PRIVACYVOORWAARDEN VOOR DE IOVERHEID

VUISTREGELS VOOR WET- EN REGELGEVERS MET BETREKKING TOT OVERHEIDSINFORMATIESYSTEMEN

Gerrit-Jan Zwenne & Wilfred Steenbruggen[1]

1. INLEIDING

Overheden en wetgever hebben een groot vertrouwen in informatie- en communicatietechnologie (ICT). In het rapport over iOverheid zet de WRR uiteen dat de technologie enthousiast wordt binnengehaald voor zowel de complexe administratieve opdracht van de overheid, als de aanpak van urgente maatschappelijke uitdagingen, zoals terrorisme, veiligheid, mobiliteit en goede en betaalbare zorg.[2] Een recent voorbeeld daarvan is het voornemen van om sociale zekerheids- en belasting fraude aan te pakken door grootschalige gegevenskoppeling en analyse, het Systeem Risico Indicatie of SyRi.[3] Ook bij de grote decentralisatieoperaties, waarbij de rijksoverheid taken op het gebied van jeugdzorg, werk en inkomen en zorg aan langdurig zieken en ouderen overhevelt naar gemeenten, wordt vertrouwd op ICT.[4]

Over dit 'ICT-enthousiasme' bij de overheid zijn zorgen. In dat verband is er vooral veel aandacht voor de soms spectaculaire budgetoverschrijdingen, vertragingen of mislukkingen waarnaar de Tijdelijke Commissie ICT-projecten bij de Overheid (Commissie Elias) de afgelopen jaren onderzoek deed.[5] Veel minder aandacht is er voor de faalfactoren verband houden met de niet-naleving van juridische vereisten, meer in het bijzonder het risico dat bij overheidsprojecten onvoldoende rekening wordt gehouden met fundamentele rechten en vrijheden.

Toch liggen, en dat is het uitgangspunt van deze bijdrage, ook daar serieus te nemen faalfactoren. We denken dan vooral aan de vereisten die voortvloeien uit het recht op bescherming van de persoonlijke levenssfeer en het daarvan te onderscheiden recht op bescherming van persoonsgegevens, zoals vastgelegd in het EVRM en het Handvest van de Europese Unie. Op grond daarvan hebben de rechtscolleges in Straatsburg respectievelijk Luxemburg meer dan een handvol uitspraken gedaan die ook betekenis hebben voor de inmiddels door de overheid opgetuigde en nog op te tuigen informatiesystemen.

---

[1] Gerrit-Jan Zwenne is hoogleraar Recht en de informatiemaatschappij aan de Universiteit Leiden, alsmede advocaat bij Bird & Bird LLP te Den Haag; Wilfred Steenbruggen is advocaat bij Bird & Bird LLP te Den Haag.

[2] WRR, *iOverheid*, rapport nr. 86, Den Haag / Amsterdam 2011, p. 11, 34 en 93.

[3] Besluit van 1 september 2014 tot wijziging van het Besluit SUWI in verband met regels voor fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens met inzet van SyRI, Stb. 2014, 320

[4] Zie bijv. de zgn. decentralisatiebrief van Plassterk aan de Tweede Kamer van 19 februari 2013, kenm. 2013-0000108917, p. 11.

[5] *Kamerstukken II* 2014/15, 33 326, nr. 5.

G-J. Zwenne & W. Steenbruggen, 'Privacyvoorwaarden voor iOverheid', *Regelmaat* 2015/2

Als zodanig heeft die rechtspraak ook betekenis voor wat wel wordt aangeduid als de privacy impact assessment of PIA, zijnde het instrument waarvan de wetgever geacht wordt gebruik te maken bij de voorbereiding van wetgeving die gevolgen kan hebben voor de bescherming van de persoonlijke levenssfeer.[6] Een PIA is vooral een instrument om in een vroegtijdig stadium van de ontwikkeling van nieuwe producten, diensten en beleidsvoornemens de privacyrisico's hiervan op overzichtelijke wijze in kaart te brengen, en als zodanig nuttig en waardevol, maar geeft nog geen garantie dat wordt voldaan aan de eisen van het EVRM en het Handvest, te meer omdat die steeds in ontwikkeling zijn en blijven.

In deze bijdrage willen wij om die reden aan de hand van een aantal recente uitspraken in kaart brengen welke voor ICT-projecten van de overheid relevante vereisten onder andere kunnen worden afgeleid uit de rechtspraak van het Europees Hof voor de Rechten van Mens (Straatsburg) en het Hof van de Europese Unie en zijn voorganger het Hof van Justitie (Luxemburg). Een onvoldoende naleving van dergelijke vereisten kan niet minder een faalfactor zijn dan een tekort aan 'projectbeheersing' of 'projectportfoliomanagement'. Ook dat kan betekenen dat een overheidsinformatiesysteem niet, of niet volledig, in gebruik kan worden genomen, of in elk geval niet de verwachtingen ervan kan waarmaken.

Onze selectie van de hier behandelde gerechtelijke uitspraken is mogelijk arbitrair. Wij menen evenwel dat het gaat om leidende uitspraken en zien dat bevestigd in de literatuur daarover.[7] We maken niettemin het onvermijdelijke voorbehoud dat het niet onze bedoeling is om een uitputtend overzicht te geven van de relevante rechtspraak. Het is al heel wat als we zouden kunnen komen tot een aantal vuistregels aan de hand waarvan een inschatting kan worden gemaakt van de mate waarin een overheidsinformatiesysteem voldoet aan vereisten die voortvloeien uit voornoemde rechtspraak.

Een en ander doen wij door in te gaan op drie aspecten of thema's die voor veel van dergelijke overheidsprojecten direct of indirect relevant zijn, te weten: (1) grootschalige gegevensopslag: de behoefte om persoonsgegevens centraal of decentraal op te slaan en beschikbaar te stellen; (2) transparantie: het al dan niet heimelijke vastleggen van persoonsgegevens en (3) de beveiliging van persoonsgegevens; juridische en andere waarborgen tegen verlies of diefstal van persoonsgegevens.

2. GEGEVENSVASTLEGGING EN -OPSLAG

Meten is weten. Wie wat bewaart heeft wat. En baat het niet, dan schaadt het niet. Voor overheden maakt het voor langere tijd bewaren van zoveel mogelijk persoonsgegevens het mogelijk om uiteenlopende problemen op te lossen. Een voorbeeld biedt het biometrisch paspoort, het paspoort met daarin een computerchip waarop een aantal vingerafdrukken van de houder zijn vastgelegd. De overweging om vingerafdrukken op te slaan, hadden aanvankelijk alleen betrekking op het tegengaan van vervalsingen en het voorkomen van identiteitsfraude. Al heel snel werd voorgesteld, vingerafdrukken ook op te slaan ter bestrijding

[6] *Kamerstukken I* 2010/11, 31051, D.

[7] Een indicatie daarvoor is het aantal annotaties bij en verwijzingen naar de desbetreffende uitspraken.

van terrorisme en de opsporing van strafbare feiten, alsmede ter bevordering van de staatsveiligheid en identificatie van de slachtoffers van rampen, zoals die met het Herculesvliegtuig in 1996. Een en ander veronderstelde dat de administratie van de biometrische identiteitsdocumenten centraal wordt georganiseerd, wat zoveel betekende dat er een nationale databank met vingerafdrukken van alle paspoorthouders moest komen.

Een ander voorbeeld van opslag van persoonsgegevens bieden de informatiesystemen, met bijbehorende infrastructuur, die door telecom- en internetaanbieders moesten worden aangelegd om te voldaan aan de bewaarplicht telecomgegevens (art. 13.2a Telecommunicatiewet). Op grond van de, inmiddels ongeldig verklaarde[8] Dataretentierichtlijn[9] moeten (moesten) EU-lidstaten ervoor zorgdragen dat voornoemde aanbieders ten behoeve van politie en justitie, en inlichtingendiensten, een paar handenvol categorieën van telecomgegevens ten minste 6 en ten hoogste 24 maanden bewaren. Om deze gegevens beschikbaar te stellen werd, deels met financiering vanuit de overheid, een infrastructuur aangelegd waarmee de behoeftestellers van politie, justitie en inlichtingendiensten zo-nodig snel en efficiënt konden beschikken over de door hen gewenste gegevens.

Wat vinden Straatsburg en Luxemburg daarvan?

Over het aanleggen van dergelijke databanken zijn er zowel Straatsburg als Luxemburg verschillende uitspraken gedaan. Van de beide rechtscolleges bespreken wij een uitspraak. Aan de hand daarvan proberen we een beter zicht te krijgen op de voorwaarden waaronder grootschalige gegevensopslag kan zijn toegestaan en wanneer niet.

Opmerking vooraf verdient dat de meeste uitspraken over grootschalige gegevensopslag betrekking hebben op databanken die worden ingericht ten behoeve van de opsporing of vervolging van strafbare feiten of nationale veiligheid. Dat geldt ook voor de door ons besproken uitspraken. Dat betekent evenwel nog niet dat deze uitspraken niet relevant zouden zijn voor databanken die worden ingericht voor andere doeleinden zoals bijvoorbeeld bij de grote decentralisatieoperaties, waarbij de rijksoverheid taken op het gebied van jeugdzorg, werk en inkomen en zorg aan langdurig zieken en ouderen overhevelt naar gemeenten, het geval is. Bij privacybeperkingen die door de aard of de omvang van de beperking als ernstig moeten worden beschouwd, plegen de beide hoven de nationale overheid veelal weinig beoordelingsruimte te laten en strikt te toetsen, ongeacht wat precies het doel van de beperking is.[10]

EHRM 4 december 2008 (Marper/VK)[11]

[8] HvJEU 8 april 2014, C-293/12 en C-594/12 (zie ook *infra* voetnoot 16).

[9] Richtlijn 2006/24/EU.

[10] Zie EHRM 4 december 2008, 30562/04 (*S. Marper/VK*) Par. 102; EHRM 10 april 2007, 6339/05 (*Evans/VK*) Par. 77; EHRM 24 april 1990, 11801/85 (*Kruslin/Frankrijk*). Par. 33.

[11] EHRM 4 december 2008, *NJ* 2009/410 m.nt. EAA; NJCM-Bulletin 2009/4, p. 391-406 m.nt. M. Van der Staak; E.J. Koops, 'S. Marper tegen het Verenigd Koninkrijk', ECHR 2009-13, p. 148-165.

In *Marper* ging het om de aanleg van een databank met daarin vingerafdrukken, celmateriaal en DNA-profielen van personen die op enig moment als verdachten van strafbare feiten waren aangemerkt, maar die voor deze strafbare feiten vervolgens níet zijn veroordeeld. Het Hof moest uitmaken onder welke voorwaarden zo een databank onder artikel 8 EVRM kan zijn toegestaan.

Het Hof onderkende dat de opslag van de vingerafdrukken, celmateriaal en DNA-profielen een inbreuk betekent op het recht op bescherming van de persoonlijke levenssfeer van artikel 8, eerste lid, EVRM ("*constitutes an interference with the right to respect for private life*").[12] Een dergelijke inbreuk kan evenwel, zo onderkent het rechtscollege, gerechtvaardigd zijn als die noodzakelijk is voor het voorkomen en opsporen van strafbare feiten. Voor de beantwoording van de vraag of de gegevensopslag voor dat doel inderdaad noodzakelijk is, maakt het Hof in het arrest gebruik van een aantal toetscriteria.

Van belang is allereerst dat de gegevens geautomatiseerd worden verwerkt en ook dat daarbij gebruik wordt gemaakt van wat het hof noemt 'moderne wetenschappelijke technieken' ('*modern scientific techniques*'). Het gebruik daarvan leidt ertoe dat er sprake zal zijn van een verdergaande inbreuk dan als gebruik zou worden gemaakt van traditionele technieken. En dat betekent dus dat er meer waarborgen nodig zijn om de inbreuk aanvaardbaar te maken. Het is, zo overweegt het Hof, onaanvaardbaar dat de bescherming van de persoonlijke levenssfeer wordt verzwakt door het gebruik van dergelijke technieken, zonder dat er sprake is van een zorgvuldige belangenafweging.[13]

Een ander toetscriterium is de aard of de gevoeligheid van de gegevens. Als het gaat om gegevens met een gevoelig karakter, zoals in de onderhavige zaak waarin het onder andere ging om gegevens betreffende etniciteit en gezondheid, moet het bewaren ervan op zichzelf worden opgevat als een inbreuk op de persoonlijke levenssfeer van de desbetreffende individuen ('*retention* perse *must be regarded as interfering'*).

Verder neemt het Hof in het arrest in aanmerking dat de bevoegdheid op grond waarvan de gegevens worden opgeslagen een onbepaald en niet-onderscheidend karakter hadden ('*blanket and indiscriminate nature of the powers of retention*'), aangezien er geen onderscheid werd gemaakt naar ernst van de strafbare feiten, of naar de leeftijd of minderjarigheid van de verdachte. Daarbij werden de gegevens opgeslagen voor onbepaalde tijd en waren er slechts beperkte mogelijkheden om de gegevens te laten verwijderen.[14] Het Hof stelt daarbij dat alleen al de opslag van de gegevens een direct effect heeft op de privacybelangen van de desbetreffende personen, alsmede dat er een risico is van stigmatisering omdat niet veroordeelde personen, die aanspraak maken op

[12] Overw. 86 van het arrest.

[13] Overw. 112 van het arrest; zie ook EHRM 5 oktober 2010 (Köpke v. Duitsland) waarin ook betekenis wordt toegekend aan de wellicht nog níet bekende inbreuken die het gevolg kunnen zijn van het gebruik van nieuwe technologieën ('new, more and more sophisticated technologies').

[14] Overw. 119.

de onschuldpresumptie, op eenzelfde wijze worden behandeld als veroordeelde personen.[15]

Voor het Hof is dat bij elkaar voldoende om te komen tot het oordeel dat deze gegevensopslag in strijd is met het recht op eerbiediging van de persoonlijke levenssfeer van artikel 8 EVRM en dus niet toelaatbaar.

HvJEU 8 april 2014 in gev. zaken C-293/12 en C-594/12 (Dataretentierichtlijn)[16]

Op grond van de Dataretentierichtlijn waren EU-lidstaten gehouden telecomaanbieders te verplichten om telecomverkeersgegevens[17] ten minste 6 en ten hoogste 24 maanden te bewaren ten behoeve van politie, justitie en inlichtingendiensten. Om aan dergelijke verplichtingen te voldoen waren telecomaanbieders genoodzaakt systemen te bouwen waarmee miljarden (!) van dergelijke telecomgegevens konden worden bewaard. In zijn uitspraak van 8 april 2014 verklaarde het HvJEU de richtlijn ongeldig omdat deze, naar zijn oordeel, niet voldeed aan de vereisten die voortvloeien uit het recht op privacy en het recht op bescherming van persoonsgegevens (resp. art. 7 en art. 8 Handvest), alsmede de uitingsvrijheid (art. 11 Handvest).

Het HvJEU begint met de vaststelling dat uit de te bewaren gegevens, in hun geheel beschouwd, zeer precieze conclusies kunnen worden getrokken over het priveleven van de personen van wie de gegevens zijn bewaard. Het gaat dan bijvoorbeeld om hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren.[18] Aldus betekent de bewaarplicht 'een zeer ruime en bijzonder zware inmenging' in het recht op bescherming van de persoonlijke levenssfeer en het recht op bescherming van persoonsgegevens. Van belang daarbij is ook dat de gegevens worden bewaard en later worden gebruikt zonder dat de abonnees of gebruikers hierover worden ingelicht, bij hen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden.[19]

Vervolgens toetste het Hof of deze inmenging gerechtvaardigd is. Het stelt voorop dat de bestrijding van terrorisme ter handhaving van de internationale vrede en veiligheid een doel van algemeen belang van de Unie, evenals de bestrijding van ernstige criminaliteit. In dit verband wijst het rechtscollege erop dat er niet alleen recht is op vrijheid, maar ook op veiligheid (art. 6 Handvest).[20] Echter,

[15] Overw. 122-126.

[16] HvJEU 8 april 2014, C-293/12 en C-594/12; daarover: H. Hijmans, 'De ongeldigverklaring van de Dataretentierichtlijn: een nieuwe stap in de bescherming van de grondrechten door het Hof van Justitie' *Nederlands tijdschrift voor Europees recht*, 2014/7; Mr. drs. D. Groenenberg, 'Ongeldigverklaring van de Dataretentierichtlijn: de gevolgen voor de Nederlandse wetgeving', *Privacy & informatie* 2014/6, p. 244-248; G. Boogaard, M. Van Emmerik, J. Uzman, W. Voermans 'Kroniek van het Nederlands en Europees constitutioneel recht', *NJB* 2014/35, p. 2475. Zie voorts over de bewaarplicht: G-J. Zwenne & F. Simons, 'Duitse bewaarplicht ongrondwettig. En in Nederland?, *Tijdschrift voor Internetrecht* 2010/3, p. 87-94 en W.A.M. Steenbruggen, Annotatie bij BVerfG 2 maart 2010 (Vorratsdatenspeicherung), TvCR 2011-1, p. 67-77.

[17] Zie art. 5 van de richtlijn.

[18] Overw. 27 van het arrest.

[19] Overw. 37 van het arrest.

[20] Overw. 42 van het arrest.

waar het gaat om de bewaarplicht is het Hof er niet van overtuigd dat deze voldoet aan het evenredigheidsbeginsel, dat wil zeggen: of de verplichting niet verder gaat dan wat voor deze doeleinden geschikt en noodzakelijk is. Voor het Hof gaat het er daarbij allereerst om dat er is voorzien in waarborgen dat de gegevens worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens. De noodzaak van dergelijke waarborgen is, stelt het Hof, des te groter wanneer de persoonsgegevens, zoals is bepaald in de richtlijn, automatisch worden verwerkt en er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze worden geraadpleegd.[21]

Verder kent het Hof betekenis toe aan het algemene, en daardoor onbepaalde karakter van de bewaarplicht. Deze heeft betrekking op wijdverspreide communicatiemiddelen die een steeds belangrijker plaats innemen in het dagelijks leven. En daarbij is de verplichting van toepassing op gegevens op alle gebruikers van deze middelen, zonder dat onderscheid wordt gemaakt, of enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het doel (nl. bestrijden van zware criminaliteit). De verplichting raakt dus ook de personen voor wie er geen enkele aanwijzing is dat hun gedrag een verband heeft met zware criminaliteit, met inbegrip van degenen die onder een beroepsgeheim vallen (advocaten, artsen, etc.). Ook wijst het Hof erop dat de richtlijn ook niet voorziet in beperkingen op te bewaren gegevens, zoals met betrekking tot een bepaalde periode of locatie, of een kring van bepaalde personen die zijn betrokken bij zware criminaliteit.[22]

In aanvulling daarop is van belang dat er evenmin in de richtlijn is voorzien in objectieve criteria ter beperking van de toegang die nationale autoriteiten kunnen hebben tot de gegevens, terwijl er evenmin is voorzien in voorafgaande controle door een rechter of onafhankelijke instantie. Verder wijst het Hof erop dat er in de richtlijn voor de bewaartermijn geen onderscheid wordt gemaakt naar de categorieën van gegevens -- sommige gegevens zouden, gelet op hun nut voor het nagestreefde doel, korter of langer moeten worden bewaard. Ten slotte voorziet de richtlijn niet erin dat de gegevens moeten worden bewaard op het grondgebied van de lidstaten, zodat het maar de vraag is of er goed toezicht kan worden gehouden op de naleving van regels met betrekking tot de beveiliging van de gegevens.

Een en ander is voor het Hof voldoende reden om de richtlijn, en de daarin geregelde bewaarplicht, ongeldig te verklaren.[23]

Vuistregels voor de grootschalige opslag van persoonsgegevens

Het is uiteraard niet zonder risico om op basis van de besproken zaken meer algemene uitspraken te doen over de toelaatbaarheid van de opslag van per-

[21] Overw. 54-55.

[22] Overw. 57-59.

[23] Op 20 november 2014 werd op www.internetconsultatie.nl een ontwerp-wetsvoorstel bekendgemaakt waarmee de regering beoogt de door het Hof genoemde gebreken van de bewaarplicht weg te nemen. Volgens velen, zoals o.a. het redactioneel hoofdcommentaar van NRC Handelsblad ('Inbreuk privacy blijft kwalijk' NRC-handelsblad, donderdag 20 november 2014, p. 2), is de regering daarin maar ten dele geslaagd.

soonsgegevens in de ICT-systemen van de overheid. In deze zaken was sprake van specifieke omstandigheden die de beide rechtscolleges in hun beoordeling hebben betrokken. Om te komen tot vuistregels moet daarvan worden geabstraheerd en dat leidt vanzelf tot de vraag of, en in hoeverre, die vuistregels wel uit deze rechtspraak kunnen worden afgeleid.

Toch laten zich naar onze mening wel enkele vuistregels uit deze zaken afleiden aan de hand waarvan kan worden beoordeeld in hoeverre er sprake is van een verdergaande privacy-inbreuk waarvoor om deze reden zwaardere waarborgen vereist zijn:

- het gebruik van geautomatiseerde middelen en/of moderne wetenschappelijke methodes duidt op een verdergaande inbreuk en vereist dus sterkere waarborgen om de opslag tot het minimum te beperken en misbruik te voorkomen;

- hetzelfde geldt voor het gebruik van gevoelige gegevens, zoals gegevens waaruit direct of indirect iets blijkt over de etniciteit en gezondheid, politieke overtuiging, religie of strafrechtelijke verleden;

- als er bij het bewaren van de gegevens geen onderscheid wordt gemaakt naar de ernst van de feiten waarop de gegevens betrekking hebben dan duidt dat op een verdergaande inbreuk;

- als er bij het bewaren van de gegevens geen onderscheid wordt gemaakt naar bijvoorbeeld leeftijd of minderjarigheid, of anderszins, dan duidt ook dat op een verdergaande inbreuk;

- als de gegevens voor een langere of onbepaalde termijn worden bewaard dan duidt dat ook op een verdergaande inbreuk;

- als degenen op wie de gegevens betrekking hebben geen of weinig inzicht en of controle hebben op de te bewaren gegevens, dan duidt ook dat op een verdergaande inbreuk;

- ten slotte zijn er de persoonlijke implicaties voor individu: welke risico's zijn er voor degene over wie gegevens worden vastgelegd? als er bijvoorbeeld sprake is van een risico van stigmatisering betekent ook dat een verdergaande inbreuk.

Deze vuistregels maken het mogelijk om een inschatting te maken van de ernst van de gemaakte inbreuk. Als daaruit blijkt dat er sprake is van een vergaande inbreuk is daarmee nog niet gezegd dat de desbetreffende gegevensopslag niet is toegestaan, maar wel dat er meer, en soms veel meer, moeite zal moeten worden gedaan om aan te tonen dat de inbreuk echt nodig is en dat voldoende waarborgen zijn aangebracht om ervoor te zorgen dat de inbreuk tot een minimum wordt beperkt en dat geen misbruik kan worden gemaakt van bevoegdheden. Omgekeerd, en natuurlijk beter, kan een overheid aan de hand ervan bij het optuigen van haar informatiesystemen, in het kader van bijvoorbeeld de voorgeschreven PIA een strategie bedenken waarmee de omvang van privacyinbreuken

effectief kan worden beperkt, teneinde dat systeem 'EVRM-proof' of 'Handvest-bestendig' te maken.

3. (IN)TRANSPARANTIE

Dat brengt ons bij het tweede thema dat bij de inrichting van grootschalige overheidsinformatiesystemen van belang is, te weten transparantie. Kenmerkend voor privacyinbreuken is dat deze zich veelal aan ons gezichtsveld onttrekken. Wij laten veelal onbewust overal gegevens achter die door derden worden verzameld en verwerkt en, samen met andere persoonsgegevens, een groot inzicht geven in ons gedrag, communicatie en gedachten en gevoelens. Ook overheden houden zich, zonder dat we dat door hebben, op zeer grote schaal bezig met het verzamelen en verwerken van persoonsgegevens, in uiteenlopende vormen en voor zeer verschillende doeleinden. Daarbij kan het bijvoorbeeld gaan om de registratie van persoonsgegevens in de gemeentelijke basisregistratie persoonsgegevens of de verwerking van inkomensgegevens door de fiscus. We hebben er vaak geen benul van door welke overheidsdienst en voor welke doeleinden onze persoonsgegevens worden verzameld en verwerkt, te meer deze gegevens vervolgens ook nog regelmatig worden verstrekt aan andere overheidsinstanties en gebruikt voor weer andere doelen. Een actueel voorbeeld biedt de discussie over de verstrekking van kentekengegevens door de politie aan de Belastingdienst ten behoeve van bijvoorbeeld de controle of leaserijders niet ook privé gebruik maken van hun auto.[24]

We kunnen nog minder overzien dat onze privacy wordt beperkt als er in het geheim wordt geobserveerd, communicatie wordt getapt of andere bijzondere opsporingsbevoegdheden worden ingezet door politie en justitie. En dat geldt in nog versterkte mate als de veiligheidsdiensten dat doen zoals de perikelen rondom de NSA wel hebben aangetoond.

Wat hebben Straatsburg en Luxemburg daarover gezegd?

Zowel het Hof in Straatsburg als het Hof in Luxemburg hebben zich in verschillende uitspraken uitgelaten over de toelaatbaarheid van geheime of intransparante vastleggingen en verwerkingen van persoonsgegevens. De al besproken zaak *Marper* van het EHRM en het arrest van het HvJEU inzake de Dataretentierichtlijn zijn daar voorbeelden van. Uit deze uitspraken blijkt dat dergelijke maatregelen niet per definitie verboden zijn, maar wel dienen te voldoen aan materiele en procedurele eisen die strenger en meer omvattender worden naar mate de maatregelen meer ingrijpen op de persoonlijke levenssfeer.

Deze eisen hebben in belangrijke mate betrekking op de voorzienbaarheid en transparantie van de gegevensverwerking. Voldoende transparantie is nodig voor een effectieve bescherming. In voorkomende gevallen moet de overheid zelfs de transparantie rondom gegevensverwerking bevorderen zonder dat daaraan een concrete privacyinbreuk door de overheid vooraf is gegaan. We bespreken van beide rechtscolleges een aantal recente uitspraken en proberen aan de hand daarvan weer enige vuistregels te formuleren.

[24] Zie bijv. http://tweakers.net/nieuws/99183/belastingdienst-gaat-meekijken-met-politiecameras-op-snelwegen.html

EHRM 1 juli 2008 (Liberty)[25]

In *Liberty* ging het om de grootschalige monitoring van telecommunicatieverkeer. Engeland had in de jaren negentig van de vorige eeuw aan de Engelse westkust een zogenaamde Electronic Test Facility (of: 'ETF') waarmee alle telecommunicatie (waaronder telefoon-, fax- en e-mailcommunicatie) van Dublin naar Londen en het Europese vaste land kon worden onderschept en gecontroleerd. Ter discussie stond of de grootschalige monitoring via deze ETF wel was voorzien van een deugdelijke wettelijke basis, nu de Secretary of State zeer brede warrants en certificates afgaf op basis waarvan communicatie grootschalig kon worden getapt en vervolgens bijna onbeperkt kon worden onderzocht voor nationale veiligheidsdoeleinden en zonder dat er verder een minister en rechter te pas kwam. Richtlijnen (zogenaamde "arrangements") van de Secretary of State boden wel enige bescherming, maar deze richtlijnen waren niet publiek en er was geen mogelijkheid voor de betrokkenen om in een individueel geval te (laten) toetsen of aan de richtlijnen was voldaan.

Het Hof had zich al voor *Liberty* in diverse uitspraken uitgelaten over de eisen die aan de wettelijke grondslag voor beperkingen op artikel 8 EVRM worden gesteld. Uit deze uitspraken werd duidelijk dat deze eis niet slechts een formeel criterium is. Belangrijker dan de vraag wat precies de status is van de norm waarop de beperking is gebaseerd, is of de beperking voldoet aan de kwalitatieve eisen die het EHRM uit de rule of law heeft afgeleid: "*one of the principles underlying the Convention is the rule of law, which implies that an interference by the authorities with the individual's rights should be subject to effective control*".[26] Het is dan niet voldoende dat de beperking is terug te voeren op een wettelijke grondslag. De grondslag moet vooral toegankelijk zijn en de beperkende maatregel voorzienbaar.

Naarmate een maatregel evenwel ingrijpender wordt en de inzet daarvan minder controleerbaar, wordt door het Hof aanzienlijk strikter aan deze eisen getoetst en moet de wettelijke grondslag bijvoorbeeld formeelwettelijk van aard zijn en bovendien zeer precies aangeven wanneer en door wie een beperkende maatregel kan worden opgelegd en daarnaast ook allerlei materiele en procedurele waarborgen bevatten om misbruik te voorkomen.[27]

In *Liberty* trekt het Hof deze lijn door. Daarbij stelt het Hof eerst vast dat er inderdaad sprake is van een inbreuk of beperking op het privacyrecht van artikel 8 lid 1 EVRM, en gaat het vervolgens in op de vraag of die beperking voldoet aan de eisen van artikel 8 lid 2 EVRM: is de beperking is "*in accordance with the law*". De Engelse regering had in dit verband een beroep gedaan op de zaak *Malone* waarin het Hof had overwogen dat "*the detailed procedures and conditions to be observed do not necessarily have to be incorporated in rules of substantive law*". Ook had de Engelse regering betoogd dat voor strategische monitoring minder strikte voorzienbaarheidseisen zouden moeten gelden. Het Hof gaat hier niet in

[25] EHRM 1 juli 2008, *NJ* 2010, 324 (*Liberty*), m.nt. EJD.

[26] EHRM 25 maart 1983, *Series A*.61 (*Silver*), par. 90.

[27] Zie bijv. EHRM 6 september 1978. *Series A*.28 (*Klass*); EHRM2 augustus 1984, *Series A*.82 (*Malone*) EHRM 24 april 1994, *Series* A.176-A en A.176. B (*Huvig* & *Kruslin*).

mee. *Malone* verwijst namelijk op haar beurt terug naar de zaak *Silver* uit 1983 waarin het Hof doorslaggevende betekenis had toegekend aan het gegeven dat de niet-wettelijke regelingen bekend waren bij de betrokkenen. Daarnaast merkt het Hof op dat de zaak *Weber & Saravia* uit 2006 ook ging over strategische monitoring en dat het ook geen aanleiding ziet om andere principes te hanteren voor de toegankelijkheid van regels met betrekking tot het aftappen van individuele communicatie en meer generieke vormen van surveillance.

Het Hof stelt voorts vast dat in casu op grond van de toepasselijke wetgeving de discretie van de autoriteiten om telecommunicatie te onderscheppen en te lezen, wel bijna onbeperkt ("*virtually unfettered*") is en dat de richtlijnen die een waarborg moeten vormen tegen misbruik, niet zijn vervat in wetgeving of anderszins aan het publiek bekend zijn gemaakt. Dat de toezichthouder in zijn jaarverslagen wel in algemene zin kon aangeven of aan de richtlijnen was voldaan, maakte dit niet goed, omdat hij niet mocht aangeven wat die richtlijnen dan wel inhielden. De procedures die gelden voor onderzoek, gebruik en opslag van onderschepte gegevens, moeten volgens het Hof zijn opgesteld in een vorm die open staat voor het publiek.

De Engelse regering had in dit verband nog betoogd dat bekendmaking van de richtlijnen en werkmethoden niet kon, omdat de veiligheidsdiensten dan hun werk niet meer effectief zouden kunnen doen, maar het Hof wijst erop dat in de al genoemde zaak *Weber & Saravia*, de Duitse autoriteiten wel zeer uitvoerig hadden aangegeven hoe moet worden omgegaan met onderschepte gegevens. Ook wijst het Hof erop dat latere Engelse wetgeving wel voorziet in de bekendmaking van uitvoerige extracten uit de Code of Practice. Dat alles suggereert dat het wel degelijk mogelijk is om bepaalde details bekend te maken zonder dat daarmee gelijk de nationale veiligheid in gevaar wordt gebracht.

De eindconclusie van het Hof is dan ook dat de nationale wetgeving niet op voldoende transparante wijze uitwerkt wat de omvang en aard van de discretie is van de overheid bij het onderscheppen en onderzoeken van communicatie. In het bijzonder is niet op voldoende toegankelijke wijze inzicht verschaft in de te hanteren procedures en waarborgen bij het onderzoek, het delen, de opslag en de vernietiging van via de ETF onderschepte gegevens. De beperking is dan ook niet "*in accordance with the law*".

EHRM 28 april 2009 (K.H. vs. Slowakije)[28]

Transparantie is niet alleen van belang om de burger inzicht te geven in de *mogelijkheid* van geheime vastlegging, de wijze van verwerking en waarborgen, maar bovendien om hem in staat te stellen te zien of *voor hem relevante* gegevens worden verwerkt. Inzage in dossiers is voor de burger vaak een noodzakelijke voorwaarde om vast te stellen of zijn rechten zijn beperkt, bijvoorbeeld omdat zijn communicatie is getapt, of juist om informatie te krijgen die voor hem noodzakelijk is om zijn rechten daadwerkelijk uit te oefenen. Het is dan ook niet

[28] EHRM 28 april 2009, *EHRC* 2012-18, m.nt. Hendriks (*K.H./ Slowakije*); EHRM 28 april 2009, *EHRC* 2009-77 m. nt. Ploem. A.C. Hendriks, A.C, 'Kroniek rechtspraak rechten van de mens', Tijdschrift voor Gezondheidsrecht 2011/7, p. 630.

voor niets dat artikel 8 lid 2 Handvest dat "eenieder recht op toegang heeft tot de over hem verzamelde gegevens en op rectificatie daarvan."

Ook het Hof in Straatsburg heeft zich in verschillende zaken uitgelaten over de vraag of en wanneer de overheid de burger op grond van artikel 8 EVRM toegang moet geven tot voor hem relevante informatie waarover de overheid beschikt. Dat is niet per definitie het geval. Indien het bijvoorbeeld de nationale veiligheid of terrorismebestrijding betreft, kan de overheid (tijdelijk) weigeren om de burger inzage te verlenen in zijn dossier.[29] In de meeste andere gevallen moet de overheid hem evenwel wel degelijk actief toegang geven tot zijn dossier, of hem tenminste in staat stellen een weigering voor te leggen aan een onafhankelijke toetsingsinstantie.[30] In die gevallen zal via wetgeving dus moeten zijn voorzien in effectieve inzageprocedures.

Een recente zaak uit Straatsburg is *K.H. vs. Slowakije*. In deze zaak ging het erom *of en in welke vorm* inzage moest worden verleend in medische dossiers. Klaagsters waren tijdens hun zwangerschap en bevalling behandeld in het ziekenhuis. Nadien lukte het niet meer om zwanger te worden. Zij machtigden hun advocaten om hun medische dossiers in te zien. De ziekenhuizen weigerden echter de gevraagde inzage te verlenen en de nationale rechter oordeelde dat de ziekenhuizen klagers niet in staat hoefde te stellen kopieën te maken en dat dit ook niet voortvloeide uit artikel 8 EVRM. Het Hof stond dus voor de vraag of uit artikel 8 EVRM inzagerechten voortvloeiden en hoever die strekten.

Het Hof stelt bij zijn beoordeling voorop dat naast onthoudingsplichten artikel 8 EVRM ook positieve verplichtingen met zich mee kan brengen. Of dat het geval is, moet volgens vaste rechtspraak bepaald worden op basis van een afweging tussen de belangen van de gemeenschap en de belangen van de individuele burger (de zogenaamde *"fair balance*"-test). Het Hof wijst er vervolgens op dat hij al in verschillende zaken heeft aangenomen dat artikel 8 EVRM positieve verplichtingen kan meebrengen ten aanzien van de inzage van informatie.

De vraag is vervolgens of deze positieve verplichtingen met zich meebrengen dat ook een kopie van het dossier moet worden verstrekt. Dat is volgens het Hof in deze zaak het geval. Dat betekent overigens niet zonder meer dat zonder meer en gratis kopieën aan de betrokkene moeten worden verstrekt. Maar de overheid kan niet simpelweg een verzoek afwijzen, omdat de betrokkene niet voldoende heeft aangetoond dat hij een kopie nodig heeft. Het is aan de overheid aan te tonen dat er zwaarwegende redenen ("*compelling reasons*") zijn om niet aan een dergelijk verzoek te voldoen.

Aan deze bewijslast heeft de Slowaakse overheid in deze zaak niet voldaan. In het bijzonder ziet het Hof niet in dat de betrokkene misbruik zou kunnen maken door de relevante documenten te kopiëren, zoals door de nationale autoriteiten betoogd. Het ging immers om documenten over henzelf. En voor zover er sprake zou kunnen zijn van misbruik door derden, zou dit volgens het Hof ook op een

[29] Zie bijv. EHRM 26 maart 1987, Series A, 1 16 (*Leander/Zweden*); EHRM 6 juni 2006, RJ&D 2006-VII (*Segerstedt-Wiberg/Zweden*).

[30] Zie bijv. EHRM 7 juli 1989, NJ 1991, 659 (Gaskin), m.nt. EJD; EHRM 19 februari 1998, NJ 1999, 690, (Guerra) en EHRM 9 juni 1998,, RJ&D 1998-III, (McGinley & Egan/VK).

andere manier worden voorkomen, bijvoorbeeld door in het nationale recht passende waarborgen op te nemen en de verdere verspreiding van de informatie aan strikte beperkingen te onderwerpen. De conclusie is dan ook dat artikel 8 EVRM is geschonden.

HvJEU 17 juli 2014 (Y.S. v. Minister II en A en Minister II en A v. M en S)[31]

Uit bovenstaande zaak blijkt dus dat de inzageverplichtingen van de overheid onder omstandigheden ver kunnen gaan. Om daaraan uitvoering te geven, zal de nationale overheid passende wetgeving moeten opstellen. Hoever zij daarin moet gaan, is evenwel niet geheel duidelijk en hangt van de omstandigheden van het geval af. Duidelijk lijkt wel dat het EHRM en het HvJEU niet helemaal op één lijn zitten voor wat betreft de inhoud en reikwijdte van de inzagerechten van betrokkenen. Dat lijkt in ieder geval de conclusie te moeten zijn op grond van de recente uitspraak van het HvJEU in de zaken *Y.S. v. Minister Immigratie, Integratie en Asiel* en *Minister Immigratie, Integratie en Asiel v. M. en S.*. In deze zaken moest het HvJEU zich naar aanleiding van prejudiciële vragen uitlaten over het begrip persoonsgegevens en de reikwijdte van het inzagerecht op grond van artikel 12 van de Privacyrichtlijn[32].

In beide zaken ging het erom dat asielzoekers inzage wilden krijgen in de juridische analyse die is gebruikt bij de voorbereiding op de uiteindelijke beslissing in hun asielprocedure. Zij verzochten daarom met een beroep op het inzagerecht uit artikel 35 van de Wet bescherming persoonsgegevens (Wbp), de nationale implementatie van artikel 12 Privacyrichtlijn, een afschrift van de minuut van de beslissing waarin die juridische analyse was neergelegd.

Het Hof beantwoordt in zijn arrest allereerst de vraag of een juridische analyse beschouwd moet worden als een persoonsgegeven. Het Hof overweegt hierover als volgt: "*De juridische analyse in een minuut kan daarentegen persoonsgegevens bevatten, maar vormt op zich niet een dergelijk gegeven in de zin van artikel 2, sub, van richtlijn 95/46*"[33]. De minuut bevat volgens het Hof namelijk geen "*informatie over de aanvrager van de verblijfstitel, maar hooguit, voor zover die analyse niet beperkt blijft tot een zuiver abstracte uitlegging van het recht, informatie over de beoordeling en toepassing van dat recht door de bevoegde autoriteit op de situatie van de aanvrager, bij die situatie met name wordt vastgesteld middels de hem betreffende persoonsgegevens waarover die autoriteit beschikt*".[34]

Vervolgens beantwoordt het Hof de vragen over de precieze inhoud en reikwijdte van het inzagerecht, meer specifiek of de betrokkene recht heeft op afschrift van bescheiden of niet. Het Hof benadrukt daarbij allereerst – onder verwijzing naar zijn bestendige lijn - dat de Privacyrichtlijn moet worden uitgelegd tegen de

[31] HvJEU 17 juli 2014, zaken C-141/12 en C-372/12, AB 2014, 365 (Y.S. v. Minister IIA en Minister IIA v. M en S), m.nt. M. van Graafeiland.; F. Borgesius & E. Brouwer, 'Inzage in de minuten van de asielzoekprocedure: persoonsgegevens of geen persoonsgegevens?' *A&MR* 2014-7.; M. Jansen, 'Arrest Hvj EU inzake begrip persoonsgegevens en karakter inzagerecht', *P&I* 2014-5, p. 200-206.

[32] Richtlijn 95/46/EG.

[33] Overw. 39.

[34] Overw. 40.

achtergrond van de grondrechten,[35] maar merkt vervolgens op dat het in artikel 8 lid 2 Handvest EU vermelde inzagerecht is uitgewerkt in artikel 12 onderdeel a Privacyrichtlijn.[36]

De Privacyrichtlijn laat het over aan de lidstaten om te bepalen op welke concrete wijze uitvoering wordt gegeven aan het inzagerecht, mits de verstrekte gegevens "*begrijpelijk*" zijn en de betrokkene in staat stellen kennis te nemen van die gegevens, deze te controleren en te verifiëren of deze in overeenstemming met de richtlijn worden verwerkt.[37] Hieruit blijkt volgens het Hof dat de betrokkene aan de Privacyrichtlijn dus geen recht op afschrift van bescheiden kan ontlenen, mits maar in andere vorm volledig aan voornoemde doelstellingen kan worden voldaan.[38] Het volstaat dan ook dat "*aan de aanvrager van de verblijfstitel een volledig overzicht, in begrijpelijke vorm, van al deze gegevens wordt gegeven, dat wil zeggen in een vorm die deze aanvragen in staat stelt kennis te nemen van die gegevens en te controleren of ze juist zijn en zijn verwerkt in overeenstemming met deze richtlijn, omdat hij eventueel de hem bij de artikelen 12, sub b en c, 14, 22 en 23 van die richtlijn verleende rechten kan uitoefenen*".[39] Met andere woorden, in deze zaken hoeft dus geen kopie van (stukken uit) het dossier te worden verstrekt.

Vuistregels voor de vereiste transparantie

Uit de besproken zaken blijkt dat bij gegevensverwerking transparantie een belangrijke rol speelt. De (in)transparantie van de gegevensverwerking speelt niet alleen een rol bij de vraag of de beperking van de privacy voorzienbaar is, maar bovendien bij de vraag of deze proportioneel is. In voorkomende gevallen zal het recht op privacy met zich meebrengen dat de overheid actief informatie over de verwerking van persoonsgegevens moet verstrekken en inzagemogelijkheden moeten bieden, ook zonder dat sprake is van een concrete privacyinbreuk. We komen mede aan de hand van de genoemde uitspraken tot de volgende vuistregels:

- naarmate de verwerking van de persoonsgegevens zich meer aan het zicht van de burger onttrekt, worden strengere eisen gesteld aan de wettelijke grondslag en zal in de wet verder moeten worden uitgewerkt wie onder welke voorwaarden toegang heeft tot de gegevens, wanneer de gegevens moeten worden vernietigd en zal de wet moeten voorzien in een effectieve vorm van toetsing door een onafhankelijke instantie.

- de overheid moet effectieve mogelijkheden tot inzage in de verwerking van persoonsgegevens verschaffen. Soms is voldoende dat een weigering van een verzoek tot inzage kan worden voorgelegd aan een onafhankelijke instantie, maar naarmate de gegevens of verwerking privacygevoeliger van aard zijn, moet de overheid ook eerder daadwerkelijk in-

[35] Overw. 54.

[36] Overw. 55.

[37] Overw. 57.

[38] Overw. 58.

[39] Overw. 59.

zage gegeven in de verwerking van gegevens, in voorkomende gevallen door verstrekking van een afschrift van het volledige dossier.

4. BEVEILIGING

De veiligheid van onze ICT-infrastructuur en de informatie daarop, is verre van gegarandeerd. Dat geldt niet alleen voor de netwerken en diensten van private partijen, ook de beveiliging van de overheids IT-infrastructuur laat nog al eens te wensen over. Dat bleek nadrukkelijk in de zaak *DigiNotar*.[40] *DigiNotar* staat evenwel niet op zichzelf. Er gaat tegenwoordig bijna geen dag voorbij zonder dat er weer een beveiligingsincident bekend wordt.[41]

Dit roept de vraag op of de overheid indien zij overgaat tot de grootschalige opslag en verwerking van persoonsgegevens niet ook vanuit grondrechtelijk oogpunt moet waarborgen dat deze goed beveiligd zijn, te meer nu er zonder een deugdelijke IT-beveiliging bijna geen sprake meer kan zijn van een effectieve privacybescherming.

Wat vinden Straatsburg en Luxemburg ervan?

Er is nog niet veel jurisprudentie uit Straatsburg of Luxemburg waaruit zich heldere lijnen laten trekken voor wat betreft de beveiliging van informatiesystemen. Er is wel rechtspraak waaruit valt op te maken dat de overheid actief voorzorgsmaatregelen moet nemen tegen kennisname van persoonsgegevens door derden om de privacy van betrokkenen te beschermen, zeker indien de overheid degene is die de persoonsgegevens onder zich heeft.

Het arrest van het Hof van Justitie over de Dataretentierichtlijn bespraken wij hierboven al. Daaruit bleek onder meer dat de (dis)proportionaliteit van de bewaarplicht mede werd bepaald door het ontbreken in de richtlijn van waarborgen dat de gegevens worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en onrechtmatig gebruik van deze gegevens. Het HvJEU zegt zelfs expliciet: *"De noodzaak om over dergelijke garanties te beschikken is des te groter wanneer de persoonsgegevens, […] automatisch worden verwerkt en er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd".*[42]

Het Hof in Straatsburg heeft vergelijkbare zaken gewezen. Hierboven werden reeds de zaken *Liberty* en *Weber & Saravia* genoemd. En in het arrest over de Dataretentierichtlijn verwijst het HvJEU ook naar de ook besproken zaak *Marper*. Uit deze zaken blijkt dat de wettelijke regeling op grond waarvan de overheid de bevoegdheid heeft op grote schaal gegevens te verwerken kenbaar moet voorzien in een aantal minimumwaarborgen om misbruik te voorkomen en effectieve rechtsbescherming te waarborgen. Deze waarborgen hebben mede betrekking op procedures bij de verdere verwerking van de verzamelde gegevens, voorzorgsmaatregelen die in acht moeten worden genomen bij het doorgeven van de

[40] Zie Rb Rotterdam, 16 mei 2013, ECLI:NL:RBROT:2013:CA1010 (*DigiNotar*).

[41] Vgl. het inmiddels afgesloten Zwartboek Datalekken van Bits of Freedom, zie www.bof.nl.

[42] Zie overw. 55 van het arrest.

gegevens en het wissen of vernietigen van de gegevens nadat ze niet meer nodig zijn. Bij deze waarborgen zou goed passen dat vooraf een PIA wordt verricht om de privacyrisico's in kaart te brengen, maar vooralsnog wordt een PIA nog niet door het Hof in Straatsburg vereist.

Duidelijk is wel dat enkel het wettelijk voorschrijven van een adequate beveiliging waarschijnlijk niet voldoende is. Ook hier zal veelal enige concretisering nodig zijn om de burger een beeld te geven van wat hij kan verwachten. Uit de zaak *Craxi II*[43] volgt ook dat de wettelijke waarborgen niet slechts van papier mogen zijn, maar moeten leiden tot een daadwerkelijke en effectieve bescherming. De overheid moet ook echt passende maatregelen nemen om ervoor te zorgen dat vertrouwelijke gegevens niet aan derden bekend worden. Dat betekende in die zaak dat een datalek onderzocht moest worden en waar mogelijk de schuldigen bestraft. In die lijn past dat de betrokkene van een dergelijk lek op de hoogte wordt gesteld indien daarmee mogelijk aanzienlijke schade aan zijn persoonlijke levenssfeer kan worden voorkomen. Dergelijke maatregelen zullen in de regel enige wettelijke inbedding vereisen. In Nederland is in de Telecommunicatiewet overigens al een dergelijke meldplicht opgenomen voor aanbieders van openbare elektronische communicatienetwerken en –diensten en wordt een brede meldplicht datalekken voorzien in de Wbp.[44]

Wij bespreken hierna in aansluiting op de genoemde zaken nog kort een vrij recente zaak van het Hof in Straatsburg over informatiebeveiliging van een medische databank en formuleren aansluitend een paar vuistregels voor de beveiliging van overheidsinformatiesystemen.

EHRM 17 juli 2008 (I. v. Finland)[45]

In deze zaak stond ter discussie of Finland had voldaan aan zijn positieve verplichtingen op grond van artikel 8 EVRM om de privacy te waarborgen door middel van regels voor de verwerking van persoonsgegevens. Klaagster I. werkte als verpleegster in een openbaar ziekenhuis en was bij hetzelfde ziekenhuis onder behandeling, omdat ze was gediagnosticeerd als HIV-positief. I had het vermoeden dat collega's in haar medische dossier hadden gekeken en dat het ziekenhuis dus niet had voorzien in adequate waarborgen tegen onbevoegde toegang. Ze sprak het ziekenhuis daarop aan, maar kreeg bij de nationale rechter nul op het rekest, omdat ze niet kon bewijzen dat haar collega's daadwerkelijk haar dossier hadden ingezien.

Het Hof moest dus beoordelen of Finland zijn positieve verplichting had geschonden om het privé-leven te beschermen door middel van regels voor de verwerking van persoonsgegevens.

Dat een dergelijke verplichting bestaat, staat voor het Hof eigenlijk niet ter discussie. Het stelt in dat verband vast dat bescherming van persoonsgegevens, in het bijzonder van medische gegevens, van fundamenteel belang is voor het ge-

[43] EHRM 17 juli 2003, www.echr.coe.int (Craxi II).

[44] Wetsvoorstel brede meldplicht datalekken, *Kamerstukken II* 2014/15, 33662 nr. 9.

[45] EHRM 17 juli 2008, *EHRC* 2008-124, mt. nt. Forder (*I.v.Finland*).

not van de burger van zijn recht op privacy. Het respecteren van de vertrouwelijkheid van medische gegevens is bovendien een vitaal principe in het recht van alle verdragsstaten. Het nationale recht moet dan ook voorzien in passende waarborgen om de communicatie of bekendmaking van medische persoonsgegevens te voorkomen.

De Finse wetgeving voorzag overigens in regels voor de bescherming van gevoelige persoonsgegevens. Op grond daarvan moest de verantwoordelijke er bijvoorbeeld voor zorgen dat persoonsgegevens op passende wijze beveiligd waren tegen onder meer onbevoegde toegang. Ook moest de verantwoordelijke ervoor zorgen dat slechts het behandelend personeel toegang had tot het medisch dossier van de patiënt.

Toch was het bestaan van deze regels in deze zaak voor het EHRM niet voldoende voor compliance met artikel 8 EVRM. In casu liet de implementatie ervan namelijk te wensen over. Het gebruik van de medische gegevens kon achteraf niet goed worden gecontroleerd, omdat telkens alleen de laatste 5 opvragingen waren geregistreerd en deze informatie werd gewist nadat het dossier terug naar het archief was gestuurd. Als gevolg daarvan konden de nationale rechters niet vaststellen of er informatie van klaagster door onbevoegden was ingezien en werd dus haar vordering afgewezen, omdat dit niet door haar was bewezen.

Het Hof is van mening dat de bewijslast niet bij klaagster had mogen worden gelegd. "*What is required in this connection is practical and effective protection to exclude any possibility of unauthorised access occurring in the first place. Such protection was not given here.*" Het Hof concludeert dan ook dat artikel 8 EVRM is geschonden.

Vuistregels voor beveiligingsvereisten

Mede aan de hand van bovenstaande zaken kunnen de volgende vuistregels voor de IT-beveiliging worden geformuleerd die mede door de wetgever moeten worden geadresseerd bij de inrichting van de wettelijke basis voor een specifiek overheidsinformatiesysteem:

- informatiesystemen moeten worden beveiligd en dit betekent in elk geval dat voorschriften moeten worden opgesteld om ervoor te zorgen dat alleen bevoegde personen toegang hebben tot de persoonsgegevens;

- naarmate de gegevens een gevoeliger karakter hebben en naarmate de implicaties van beveiligingsinbreuken ernstiger kunnen zijn, geldt een verdergaande beveiligingsplicht en dient de overheid ook te zorgen voor technische en organisatorische maatregelen om de vertrouwelijkheid, integriteit en authenticiteit van de gegevens te waarborgen; in dat verband moet in elk geval voor langere tijd worden vastgelegd wie kennis hebben genomen van de gegevens en aan wie gegevens zijn verstrekt (zgn. log-file verplichting);

- maatregelen moeten worden genomen om bij beveiligingsincidenten schade voor de betrokkene zoveel mogelijk te beperken en indien mogelijk nodig de verantwoordelijke personen te kunnen bestraffen.

5. AFSLUITEND

Fundamentele rechten en vrijheden stellen grenzen en voorwaarden stellen aan de iOverheid. Het is een open deur. Maar wel een die, zo wijst de praktijk uit, zo nu en dan moet worden opengetrapt. Overheden en wetgevers doen er, juist omdat er bij hen sprake is van een onverminderd groot vertrouwen in informatie- en communicatietechnologie, verstandig aan om nadrukkelijk rekening te houden met de bescherming van fundamentele rechten en -vrijheden, waaronder privacyrechten.

Dat gaat verder dan de obligate paragrafen in de memorie van toelichting van een wetsvoorstel dat ten grondslag ligt aan een of andere privacybeperkend overheidsinformatiesysteem. Dit natuurlijk in de eerste plaats omdat we juist van overheden en wetgevers mogen verwachten dat zij instaan voor deze rechten. Maar als dat niet voldoende reden zou zijn, dan toch ook omdat een onvoldoende naleving van dergelijke vereisten kan betekenen dat een kostbaar informatiesysteem niet (volledig) in gebruik kan worden genomen, of in elk geval niet de verwachtingen ervan kan waarmaken.

In deze bijdrage hebben we geprobeerd inzichtelijk te maken hoe vooral de bescherming van privacyrechten als slagingsfactor kan en moet worden betrokken bij de bouw van ICT-systemen en de aanleg van grootschalige databanken . Het ligt voor de hand dit te doen bij de toepassing van het instrument van de privacy impact assessment (PIA). Daarmee kunnen in een vroeg stadium van de ontwikkeling van beleidsvoornemens de risico's in relatie tot bescherming persoonsgegevens in kaart worden gebracht. Voor de rijksoverheid is inmiddels een PIA-toetsmodel ontwikkeld. Dat is een goed begin, maar niet meer dan dat. Waar het om gaat is dat op basis van die inventarisatie vervolgens adequate juridische en andere maatregelen worden genomen en zo nodig ook worden aangepast om nieuwe risico's te adresseren die later nog kunnen opkomen. Immers, de technologie is dynamisch en dat betekent dat de effectiviteit van de genomen maatregelen steeds moet worden heroverwogen in wat wordt aangeduid *"the lights of present-day conditions*".[46] De adequatie bescherming van privacyrechten is en blijft daarom voorwerp van aanhoudende zorg.

[46] EHRM 25 april 1978, Series A.26 (*Tyrer*).