Hoofdstuk 7.

Het recht op bescherming van persoonsgegevens

Friederike van der Jagt

1. Inleiding

Het recht op bescherming van persoonsgegevens maakt deel uit van het recht op privéleven, ofwel het recht op privacy, dat wij in hoofdstuk 6 hebben besproken. Het recht op privacy is een klassiek vrijheidsrecht dat uitgaat van de bescherming van het individu op inbreuken van buitenaf op zijn privéleven. Onder dit recht kunnen bijvoorbeeld de relationele privacy (bescherming van het gezinsleven) en de ruimtelijke privacy (bescherming van de woning) worden geschaard. Het recht op bescherming van persoonsgegevens heeft een enigszins ander karakter: het individu heeft er recht op dat zijn persoonsgegevens op een rechtmatige wijze worden verwerkt, om te voorkomen dat hij hier nadeel van ondervindt. De gevolgen van een onrechtmatige verwerking kunnen immers enorm zijn; zo kan een fout in een schuldregistratiesysteem er toe leiden dat aan iemand geen hypotheek wordt verstrekt, kan het al dan niet noteren van medische gegevens van een werknemer gevolgen hebben voor iemands arbeidsovereenkomst en kan het profileren van personen aan de hand van verzamelde persoonsgegevens discriminatie tot gevolg hebben.

Door de snelle technologische ontwikkelingen en de opkomst van internet en social media, is er een enorme groei aan wereldwijde informatiestromen. Deze ontwikkelingen brengen met zich dat het steeds moeilijker wordt om bescherming van persoonsgegevens te garanderen. Dit speelt vooral bij het verwerken van persoonsgegevens online, nu het in de praktijk lastig blijkt om foutieve informatie definitief te verwijderen. Het waarborgen van de persoonsgegevensbescherming, ook wel aangeduid als de informationele privacy, is daarom van vitaal belang.

Het recht op privéleven is als fundamenteel recht terug te vinden in art. 12 van de Universele Verklaring van de Rechten van de Mens, art. 8 EVRM, art. 17 IVBPR en art. 10 van de Grondwet. Daarnaast wordt het recht via diverse instrumenten van de Europese Unie-wetgever gewaarborgd. Op nationaal niveau speelt met name de Wet bescherming persoonsgegevens een belangrijke rol. Anders dan voor veel andere grondrechten geldt dat de bescherming van persoonsgegevens in de rechtspraak van het Europees Hof voor de Rechten van de Mens niet heel sterk is ontwikkeld. In het navolgende leggen wij het accent dan ook vooral op de bespreking van andere instrumenten, zoals het Verdrag van Straatsburg en het EU-recht.

2. Europa

2.1 EVRM

2.1.1 Art. 8 EVRM

In het EVRM is het recht op bescherming van het privéleven neergelegd in art. 8. De bepaling luidt in de Nederlandse vertaling als volgt:

Artikel 8 EVRM

1. Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

Zoals uiteengezet valt ook de bescherming van de informationele privacy binnen de werkingssfeer van art. 8 EVRM. Om de informationele privacy nader te waarborgen, werd binnen de Raad van Europa in 1981 een apart verdrag gesloten, het Verdrag van Straatsburg, dat wij in paragraaf 2.2 behandelen. Gezien de grote omvang van het aantal zaken van het Hof, verwijzen wij in deze paragraaf slechts beperkt verwezen naar relevante uitspraken. Waar wij dat doen is het doel vooral om de reikwijdte van de begrippen en de beperkingsvoorwaarden zoals in het artikel geformuleerd, toe te lichten.

Hoewel art. 8 EVRM in essentie beoogt om de betrokkene te beschermen tegen willekeurige overheidsbemoeienis, betekent dit niet alleen dat de overheid zich van deze bemoeienis moet onthouden; uit art. 8 EVRM kunnen ook positieve verplichtingen voortvloeien.[1] Daarnaast geldt dat, via de band van de positieve verplichtingen, art. 8 EVRM eveneens effecten sorteert in horizontale rechtsverhoudingen.

De systematiek van art. 8 EVRM is dat eerst dient te worden vastgesteld of er sprake is van een inmenging in het 'privéleven'. Zoals wij in hoofdstuk 6 nader hebben toegelicht legt het Hof dit begrip ruim uit. Zo heeft het in de zaak *Niemietz* aangegeven dat werknemers een gerechtvaardigd belang hebben om ook onder werktijd contacten met anderen te kunnen aangaan en dat het recht op bescherming van het privéleven derhalve de werknemer ook beschermt tegen inbreuken op dergelijke contacten.[2] In de zaak *Halford*, waarin de telefoon van een werkneemster zonder haar medeweten was afgeluisterd door haar werkgever, heeft het Hof geoordeeld dat ook het telefoneren vanaf een werkplek onder het begrip 'privéleven' valt.[3] Wel heeft het Hof in deze zaak opgemerkt dat bij de kwalificatie als inbreuk op art. 8 EVRM moet worden bekeken of de betrokkene redelijkerwijs kon verwachten dat haar privacy zou worden gerespecteerd.[4]

In lijn met bovenstaande gaf het Hof in de zaak *Copland* aan dat ook het monitoren van persoonlijk internet- en e-mailgebruik, waarbij persoonlijke informatie wordt verzameld en opgeslagen, een schending van het recht op privéleven kan opleveren nu de betrokkene niet geïnformeerd was over de controle en redelijkerwijs had kunnen aannemen dat de persoonlijke e-mails privé zouden blijven.[5] Uit de jurisprudentie van het Hof is af te leiden dat als het Hof constateert dat een bepaalde situatie onder het begrip 'privéleven' valt, vrij gemakkelijk geconcludeerd wordt dat er eveneens sprake is van *inmenging* in het privéleven.

Ook het begrip 'persoonsgegeven' wordt door het Hof ruim uitgelegd. In de zaak *S. en Marper* oordeelde het Hof over het opslaan van DNA-materiaal, DNA-profielen en vingerafdrukken door

1 EHRM 9 oktober 1979, nr. 6289/73 (*Airey/Ierland*).
2 EHRM 16 december 1992, nr. 13710/88 (*Niemietz/Duitsland*).
3 EHRM 25 juni 1997, nr. 20605/92 (*Halford/Verenigd Koninkrijk*).
4 *Idem*, zie § 42.
5 EHRM 3 april 2007, 62617/00 (*Copland/Verenigd Koninkrijk*).

de Britse overheid in het kader van een strafrechtelijke procedure.[6] Nu uit deze informatie gevoelige gegevens van een individu zijn af te leiden, zoals informatie over zijn gezondheid en etnische oorsprong, vormden het bewaren van deze gegevens zonder toestemming van de betrokkene een inbreuk op het recht op privéleven die niet kon worden gerechtvaardigd.[7]

Als geconstateerd wordt dat er sprake is van een inmenging in het privéleven, dient vervolgens te worden bezien of de inmenging op grond van art. 8 lid 2 EVRM gerechtvaardigd is.

Hierbij geldt allereerst het vereiste dat de inmenging bij wet voorzien moet zijn. Dit betekent dat de nationale wetgeving een grondslag voor de inmenging dient te bieden waarbij wordt voldaan aan de rechtstatelijke vereisten. De grondslag hoeft geen wet in formele zin te zijn. In bepaalde gevallen kan zelfs standaardjurisprudentie als een afdoende grondslag worden aangemerkt, zoals blijkt uit de zaak *Köpke*.[8] In deze zaak waren verborgen camera's ingezet om een stelende werkneemster op heterdaad te betrappen. De voorwaarden voor het instellen van cameratoezicht waren ten tijde van de inzet van de camera's nog niet in een wettelijke regeling vastgelegd. Wel waren er in de jurisprudentie van het federale arbeidsgerecht al duidelijke beperkingen ten aanzien van het gebruik van cameratoezicht vastgesteld. Het Hof was van oordeel dat hierdoor voldoende bescherming werd geboden, temeer nu juist deze beperkingen in de later opgestelde wetgeving waren opgenomen.

Van belang is dat de wettelijke grondslag voor de betrokkene toegankelijk is en dat hij kan voorzien wat de consequenties van de wettelijke bepaling in zijn specifieke geval zullen zijn, zodat hij zijn gedrag erop af kan stemmen.[9] Deze eisen van toegankelijkheid en voorzienbaarheid kunnen onder stringente voorwaarden worden verzacht in het geval van heimelijk toezicht, waarbij het in beginsel juist niet wenselijk is dat de persoon zijn gedrag aanpast omdat het doel van een dergelijke maatregel vaak het aantonen van dat gedrag behelst.[10] De beperking van de voorzienbaarheid brengt echter een risico van willekeur met zich. Daarom heeft het Hof een aantal minimumvoorwaarden geformuleerd waaraan de toepassing van heimelijke maatregelen moet voldoen. Zo dient een betrokkene te weten wanneer heimelijk toezicht kan worden ingezet en welke procedurele waarborgen in acht worden genomen.[11] De eisen die het Hof daarbij stelt zijn strikt waar het gaat om alle elementen van gegevensverwerking: verzameling, opslag, opslagduur, gebruik en toegang voor derden. Dat geldt zeker waar het gevoelige gegevens betreft, zoals gegevens over iemands strafblad, en de feiten waarvoor deze gegevens verzameld zijn verder in het verleden liggen.[12] Het creëren van een nationale databank, bijvoorbeeld met vingerafdrukken van mensen die ooit verdacht zijn geweest van een strafbaar feit, is daarbij evenmin zomaar toelaatbaar, in het bijzonder vanwege het potentieel stigmatiserende effect daarvan.[13]

Tot slot moet worden beoordeeld of de inmenging in het privéleven noodzakelijk is in een democratische samenleving om de in art. 8 lid 2 EVRM opgesomde legitieme doeleinden te bereiken. Een maatregel is noodzakelijk indien er sprake is van een 'pressing social need' (dringende maatschappelijke behoefte). Daarbij dient de maatregel proportioneel te zijn: de inbreuk op de privacy van de betrokkene mag niet onevenredig zijn in verhouding met het doel dat met de verwerking wordt ver-

6 EHRM 4 december 2008, nrs. 30562/04 en nr. 30566/04 (*S. en Marper/Verenigd Koninkrijk*).
7 Zie ook EHRM 4 mei 2000, nr. 28451/95 (*Rotaru/Roemenië*).
8 EHRM 5 oktober 2010 (ontv.), *nr. 420/07* (*Köpke/Duitsland*).
9 Zie onder meer: EHRM 26 april 1979, nr. 6538/74 (*Sunday Times/Verenigd Koninkrijk*) en EHRM 4 mei 2000, nr. 28451/95 (*Rotaru/Roemenië*), § 52.
10 Zie onder meer: EHRM 26 augustus 1987, nr. 9248/81 (*Leander/Zweden*), § 51.
11 EHRM 29 juni 2006 (onv.), *nr. 54934/00* (*Weber en Saravia/Duitsland*).
12 Zie bijv. EHRM 13 november 2012, nr. 24029/07 (*M.M./Verenigd Koninkrijk*).
13 Zie bijv. EHRM 4 december 2008, nrs. 30562/04 en nr. 30566/04 (*S. en Marper/Verenigd Koninkrijk*) en EHRM 18 april 2013, nr. 19522/09 (*M.K./Frankrijk*).

wezenlijkt. Het proportionaliteitsbeginsel vergt ook dat er steeds een belangenafweging plaatsvindt, waarbij gekeken moet worden naar de omstandigheden van het geval, het algemeen belang en de op het spel staande belangen van het individu.[14] Op dit punt komt aan de verdragstaten volgens vaste rechtspraak van het Hof een *margin of appreciation* toe.

Het subsidiariteitsvereiste – waarbij de vraag centraal staat of het doel van de gegevenswerking niet op een andere, minder inbreukmakende wijze kan worden bereikt – maakt geen expliciet onderdeel van het noodzakelijkheidsvereiste, maar speelt soms wel een rol bij de beoordeling van de proportionaliteit van de maatregel. Dit is bijvoorbeeld terug te vinden in de zaak *Peck*, waarin geklaagd werd over het feit dat een man die een mislukte zelfmoordpoging had gedaan, in de media herkenbaar in beeld was gebracht.[15] Het Hof was van oordeel dat de openbaarmaking op een minder inbreukmakende manier had kunnen geschieden, bijvoorbeeld door het gezicht van de man te maskeren.

Bij de invulling van het proportionaliteitsvereiste kunnen verder diverse elementen een rol spelen. Hierbij is van belang dat het noodzakelijkheidsbegrip soms ook met zich brengt dat er actief maatregelen dienen te worden genomen om misbruik van gegevens te voorkomen.[16] In de zaak *I t. Finland* kwam een werkneemster van de afdeling oogheelkunde van een ziekenhuis erachter dat haar patiëntdossier niet goed beveiligd was.[17] Het bleek namelijk dat haar collega's haar patiëntdossier, waarin vermeld stond dat zij in het ziekenhuis onder behandeling was voor de ziekte aids, hadden kunnen inzien. Het Hof was van oordeel dat er juist bij dergelijke gevoelige gegevens maatregelen moeten worden getroffen om onrechtmatige toegang en misbruik van de gegevens tegen te gaan. Uit deze zaak blijkt eveneens dat de aard van de gegevens het belang van de betrokkene om deze te beschermen, kan versterken. Vooral medische gegevens verdienen volgens het Hof bijzondere, ook procedurele, bescherming. Dit blijkt ook uit de zaak *Eternit*, waarin het Hof gevraagd werd te oordelen over een inzage in medisch dossier van een werknemer door een werkgever.[18] Bij deze zaak ging het derhalve niet om de inzage van de betrokkene zelf in zijn gegevens, maar de inzage door een derde. Deze zaak is noemenswaardig omdat hier een botsing van grondrechten plaatsvond, namelijk tussen art. 6 EVRM (het recht op een eerlijk proces) en art. 8 EVRM. De werknemer had aan de werkgever medegedeeld dat hij leed aan asbestose en longkanker. De Franse uitkeringsinstantie verrichtte een onderzoek en concludeerde dat de werknemer leed aan een beroepsziekte. Deze kwalificatie had gevolgen voor de premies die de werkgever moest afdragen. In de procedure die de werkgever hierover voerde kreeg hij echter geen inzage in het medische dossier van de werknemer; hij vond dat hij zich daardoor niet tegen de kwalificatie als beroepsziekte kon verdedigen. Het Hof overwoog dat de privacy van de werknemer, juist nu het ging om medische gegevens, zwaarder diende te wegen dan het belang van de werkgever om het dossier in te zien. Nu de werkgever in de nationale procedure wel de mogelijkheid had gehad om de rechter te verzoeken om de medische gegevens door een onafhankelijke deskundige de gegevens te laten beoordelen, was geen sprake van een schending van art. 6 EVRM.

Een ander element dat in de belangenafweging een rol kan spelen is de aan- of afwezigheid van de mogelijkheid voor de betrokkene om een inzage-, correctie- of verwijderingsrecht ten aanzien van zijn persoonsgegevens uit te oefenen. In de zaak *Leander* erkende het Hof dat in het licht van art. 8 EVRM een inzage- en correctierecht moest worden geboden.[19] Zonder inzage zou een betrokkene

14 EHRM 19 juni 2006, nr. 35014/97 (*Hutten-Czapska/Polen*).
15 EHRM 28 januari 2001, nr. 44647/98 (*Peck/Verenigd Koninkrijk*).
16 EHRM 2 december 2008, nr. 2872/02 (*K.U./Finland*).
17 EHRM 17 juli 2008, nr. 20511/03 (*I/Finland*).
18 EHRM 18 april 2012 (ontv.), nr. 20041/10 (*Eternit/Frankrijk*).
19 EHRM 26 maart 1987, nr. 9248/81 (*Leander/Zweden*); zie ook EHRM 4 mei 2000, nr. 28341/95 (*Rotaru/Roemenië*) en EHRM 14 februari 2006, nr. 57986/00 (*Turek/Slowakije*).

immers zijn claim dat zijn gegevens in strijd met art. 8 EVRM worden verwerkt, niet hard kunnen maken. In de zaak *Gaskin* werd een betrokkene die zijn jeugd in diverse gastgezinnen had doorgebracht, inzage geweigerd in overheidsdossiers waarin informatie over die periode was opgenomen.[20] De registratie van deze gegevens kwam volgens het Hof binnen het bereik van art. 8 EVRM, nu deze gegevens de betrokkene een beeld konden geven van zijn verleden en ontwikkeling; daardoor was er sprake van een direct verband met zijn privéleven. De autoriteiten hadden in dit geval inzage geweigerd omdat andere personen die in de dossiers waren vermeld, hier bezwaar tegen hadden gemaakt. Hoewel het Hof aangaf te beseffen dat in deze zaak een belangenafweging moest plaatsvinden, oordeelde het dat er sprake was van een schending van art. 8 EVRM nu voor Gaskin de mogelijkheid ontbrak om zich tot een onafhankelijke autoriteit te wenden die een eindbeslissing over het inzageverzoek zou kunnen nemen.

In onder meer de zaak *Mosley* boog het Hof zich over het spanningsveld tussen art. 8 EVRM en art. 10 EVRM (vrijheid van meningsuiting).[21] De vraag die in deze zaak centraal stond was of een journalist of uitgever voorafgaand aan een publicatie inzage zoud moeten bieden aan een persoon indien zij artikelen wensen te publiceren die privacygevoelige informatie over die persoon bevatten. Het Hof wees een dergelijke verplichting af, nu hiervan een afschrikkende werking zou uitgaan die de persvrijheid ernstig zou belemmeren. Tegelijkertijd heeft het Hof in zijn rechtspraak wel duidelijk gemaakt dat de vrijheid van meningsuiting niet impliceert dat, zonder goede reden, persoonsgegevens bekend mogen worden gemaakt. Zo vond het in de zaak *Alkaya* dat er geen rechtvaardiging was voor het publiceren van foto's met adresgegevens van een bekende actrice, nu daarmee geen enkel ander doel werd gediend dan dat van nieuwsgierigheidsbevrediging.[22] Over het onderwerp van bescherming van reputatie en privacy in verhouding tot de vrijheid van meningsuiting is meer informatie te vinden in de hoofdstukken 4 en 6 van dit boek.

Ten slotte heeft het EHRM zich uitgesproken over de manier waarop autoriteiten moeten omgaan met gestolen persoonsgegevens. In de zaak *Romet* was de klager in 1995 het slachtoffer geworden van diefstal van zijn rijbewijs, waarna op zijn naam maar liefst 1737 voertuigen werden geregistreerd in het kentekenregister.[23] De klager ontving daarop een steeds groter aantal aanslagen voor motorrijtuigenbelasting en verkeersboetes en uiteindelijk werden vanwege vermeende fraude zelfs zijn socialezekerheidsuitkeringen stopgezet. Pas in 1997 werd het gestolen rijbewijs ongeldig verklaard. Het Hof oordeelde dat art. 8 EVRM in een dergelijk geval van diefstal van het rijbewijs van toepassing is, nu iemand anders daardoor in de gelegenheid was gesteld de identiteit van klager te misbruiken. Art. 8 EVRM was geschonden in deze zaak, nu de autoriteiten meteen na de aangifte van de diefstal het rijbewijs ongeldig hadden kunnen verklaren; daardoor had misbruik voorkomen kunnen worden. Hieruit blijkt dat de verdragsstaten een positieve verplichting kunnen hebben om ervoor te zorgen dat ook in horizontale rechtsverhoudingen zorgvuldig met persoonsgegevens wordt omgegaan en om individuen te beschermen tegen diefstal van hun identiteit.[24]

20 EHRM 7 juli 1989, nr. 10454/83 (*Gaskin/Verenigd Koninkrijk*).
21 EHRM 10 mei 2011, nr. 48009/08 (*Mosley/Verenigd Koninkrijk*).
22 EHRM 9 oktober 2012, nr. 42811/06 (*Alkaya/Turkije*).
23 EHRM 14 februari 2012, nr. 7094/06 (*Romet/Nederland*).
24 Zie echter ook EHRM 4 december 2008, nrs. 30562/04 en nr. 30566/04 (*S. en Marper/Verenigd Koninkrijk*) en EHRM 18 april 2013, nr. 19522/09 (*M.K./Frankrijk*) voor de grenzen die kunnen worden gesteld aan het verzamelen van persoonsgegevens in verband met de bescherming tegen identiteitsfraude.

2.2 Raad van Europa; overig

2.2.1 Verdrag van Straatsburg

Nederland heeft in 1988 het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens uit 1981 (ook wel het Verdrag van Straatsburg of Conventie 108 genoemd) getekend en in 1993 geratificeerd.[25] Dit Verdrag vormt een uitwerking van art. 8 EVRM en bevat algemene beginselen voor de verwerking van persoonsgegevens. Momenteel hebben zesenveertig landen het Verdrag geratificeerd. In 2001 verscheen een aanvullend protocol[26] waarin onder meer is opgenomen dat verdragspartijen verplicht zijn om een onafhankelijke toezichthoudende autoriteit in te stellen. Deze autoriteit moet toezien op de naleving van de nationale wetgeving en dient te beschikken over onderzoeksmogelijkheden. Daarnaast zijn bepalingen opgenomen omtrent de doorgifte van persoonsgegevens naar landen die geen verdragspartij zijn. Inmiddels hebben vierendertig landen, waaronder Nederland, dit additionele protocol geratificeerd.

Zoals uit de naam van het Verdrag is af te leiden, ziet het Verdrag in beginsel alleen op de g*eautomatiseerde* verwerking van persoonsgegevens. Wel kunnen verdragspartijen ervoor kiezen om de verdragsbepalingen eveneens van toepassing te verklaren op niet-geautomatiseerde verwerkingen of op de verwerking van gegevens van niet-natuurlijke personen. Een persoonsgegeven wordt gedefinieerd als 'any information relating to an identified or identifiable individual' (art. 2 sub a).

Het Verdrag bevat allereerst een aantal algemene beginselen (Chapter II) over het verwerken van persoonsgegevens. Het stelt onder meer eisen aan de zorgvuldigheid, kwaliteit en beveiliging (van de verwerking) van persoonsgegevens. Ook is opgenomen dat de betrokkene van wie de persoonsgegevens worden verwerkt, het recht heeft om de gegevens in te zien en indien nodig te corrigeren en is het recht op een rechtsmiddel vastgelegd om deze rechten af te kunnen dwingen.

Daarnaast worden regels gegeven voor de doorgifte van persoonsgegevens (Chapter III) tussen de verdragspartijen, waarbij als hoofdlijn geldt dat de privacybescherming er niet toe mag leiden dat de doorgifte wordt verhinderd of aan speciale toestemming onderhevig is. Tot slot zijn regels opgesteld over wederzijdse bijstand (Chapter IV) en de totstandkoming van een Raadgevend Comité (Chapter V).

Momenteel wordt het Verdrag van Straatsburg herzien. In juni 2012 heeft het Raadgevend Comité bij het Verdrag zijn definitieve rapport ten aanzien van de modernisering van het verdrag opgeleverd.[27] Het idee is dat, hoewel het Verdrag technologieneutraal is geschreven, het nu ruim dertig jaar oud is. In de tussentijd hebben de ontwikkelingen op het gebied van informatie- en communicatietechnologie een hoge vlucht genomen en daarom is herziening nodig. Ook dienen de samenhang en de coherentie met het recht van de Europese Unie te worden gewaarborgd. Door de enorme toename van wereldwijd dataverkeer acht het Raadgevend Comité het van het grootste belang dat in ieder geval een minimum beschermingsniveau wordt geboden.[28] De herziening zal waar mogelijk worden afgestemd op de voorgenomen herziening van het Europeesrechtelijke kader (waarover nader in par. 2.3). De definitieve herziening kan hierdoor nog enige tijd op zich laten wachten.

25 Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, Raad van Europa, 28 januari 1981, *Trb.* 1988, 7.

26 Aanvullend Protocol bij het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens inzake toezichthoudende autoriteiten en grensoverschrijdend verkeer van gegevens, Straatsburg: 8 november 2001, *Trb.* 2003, 122.

27 Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (T-PD), Final Document on the modernization of Convention 108, 15 juni 2012, T-PD (2012)04Mos.

28 *Idem*, p. 5.

2.2.2 Verhouding EVRM en Verdrag van Straatsburg

Ook voor het sluiten van het Verdrag van Straatsburg had het Hof reeds verduidelijkt dat bepaalde gegevensverwerkingen binnen de reikwijdte van art. 8 EVRM konden vallen. Zo had het in de zaak *Klass*[29] geoordeeld dat het heimelijk afluisteren van telefoongesprekken, waarbij de overheid gegevens van burgers verzamelt, een inmenging vormt in het privéleven. Ook het afluisteren van telefoongesprekken en het verzamelen van telefoongegevens door of in opdracht van de politie in het kader van een opsporingsonderzoek vormt volgens het Hof in de zaak *Malone*[30] een inmenging in het privéleven van de betrokkene. Inmiddels spelen de bepalingen van het Verdrag van Straatsburg een belangrijke rol bij de nadere invulling van art. 8 EVRM, waardoor zij indirect een belangrijke werking hebben gekregen, zelfs waar zij geen rechtstreekse werking hebben. In de zaak *Z t. Finland*[31] heeft het Hof de betekenis van het Verdrag van Straatsburg nadrukkelijk erkend. In de zaak hadden artsen in het kader van een strafrechtelijk onderzoek naar de echtgenoot van Z, medische informatie over Z aan de rechtbank verstrekt. Deze informatie behelsde onder meer dat Z HIV-positief was. Hoewel de zitting gelet op de privacy van de betrokkenen achter gesloten deuren plaatsvond, werd Z, in het arrest dat voor de pers en het publiek openbaar werd gemaakt, met naam en toenaam genoemd. Daarbij werd eveneens vermeld dat zij HIV-positief was. Het Hof kwam onder verwijzing naar diverse bepalingen van het Verdrag van Straatsburg tot de conclusie dat dit een schending van art. 8 EVRM opleverde. In de jurisprudentie van het Hof is een dergelijke argumentatie sindsdien gebruikelijk indien het Hof in het licht van art. 8 EVRM oordeelt over gegevensverwerkingen.

2.2.3 Activiteiten Comité van Ministers

Los van het Verdrag publiceert het Comité van Ministers van de Raad van Europa regelmatig niet-bindende aanbevelingen omtrent de verwerking (en bescherming) van persoonsgegevens en het alomvattende recht op privéleven.[32] Zo verschenen in 2012 aanbevelingen aangaande privacybescherming bij het gebruik van social media[33] en zoekmachines.[34]

2.3 Europese Unie

2.3.1 Europese Privacyrichtlijn

Op Europees niveau kwam in 1995 de Europese Privacyrichtlijn tot stand.[35] Deze Richtlijn is, gebaseerd op art. 95 van het toenmalige EG-Verdrag op grond waarvan regels konden worden gesteld om de werking van de interne markt te verwezenlijken. De Richtlijn is dan ook een internemarktrichtlijn die het vrije gegevensverkeer beoogt te garanderen, een doelstelling die niet ten grondslag ligt aan het Verdrag van Straatsburg. Dit doel blijkt duidelijk uit art. 1 van de Richtlijn:

Artikel 1 Europese Privacyrichtlijn

1. De Lid-Staten waarborgen in verband met de verwerking van persoonsgegevens, overeenkomstig de bepalingen van deze richtlijn, de bescherming van de fundamentele rechten en vrijheden van natuurlijke personen, inzonderheid van het recht op persoonlijke levenssfeer.

29 EHRM 6 september 1987, nr. 5029/71 (*Klass/Duitsland*).
30 EHRM 2 augustus 1984, nr. 8691/79 (*Malone/Verenigd Koninkrijk*).
31 EHRM 25 februari 1997, nr. 22009/93 (*Z/Finland*).
32 Zie <http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp>.
33 Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services, 4 april 2012.
34 Recommendation CM/Rec(2012)3 on the protection of human rights with regard to search engines, 4 april 2012.
35 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, Pb EG 1995 L 281/31.

2. De Lid-Staten mogen het vrije verkeer van persoonsgegevens tussen Lid-Staten beperken noch verbieden om redenen die met de uit hoofde van lid 1 gewaarborgde bescherming verband houden.

Deze doelstelling laat onverlet dat de Richtlijn eveneens beoogt om het fundamentele recht op informationele privacy te versterken. Zo wordt in overweging 10 bij de Richtlijn opgemerkt dat:

> (…) met de nationale wetgevingen betreffende de verwerking van persoonsgegevens de eerbiediging moet worden gewaarborgd van de fundamentele rechten en vrijheden, en met name van het recht op bescherming van de persoonlijke levenssfeer, dat tevens in art. 8 EVRM [afk. FvdJ] en in de algemene beginselen van het Gemeenschapsrecht is erkend; dat derhalve de onderlinge aanpassing van deze wetgevingen niet tot een verzwakking van de aldus geboden bescherming mag leiden, maar juist erop gericht moet zijn een hoog beschermingsniveau in de Gemeenschap te waarborgen.

In overweging 11 wordt de samenhang met het Verdrag van Straatsburg weergegeven; doel is:

> (…) de in deze richtlijn vervatte beginselen met betrekking tot de bescherming van de rechten en de vrijheden van personen, inzonderheid van de persoonlijke levenssfeer, de beginselen van het Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen ter zake van de geautomatiseerde verwerking van persoonsgegevens *verduidelijken* en *versterken* [cursivering FvdJ].

De Richtlijn heeft, in tegenstelling tot het Verdrag van Straatsburg, onder bepaalde omstandigheden niet alleen betrekking op de geautomatiseerde verwerking, maar ook op de niet-geautomatiseerde verwerking van persoonsgegevens. De verwerking van persoonsgegevens voor huishoudelijke en persoonlijke doeleinden valt buiten de reikwijdte van de Richtlijn. Volgens de Richtlijn is een persoonsgegeven:

> (…) iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna 'betrokkene' te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.

De Richtlijn beoogt een gelijkwaardig beschermingsniveau binnen de Europese Unie te waarborgen en ziet op gegevensverwerkingen binnen de private en de publiekrechtelijke sector. Doordat de Richtlijn van voor de afschaffing van de Europese pijlerstructuur dateert, valt onder meer de verwerking van persoonsgegevens in het kader van politiële en justitiële samenwerking niet binnen de reikwijdte van de Richtlijn.

Net als het Verdrag van Straatsburg stelt de Richtlijn algemene voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens. Deze voorwaarden zien op de kwaliteit van de gegevens (art. 6) en de toelaatbaarheid van de verwerking (art. 7). De beginselen van proportionaliteit (is de inbreuk op de privacy evenredig tot het met de verwerking te dienen doel?) en subsidiariteit (kan het doel ook op een minder inbreukmakende wijze worden bereikt?) spelen steeds een rol bij de verwerking van persoonsgegevens. Voor bepaalde categorieën van meer gevoelige gegevens, zoals gegevens over iemands gezondheid of ras, zijn bovendien bijzondere beschermingsbepalingen opgenomen.

In de Richtlijn wordt expliciet aandacht besteed aan de mogelijke botsing tussen het recht op de vrijheid van meningsuiting en het recht op privacy. Lidstaten moeten conform art. 9 uitzonderingen

op en afwijkingen van bepaalde bepalingen uit de Richtlijn in hun nationale wetgeving opnemen, indien dit nodig is om deze rechten met elkaar te verenigen.

De belangrijkste bepalingen met betrekking tot de rechten van de betrokkenen wier persoonsgegevens worden verwerkt staan in art. 10-14 van de Richtlijn. In art. 10 en 11 is de verplichting tot verstrekking van informatie, en derhalve het recht op informatie voor de betrokkene van wie de persoonsgegevens worden vastgelegd, opgenomen. Art. 12 bevat de mogelijkheid voor de betrokkene om bij navraag te doen naar de persoonsgegevens die over hem worden verwerkt en deze te corrigeren. Art. 14 biedt de betrokkene het recht om zich tegen bepaalde gegevensverwerkingen te verzetten.

De Richtlijn bevat daarnaast bepalingen over de beveiliging van de gegevens en de doorgifte van gegevens naar landen buiten de Europese Unie. Ook is er een verplichting opgenomen om gegevensverwerkingen bij de nationale toezichthouder aan te melden en is er een adviesorgaan (de Artikel 29 Werkgroep) ingesteld. Tot slot zijn er bepalingen omtrent het bieden van rechtsmiddelen opgenomen.

Ondanks het feit dat de Richtlijn uit 1995 dateert, roept de uitleg van de bepalingen (en de omzetting daarvan in de Nederlandse wetgeving) nog regelmatig vragen op. Het HvJ EU heeft zich meerdere malen gebogen over de relatie tussen de privacybescherming onder de Richtlijn en de journalistieke exceptie in het kader van de vrijheid van meningsuiting ex art. 10 EVRM. De zaak *Satamedia* betrof bijvoorbeeld een Finse uitgever die elk jaar op papier lijsten publiceerde van bepaalde inkomensgegevens.[36] Op grond van de Finse wetgeving waren deze lijsten openbaar. De uitgever wilde deze gegevens ook via een betaalde sms-dienst ter beschikking stellen. In zijn oordeel gaf het HvJ allereerst aan dat ook reeds eerder gepubliceerde persoonsgegevens onder de Richtlijn bescherming genieten. Daarnaast dient volgens het HvJ het begrip 'journalistieke activiteiten' ruim te worden geïnterpreteerd en kunnen deze activiteiten eveneens een winstoogmerk hebben. Uiteindelijk werd het aan de nationale rechter overgelaten om de daadwerkelijke belangenafweging te verrichten.

2.3.2 ePrivacyrichtlijn

In verband met de opkomst van nieuwe technologieën werd in 1997 een tweede privacyrichtlijn gepresenteerd, specifiek voor de telecommunicatiesector.[37] Deze richtlijn werd echter al snel ingehaald door de actualiteit en daarom in 2002 vervangen door de zogenaamde ePrivacyrichtlijn.[38] De ePrivacyrichtlijn vormt een specificatie en aanvulling van de Privacyrichtlijn op het gebied van gegevensverwerkingen met betrekking tot elektronische communicatie. De Richtlijn grijpt dan ook voor veel definities, waaronder de definitie van het begrip persoonsgegeven, terug op de Privacyrichtlijn.

De ePrivacyrichtlijn biedt bescherming ongeacht welke techniek voor de elektronische communicatie wordt gebruikt. De ePrivacyrichtlijn is in Nederland geïmplementeerd in de Telecommunicatiewet.[39] De reikwijdte van de bescherming onder de ePrivacyrichtlijn strekt zich niet alleen

36 HvJ EG 16 december 2008, zaak C-73/07 (*Satamedia*). Zie eerder ook HvJ EG 6 november 2003, zaak C-101/01 (*Lindqvist*).

37 Richtlijn 97/66/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector, Pb EG 1998 L 24/1.

38 Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, Pb EG 2002 L 201/37, aangepast door Richtlijn 2009/136 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming, Pb EU 2009 L 337/11.

39 Richtlijn 2006/24 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, Pb EU 2006 L 105/54 wordt in deze bijdrage buiten beschouwing gelaten.

uit tot natuurlijke personen, maar ook tot 'abonnees' die rechtspersonen zijn (art. 1 lid 2). Net als de Privacyrichtlijn is de ePrivacyrichtlijn beperkt tot activiteiten die onder het oude EG-verdrag vallen, waardoor onder meer gegevensverwerkingen in het kader van de openbare veiligheid, defensie en staatsveiligheid buiten de reikwijdte van de ePrivacyrichtlijn vallen (art. 1 lid 3).

Aanbieders van openbare elektronische communicatiediensten zijn op grond van de ePrivacyrichtlijn gehouden om het netwerk adequaat te beveiligen (art. 4) en het vertrouwelijke karakter van de communicatie te waarborgen (art. 5). Ook stelt de ePrivacyrichtlijn eisen aan het gebruik van *cookies*. Cookies zijn kleine bestanden met informatie die op de eindapparatuur (bijvoorbeeld een computer of smartphone) worden geplaatst waardoor een website de gebruiker bij een volgend bezoek 'herkent'. Bepaalde cookies maken het mogelijk om het internetgedrag van een gebruiker te monitoren (*tracking cookies*) en daarop advertenties af te stemmen (*targeted advertising*). Bij het gebruik van cookies kunnen persoonsgegevens worden verwerkt. Daarom is het gebruik van cookies alleen toegestaan nadat de gebruiker van de eindapparatuur hieromtrent duidelijk en volledig is geïnformeerd en hiervoor zijn toestemming heeft verleend.

Openbare communicatienetwerken brengen met zich dat ook verkeersgegevens, dat zijn gegevens die worden verwerkt voor overbrengen (transmissie) van de communicatie over het netwerk of voor de facturering daarvan, worden verwerkt. Deze gegevens moeten op grond van art. 6 wanneer zij niet langer nodig zijn voor de transmissie worden gewist of anoniem worden gemaakt. Voor de facturering mogen de verkeersgegevens worden gebruikt totdat de rekening niet meer door de abonnee kan worden aangevochten. Art. 8 bevat regels omtrent het gebruik en de mogelijkheid tot afscherming van nummeridentificatie. Voor locatiegegevens waarmee het mogelijk is om de geografische positie van bijvoorbeeld iemands smartphone aan te geven, is bepaald dat deze slechts anoniem mogen worden verwerkt (art. 9). Ongeanonimiseerde verwerking is alleen mogelijk indien de abonnee daar toestemming voor heeft gegeven. In art. 13 worden regels gegeven omtrent direct marketing (spam). Van een aantal bepalingen van de ePrivacyrichtlijn mag worden afgeweken indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is in het kader van onder meer de nationale en de openbare veiligheid en het voorkomen en opsporen van strafbare feiten (art. 15).

In verschillende uitspraken van het HvJ EU is aan de orde geweest of aanbieders van openbare communicatiediensten gehouden zijn om in bepaalde gevallen de gegevens over naam, adres en woonplaats (NAW-gegevens) van abonnees te verstrekken. Doorgaans gaat het daarbij om een vordering van een derde die de identiteit van een abonnee wil achterhalen omdat de abonnee zich schuldig heeft gemaakt aan auteursrechtschendingen. In de zaak *Promusicae* heeft het HvJ EU bepaald dat er geen algemene verplichting bestaat tot het verstrekken van dergelijke gegevens.[40] Er dient een afweging tussen de verschillende grondrechten plaats te vinden. Dit houdt in dat er zowel rekening moet worden gehouden met de intellectuele eigendomsrechten van de rechthebbenden als de privacybelangen van de abonnees. De belangenafweging kan zo uitvallen dat de gegevens moeten worden verstrekt. In de zaak *Bonnier Audio* heeft het HvJ EU verduidelijkt dat art. 15 van de ePrivacyrichtlijn niet in de weg staat aan een nationale verplichting die aanbieders van telecommunicatiediensten verplicht om NAW-gegevens aan een derde te verstrekken.[41] Momenteel wordt voor de afweging door de Nederlandse rechter de uit het arrest *Lycos-Pessers* afgeleide maatstaf gehanteerd, waarin is bepaald dat het niet verstrekken van NAW-gegevens onder bepaalde omstandigheden, zoals het feit dat de betrokkene de gegevens niet op een andere manier kan achterhalen, strijd kan opleveren met de zorgvuldigheid die jegens een derde in acht moet worden genomen.[42]

40 HvJ EG 29 januari 2008, C-275/06 (*Promusicae/Telefónica*).
41 HvJ EU 19 april 2012, C-461/10 (*Bonnier Audio/ePhone*).
42 HR 25 november 2005, LJN AU4019 (*Lycos/Pessers*).

2.3.3 Verordening 45/2001

De verwerking van persoonsgegevens door de instellingen, organen en instanties van de Europese Unie valt buiten de reikwijdte van de Privacyrichtlijn. Nu het wenselijk was om ook op dit niveau een adequate gegevensbescherming te waarborgen, werd het toenmalige EG-Verdrag aangepast (art. 286 EG-Verdrag (oud)) en werd ter uitvoering van deze wijziging Verordening 45/2001[43] aangenomen. De Verordening geeft algemene voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens. Er worden eisen gesteld aan de kwaliteit en de beveiliging van de gegevens. Daarnaast schetst de Verordening een kader waarbinnen de gegevens mogen worden uitgewisseld tussen de instellingen en/of verstrekt aan andere ontvangers die al dan niet onder de Privacyrichtlijn vallen. Ook biedt de Verordening betrokkenen diverse waarborgen. Zo dient conform art. 11 en 12 adequate informatieverschaffing plaats te vinden en heeft de betrokkene recht op inzage (art. 13), correctie en afscherming van de gegevens (art. 14 en 15). Daarnaast kan de betrokkene onder bepaalde omstandigheden ook verlangen dat gegevens worden gewist (art. 16). De betrokkene kan ook eisen dat derden aan wie de gegevens zijn verstrekt, op de hoogte worden gebracht van elke rectificatie, wissing of afscherming van zijn persoonsgegevens (art. 17). Tot slot kan de betrokkene gebruik maken van het recht van verzet (art. 18). Dit betekent dat een betrokkene kan betogen dat er, gelet op zijn bijzondere individuele omstandigheden, zwaarwegende of gerechtvaardigde redenen om zijn persoonsgegevens niet te verwerken.

In de zaak *Bavarian Lager* heeft het Hof de relatie tussen art. 8 EVRM, de Verordening en de zogenaamde Openbaarmakingsverordening (Eurowob)[44] nader gespecificeerd.[45] Bavarian Lager had bij de Europese Commissie een klacht ingediend tegen het Verenigd Koninkrijk, dat aan de mogelijkheid om bepaald bier op fust te verkopen dusdanige eisen stelde, dat er sprake zou zijn van een kwantitatieve invoerbeperking. Lopende de procedure had Bavarian Lager op grond van de Openbaarmakingsverordening de notulen van een bepaalde Commissievergadering opgevraagd. De Commissie had een geschoonde versie van de notulen verstrekt, nu een aantal mensen zich had verzet tegen de openbaarmaking van hun namen of niet om toestemming kon worden gevraagd. Indien Bavarian Lager ook de gegevens van deze personen wenste te ontvangen, dan diende zij volgens de Commissie de noodzaak van de doorgifte van deze persoonsgegevens aan te tonen. In de Openbaarmakingsverordening is een verwijzing naar Verordening 45/2001 opgenomen op grond waarvan een dergelijke weigering mogelijk is. Het HvJ wijst erop dat uit de considerans bij Verordening 45/2001 blijkt dat art. 8 EVRM via de band van art. 6 EU (oud) door de instellingen in acht moet worden genomen bij de uitvoering van werkzaamheden buiten het toepassingsgebied van Verordening 45/2001. Het HvJ leidt hieruit af dat wanneer een openbaarmakingsverzoek er toe leidt dat door de instellingen toegang wordt gegeven tot documenten die persoonsgegevens bevatten, de bepalingen van Verordening 45/2001 in volle omvang van toepassing zijn. Nu Bavarian Lager de noodzaak voor de doorgifte niet heeft aangetoond heeft de Commissie de verschillende belangen niet kunnen afwegen en heeft zij volgens het HvJ terecht het verzoek op volledige toegang geweigerd.

Op basis van de Verordening is de Europese toezichthouder voor de gegevensbescherming (EDPS) ingesteld die toeziet op de naleving van de Verordening door de instellingen. De EDPS controleert niet alleen de gegevensverwerkingen van de instellingen maar heeft ook een adviserende rol. De instellingen zijn verplicht om de EDPS te raadplegen indien zij administratieve maatregelen over de verwerking van persoonsgegevens willen opstellen of wanneer de Europese Commissie een

43 Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van hun persoonsgegevens door de communautaire instellingen en organen betreffende het vrije verkeer van die gegevens, Pb EG 2001 L 8/1.

44 Verordening 1049/2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie, Pb EG L 145/43.

45 HvJ EU 29 juni 2010, zaak C-28/08P (*Bavarian Lager*).

wetgevingsvoorstel aanneemt betreffende de bescherming van de fundamentele rechten en vrijheden van personen op het gebied van de verwerking van persoonsgegevens. De EDPS heeft ook handhavingsbevoegdheden.

Momenteel bestaat eenige onduidelijkheid over de reikwijdte van de Verordening. De Verordening dateert van voor de inwerkingtreding van het Verdrag van Lissabon en was gericht op de instellingen die zich in de voormalige eerste pijler bevinden. Wel was het al gebruikelijk dat ook instellingen die zich in de derde pijler bevonden advies vroegen aan de EDPS.[46] Nu de pijlerstructuur niet meer bestaat, zal de Verordening moeten worden aangepast om ervoor te zorgen dat duidelijkheid wordt gecreëerd over de vraag of en in hoeverre de bevoegdheden van de EDPS onverkort jegens de andere instellingen kunnen worden uitgeoefend.[47]

2.3.4 Verdrag van Lissabon en EU-Grondrechtenhandvest

Artikel 16 VwEU en Kaderbesluit persoonsgegevens bij samenwerking in strafzaken
Door het Verdrag van Lissabon[48], dat leidde tot wijziging van het Verdrag betreffende Europese Unie en het Verdrag tot oprichting van de Europese Gemeenschap (door het Verdrag van Lissabon gewijzigd in het Verdrag betreffende de werking van de Europese Unie, VwEU), is een algemene rechtsbasis voor de bescherming van persoonsgegevens gecreëerd. In art. 16 VwEU is de volgende bepaling opgenomen:

Artikel 16 VwEU
1. Eenieder heeft recht op bescherming van zijn persoonsgegevens.
2. Het Europees Parlement en de Raad stellen volgens de gewone wetgevingsprocedure de voorschriften vast betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie, alsook door de lidstaten, bij de uitoefening van activiteiten die binnen het toepassingsgebied van het recht van de Unie vallen, alsmede de voorschriften betreffende het vrij verkeer van die gegevens. Op de naleving van deze voorschriften wordt toezicht uitgeoefend door onafhankelijke autoriteiten.
3. De op basis van dit artikel vastgestelde voorschriften doen geen afbreuk aan de in artikel 39 van het Verdrag betreffende de Europese Unie bedoelde specifieke voorschriften.

In een aangehechte verklaring bij het Verdrag van Lissabon is erkend dat op het gebied van de justitiele samenwerking in strafzaken en op het gebied van politiële samenwerking specifieke voorschriften inzake de bescherming van persoonsgegevens en het vrije verkeer van die gegevens op basis van art. 16 VwEU nodig kunnen zijn.[49] Dit heeft in 2008 geleid tot een Kaderbesluit inzake de bescherming van persoonsgegevens bij politiële en justitiële samenwerking in strafzaken.[50] Het Kaderbesluit is alleen van toepassing op de verwerking van grensoverschrijdende persoonsgegevens. In het Kader-

46 Kranenborg en Verhey 2011, p. 53.
47 Dit kan tot een samenloop van bevoegdheden leiden, zie Kranenborg en Verhey 2011, p. 53.
48 Verdrag van Lissabon tot wijziging van het Verdrag betreffende de Europese Unie en het Verdrag tot oprichting van de Europese Gemeenschap, Lissabon 13 december 2007, Pb EU 2007 C 306/1.
49 Annex A bij het Verdrag van Lissabon – Verklaringen betreffende bepalingen van de Verdragen, p. 21 – Verklaring betreffende de bescherming van persoonsgegevens op het gebied van justitiële samenwerking in strafzaken en op het gebied van politiële samenwerking.
50 Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken, Pb EU 2008 L 350/60. De juridische status van een kaderbesluit is vergelijkbaar met die van een Richtlijn. Een kaderbesluit heeft bij onjuiste of ontijdige implementatie echter geen rechtstreekse werking.

besluit wordt voor het begrip 'persoonsgegeven' een vrijwel identieke definitie gebruikt als in de in paragraaf 2.3.1 besproken Privacyrichtlijn. Dit zou kunnen betekenen dat de lidstaten hun interne gegevensverwerkingen aan een ander nationaal beschermingsregime onderwerpen. In Nederland wordt dit onderscheid niet gemaakt omdat het van te voren vaak niet te voorzien is of gegevens wellicht in een later stadium aan een andere lidstaat zullen worden doorgegeven.[51]

Het Kaderbesluit geeft aan dat een aantal algemene beginselen die ook in de Privacyrichtlijn en het Verdrag van Straatsburg zijn opgenomen, een rol speelt bij de gegevensverwerking in het kader van opsporing en vervolging van strafbare feiten. Zo dienen de bevoegde instanties de beginselen van rechtmatigheid, evenredigheid en doelbinding in acht te nemen (art. 3). De mogelijkheden om gegevens te verwerken voor andere doeleinden dan waarvoor de gegevens oorspronkelijk zijn verwerkt, is specifiek uitgewerkt (art. 3 lid 2 jo. art. 11).

Het Kaderbesluit verplicht de bevoegde autoriteiten om gegevens te corrigeren wanneer zij incorrect zijn en ze te wissen of te anonimiseren als zij niet meer nodig zijn voor de doeleinden waarvoor zij zijn verwerkt. In bepaalde gevallen kan het zo zijn dat de gegevens worden afgeschermd als het wissen van de gegevens de belangen van de betrokkene zou kunnen schaden (art. 4). De betrokkene heeft het recht op informatie omtrent de verwerking van zijn gegevens (art. 16). Het is echter aan de lidstaten om via het nationale recht hier zorg voor te dragen.

Aan de betrokkene wordt een recht op inzage geboden (art. 17), alsmede een recht op correctie, uitwissing en afscherming van zijn gegevens (art. 18). Bijzonder is dat als de juistheid van een gegeven door de betrokkene wordt betwist en niet kan worden vastgesteld of het gegeven al dan niet juist is, het gegeven kan worden gemarkeerd (art. 18 lid 2). Het Kaderbesluit biedt de betrokkene eveneens een recht op schadevergoeding en een rechtsmiddel indien zijn rechten worden geschonden. Net als de Privacyrichtlijn bevat het Kaderbesluit bepalingen omtrent de beveiliging van de persoonsgegevens en de doorgifte van persoonsgegevens naar landen buiten de Europese Unie.

Naast het Kaderbesluit zijn er nog diverse specifieke regelingen omtrent het uitwisselen en verwerken van persoonsgegevens door politie en justitie. Te denken valt aan de verwerking van gegevens door instanties als Europol en Eurojust, maar ook aan de Schengen Uitvoeringsovereenkomst (Schengen Informatie Systeem).[52]

EU-Grondrechtenhandvest

In het EU-Grondrechtenhandvest is naast het recht op privacy ook een separaat recht op de bescherming van persoonsgegevens opgenomen.[53] Art. 8 van het Handvest luidt als volgt:

Artikel 8 EU-Grondrechtenhandvest

1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.
2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.
3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels.

Art. 8 Hv kan worden gezien als een aanvulling op art. 16 VwEU, nu niet alleen het subjectieve recht op bescherming van persoonsgegevens wordt vastgelegd, maar hier eveneens – hoe beperkt dan ook – een uitwerking aan wordt gegeven.[54] Art. 52 Hv stelt wel dat er aan de uitoefening van de

51 Kranenborg en Verhey, 2011, p. 49.
52 Het Kaderbesluit laat deze regelingen onverlet, zie overweging 39.
53 Handvest van de Grondrechten van de Europese Unie, 7 december 2000, Pb EG 2000 C 364/1.
54 Kranenborg & Verhey 2011, p. 35.

voornoemde rechten beperkingen mogen worden gesteld. Deze moeten dan wel voorzien zijn bij wet en de essentie van de fundamentele grondrechten respecteren. Conform het evenredigheidsbeginsel kunnen alleen beperkingen worden gesteld die noodzakelijk zijn en daadwerkelijk het algemene belang of de fundamentele rechten van anderen beschermen. Eveneens is in dat artikel aangegeven dat aan de rechten die zijn opgenomen in het Handvest en die corresponderen met rechten die zijn gegarandeerd door het EVRM, dezelfde inhoud en reikwijdte moet worden toegekend als aan de EVRM-bepalingen. Art. 53 Hv geeft aan dat geen van de bepalingen van het Handvest mag worden uitgelegd als een beperking of afbreuk van de rechten die met name door het EVRM worden erkend.

Inmiddels is er in de rechtspraak van het HvJ EU ook al toepassing gegeven aan deze bepaling. In de zaak *Eifert* bepaalde het HvJ EU bijvoorbeeld dat EU-bepalingen die een verplichting met zich brengen om de bedragen van aan natuurlijke personen uitgekeerde Europese landbouwsubsidies op naam te publiceren op een voor een ieder toegankelijke website, strijdig zijn met art. 7 (algemeen recht op privacy) en art. 8 Hv.[55] In deze zaak was een wettelijke basis voor de publicatie van de namen van de subsidieontvangers voorhanden. De vraag die het HvJ EU derhalve moest beantwoorden was of de publicatie van de namen noodzakelijk was. Het doel van de maatregel was om transparant te zijn over het gebruik van overheidsgelden. Het vermelden van de namen van de subsidieontvangers was volgens het HvJ EU echter niet noodzakelijk om dit doel te bereiken. Er waren andere methoden denkbaar, zoals een beperktere nominatieve bekendmaking. Derhalve was aan het noodzakelijksheidsvereiste niet voldaan.

Onafhankelijke toezichthouder

Het EU-Grondrechtenhandvest legt, evenals art. 16 VwEU, de verplichting op aan alle lidstaten tot het instellen van een onafhankelijke toezichthouder. Deze verplichting bestond voor Nederland al op grond van het additionele protocol bij het Verdrag van Straatsburg, zie paragraaf 2.2. Deze verplichting heeft tot de nodige jurisprudentie geleid. Zo zijn zowel Oostenrijk, Duitsland als Hongarije op de vingers getikt omdat hun nationale toezichthouders niet onafhankelijk genoeg konden opereren. In *Commissie t. Oostenrijk* bepaalde het HvJ EU onder meer dat het enkele risico van invloeden van buiten, zoals het feit dat het secretariaat dat ter beschikking wordt gesteld bestaat uit personeel dat voor de bondskanselarij werkt, voldoende is om aan te nemen dat er geen sprake is van voldoende onafhankelijkheid.[56] Deze uitspraak bevestigde een eerdere uitspraak van het Hof in *Commissie t. Duitsland*, waarin het overheidstoezicht in strijd met de onafhankelijkheid van de toezichthouder had aangemerkt. [57]

In *Commissie t. Hongarije* ging het om de nationale reorganisatie van de Hongaarse toezichthouder door de oprichting van een nationale autoriteit. [58] Door deze reorganisatie verloor de toenmalige toezichthouder vroegtijdig zijn mandaat en keerde hij niet terug bij de nieuwe nationale autoriteit. Volgens het Hof is de persoonlijke onafhankelijkheid van de toezichthouder een kernelement van het EU-recht en omvat dit eveneens de bescherming tegen een vroegtijdige verwijdering uit het toezichtsambt. Hiervan kan niet worden afgeweken, ook niet door een nationale reorganisatie. Ten tijde van schrijven had Hongarije beroep tegen de uitspraak aangetekend.

Herziening Europeesrechtelijk kader ten aanzien van de bescherming van persoonsgegevens

Op 25 januari 2012 heeft de Europese Commissie een pakket voorstellen tot hervorming van het huidige Europeesrechtelijke kader ten aanzien van de bescherming van de persoonsgegevens gepre-

55 HvJ EU 9 november 2010, gev. zaken C-92/09 en C-93/09 (*Eifert*).
56 HvJ EU 16 oktober 2012, zaak C-614/10 (*Europese Commissie/Oostenrijk*).
57 HvJ EU 9 oktober 2010, zaak C-518/07 (*Europese Commissie/Duitsland*).
58 HvJ EU 8 juni 2012, zaak C-288/12 (*Europese Commissie/Hongarije*).

senteerd. De Europese Privacyrichtlijn dateert van voor het internet- (en sociale media-)tijdperk en biedt daardoor onvoldoende bescherming in een tijdperk waarin de datastromen enorm zijn toegenomen, databases gemakkelijk aan elkaar gekoppeld kunnen worden en persoonsgegevens zich vaak niet meer op een plaats, maar in de 'cloud' bevinden.

Het gepresenteerde pakket voorziet in een algemene verordening voor de bescherming van persoonsgegevens[59] en een aparte richtlijn voor de verwerking van persoonsgegevens in de politiële en justitiële samenwerking.[60] De Europese Commissie heeft aangegeven dat dit pakket moet waarborgen dat het EU-Grondrechtenhandvest op het punt van het recht op bescherming van persoonsgegevens ook in dit digitale tijdperk effect heeft en houdt.[61]

De voorgestelde verordening grijpt direct in op het zelfbeschikkingsrecht van de lidstaten door de directe werking die van dit instrument uitgaat. Daarbij geldt dat door de keuze voor een verordening geen implementatie in nationale wetgeving meer benodigd is. De toepasselijkheid van Verordening wordt uitgebreid: de privacyregels gaan ook gelden voor bedrijven die buiten de Europese Unie persoonsgegevens verwerken van Europese burgers indien deze bedrijven goederen of diensten aanbieden aan Europese burgers of hun gedrag observeren. De Verordening beoogt onder meer het invoeren van hoge sancties (bijvoorbeeld boetes tot 2% van de wereldwijde omzet van een onderneming). Ook is er een verplichting voor bedrijven met meer dan 250 werknemers opgenomen om een *data protection officer* aan te stellen. Daarnaast worden er strengere eisen aan de beveiliging van persoonsgegevens gesteld. Ook wordt er een meldplicht ingevoerd in geval van datalekken, waaronder kort gezegd het verlies van persoonsgegevens of de ongeautoriseerde toegang daartoe wordt verstaan. Verder is voorgesteld om een 'recht op vergetelheid' in te voeren, dat kort gezegd inhoudt dat persoonsgegevens van betrokkenen definitief moeten worden verwijderd, niet alleen bij de partij waar verwijdering verzocht wordt, maar ook bij derden aan wie de gegevens zijn verstrekt. De algehele consensus lijkt te zijn dat dit recht in de praktijk onuitvoerbaar zal zijn.

In de voorgestelde richtlijn zijn algemene beginselen opgenomen voor de gegevensverwerking door de daartoe bevoegde autoriteiten bij het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten. In tegenstelling tot het Kaderbesluit, dat zal komen te vervallen, is de voorgestelde richtlijn niet alleen van toepassing op grensoverschrijdende gegevensverwerkingen maar ook op binnenlandse gegevensverwerkingen.

Bij het verwerken van persoonsgegevens moet in het vervolg onderscheid worden gemaakt tussen de verschillende categorieën van personen waarvan gegevens worden verwerkt (verdachten, veroordeelden, slachtoffers, getuigen of anderen). De voorgestelde Richtlijn formuleert tevens een ruime informatieverplichting voor de bevoegde autoriteiten die de gegevens verwerken. De betrokkene moet adequaat, in duidelijke en begrijpelijke taal, over zijn inzage- en correctierecht en het recht om persoonsgegevens te laten wissen worden geïnformeerd. Ook moet hij worden gewezen op de mogelijkheid om via de toezichthouder op indirecte wijze inzage in de persoonsgegevens te krijgen. De toezichthouder kan dezelfde toezichthouder zijn als de toezichthouder die toezicht houdt op de naleving van de voorgestelde verordening en zal in Nederland derhalve vermoedelijk het College bescherming persoonsgegevens zijn. De meldplicht voor datalekken is ook in de richtlijn terug te

59 Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming), 25 januari 2012, COM(2012) 11 def.

60 Voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende bescherming van natuurlijke personen in verband met de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens, 25 januari 2012, COM(2012) 10 def.

61 Europese Commissie, *2012 Report on the Application of the EU Charter of Fundamental Rights*, p. 7.

vinden. Daarnaast zijn bepalingen opgenomen aangaande de doorgifte van persoonsgegevens naar derde landen (landen buiten de Europese Unie) en/of internationale organisaties.[62]

Het voorgestelde pakket creëert geen uniform privacyrechtelijk kader, nu er een aparte richtlijn voor de verwerking van persoonsgegevens door politie en justitie naast de verordening zal gelden. Ook worden Verordening 45/2001 en diverse specifieke regelingen ten aanzien van het verwerken en uitwisselen van persoonsgegevens op het gebied van politiële en justitiële samenwerking niet in de herziening meegenomen. Nu in de voorstellen een implementatietermijn van twee jaar is opgenomen, wordt de inwerkingtreding van het pakket niet voor 2017 verwacht.

3. Nederland

3.1 De Grondwet

In Nederland is het recht op bescherming van persoonsgegevens sinds 1983 neergelegd in art. 10 van de Grondwet:

Artikel 10 Grondwet

1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.
3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

Art. 10 lid 2 en 3 Gw leggen aan de wetgever de verplichting op om het recht op bescherming van persoonsgegevens nader wettelijk te verankeren. Daarbij wordt specifiek gewezen op de mogelijkheid voor personen om inzage te kunnen krijgen in de gegevens die over hen zijn vastgelegd en deze te corrigeren. Deze instructienormen kunnen worden aangemerkt als positieve verplichtingen die voortvloeien uit het eerste lid.[63]

In november 2010 heeft de Staatscommissie Grondwet in haar rapport geadviseerd om art. 10 Gw te splitsen in een bepaling inzake het recht op bescherming van de persoonlijke levenssfeer en een bepaling inzake het recht op bescherming van persoonsgegevens.[64] Volgens de Staatscommissie wordt door een zelfstandig recht op bescherming van persoonsgegevens bewerkstelligd dat de bescherming niet alleen is gekoppeld aan de persoonlijke levenssfeer van de betrokkene, maar ook kan samenhangen of botsen met andere grondrechten.[65] Ook is, zoals in de voorgaande paragrafen besproken, op Europees niveau het recht op bescherming van persoonsgegevens eveneens als een zelfstandig grondrecht aangemerkt. De technologische ontwikkelingen en de daarmee gepaard gaande explosieve stijging van de verwerking van persoonsgegevens vormen een derde reden om te komen tot een

62 Voor een uitgebreide bespreking zie Van der Jagt 2012, p. 118-126.
63 Overkleeft-Verburg 2000, p. 158.
64 *Rapport Staatscommissie Grondwet*, Den Haag november 2010, *Kamerstukken II* 2010/11, 31570, nr. 17, bijlage, p. 80.
65 *Idem*, p. 81.

zelfstandig recht op de bescherming van persoonsgegevens.[66] De Staatscommissie heeft verschillende voorstellen gedaan voor een nieuwe tekst van het artikel.[67] Vooralsnog heeft de regering echter aangegeven geen reden te zien om de Grondwet op dit punt daadwerkelijk te wijzigen.[68]

3.2 Uitwerking in wetgeving: Wbp en andere wetten

De in art. 10 Gw opgenomen verplichting tot het vaststellen van regels met betrekking tot persoonsgegevens heeft de basis gevormd voor de invoering van de Wet persoonsregistraties (Wpr)[69], de Wet politieregisters (WPolr)[70] en de Wet gemeentelijke basisadministraties (Wet GBA)[71] met de daarbij horende uitvoeringsregelingen. De opvolger van de Wpr, de Wet bescherming persoonsgegevens (Wbp) is voor dit boek echter het meest relevant. Om die reden concentreren wij ons op deze wet (par. 3.2.1), net als op de Wet bescherming persoonsgegevens BES (par. 3.2.2). De overige wetgeving komt kort aan bod in par. 3.2.3.

3.2.1 De Wet bescherming persoonsgegevens

In 2001 werd de Wpr vervangen door de Wbp[72], die de implementatie vormde van de Europese Privacyrichtlijn.

De Wbp is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens en op de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand (bijvoorbeeld een kaartenbak) zijn opgenomen (art. 2 lid 1 Wbp). Kernbegrippen van de wet zijn dan ook het begrip 'persoonsgegeven' en het begrip 'verwerking'. Een persoonsgegeven is kort gezegd elk gegeven betreffende een geïdentificeerde of een identificeerbare persoon (art. 1 sub a Wbp). Het begrip verwerking ziet op alle handelingen die met betrekking tot de persoonsgegevens kunnen worden verricht (art. 1 sub b Wbp), zoals het opslaan, ordenen en bewaren van gegevens, maar ook het vernietigen daarvan. Beide begrippen worden ruim uitgelegd.[73] Zo worden een IP-adres, de reisgegevens van de OV-chipkaart en de foto daarop, maar ook bepaalde informatie van WiFi-routers, aangemerkt als persoonsgegevens.

De meeste verplichtingen op grond van de Wbp berusten op de verantwoordelijke: degene die het doel en de middelen van de gegevensverwerking bepaalt (art. 1 sub d Wbp). De verantwoordelijke moet onder meer de gegevens op een zorgvuldige en behoorlijke wijze verwerken (art. 6 Wbp) en mag dit alleen doen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (art. 7 Wbp). Ook moet de gegevensverwerking worden gebaseerd op een van de limitatief in de wet opgesomde verwerkingsgronden (art. 8 Wbp). De beginselen van proportionaliteit en subsidiariteit gelden onverkort.

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is voor de verwezenlijking van de doeleinden (art. 10 Wbp). Daarnaast gelden er eisen met betrekking tot de beveiliging

66 *Idem*, p. 82.
67 Voor een uitgebreide analyse zie Verhey 2011 en Koops 2011.
68 Kabinetsreactie rapport Staatscommissie, *Kamerstukken II* 2011/12, 31570, nr. 20, p. 8.
69 Wet van 28 december 1988, houdende regels ter bescherming van de persoonlijke levenssfeer in verband met persoonsregistraties (Wet Persoonsregistraties), *Stb.* 1988, 665.
70 Wet van 21 juni 1990, houdende regels ter bescherming van de persoonlijke levenssfeer in verband met politieregisters (*Wet politieregisters*), *Stb.* 1990, 414.
71 Wet van 9 juni 1994, houdende regels ter zake van de gemeentelijke basisadministratie van persoonsgegevens (*Wet GBA*), *Stb.* 1994, 494.
72 Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (*Wet bescherming persoonsgegevens*), *Stb.* 2000, 302.
73 Zie onder meer Artikel 29 Werkgroep: *Advies 4/2007 over het begrip persoonsgegeven*, goedgekeurd op 20 juni 2007, WP 136.

van de persoonsgegevens (art. 13 en 14 Wbp). Tevens gelden additionele eisen voor het verwerken van bijzondere gegevens (art. 16 Wbp). Bijzondere gegevens zijn gegevens waarvan de kans dat inbreuk wordt gemaakt op de privacy van de betrokkene groter is dan bij andere gegevens. Voorbeelden hiervan zijn medische gegevens, gegevens over iemands ras of seksuele voorkeur. In beginsel mag de verantwoordelijke deze gegevens niet verwerken, tenzij hij een beroep kan doen op een wettelijke uitzondering. Ook zijn er speciale regels voor de doorgifte van persoonsgegevens naar landen buiten de Europese Unie.[74]

Aan de betrokkene, dat is degene op wie de persoonsgegevens betrekking hebben (art. 1 sub d Wbp), worden verscheidene rechten toegekend. Van belang is om hierbij op te merken dat de Wbp rechten voor de betrokkene creëert, ook als er bij de verwerking van persoonsgegevens *geen* sprake is van een inbreuk op zijn persoonlijke levenssfeer.[75] Zo heeft een betrokkene recht op informatie omtrent de verwerking van zijn persoonsgegevens (art. 33 en 34 Wbp) en mag hij op verzoek zijn gegevens inzien (art. 35 Wbp). Daarnaast heeft hij het recht om zijn persoonsgegevens te laten corrigeren (art. 36 Wbp) en om in bepaalde gevallen zich te verzetten tegen de verwerking van zijn persoonsgegevens (art. 40 en 41 Wbp). Met de toekenning van deze rechten wordt voldaan aan art. 10 lid 3 Gw.

Het College bescherming persoonsgegevens (Cbp) houdt toezicht op de naleving van de Wbp. De verantwoordelijke heeft in beginsel de plicht om gegevensverwerkingen bij het Cbp aan te melden. Het Cbp houdt een online-register van deze meldingen bij. Ook op deze wijze wordt getracht de betrokkene meer inzicht te geven in gegevensverwerkingen die op hem betrekking hebben.

3.2.2 De Wet bescherming persoonsgegevens BES

Door de ontmanteling van de Nederlandse Antillen per 10 oktober 2010 zijn de zogeheten BES-eilanden (Bonaire, Sint Eustatius en Saba) onderdeel van het Nederlandse staatsbestel geworden.[76] Hierdoor is de Grondwet en derhalve het recht op bescherming persoonsgegevens op de BES-eilanden van rechtstreekse toepassing. Dit leidde tot de noodzaak om ook voor de BES-eilanden te voorzien in een wettelijke regeling nu in het voormalige land de Nederlandse Antillen geen algemene regeling voor de verwerking van persoonsgegevens bestond.

Het Europese recht is op de BES-eilanden niet van toepassing, nu de BES-eilanden hun status als 'Landen en Gebieden Overzee' (LGO) hebben behouden. Dit brengt met zich dat ook de Europese Privacyrichtlijn niet van toepassing is. Wel gelden art. 8 EVRM en 17 IVBPR onverkort. Daarnaast is het Verdrag van Straatsburg met het bijbehorende additionele protocol van de Raad van Europa voor de BES-eilanden bekrachtigd.[77]

74 Er zijn ook nog diverse specifieke verdragen gesloten over de doorgifte van persoonsgegevens, zoals het SWIFT-verdrag voor de uitwisseling van bankgegevens tussen de EU en de Verenigde Staten. Deze specifieke verdragen laten wij in dit hoofdstuk buiten beschouwing.

75 *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 7.

76 Rijkswet van 7 september 2010 tot wijziging van het Statuut voor het Koninkrijk der Nederlanden in verband met de wijziging van de staatkundige hoedanigheid van de eilandgebieden van de Nederlandse Antillen (Rijkswet wijziging Statuut in verband met de opheffing van de Nederlandse Antillen), *Stb.* 2010, 333.

77 Wet van 17 mei 2010, houdende goedkeuring van verdragen met het oog op het voornemen deze toe te passen op Bonaire, Sint Eustatius en Saba, en van het voornemen tot opzegging van verdragen voor Bonaire, Sint Eustatius en Saba, *Stb.* 2010, 348, art. 1 onder 48 en 50. Zie ook: Council of Europe, Communication contained in a Note verbale from the Permanent Representation of the Netherlands, dated 27 September 2010, registered at the Secretary General on 28 September 2010.

De wetgever heeft ervoor gekozen om voor de BES-eilanden de Wbp niet één op één over te nemen, mede gelet op het feit dat de Wbp voortvloeit uit een Europese richtlijn welke niet op de eilanden van toepassing is. Daarnaast geldt dat er afwijkende wetgeving kan worden opgesteld voor de BES-eilanden, gelet op het onder meer de bevolkingsomvang, de grote afstand tot Nederland en het insulaire karakter.[78] Daarom is op 10 oktober 2010 de Wet bescherming persoonsgegevens BES (Wbp BES)[79] in werking getreden, waarvoor een aparte toezichthouder zal worden opgericht (Commissie bescherming persoonsgegevens BES). De Wbp en Wbp BES vertonen grote gelijkenissen.[80] In de Wbp BES zijn eveneens de rechten van de betrokkenen zoals opgenomen in de Wbp, terug te vinden.[81]

3.2.3 Andere Nederlandse wetgeving inzake de verwerking van persoonsgegevens

Het Europese Kaderbesluit voor de bescherming van persoonsgegevens bij politiële en justitiële samenwerking in strafzaken is in Nederland omgezet in de Wet politiegegevens (Wpg) die de WPolr heeft vervangen en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Beide wetten zijn op 1 januari 2012 in werking getreden. De eerdergenoemde Wet GBA wordt ten tijde van schrijven herzien.[82] In al deze wetten zijn de hiervoor besproken rechten van de betrokkenen conform art. 10 lid 3 Gw gewaarborgd. Het toezicht op de Wpg, Wjsg en de Wet GBA berust bij het Cbp.

In diverse andere wetten zijn bepalingen opgenomen om het recht op bescherming te waarborgen. Hierbij kan onderscheid worden gemaakt tussen twee modellen.[83] In het eerste model is ervoor gekozen om regels in een bijzondere wet op te nemen, waarbij de Wbp van toepassing is op de gebieden die niet in de specifieke wet geregeld zijn. Voorbeelden zijn de Kadasterwet en de Wet op de Geneeskundige Behandelingsovereenkomst. Daarnaast is er voor verschillende sectoren een uitputtend privacyregime geschapen. Hier vallen de voornoemde Wpg, Wjsg en Wet GBA onder, maar bijvoorbeeld ook de Wet op de inlichtingen- en veiligheidsdiensten 2002.

4. Internationaal

4.1 IVBPR

4.1.1 Artikel 17 IVBPR

In art. 17 IVBPR is neergelegd:

78 *Kamerstukken II* 2006/07, 30 800 IV, nr. 5, met aangehechte Slotverklaring en de brief van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van 26 september 2008 inzake juridische keuzes, *Kamerstukken II* 2008/09, 31 568, nr. 3, p. 3

79 Wet van 17 mei 2010, houdende regels inzake de bescherming van persoonsgegevens van Bonaire, Sint Eustatius en Saba (Wet bescherming persoonsgegevens BES), *Stb.* 2010, 349.

80 Voor een uitgebreide vergelijking zie Van der Jagt 2010, p. 289-295.

81 Zie art. 25 en 26 voor het recht op informatie, art. 27 voor het inzagerecht, art. 28 (correctierecht) en art. 32 en 33 voor het recht van verzet.

82 *Kamerstukken I* 2012/13, 33 219 A, Nieuwe regels voor een basisregistratie personen (Wet basisregistratie personen). Het voorstel is op 16 april 2013 aangenomen door de Eerste Kamer.

83 *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 12.

Artikel 17 IVBPR

1. Niemand mag worden onderworpen aan willekeurige of onwettige inmenging in zijn privéleven, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer een goede naam.
2. Een ieder heeft recht op bescherming door de wet tegen zodanige inmenging of aantasting.

Art. 17 IVBPR heeft als een ieder verbindende verdragsbepaling rechtstreekse doorwerking in het nationale recht. De daadwerkelijke doorwerking van dit artikel lijkt in de praktijk echter beperkt: in de Nederlandse jurisprudentie wordt, gelet op de uitgebreide bescherming die art. 8 EVRM biedt, art. 17 IVBPR nauwelijks als toetsingskader gehanteerd.[84]

4.2 OESO Guidelines

De Organisatie voor Economische Samenwerking en Ontwikkeling, de OESO, heeft in 1980 de OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* aangenomen.[85] De Guidelines zijn niet-bindend. Nu de OESO als doelstelling het stimuleren van sociaal en economisch beleid heeft, is de achtergrond van deze Guidelines dat handel niet belemmerd mag worden door discrepanties in de wijzen waarop persoonsgegevens door de 34 bij de OESO aangesloten landen, waaronder Nederland, worden beschermd.

De Guidelines zijn opgedeeld in vijf hoofdstukken. Na het uiteenzetten van de definities (Part I) worden algemene beginselen (principles) voor het verwerken van persoonsgegevens geschetst, zoals het doelbindings- en transparantiebeginsel (Part II). Daarna wordt aandacht besteed aan het faciliteren van de doorgifte van persoonsgegevens door (en tussen) de bij de OESO aangesloten landen (Part III). Tot slot wordt aandacht besteed aan de implementatie van beginselen en doorgiftemogelijkheden in de nationale wetgeving (Part IV) en de internationale samenwerking op dit gebied tussen de bij de OESO aangesloten landen (Part V).

5. Vergelijking en integratie

Het recht op gegevensbescherming wordt zowel beschermd via internationale normen als door de rechtsnormen die in het kader van de Europese Unie zijn ontwikkeld. Hierdoor is op verschillende punten overlap ontstaan. Daarbij geldt bovendien dat, doordat de meeste Europese Uniewetgeving dateert uit het tijdperk van de pijlerstructuur, het leeuwendeel van de Europese wetgeving niet of slechts gedeeltelijk en in aangepaste vorm van toepassing is op de gegevensverwerking door politie en justitie. Ook op nationaal niveau gelden naast de algemene Wbp, tal van sectorspecifieke regelingen. Bij de interpretatie van alle bepalingen speelt art. 8 EVRM een rol. Dit levert een kaleidoscopische en gefragmenteerde bescherming van persoonsgegevens op, waarbij een volledig vergelijkend overzicht moeilijk is te geven.

Dit blijkt bijvoorbeeld als wordt gekeken naar de vraag welke gegevens nu eigenlijk worden beschermd. Ten aanzien van de verhouding tussen art. 8 EVRM en het Verdrag van Straatsburg geldt dat het Verdrag van Straatsburg in beginsel niet ziet op de niet-automatische verwerking van

84 Koekkoek 2000, p. 159.

85 OECD, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 23 september 1980.

persoonsgegevens. Deze gegevensverwerkingen kunnen echter wel binnen de reikwijdte van art. 8 EVRM worden gebracht, indien er sprake is van een inmenging in het privéleven. De Europese Privacyrichtlijn (en de daaruit voortvloeiende Wbp), beschermt alle verwerkingen van persoonsgegevens. Niet bij alle gegevensverwerkingen is echter sprake van een inmenging in het privéleven van de betrokkene. Indien er geen sprake is van een dergelijke inmenging, dan komt aan deze gegevensverwerking geen bescherming toe op grond van art. 8 EVRM. De gegevens kunnen eventueel wel voor bescherming in aanmerking komen via de band van het Verdrag van Straatsburg. Bij de verwerking van gegevens door politie en justitie geldt dit op dezelfde manier. Daarbij dient bovendien te worden opgemerkt dat op Europees niveau onder het Kaderbesluit, alleen aan grensoverschrijdende gegevensverwerkingen bescherming toekomt. Op nationaal niveau bestaat een dergelijk onderscheid niet en genieten ook de nationale verwerkingen van politie en justitie de bescherming van de relevante Europese regelgeving.

Het door de Europese Commissie voorgestelde nieuwe pakket van wetgeving zal deze fragmentatie slechts gedeeltelijk ongedaan maken. Het zou het recht op gegevensbescherming ten goede komen indien in ieder geval op het niveau van de Europese Unie, de lappendeken wordt omgevormd tot een prachtige sprei.

6. Literatuur

Van der Jagt, F.C. (2010), 'Privacybescherming op de voormalige Nederlandse Antillen: de Wbp BES', *Privacy & Informatie* 2010 (6), p. 289-295

Van der Jagt, F.C. (2012), 'De ontwerprichtlijn gegevensbescherming opsporing en vervolging', *Privacy & Informatie* 2012 (3), p. 118-126

Kingma, S.H. (2012), 'De botsing tussen IE- en privacyrechten. Het einde van het Lycos/Pesserstijdperk', *Privacy & Informatie* 2012 (4), p. 170-176

Koops, B.J. (2011), 'Digitale grondrechten en de Staatscommissie: op zoek naar de kern', *Tijdschrift voor Constitutioneel Recht* 2011 (2), p. 168-185

Kranenborg, H.R. & Verhey, L.F.M. (2011), *Wet bescherming persoonsgegevens in Europees perspectief*, Deventer: Kluwer 2011

Overkleeft-Verburg, G. (2000), 'Het grondrecht op eerbiediging van de persoonlijke levenssfeer', in: Koekkoek, A.K., *De Grondwet, Een systematisch en artikelsgewijs commentaar*, Deventer: Kluwer 2000

Verhey, L.F.M. (2011), Grondrechten in het digitale tijdperk: driemaal is scheepsrecht?, *Tijdschrift voor Constitutioneel Recht* 2011 (2), p. 152-167