, Richtlijn 2002/58, Verordening nr. 45/2001 en Richtlijn 2006/24, alsook, op het domein dat valt onder de politiële en justitiële samenwerking in strafzaken, door kaderbesluit 2008/977/JBZ.[39]
Omdat de 'privésfeer' de kern van de 'persoonlijke levenssfeer' vormt, valt omgekeerd niet uit te sluiten dat een regelgeving die het recht op bescherming van persoonsgegevens in overeenstemming met artikel 8 van het Handvest beperkt, niettemin kan worden geacht een buitensporige inbreuk op artikel 7 van het Handvest te vormen.[40]
Natuurlijk berust het recht op bescherming van persoonsgegevens op het fundamenteel recht op eerbiediging van het privéleven. Net als het HJEU kunnen we zeggen dat "*les articles 7 et 8 de la Charte sont étroitement liés, au point de pouvoir être considérés comme établissant un « droit à la vie privée à l'égard du traitement des données à caractère personnel*"[41] [42]

5. Richtlijn 95/46/EG van 24 oktober 1995

Richtlijn 95/46 van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, die in oktober 1998 in werking is getreden, is de basisnorm in het afgeleid communautair recht. Richtlijn 95/46 heeft tot doel aan de Lidstaten de verplichting op te leggen het recht op eerbiediging van de persoonlijke levenssfeer van natuurlijke personen ten aanzien van de verwerking van hun persoonsgegevens te waarborgen teneinde het vrije verkeer van die gegevens tussen de Lidstaten mogelijk te maken.
Bijgevolg legt ze de inachtneming op van regels die de voorwaarden van rechtmatigheid van de verwerking van persoonsgegevens bepalen, met vermelding van de rechten van personen wiens gegevens worden ingezameld en verwerkt (recht op informatie, recht op toegang en rectificatie of recht van verzet en recht op beroep, en recht op de vertrouwelijkheid en veiligheid van de verwerking).
Deze richtlijn werd aangevuld door Richtlijn 2002/58 van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector

---

38 Conclusies van advocaat-generaal Pedro Cruz Villalon van 12 december 2013 in de zaken C-293/12 en C-494/12 die hangende zijn voor het HJEU.
39 Zie *infra.*
40 Conclusies van advocaat-generaal Pedro Cruz Villalon, voornoemd.
41 Arresten C-92/09 en C-93/09 van 9 november 2010.
42 "artikelen 7 en 8 van het Handvest nauw met elkaar zijn verbonden, in die mate dat ze kunnen worden geacht een recht op eerbiediging van het privéleven ten aanzien van de verwerking van persoonsgegevens te vestigen" (vrije vertaling).

elektronische communicatie, die de vertrouwelijkheid van elektronische communicatie waarborgt. De verplichting om deze vertrouwelijkheid te waarborgen ligt bij de aanbieders van voor het publiek toegankelijke elektronische-communicatiediensten. Ze brengt voor de Lidstaten ook de verplichting mee, behoudens uitzondering, om de vertrouwelijkheid te waarborgen van niet alleen de communicatie, maar ook de verkeersgegevens van abonnees en gebruikers van elektronische-communicatiediensten. Artikel 6 verplicht aanbieders van elektronische-communicatiediensten ertoe om verkeersgegevens met betrekking tot abonnees en gebruikers die worden verwerkt en opgeslagen, te wissen of anoniem te maken.

- Beginselen

Richtlijn 95/46 heeft tot doel de rechten en vrijheden van personen te beschermen ten opzichte van de verwerking van persoonsgegevens, door beginselen vast te stellen tot bepaling van de rechtmatigheid van die verwerkingen.
Die beginselen[43] hebben betrekking op:

- de kwaliteit van de gegevens: persoonsgegevens moeten meer bepaald eerlijk en rechtmatig worden verwerkt en moeten worden ingezameld om welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Bovendien moeten ze nauwkeurig zijn en zo nodig worden bijgewerkt;
- de toelaatbaarheid van de gegevensverwerking: persoonsgegevens mogen alleen worden verwerkt indien de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend of wanneer de verwerking noodzakelijk is:
- voor de uitvoering van een overeenkomst waarbij de betrokkene partij is; of
- om een wettelijke verplichting na te komen waaraan de verantwoordelijke voor de verwerking onderworpen is; of
- ter vrijwaring van een vitaal belang van de betrokkene; of
- voor de vervulling van een taak van algemeen belang; of
- voor de behartiging van het gerechtvaardigd belang van de verantwoordelijke voor de verwerking;
- bijzondere categorieën van verwerking: verboden is de verwerking van persoonsgegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt, alsook de verwerking van gegevens die de gezondheid of het seksuele leven betreffen. Deze bepaling is onder voorbehoud voor bijvoorbeeld het geval waarin de verwerking noodzakelijk is met het oog op de verdediging van de vitale belangen van de betrokkene of voor de doeleinden van preventieve geneeskunde of medische diagnose;
- informatie van de personen die betrokken zijn bij de gegevensverwerking: bepaalde gegevens (identiteit van de verantwoordelijke voor de verwerking, doeleinden van de verwerking, ontvangers van de gegevens …*)* moeten door de verantwoordelijke voor de verwerking worden verstrekt aan de persoon bij wie hij gegevens betreffende die persoon verzamelt;

---

[43] Zie synthese van de wetgeving op: http://europa.eu/legislation_summaries/information_society/data_protection/l14012_nl.htm (december 2013)

- het recht van toegang van die personen tot de gegevens: elke betrokkene moet het recht hebben om van de verantwoordelijke voor de verwerking de volgende zaken te verkrijgen:
- uitsluitsel omtrent het al dan niet bestaan van verwerkingen van gegevens betreffende hem en verstrekking van de gegevens die zijn verwerkt;
- de rectificatie, de uitwissing of de afscherming van de gegevens waarvan de verwerking niet overeenstemt met de bepalingen van deze richtlijn, met name op grond van het onvolledige of onjuiste karakter van de gegevens, net als kennisgeving van deze wijzigingen aan derden aan wie de gegevens zijn verstrekt;
- uitzonderingen en beperkingen: de reikwijdte van de beginselen betreffende de kwaliteit van de gegevens, de informatieverstrekking aan de betrokkene, het recht van toegang en de openbaarheid van de verwerkingen kan worden beperkt ter vrijwaring, onder meer, van de veiligheid van de Staat, de landsverdediging, de openbare veiligheid, het vervolgen van strafbare feiten, een belangrijk economisch en financieel belang van een Lidstaat of van de EU of de bescherming van de betrokkene;
- het recht van verzet tegen gegevensverwerking: de betrokkene moet het recht hebben zich om gerechtvaardigde redenen te verzetten tegen de verwerking van gegevens die op hem betrekking hebben. De betrokkene moet zich, op verzoek en kosteloos, ook kunnen verzetten tegen de verwerking van gegevens met het oog op direct marketing. Tot slot moet de betrokkene worden ingelicht voordat persoonsgegevens aan derden worden verstrekt voor direct marketing en moet hij het recht ter kennis gebracht krijgen zich tegen deze verstrekking te kunnen verzetten;• de vertrouwelijkheid en beveiliging van de verwerking: eenieder die handelt onder het gezag van de verantwoordelijke voor de verwerking of van de verwerker alsmede de verwerker zelf, die toegang heeft tot persoonsgegevens, mag deze slechts in opdracht van de verantwoordelijke voor de verwerking verwerken. Voorts moet de verantwoordelijke voor de verwerking passende maatregelen nemen om persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang;
- aanmelding van de verwerking bij een toezichthoudende autoriteit: de verantwoordelijke voor de verwerking moet de nationale toezichthoudende autoriteit van tevoren kennis geven van de uitvoering van een verwerking. Na ontvangst van de kennisgeving voert de toezichthoudende autoriteit voorafgaande onderzoeken uit naar mogelijke risico's voor de rechten en vrijheden van de betrokkenen. De openbaarheid van de verwerkingen moet worden gewaarborgd en de toezichthoudende autoriteit moeten een register bijhouden van de aangemelde verwerkingen.

Eenieder kan zich tot de rechter wenden wanneer de rechten die hem worden gegarandeerd door het op de betrokken verwerking toepasselijke nationale recht geschonden worden. Bovendien hebben personen die schade hebben geleden ten gevolge van een onrechtmatige verwerking van hun persoonsgegevens het recht vergoeding van de geleden schade te verkrijgen.

- Territoriale werkingssfeer

Deze richtlijn brengt verplichtingen mee voor de aanbieders van internettoegang, zoekmachines, sociale netwerken en andere aanbieders van communicatiediensten die verantwoordelijk zijn voor

de verwerking van persoonsgegevens. In ieder afzonderlijk geval kan de omvang van de aansprakelijkheid van de verantwoordelijke voor de gegevensverwerking worden geanalyseerd, meer bepaald ten aanzien van de territoriale werking van Richtlijn 95/46. Krachtens artikel 4 van de richtlijn moet een Staat zijn wetgeving inzake de bescherming van persoonsgegevens ter uitvoering van deze richtlijn toepassen indien de verantwoordelijke voor de verwerking vestiging heeft op zijn grondgebied of in functie van de plaats van de middelen voor de gegevensverwerking, dit wil zeggen indien de middelen voor gegevensverwerking op het grondgebied van deze Staat bevinden.
De werkgroep 'Artikel 29'[44] benadrukte in zijn advies 5/2009 over de bescherming van gegevens door online sociale netwerken[45] dat
''De richtlijn gegevensbescherming is in de meeste gevallen van toepassing op aanbieders van sociale-netwerkdiensten, ook als hun hoofdkantoor buiten de EER is gevestigd.''
Ook een van de voornaamste conclusies van advies 1/2008 over gegevensbescherming en zoekmachines bepaalt dat de richtlijn inzake gegevensbescherming algemeen van toepassing is op de verwerking van persoonsgegevens door zoekmachines, ook al staat hun hoofdkantoor buiten de EER, en dat het aan de betreffende zoekmachines toekomt duidelijk te maken welke rol zij spelen in de EER en hoe ver hun verantwoordelijkheden overeenkomstig de richtlijn reiken.[46]
De doorgifte van persoonsgegevens van een Lidstaat naar een derde land met een passend niveau van bescherming is toegelaten. Dergelijke doorgiftes zijn echter niet toegelaten wanneer ze bestemd zijn voor een derde land dat niet over een dergelijk niveau van bescherming beschikt, behoudens afwijkingen die op beperkende wijze worden opgesomd.
Bijgevolg past het om de verantwoordelijkheid van elke speler te bepalen in functie van precieze feiten.

- Uitsluitingen van de materiële werkingssfeer

Artikel 3, lid 2 van voornoemde richtlijn geeft een van de grenzen van de materiële werkingssfeer van de richtlijn aan en bepaalt:
''De bepalingen van deze richtlijn zijn niet van toepassing op de verwerking van persoonsgegevens:

- die met het oog op de uitoefening van niet binnen de werkingssfeer van het Gemeenschapsrecht vallende activiteiten geschiedt zoals die bedoeld in de titels V en VI van het Verdrag betreffende de Europese Unie en in ieder geval verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de Staat (waaronder de economie van de Staat, wanneer deze verwerkingen in verband staan met vraagstukken van Staatsveiligheid), en de activiteiten van de Staat op strafrechtelijk gebied''.

De bescherming van persoonsgegevens in het kader van de openbare veiligheid en het strafrecht wordt dus geregeld in verschillende specifieke instrumenten. Het gaat met name om instrumenten waarbij gemeenschappelijke informatiesystemen op Europees niveau worden ingesteld, zoals de Schengenuitvoeringsovereenkomst met specifieke gegevensbeschermingsbepalingen die gelden

---

44 Deze werkgroep werd opgericht krachtens artikel 29 van Richtlijn 95/46. Het is een Europees adviesorgaan, van wie de taken worden beschreven in artikel 30 van de Richtlijn en in artikel 15 van Richtlijn 2002/58.
45 Groep 29, WP 163 "Advies 5/2009 over online sociale netwerken" van 12 juni 2009.
46 Groep 29, WP 148 "Advies 1/2008 over gegevensbescherming en zoekmachines" van 4 april 2008.

voor het Schengeninformatiesysteem (SIS); de overeenkomst op grond van artikel K.3 van het Verdrag betreffende de Europese Unie tot oprichting van een Europese Politiedienst; het besluit van de Raad betreffende de oprichting van Eurojust en de beschikkingen van het interne reglement van Eurojust betreffende de verwerking en bescherming van persoonsgegevens; de Overeenkomst op grond van artikel K.3 van het Verdrag betreffende de Europese Unie inzake het gebruik van informatica op douanegebied, met de gegevensbeschermingsbepalingen die van toepassing zijn op het douane-informatiesysteem, en de Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de Lidstaten van de Europese Unie.[47] Op 27 november 2008 keurde de Raad kaderbesluit 2008/977/JBZ van de Raad goed over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en gerechtelijke samenwerking in strafzaken. Deze is echter alleen van toepassing op de doorgifte van gegevens tussen Lidstaten (artikelen 26 en 13).

6. Richtlijn 2006/24/EG betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van elektronische communicatiediensten

Richtlijn 2006/24 is in deze belangrijk omdat ze wijzigingen aanbrengt aan richtlijnen 95/46 en 2002/58 door te bepalen dat de Lidstaten een verplichting moeten opleggen inzake het verzamelen en bewaren van verkeers- en lokalisatiegegevens, namelijk door aan de aanbieders van openbaar beschikbare elektronische communicatiediensten of openbare communicatienetwerken verplichtingen op te leggen inzake de bewaring van de verkeers- en lokalisatiegegevens die zij bepaalt, teneinde hun beschikbaarheid te waarborgen "voor het onderzoeken, opsporen en vervolgen van zware criminaliteit zoals gedefinieerd in de nationale wetgevingen van de Lidstaten". Aldus wijkt deze richtlijn af van de afwijkende regels zoals vastgesteld door artikel 15, lid 1 van Richtlijn 2002/58 die de mogelijkheid regelen, voor de Lidstaten, om de reikwijdte van het recht op bescherming van persoonsgegevens en, algemener, het recht op eerbiediging van het privéleven in het specifieke kader van de levering van elektronische communicatiediensten of openbare communicatienetwerken te beperken om de redenen zoals bepaald in artikel 13, lid 1 van Richtlijn 95/46.
Richtlijn 2006/24 heeft tot doel een harmonisatie tot stand te brengen van de regelgevingen van de Lidstaten betreffende de bewaring van verkeers- en lokalisatiegegevens inzake elektronische communicatie en legt bijgevolg aan de Lidstaten die niet over dergelijke regelgeving zouden beschikken, een verplichting op om de voornoemde gegevens te verzamelen en te bewaren.
Volgens advocaat-generaal Pedro Cruz Villalon (12 december 2013) is deze verplichting die de richtlijn aan de Lidstaten oplegt in strijd met het Handvest van de grondrechten.[48] Het HJEU moet nog een arrest vellen.
Het is interessant om de motivering van de advocaat-generaal hier over te nemen[49] :
"72. Dat neemt niet weg dat het verzamelen en vooral het bewaren, in gigantische databases, van de talloze gegevens die zijn gegenereerd of verwerkt in het kader van het grootste deel van de gebruikelijke elektronische communicatie van de burgers van de Unie, een duidelijke inmenging in

---

47 HJEU, arresten C-317/04 en C-318/04 van 30 mei 2005, conclusies van advocaat-generaal LEGER, punt 41.
48 Conclusies in de zaken C-293/12 en C-494/12 die hangende zijn voor het HJEU.
49 De verwijzingen zijn weggelaten met het oog op de leesbaarheid; zie de verwijzing in de vorige voetnoot.

hun privéleven vormt, ook al worden daarmee enkel de voorwaarden geschapen om achteraf hun persoonlijke alsook beroepsmatige activiteiten te kunnen controleren. Het verzamelen van deze gegevens creëert de voorwaarden voor een toezicht dat, ook al wordt dit slechts met terugwerkende kracht uitgevoerd bij de exploitatie van de gegevens, niettemin, zolang de gegevens worden bewaard, het recht van de burgers van de Unie op vertrouwelijkheid van hun persoonlijke levenssfeer permanent bedreigt. Het opgewekte vage gevoel van gecontroleerd worden leidt bijzonder acuut tot de vraag wat de bewaringstermijn van de gegevens is.
73. Dienaangaande moet ten eerste rekening worden gehouden met het feit dat de gevolgen van deze inmenging worden verveelvoudigd door de plaats die de elektronische communicatiemiddelen in de moderne samenleving hebben ingenomen, of het nu gaat om digitale mobiele netwerken dan wel om internet, en het massale en intensieve gebruik ervan door een zeer groot deel van de Europese burgers op alle terreinen van hun privé - of beroepsactiviteiten.
74. De betrokken gegevens, zo wil ik nogmaals benadrukken, zijn geen persoonsgegevens in de klassieke zin des woords die verband houden met precieze informatie over de identiteit van personen, maar in feite 'gekwalificeerde' persoonsgegevens, die, wanneer zij worden geëxploiteerd, een belangrijk deel van het gedrag van een persoon, dat strikt onder zijn privéleven valt, op getrouwe en uitputtende wijze in kaart kunnen brengen of zelfs een volledig en precies beeld kunnen schetsen van zijn privé-identiteit.
75. De intensiteit van deze inmenging wordt des te duidelijker door factoren die het risico vergroten dat de bewaarde gegevens, ondanks de verplichtingen die door richtlijn 2006/24 aan zowel de lidstaten zelf als de aanbieders van elektronische communicatiediensten worden opgelegd, worden gebruikt voor onrechtmatige doeleinden die potentieel inbreuk maken op het privéleven, of ruimer, voor frauduleuze of zelfs kwaadwillende doeleinden.
76. Deze gegevens worden namelijk niet bewaard door de autoriteiten zelf of zelfs maar onder hun directe toezicht, maar door de aanbieders van elektronische communicatiediensten, op wie het merendeel van de verplichtingen rust die als waarborg van de bescherming en de veiligheid van de gegevens moeten dienen.''
En verder:
"102. De duidelijke inmenging in recht op eerbiediging van het privéleven die de lidstaten, als gevolg van de constitutieve werking van richtlijn 2006/24 geacht worden op te nemen in hun eigen rechtsorde, lijkt aldus buiten verhouding te staan tot enkel de noodzaak om de werking van de interne markt te waarborgen, ook al worden dit verzamelen en bewaren overigens als geschikte en zelfs noodzakelijke middelen beschouwd ter bereiking van de uiteindelijke doelstelling van de richtlijn, namelijk ervoor zorgen dat de gegevens beschikbaar zijn voor het opsporen en vervolgen van zware criminaliteit. Samenvattend zou richtlijn 2006/24 de evenredigheidstoets niet doorstaan op basis van de redenen die de keuze van haar rechtsgrondslag rechtvaardigden. Paradoxaal genoeg zouden de redenen die haar sauveerden vanuit het oogpunt van de rechtsgrondslag, de redenen zijn waarom zij geen stand houdt in het licht van de evenredigheid.''
Alvorens te besluiten:
"131. Concluderend meen ik dat richtlijn 2006/24 in haar geheel onverenigbaar is met artikel 52, lid 1, van het Handvest, aangezien de beperkingen die zij aan de uitoefening van de grondrechten stelt door de opgelegde verplichting tot het bewaren van gegevens, niet gepaard gaan met de

onmisbare beginselen die hebben te gelden voor de waarborgen waarmee de toegang tot deze gegevens en de exploitatie ervan behoren te zijn omkleed."

7. *Safe Harbor*-akkoord ('veilige haven') – Beschikking van de Commissie van 26 juli 2000 [50]

De normen inzake bescherming van de persoonlijke levenssfeer in Europa enerzijds en de Verenigde Staten anderzijds verschillen duidelijk van elkaar en meer bepaald in de Verenigde Staten biedt het recht op eerbiediging van het privéleven zoals hierboven omschreven nagenoeg geen bescherming voor wie niet in de VS verblijft.[51]
Het bleek dan ook noodzakelijk om een rechtskader te creëren dat geschikt is om de doorgifte van gegevens voor commerciële doeleinden van de Europese Economische Ruimte[52] naar de Verenigde Staten mogelijk te maken.
Dit rechtskader was des te noodzakelijker omdat, zoals we hebben gezien, de specifieke regels van Richtlijn 95/46 betreffende het uitwisselen van gegevens met derde Staten de doorgifte verbiedt van persoonsgegevens buiten Staten die geen lid zijn van de EER en die minder bescherming van persoonsgegevens zouden bieden dan de EER.
De Verenigde Staten beschikken over een systeem voor de bescherming van de gegevens van hun burgers dat niet voldoet aan dezelfde normen degene die binnen de EER zijn aangenomen. Zonder het *Safe Harbor*-systeem hadden de door Richtlijn 95/46 ingestelde vereisten een obstakel kunnen vormen voor de trans-Atlantische uitwisselingen en transacties, omdat het gebrek aan naleving van de Europese regels betreffende persoonsgegevens door een Amerikaanse onderneming de commerciële onderhandelingen had kunnen vertragen of opschorten of zelfs had kunnen leiden tot gerechtelijke vervolgingen in geval van schending van de toepasselijke regels.
Het rechtskader van de 'veilige haven' of *Safe Harbor* slaat de brug tussen beide visies op de eerbiediging van het privéleven door een gemeenschappelijke noemer in het leven te roepen die Amerikaanse ondernemingen en organisaties in acht moeten nemen en die de doorgifte van persoonsgegevens mogelijk maakt met inachtneming van het recht van de EER.
Het *Safe Harbor*-akkoord werd gesloten tussen de Amerikaanse *Federal Trade Commission* (*FTC*) en de Europese Commissie met als doel Amerikaanse ondernemingen in staat stellen te certificeren dat ze de EER-wetgeving in acht nemen om aldus de toelating te verkrijgen persoonsgegevens voor commerciële doeleinden door te geven van de EER naar de Verenigde Staten.
Bijlage I van de beschikking van 26 juli 2000 bepaalt dat "persoonsgegevens en persoonlijke informatie gegevens zijn over een specifieke of een identificeerbare persoon die binnen de

---

50 Beschikking van de Commissie van 26 juli 2000 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende vaak gestelde vragen, die door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd document C(2000) 2441 (http://eur lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:NL:PDF)

51 Nota van het Directoraat-generaal intern beleid, Beleidsondersteunende afdeling C: Rechten van de burgers en constitutionele zaken, IPOL-LIBE_NT(2013)474405_FR.

52 Hierna "EER"; *Safe Harbor* werd opgenomen in het akkoord over de EER, zodat IJsland, Liechtenstein en Noorwegen niet worden beschouwd als derde Staten bij de toepassing van deze norm.

werkingssfeer van de richtlijn vallen, vanuit de Europese Unie door een organisatie in de Verenigde Staten worden ontvangen en in de een of andere vorm zijn vastgelegd.''
Indien een Amerikaanse onderneming schriftelijk verklaart de Veiligehavenbeginselen te onderschrijven, dan zou de Europese onderneming in principe persoonsgegevens naar die onderneming moeten kunnen uitvoeren.

- Beginselen

Het rechtskader van *Safe Harbor* berust op zeven beginselen die de onderneming die de certificering wenst te verkrijgen in acht moet nemen. Deze beginselen worden uitvoerig beschreven in Bijlage I van de Beschikking van de Commissie van 26 juli 2000 betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen en zijn grotendeels geïnspireerd op de beginselen van Richtlijn 95/46:

- Kennisgeving: in kennis stellen van personen,
- Keuze: de mogelijkheid voor de betrokkene om zich te verzetten tegen een doorgifte aan derden of tegen het gebruik van de gegevens om andere doeleinden, de expliciete toestemming van de personen voor het verzamelen van gevoelige informatie,
- Verdere doorgifte: de beginselen inzake kennisgeving en keuze zouden van toepassing moeten zijn op de doorgifte van gegevens aan derden,
- Beveiliging: maatregelen tot bescherming van de gegevens,
- Integriteit van de gegevens: kwaliteit en gepastheid van de gegevens,
- Toegang: het recht op toegang, correctie, verwijdering van gegevens,
- Rechtshandhaving: recht op verhaal, procedures van opvolging en sancties.[53]

Op te merken valt echter dat de beginselen worden omschreven in vage bewoordingen die open staan voor een interpretatie die bovendien onderworpen is aan het Amerikaans recht.
Het proces berust op een systeem van vrijwillige zelfcertificering door Amerikaanse ondernemingen en voorziet in een hernieuwing van de certificering om de twaalf maanden. De onderneming die een certificering wenst te verkrijgen, moet aan de *Federal Trade Commission* een jaarlijkse schriftelijke verklaring bezorgen waarin ze bevestigt de Veiligehavenbeginselen in acht te nemen. De *Federal Trade Commission* heeft de taak het certificeringsprogramma te beheren en te waken over de uitvoering ervan. Ze kan vorderingen in rechte instellen tegen een onderneming die in gebreke blijft of administratieve boetes opleggen aan ondernemingen die ondanks hun verklaring de Veiligehavenbeginselen *de facto* niet in acht nemen.
Eens de Amerikaanse onderneming een *Safe Harbor*-certificering heeft verkregen, wordt ze toegevoegd aan de lijst van geaccrediteerde ondernemingen die de *Federal Trade Commission* bijhoudt. De lijst telt 3.246 ondernemingen en kan worden geraadpleegd op de website van de Federal Trade Commission.[54]
Het *Safe Harbor*-systeem bepaalt ook dat de klachten van EER-burgers tegen een Amerikaanse onderneming of organisatie betreffende de bescherming van persoonsgegevens voor een Amerikaans rechtscollege moeten worden ingediend (behoudens enkele uitzonderingen).

---

53 Voor een gedetailleerde beschrijving van de 7 beginselen, zie Bijlage I van de beschikking van de Commissie van 26 juli 2000 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:NL:PDF)

54 http://export.gov/safeharbor/ (eind september 2013)

In de praktijk gaat het er echter anders aan toe, zoals blijkt uit de recente studie in opdracht van het Europees Parlement over het *Safe Harbor-systeem:* "De Amerikaanse onderhandelaars van het ministerie van handel hebben nauw samengewerkt met de Amerikaanse commerciële lobby's om een lijst van 'vaak gestelde vragen' op te stellen die het voor Amerikaanse ondernemingen mogelijk maken het Veiligehavenakkoord op zodanige wijze te interpreteren dat de rechten van de EU inzake de bescherming van de persoonlijke levenssfeer worden beperkt en die aangeven hoe ze de regels inzake identificeerbare gegevens kunnen omzeilen, het recht op toegang kunnen weigeren en zich kunnen onttrekken aan elke plicht tot finaliteit of elk verzoek tot schrapping. De veilige haven is zo complex gebleken dat er jarenlang geen enkele EU-burger is geweest die alle stappen van het bureaucratisch proces om klacht in te dienen heeft doorlopen." (vrije vertaling).[55]
Richtlijn 95/46 en de *Veiligehavenbeginselen* hebben geen betrekking op persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken[56], wat alle politie-, gerechts- en inlichtingenbestanden omvat. Artikel 1 van de Beschikking van de Commissie van 26 juli 2000 betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen bepaalt immers dat de beschikking alleen van toepassing is op activiteiten die binnen de werkingssfeer van Richtlijn 95/46 vallen.
Voorts bepaalt Bijlage I lid 4 van voornoemde beschikking dat "de naleving van de beginselen kan worden beperkt: a) voor zover dit nodig is om aan de eisen van de nationale veiligheid, het algemeen belang en de rechtshandhaving van de Verenigde Staten te voldoen; b) door wettelijke of bestuursrechtelijke bepalingen of rechtspraak die tegenstrijdige verplichtingen of uitdrukkelijke machtigingen scheppen, mits een organisatie die van een dergelijke machtiging gebruikmaakt, kan aantonen dat de niet-naleving van de beginselen beperkt is tot de mate die nodig is om de met de machtiging beoogde hogere legitieme belangen te waarborgen; c) indien de richtlijn of de wetgeving van de betrokken lidstaat uitzonderingen of afwijkingen toestaat, mits deze ook in vergelijkbare contexten worden toegepast."
De uitwisseling van persoonsgegevens tussen de Europese Unie en de Verenigde Staten voor rechtshandhavingsdoeleinden, met inbegrip van het voorkomen en bestrijden van terrorisme en andere vormen van zware criminaliteit, is, althans in theorie, geregeld in een aantal overeenkomsten op EU-niveau. Het gaat om de overeenkomst inzake wederzijdse rechtshulp, de overeenkomst inzake het gebruik en de doorgifte van persoonsgegevens van passagiers (PNR), de overeenkomst inzake de verwerking en doorgifte van gegevens betreffende het financiële-berichtenverkeer ten behoeve van het programma voor het traceren van terrorismefinanciering (TFTP), evenals de overeenkomst tussen Europol en de Verenigde Staten.

- Lacunes

Als gevolg van de verschillende onthullingen die we hier analyseren met betrekking tot Amerikaanse programma's voor het verzamelen van inlichtingen op grote schaal is het vertrouwen dat vooral op grond van de Veiligehavenbeginselen was opgebouwd, ernstig aan het wankelen

55 Le programme de surveillance des Etats-Unis et leurs effets sur les droits fondamentaux des citoyens de l'UE, Nota van het Directoraat-generaal intern beleid, Beleidsondersteunende afdeling C: Rechten van de burger en constitutionele zaken, IPOL-LIBE_NT(2013)474405_FR.
http: //www.europarl.europa.eu/RegData/etudes/note /join/2013/474405/IPOL-LIBE_NT%282013%29474405_FR.pdf

56 Artikel 25 van Richtlijn 95/46.

gebracht. Die onthullingen hebben het besef doen ontstaan dat de huidige bescherming van persoonsgegevens ontoereikend is en dat het noodzakelijk is om de bestaande regels, die ernstige lacunes vertonen, te herbekijken en te versterken.
Sinds de *FISA* werd geamendeerd en uitgebreid, meer bepaald in 2008, kunnen Amerikaanse ondernemingen er namelijk toe worden gedwongen om aan het NSA elektronische informatie over niet-Amerikanen te bezorgen. Artikel 702 van de FISA[57] vormt een algemene volmacht die het de Amerikaanse autoriteiten mogelijk maakt om gegevens te verzamelen en informatie te onderscheppen die betrekking heeft op de buitenlandse aangelegenheden van de Verenigde Staten, terwijl de persoonsgegevens van Amerikanen een betere bescherming genieten. De mogelijke omvang van een dergelijke bevoegdheidsoverdracht komt vandaag op duidelijke en onevenredige wijze naar voren in het licht van de onthullingen van Snowden en de technologische ontwikkelingen die de captatie van immense hoeveelheden gegevens op wereldniveau mogelijk maken.
Op 27 november 2013 publiceerde de Europese Commissie[58] het resultaat van haar overleg in (1) een strategiedocument (mededeling) over trans-Atlantische gegevensstromen waarin de problemen en risico's worden uiteengezet die voortvloeien uit de onthullingen over Amerikaanse programma's voor het verzamelen van inlichtingen, alsook de stappen die moeten worden ondernomen om deze problemen aan te pakken, (2) een analyse van de werking van 'Safe Harbor' (veilige haven) dat het doorgeven van gegevens voor commerciële doeleinden tussen de EU en de VS regelt, en (3) een verslag van over de bevindingen van de EU-VS-werkgroep (MEMO/13/1059) over gegevensbescherming, die in juli 2013 is opgericht.
Uit dit rapport blijkt ook dat grote bedrijven die actief zijn in de nieuwe technologieën en die aan de operatie *PRISM* hebben deelgenomen over een *Safe Harbor*-certificering beschikken, zodat we kunnen besluiten dat het *Safe Harbor*-systeem kan worden beschouwd als een belangrijk kanaal voor persoonsgegevens dat tot de grootschalige inzameling van gegevens door het NSA heeft geleid.
Hoewel deze praktijken door de Amerikaanse wet zijn toegelaten, zijn ze niet voorzien in het rechtskader van de *Safe Harbor*, zodat ze plaats hebben gevonden bij inbreuk op dit akkoord en op de beschikking van de Commissie die het akkoord formaliseert in het Europees rechtskader. Omdat de *Safe Harbor*-beginselen zijn vastgesteld om voor de Verenigde Staten een 'passend beschermingsniveau' te waarborgen dat borg staat voor een bescherming van persoonsgegevens op een niveau dat in de buurt komt van het beschermingsniveau binnen de EER, moeten we beschouwen dat de Verenigde Staten de geest van het akkoord in hun voordeel hebben omgebogen. Het *Safe Harbor*-systeem werd geenszins gecreëerd om de doorgifte mogelijk te maken van gegevens die vervolgens massaal aan de Amerikaanse veiligheidsautoriteiten kunnen worden bezorgd, terwijl de Europese veiligheidsautoriteiten niet op dezelfde wijze kunnen handelen.
Volgens de Europese Commissie kan de grootschalige onderschepping van persoonsgegevens door het NSA niet worden geacht te zijn gedekt door de beperking van de gegevensbescherming zoals

---

[57] Foreign Intelligence Surveillance Act van 1978 (beschrijft de procedures van fysieke en elektronische monitoring evenals het verzamelen van informatie bij vreemde mogendheden, hetzij rechtstreeks, hetzij door uitwisseling van informatie met andere vreemde mogendheden), zoals gewijzigd in 2008 door de FISA Amendments Act.

[58] Newsroom van de Europese Commissie: http://europa.eu/rapid/press-release_MEMO-13-1059_nl.htm.

bedoeld in het *Safe Harbor*-akkoord, met het oog op de nationale veiligheid. Als gevolg van de grootschaligheid en het feit dat er geen voorafgaande toestemming is verleend om gegevens op te slaan, kan dit proces immers niet worden beschouwd als noodzakelijk en in verhouding staand tot de belangen van de nationale veiligheid. Omdat er sprake is van een inbreuk op een fundamenteel mensenrecht, moet deze op restrictieve wijze worden beoordeeld, zoals bedoeld en beperkt door de wet.
Voorts stelt de Europese Commissie ook haar nieuwe onderzoek voor naar de bestaande akkoorden over passagiersgegevens (PNR) (MEMO/13/1054) en naar het programma voor het traceren van terrorismefinanciering (TFTP), die de uitwisseling van gegevens voor repressieve doeleinden in deze sectoren regelen.
In deze mededeling geeft de Commissie meer bepaald blijk van haar wil om uiterlijk in het voorjaar van 2014 een hervorming van de gegevensbescherming in de EU goed te keuren om ervoor te zorgen dat persoonsgegevens effectief en volledig worden beschermd.
Met betrekking tot de trans-Atlantische relaties heeft de Commissie bovendien 13 aanbevelingen gedaan om de werking van de veiligehavenregeling te verbeteren, nadat uit een op dezelfde dag bekendgemaakte analyse is gebleken dat de werking van de regeling op verscheidene punten tekortschiet. Het geheel van regels zou dus moeten worden herzien en verbeterd.
Op het vlak van de politiële en justitiële samenwerking in strafzaken zou de Commissie druk willen uitoefenen op de Amerikaanse regering opdat zij zich ertoe zou verbinden, als algemeen beginsel, gebruik te maken van een rechtskader zoals de sectorale overeenkomsten en de overeenkomsten inzake wederzijdse rechtshulp die tussen de EU en de Verenigde Staten zijn gesloten (bv. de overeenkomst over PNR en het programma voor het traceren van terrorismefinanciering) telkens wanneer de doorgifte van gegevens vereist is voor rechthandhavingsdoeleinden. Rechtstreekse verzoeken aan de ondernemingen mogen alleen mogelijk zijn in welbepaalde, uitzonderlijke en door de rechter toetsbare situaties.
Meer algemeen heeft de Europese Commissie verklaard te wensen dat de door de Amerikaanse president aangekondigde evaluatie van de activiteiten van de nationale veiligheidsautoriteiten voorziet in de bescherming van EU-burgers die hun verblijfplaats buiten de USA hebben. Die laatsten zouden dezelfde waarborgen moeten genieten als Amerikaanse burgers.

- Globale hervorming van de regels inzake gegevensbescherming

Zoals aangekondigd in januari 2012[59] werkt de Commissie aan een globale hervorming van de gegevensbescherming. De hervorming wil de beginselen van de gegevensbeschermingsrichtlijn van 1995 actualiseren en moderniseren om de privacyrechten te waarborgen in de toekomst. Deze hervorming omvat twee wetgevingsvoorstellen: een verordening tot vaststelling van het algemene EU-kader voor gegevensbescherming en een richtlijn inzake de bescherming van persoonsgegevens die worden verwerkt voor het voorkomen, opsporen, onderzoeken of vervolgen van strafbare feiten en aanverwante gerechtelijke activiteiten.
De hervorming beoogt meer bepaald de volgende voornaamste wijzigingen[60]:

---

59 Persbericht: http://europa.eu/rapid/press-release_IP-12-46_nl.htm
60 Persbericht: http://europa.eu/rapid/press-release_IP-12-46_nl.htm

- ‘‘Eén stel regels inzake gegevensbescherming, geldend in de gehele EU. Overbodige administratieve formaliteiten, zoals sommige verplichte meldingen door bedrijven, worden afgeschaft. Dit moet hen circa 2,3 miljard euro aan kosten per jaar besparen.
- Elk bedrijf is momenteel verplicht om alle maatregelen inzake gegevensbescherming aan de toezichthouders te melden, wat overbodige administratieve lasten meebrengt en bedrijven jaarlijks 130 miljoen euro kost. In plaats daarvan verplicht de verordening de verwerkers van persoonsgegevens meer verantwoording en rekenschap af te leggen.
- Zo moeten bedrijven en organisaties ernstige gegevenslekken zo snel mogelijk (zo mogelijk binnen 24 uur) aan de nationale toezichthouder melden.
- Organisaties krijgen te maken met slechts één nationale gegevensbeschermingsautoriteit, in de EU-lidstaat waar zij hun belangrijkste vestiging hebben. Insgelijks is de nationale gegevensbeschermingsautoriteit het aanspreekpunt voor burgers, ook als hun gegevens worden verwerkt door een bedrijf dat buiten de EU is gevestigd. Wanneer voor de verwerking van gegevens toestemming vereist is, moet deze uitdrukkelijk worden gegeven, en niet worden verondersteld stilzwijgend te zijn gegeven.
- Mensen zullen gemakkelijker toegang krijgen tot hun eigen gegevens en hun persoonsgegevens gemakkelijker van de ene dienstverstrekker naar de andere kunnen overdragen (recht op gegevensoverdraagbaarheid), wat de onderlinge concurrentie zal vergroten.
- Een 'recht om te worden vergeten' moet mensen in staat stellen om privacyrisico's op internet beter te beheren, d.w.z. hun gegevens te wissen als er geen gegronde redenen zijn om ze te bewaren.
- De EU-regels zijn van toepassing wanneer persoonsgegevens buiten de EU worden verwerkt door bedrijven die op de markt van de EU actief zijn en hun diensten aan EU-burgers aanbieden.
- Onafhankelijke nationale gegevensbeschermingsautoriteiten zullen meer bevoegdheden krijgen om de EU-regels op hun grondgebied te doen eerbiedigen, onder meer om boetes op te leggen aan bedrijven die die regels overtreden. Die boetes kunnen oplopen tot 1 miljoen euro of tot 2% van de totale jaarlijkse omzet van een bedrijf.
- In een nieuwe richtlijn zullen grondbeginselen en algemene regels worden vastgesteld voor de bescherming van persoonsgegevens in het kader van de politiële en justitiële samenwerking in strafzaken. De voorschriften zullen zowel op binnenlandse als grensoverschrijdende gegevensoverdrachten van toepassing zijn.’’

B. Soevereiniteit van België

Het traceerprogramma waarvan sprake in deze studie steunt duidelijk op een internationale structuur waaraan zeker de Verenigde Staten (NSA) en het Verenigd Koninkrijk (*GCHQ)* deelnemen, maar wellicht nog andere Lidstaten van de Raad van Europa en de Europese Unie. Die laatste werden wellicht ‘ingehaald’ door de structuur waaraan ze hebben meegewerkt en zijn zelf het slachtoffer geworden van de grootschalige controleoperaties.
Laten we niet vergeten dat het UKUSA-akkoord betreffende inlichtingen inzake telecommunicatie, dat in 1947 werd gesloten door vijf Angelsaksische landen (Verenigde Staten, Verenigd Koninkrijk,

Canada, Nieuw-Zeeland en Australië), het basisakkoord is voor de controle van communicatie in de ruime betekenis en al aan de basis stond van de ruggengraat van het controlesysteem Echelon, dat in de jaren 2000 voor schokgolven zorgde in Europa. De uitstekende studie van Dimitri Yernault over dit afluistersysteem is nog steeds brandend actueel en zou hier bijna volledig kunnen worden overgenomen.[61]

Een fundamentele vraag rond de grootschalige controle van elektronische communicatie zonder instemming van de Staat op wiens grondgebied de controle plaats heeft, zelfs vanaf een installatie op het grondgebied van een derde Staat, bestaat erin te weten of ze de soevereiniteit van die Staat schendt. Het antwoord is positief indien de Staat er niet mee heeft ingestemd, zelfs indien de afluisteroperaties conform zijn aan het recht van de Staat die ze uitvoert (rechtstreeks of via handelsondernemingen die er vrijwillig of gedwongen aan deelnemen): dit type afluisteroperaties schendt de soevereiniteit van de Staat op wiens grondgebied de communicaties worden onderschept.

Het onderscheppen van communicatie is namelijk per definitie een daad van dwang – clandestien of toegestaan door de wetgeving van de derde Staat – die wordt uitgeoefend op het grondgebied van een andere Staat en zijn soevereiniteit schendt.[62]

De Staat op wiens grondgebied de dwang wordt uitgeoefend, moet zijn voorafgaande toestemming geven[63]. Gebeurt dat niet, dan schenden de afluisteroperaties, de controle, de clandestiene onderschepping en *a fortiori* de operaties door *malware*systemen de soevereiniteit van die Staat. Aldus kan die dwang een diplomatieke reactie rechtvaardigen.

Hetzelfde geldt voor de clandestiene afluisteroperaties vanuit ambassades van derde Staten op het grondgebied van de Staat waar de afluister- en controleoperaties plaatsvinden. Ook die kunnen de goede diplomatieke relaties in gevaar brengen.

Ze vormen immers een inbreuk op het Verdrag van Wenen inzake diplomatiek verkeer van 18 april 1961, meer bepaald op artikel 3d, dat voor de diplomatieke zending [alleen] het volgende mogelijk maakt:

d) het met alle wettige middelen nagaan van de toestanden en ontwikkelingen in de ontvangende Staat en het uitbrengen van verslag daarvan aan de regering van de zendstaat;

Krachtens artikel 41.1 hebben diplomatieke zendingen de plicht "de wetten en regelingen van de ontvangende Staat te eerbiedigen. Ze hebben ook de plicht zich niet in te laten met de binnenlandse aangelegenheden van die Staat." Voor het overige mogen de gebouwen van de zending, overeenkomstig artikel 41.3, niet worden gebruikt op een wijze die onverenigbaar is met de functie van de zending, die, zoals we net hebben gezien, alleen inlichtingen mag inwinnen met behulp van wettige middelen (voornoemd artikel 3d).

Tot slot bepaalt artikel 27.1: "1. Door de ontvangende Staat wordt aan de zending toegestaan voor alle officiële doeleinden onbelemmerd verbindingen te onderhouden; deze verbindingen worden door de ontvangende Staat beschermd. Ten einde zich met de regering en met andere zendingen en consulaire posten – waar deze zich ook mogen bevinden – van de zendstaat in verbinding te stellen, mag de zending alle daarvoor in aanmerking komende middelen gebruiken, diplomatieke

---

61 Dimitri Yernault, De la fiction à la réalité : le programme d'espionnage électronique global "Echelon" et la responsabilité internationale des Etats au regard de la convention européenne des droits de l'homme, *RBDI,* 2000, p. 137 e.v.

62 PHIJ, *Lotus case,* 7 september 1927, *Recueil,* Série A, nr. 9, p. 18.

63 Zie de werkzaamheden van het Institut de droit international, *Annuaire de droit international,* vol. 68-I, 1999; zie ook Dimitri Yernault, *op. cit.,* p. 180.

koeriers en codeberichten daarbij inbegrepen. De zending mag evenwel geen radiozender installeren en gebruiken zonder toestemming van de ontvangende Staat.''
Het spreekt voor zich dat dit type clandestiene en ongecontroleerde onderschepping van communicatie op zich het recht op privacy schendt zoals het wordt beschermd door de voornoemde bepalingen en tot gevolg heeft dat de Staat internationaal aansprakelijk wordt, ongeacht of die Staat al dan niet lid is van de Raad van Europa of de Europese Unie. Is dat het geval, dan gaat de internationale aansprakelijkheid voor schending van de soevereiniteit van de Staat gepaard met de schending van de internationale verdragen die van toepassing zijn op het recht op eerbiediging van het privéleven.

C. Overzicht van de actiemiddelen ter beschikking van de Staat, burgers en bedrijven

Natuurlijk is het onmogelijk, tenzij er precieze bewezen feiten aanhangig worden gemaakt die in specifieke gevallen worden aangeklaagd, om alle mogelijke rechtsmiddelen te bestuderen in een zaak met een dergelijke reikwijdte zoals die welke E. Snowden heeft aangeklaagd en waarin alle verantwoordelijken nog niet zijn aangewezen. Een van de te voeren acties zou erin kunnen bestaan te vragen dat er een parlementair onderzoek wordt gehouden om de feiten en de elementen van verantwoordelijkheid van de betrokkenen nauwkeurig vast te stellen. De Staat op wiens grondgebied structurele inbreuken op de mensenrechten worden begaan, is algemeen verplicht die te 'voorkomen' of te bestraffen.[64] Die Staat kan dus niet onverschillig blijven. In dit geval lijkt het duidelijk dat de grootschalige controle van persoonsgegevens door het NSA en/of andere spelers op het Belgisch grondgebied van structurele aard is.
In deze fase kunnen we hier alleen maar enkele pistes naar voren schuiven.

1. Internationaal Gerechtshof

De Staat kan het internationaal geschil, dit wil zeggen de internationale aansprakelijkheid van de vreemde Staat die de illegale afluisterpraktijken heeft begaan of die heeft toegestaan dat dergelijke afluisterpraktijken hebben plaatsgevonden, bijvoorbeeld door zijn grondgebied ter beschikking te stellen voor het onderscheppen en illegaal afluisteren, voor het Internationaal Gerechtshof brengen indien de zeer restrictieve voorwaarden betreffende de bevoegdheid van dit Hof vervuld zijn. De vraag betreffende de naleving van het Verdrag van Wenen inzake diplomatiek verkeer en consulaire betrekkingen kan bij hetzelfde Hof aanhangig worden gemaakt.

2. Europees Hof voor de Rechten van de Mens[65]

Indien de Staat die aansprakelijk is voor de controle of eraan heeft meegewerkt lid is van de Raad van Europa, dan is een transnationaal beroep voor het Europees Hof voor de Rechten van de Mens een rechtsmiddel om de schendingen te doen ophouden en schadevergoeding te verkrijgen. Een

---

64 Zie meer bepaald Dimitri Yernault, op. cit., p. 214.

65 Dit beroep lijkt efficiënter dan een beroep voor het Mensenrechtencomité, maar deze mogelijkheid mag niet worden uitgesloten.

dergelijk beroep werd ernstig overwogen in de zogenaamde zaak 'Echelon' [66]. Indien in deze zaak het bewijs zou worden geleverd van interventies van de geheime diensten van het Verenigd Koninkrijk of andere Staten die het EVRM hebben ondertekend, dan zou het om een exemplarische actie gaan.

3. Belgische gerechten: hacking en strafbare feiten

- Belgische bedrijven die het slachtoffer zijn van illegale onderschepping van gegevens in hun bezit kunnen – naargelang de feiten – klacht indienen tegen de vreemde Staat voor de gerechten van de betrokken Staat, maar ook voor de Belgische gerechten indien bewezen is dat de feiten een verband hebben met België (onderschepping in België). Zo kan de malware die het informaticasysteem van Belgacom lijkt te hebben besmet, het voorwerp zijn van een rechtsvordering in België. Een nauwkeuriger uiteenzetting van de feiten is echter noodzakelijk om een juridische studie aan deze mogelijkheid te wijden.
- In de mate waarin specifieke bepalingen betreffende de bescherming van persoonsgegevens daarin voorzien, kunnen ze natuurlijk van toepassing zijn op private personen zodra die verantwoordelijk zijn voor de verwerking van persoonsgegevens in de betekenis van de hierboven bestudeerde bepalingen. Dit is meer bepaald het geval met de richtlijnen die ook bestemd zijn voor de aanbieders van netwerken, telecommunicatiediensten enzovoort; dit moet natuurlijk verder worden uitgeklaard in elk afzonderlijk geval. Voor Facebook bijvoorbeeld werd er een grondige studie gevoerd.[67] Dit zou moeten gebeuren voor elke potentiële verantwoordelijke wiens rol zou kunnen worden bepaald in de zaak die ons bezighoudt.
- Volgens de vaststelling van de feiten, indien bewezen was dat private bedrijven buiten medeweten van de Staat hebben meegewerkt aan de uitvoering van de onderscheppingspraktijken (bv. op de optische kabel in Oostende of door vrijwillig persoonsgegevens door te geven aan een vreemde Staat (NSA of ander)), dan kunnen de Staat of particulieren of bedrijven die het slachtoffer zijn van deze hacking een strafrechtelijke klacht indienen krachtens de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, meer bepaald op grond van artikelen 550bis en 314bis van het Strafwetboek en van de artikelen 124 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie. Hacking wordt immers strafrechtelijk bestraft.[68]

Titel IXbis van het Belgisch Strafwetboek heeft als titel "Misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en van de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen". Artikelen 550*bis* en 550*ter* bestraffen diverse gedragingen met straffen die gaan van 3 maanden tot 5 jaar opsluiting. De Belgische strafwet verbiedt het feit "zich toegang te verschaffen tot een informaticasysteem" of "zich daarin te handhaven" (artikel 550bis, § 1, 1ste lid), maar ook "om enig gebruik te maken van een

---

66 Zie Dimitri Yernault, *op. cit.,* p. 154 e.v.

67 Jean-Philippe Moiny, Facebook au regard des règles européennes concernant la protection des données, *Rev. Eur.de droit de la consommation,* p. 235.

68 De Belgische wetgeving strekt in dit verband tot voorbeeld.

informaticasysteem van een derde" (artikel 550bis,§ 3, 2°) of "enige schade aan dit systeem te veroorzaken" (artikel 550bis, § 1, 3°). De wet bestraft "hij die opdracht geeft of aanzet tot het plegen van een van de misdrijven bedoeld in §§ 1 tot 5" (artikel 550bis, § 6) en "hij die, terwijl hij weet dat gegevens bekomen zijn door het plegen van een van de misdrijven bedoeld in §§ 1 tot 3, deze gegevens onder zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt" met gevangenisstraf van zes maanden tot drie jaar en/of met geldboete van 26 tot 100.000 euro (artikel 550*bis,* §7).

Titel V van het Belgisch Strafwetboek ("Misdaden en wanbedrijven tegen de openbare orde door bijzondere personen gepleegd") bevat een hoofdstuk VII*bis* met als titel "Misdrijven betreffende het geheim van privé-communicatie en -telecommunicatie". Artikel 314*bis,* § 1 bestraft met gevangenisstraf van zes maanden tot één jaar en/of honderd tot tienduizend euro hij die "privé-communicatie", "waaraan hij niet deelneemt", "tijdens de overbrenging ervan", […], "er kennis van neemt", "opneemt", "zonder de toestemming van alle deelnemers aan die communicatie of telecommunicatie" of die daartoe "enig toestel opstelt of doet opstellen". Artikel 314*bis,* § 2 bestraft met gevangenisstraf van zes maanden tot twee jaar en/of met geldboete van vijfhonderd tot twintigduizend euro hij die "een op die manier verkregen inlichting" "onthult, verspreidt of er wetens enig gebruik van maakt".

Personen en bedrijven die het slachtoffer van deze misdrijven zijn geweest, kunnen in België een strafrechtelijke klacht indienen bij de procureur des Konings of zich burgerlijke partij stellen. De vraag naar de territoriale bevoegdheid om een dergelijke klacht te kunnen indienen wordt opgelost in functie van de feiten van de zaak. Ofwel werd het misdrijf in België gepleegd (bv. onwettige toegang tot een informaticasysteem in België), ofwel hebben de gevolgen van de misdaad zich voorgedaan in België (indien jurisprudentie van het Hof van Cassatie ter gelegenheid van een zaak met betrekking tot een cheque die in Teheran werd uitgegeven en op een Belgische bank werd getrokken, op cybercrime wordt toegepast[69]).

Dit gezegd zijnde, in het Belgisch recht kunnen deze feiten van hacking wettelijk zijn indien ze, overeenkomstig de bepalingen van het Wetboek van Strafvordering betreffende de opslag van informaticagegevens, worden begaan met behulp van het procedé van de zoeking in een informaticasysteem en de uitbreiding van die zoeking, bevolen door de onderzoeksrechter bij gemotiveerde beschikking, "naar een informaticasysteem dat zich op een andere plaats bevindt" (artikel 88*ter* van het Wetboek van Strafvordering) en door het bevel dat dezelfde magistraat geeft aan een persoon die "bijzondere kennis" heeft om toegang te verkrijgen tot gegevens die zijn opgeslagen "in een verstaanbare vorm" (artikel *88quater* van het Wetboek van Strafvordering). Deze onderzoeksmaatregel kan ook onder strenge voorwaarden plaatsvinden als "uitzonderlijke methode voor het verzamelen van gegevens" door de Veiligheid van de Staat of de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht (artikel 18/16, §§ 1 tot 5 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst).

Hacking of het gebruik van gegevens die in België zijn verzameld of gebruikt, zonder wettelijke toelating, blijft een strafbaar feit. Het Belgisch Wetboek van Strafvordering bevat in artikel 29 voor elke ambtenaar die kennis krijgt van een misdrijf de verplichting om die te melden aan de

---

69 Correctionele rechtbank, Dendermonde, 29 september 2008, *Tijdschrift voor Strafrecht,* 2009/2, 111-114.

procureur des Konings. Het gaat om een algemene verplichting die betrekking heeft op eender welk misdrijf.[70]

4. Gebruik van de informatie verkregen door een onwettig controlesysteem

De vraag stelt zich of een politie- of inlichtingendienst die dit soort informatie ontvangt, die informatie mag gebruiken in het kader van zijn opdrachten. De wet betreffende de bijzondere methoden voor het verzamelen van gegevens bepaalt dat indien een uitzonderlijke maatregel voor het verzamelen van gegevens, zoals hacking, op onwettige wijze heeft plaatsgevonden, de commissie die belast is met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens van de inlichtingen- en veiligheidsdiensten die gegevens bewaart en de inlichtingen- en veiligheidsdiensten verbiedt die gegevens te exploiteren (artikel 18/10, § 6, lid 4 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst). Op te merken valt dat geen enkele bepaling de gevolgen reglementeert die moeten worden gegeven in het geval waarin deze onwettigheid door een buitenlandse dienst werd begaan. Een mogelijke oplossing kan worden gevonden in de besprekingen die zijn voorafgegaan aan de goedkeuring van de wet van 4 februari 2010 betreffende de bijzondere methoden voor het verzamelen van inlichtingen. De wet van 1998 betreffende de inlichtingendiensten verwijst in artikel 20, § 1 immers naar de samenwerking met buitenlandse diensten. De voorzitter van het Vast Comité I heeft echter aangegeven dat "het Comité geen toezicht kan uitoefenen op de buitenlandse inlichtingendiensten. Het zou aangewezen zijn om de wet op dit punt aan te vullen zodat de wettelijkheid van de operaties van bevriende buitenlandse inlichtingendiensten, die op ons grondgebied worden toegelaten, eveneens kan worden gecontroleerd door de Veiligheid van de Staat."[71] De heer Winants heeft bij deze gelegenheid verklaard: "Indien een buitenlandse inlichtingendienst zijn bevoegdheden te buiten gaat, dan geniet de Veiligheid van de Staat de mogelijkheid om tussen te komen op grond van voornoemd artikel 20 van de wet van 1998)."[72] De heer Hellemans, directeur van de ADIV, verklaarde van zijn kant: "De ADIV gaat uit van het principe dat het stelselmatig door de buitenlandse diensten op de hoogte wordt gebracht wanneer die diensten een doel nastreven in België. De dienst onderhoudt goede contacten met de bevriende landen en maakt gebruik van een systeem voor gegevensuitwisseling. Natuurlijk blijft de dienst aansprakelijk voor de gegevens die op het Belgisch grondgebied worden verzameld."[73]
Uit dit alles blijkt ten eerste dat het aanwenden door een buitenlandse dienst van een uitzonderlijke methode voor het verzamelen van gegevens in België, zoals hacking, niet gereglementeerd is, ten tweede dat deze methode om inlichtingen te verzamelen een strafbaar feit vormt en ten derde dat het voor de Belgische diensten verboden is om op onwettige wijze verkregen inlichtingen te gebruiken, zo niet zouden de Belgische diensten zich eveneens schuldig maken aan het plegen van een misdrijf als ze dit wetens en willens doen.

---

70 Alain Winants, De Veiligheid van de Staat en de BIM-Wet, in Wauter Van Laethem, Dirk Van Daele en Bart Vangeebergen(Eds), *De Wet op de bijzondere inlichtingenmethoden,* Intersentia, Antwerpen Oxford, p. 141.

71 *Parl. st.,* Kamer, 52ste zittingsperiode, 2009-2010, DOC 52 / 2128/000, p. 41.

72 *Ibid.*

73 *Op. cit.,* p. 46

De problematiek van de samenwerking met buitenlandse diensten en de manier om daarop toezicht uit te oefenen is een van de prioriteiten van het Vast Comité I. Al in het activiteitenverslag van 2008 bracht het Comité verslag uit over verschillende bijdragen in het buitenland teneinde een doeltreffende democratische controle op de inlichtingendiensten te bevorderen en deze initiatieven krijgen de steun van Martin Scheinin, Speciaal Rapporteur van de Verenigde Naties voor bevordering en bescherming van de mensenrechten en de fundamentele vrijheden in de strijd tegen het terrorisme.[74] De uitwisseling van informatie met 'bevriende' diensten is momenteel slechts onderworpen aan ethische beginselen. Deze lacune in de wetten betreffende het toezicht op de inlichtingendiensten werd bekritiseerd en er werd voorgesteld dat nieuwe regelgeving dit juridisch vacuüm zou opvullen.[75]
De kwestie betreffende het gerechtelijk gebruik van dit soort informatie krijgt een andere oplossing. Het Belgisch strafprocesrecht voorziet immers in een regel die onwettig verkregen bewijselementen uitsluit. Deze uitsluiting is echter niet absoluut. De wet van 24 oktober 2013 heeft in het Wetboek van Strafvordering immers een nieuw artikel 32 ingevoegd, dat als volgt luidt:
''Art. 32. Tot nietigheid van onregelmatig verkregen bewijselement wordt enkel besloten indien:

- de naleving van de betrokken vormvoorwaarden wordt voorgeschreven op straffe van nietigheid, of;
- de begane onregelmatigheid de betrouwbaarheid van het bewijs heeft aangetast, of;
- het gebruik van het bewijs in strijd is met het recht op een eerlijk proces.''

Deze wet geeft gevolg aan de zogenaamde arrest-'Antigone' van 14 oktober 2003 van het Belgisch Hof van Cassatie [76]. Deze rechtspraak had al aanleiding gegeven tot de wet van 9 december 2004 betreffende de wederzijdse internationale rechtshulp in strafzaken en tot wijziging van artikel 90*ter* van het Wetboek van strafvordering, die in artikel 13 bepaalt:
''Art. 13. In het kader van een in België gevoerde strafrechtspleging mag geen gebruik worden gemaakt van bewijsmateriaal:

1° dat in het buitenland op onregelmatige wijze is verzameld indien de onregelmatigheid:

- volgens het recht van de Staat waarin het bewijsmateriaal is verzameld volgt uit de overtreding van een op straffe van nietigheid voorgeschreven vormvereiste;
- de betrouwbaarheid van het bewijsmateriaal aantast;

2° waarvan de aanwending een schending inhoudt van het recht op een eerlijk proces.''

Deze reglementering van het bewijs impliceert dus dat eender welke onwettigheid of onregelmatigheid er niet automatisch toe leidt dat dit bewijselement terzijde wordt geschoven. In een belangrijk boek[77] heeft de voorzitter van de strafkamer van het Belgische Hof van Cassatie

[74] Vast Comité I, Activiteitenverslag 2008, p. 87.
Voor een grondige studie hierover, zie o.a. Elizabeth Sepper, Democracy, Human Rights and Intelligence Sharing, *Texas International Law Journal,* Vol. 46: 151, 2010, pp. 153-206; Europees parlement, Comité burgerlijke vrijheden, justitie en binnenlandse zaken, *Working Document 5 on Democratic oversight of Member State intelligence services and of EU intelligence bodies,* 11 november 2013, DT\1009342EN.doc

[76] AR P.03.0762.N

[77] Jean de CODT, *Des nullités de l'instruction et du jugement,* Brussel, Larcier, 2006, 233 pp.

echter verklaard dat er, naast de nietigheden waarin een wettekst specifiek voorziet of die welke de betrouwbaarheid van het bewijsmateriaal aantasten of waarvan het gebruik het recht op een eerlijk proces schendt, ook nietigheden bestaan als gevolg van onrechtmatig verkregen bewijs, dit wil zeggen het geval waarin het bewijsmateriaal is aangetast door het plegen van een misdrijf.[78] Ter gelegenheid van een studie naar de rechtspraak in deze materie maakt deze eminente magistraat, met betrekking tot misdrijven gepleegd door onderzoeksorganen, een onderscheid tussen enerzijds de situatie van een misdrijf dat wordt begaan om een bewijs te verkrijgen en anderzijds de situatie van een misdrijf dat al is gepleegd op het ogenblik waarop de vaststelling wordt gemaakt van een door een delinquent gepleegd misdrijf.[79] In het eerste geval, bijvoorbeeld onwettige hacking, is het bewijs niet ontvankelijk. In het tweede geval, bijvoorbeeld de deelname aan de handel in verdovende middelen teneinde de daders aan te houden, ‘‘zou het bewijs ontvankelijk zijn wanneer het misdadig voornemen duidelijk voorafgaat aan de interventie van de politie en de verbaliserende overheid slechts onregelmatigheden begaat die extern zijn aan de beslagleggingen, zoekingen, observaties en verhoren’’ (vrije vertaling).[80]

---

78 *Op. cit.,* p. 16.
79 *Op. cit.,* p. 103-104.
80 *Op. cit.,* p. 105.