

### **Gepubliceerd artikel**

*Draft* versie : uitsluitend voor academisch gebruik, alleen refereren naar de gepubliceerde versie

DE HERT P., DE VRIES K. & GUTWIRTH S. <sup>1</sup>

Duitse rechtspraak over remote searches, datamining en afluisteren op afstand. Het arrest Bundesverfassungsgericht 27 februari 2008 (Online Durchsuehung) in breder perspectief”, *Computerrecht* 5/2009 , 200-211

Op 27 februari 2008 velde het Duitse *Bundesverfassungsgericht* (BverfG) een arrest (*Online Durchsuehung*, 1 BvR 370/07, 1 BvR 595/07) dat belangrijke grenzen stelt aan het op afstand uitlezen van harde schijven (‘online doorzoeken’ of ‘remote searches’) door politie en veiligheidsdiensten.<sup>2</sup> In dit arrest leidt de hoogste Duitse constitutionele rechter een nieuw IT-grondrecht af uit het algemeen persoonlijkheidsrecht. De formulering van een nieuw grondrecht is een vrij zeldzame en bijzondere gebeurtenis. Dit nieuwe “grondrecht op de vertrouwelijkheid en integriteit van informatietechnologische systemen”<sup>3</sup> wordt door velen dan ook gezien als de grootste mijlpaal sinds 1983 – toen het Hof ook een nieuw grondrecht (het recht op informatiele zelfbeschikking) afleidde uit het algemeen persoonlijkheidsrecht.<sup>4</sup>

In dit artikel wordt ingegaan op de bredere juridische context waarin het arrest is ingebed. Eerst zal daarom stil worden gestaan bij het stelsel van grondrechtelijke bescherming zoals dat in Duitsland ontwikkeld is, de positie van ‘digitale’ grondrechten binnen dit stelsel en het hybride karakter van de Duitse samenleving die binnen Europa een koploper is op zowel het vlak van verregaande politiebevoegdheden met het oog op veiligheid, als van verregaande privacybescherming. Tegen deze achtergrond zal het *Online Durchsuehung* arrest grondig besproken worden, waarbij wordt stilgestaan bij de formulering van het nieuwe grondrecht, en bij de afwegingen van het Hof over de voorwaarden waaronder inbreuken op dit grondrecht toelaatbaar zijn (*Schranken-Schranken*) (2).

De wijze waarop in *Online Durchsuehung* deze ‘grenzen aan inbreuken’ worden vormgegeven is in het bijzonder interessant omdat het *BVerfG* daarin aansluit bij een aantal andere oordelen<sup>5</sup> die het recentelijk heeft geveld met betrekking tot nieuwe surveillancetechnologie zoals *datamining* en afluisteren op afstand (3). De rode lijn door deze uitspraken is dat het Hof zich weliswaar niet principieel uitspreekt tegen het gebruik

<sup>1</sup> Alle drie verbonden aan de onderzoeksgroep Law, Science, Technology and Society Studies (LSTS), Vrije Universiteit Brussel en actief in een onderzoeksproject *Law and Automatic Computing: Mutual Transformations* (GOA). Eerstgenoemde is tevens verbonden aan het onderzoeksinstituut TILT, Universiteit Tilburg. De auteurs zijn Christoph Schnabel en Gerrit Hornung (Universität Kassel) dankbaar voor de hulp bij het vergaren van Duitse literatuur.

<sup>2</sup> Online beschikbaar op: [http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227\\_1bvr037007.html](http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html)

Engelse vertaling: [http://www.bundesverfassungsgericht.de/en/decisions/rs20080227\\_1bvr037007en.html](http://www.bundesverfassungsgericht.de/en/decisions/rs20080227_1bvr037007en.html)

<sup>3</sup> “Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme”, (paragrafen 203-206, *Online Durchsuehung*, Bundesverfassungsgerichtshof 27 februari 2008).

<sup>4</sup> BVerfG 15 december 1983, (*Volkszählung*), BVerfGE 65, 1.

<sup>5</sup> *Großer Lauschangriff*, BVerfG 3 maart 2004, 1 BvR 2378/98 en 1 BvR 1084/99; *Rastererfahndung*, BVerfG 4 april 2006, 1 BvR 518/02; *Automatisierte Erfassung von Kfz-Kennzeichen*, BVerfG 11 maart 2008, 1 BvR 2074/05, 1 BvR 1254/07; *Vorratsdatenspeicherung* (‘Einstweilige Anordnung’: voorlopige voorziening in kort geding), BVerfG 11 maart en 28 oktober 2008, 1 BvR 256/08.

van ingrijpende en uitgebreide surveillancetechnologie, maar dat het daarentegen wel stelt dat zulke maatregelen proportioneel en constitutioneel verantwoord ingezet moeten worden. Hiermee vernieuwt het Hof op belangwekkende wijze de grondrechtelijke bescherming die aan burgers in de informatiesamenleving wordt geboden. Tot slot bekijken we in deze bijdrage in hoeverre de betekenis van het *Online Durchsuchung* arrest over de Duitse grenzen heen reikt (4). Daarbij zal duidelijk worden dat het ook voor niet-Duitse *ICT & Law* juristen een inspiratiebron kan vormen. Zo werd het arrest in Nederland al bondig en helder van commentaar voorzien door Steenbruggen.<sup>6</sup> Ondanks het feit dat Steenbruggen erkent dat het onmogelijk is om een rechtstreekse parallel te trekken met het Nederlandse recht – bij gebreke aan constitutionele rechtspraak kennen – onderstreept hij dat de lacunes in de bescherming in Nederland misschien nog wel groter zijn dan degene die in Duitsland zijn opgevuld door het nieuw geformuleerde grondrecht.<sup>7</sup>

## 1. De bredere juridische context van het *Online Durchsuchung* arrest

### *Overzicht van het Duitse grondwetsysteem*<sup>8</sup>

Het Duitse grondwettelijke recht is in meerdere opzichten een spannend en inspirerend terrein.<sup>9</sup> Zo kent de in 1949 opgestelde Duitse Grondwet een unieke, waardengeladen redactie.<sup>10</sup> Dit komt onder andere goed tot uitdrukking in de *Ewigkeitsgarantie* van art. 79 GG, lid 3, die niet alleen de absolute onaantastbaarheid garandeert van de politieke idee van de democratische en sociale bondsstaat, maar ook van de rechten en maatschappelijke goederen beschermd door de eerste twintig grondrechtartikelen.<sup>11</sup> De betekenis van de grondrechten vervat in de Duitse Grondwet is tweeledig. In de eerste plaats dienen de grondrechten ter garantie van de bescherming van de individuele vrijheid

---

<sup>6</sup> BVerfG 27 februari 2008, *Online-Durchsuchung* (m.nt. W. Steenbruggen), *Mediaforum. Tijdschrift voor Media en Communicatierecht*, 2008, vol. 20, nr. 5, p. 223-235.

<sup>7</sup> Steenbruggen (2008), p. 235.

<sup>8</sup> Zie voor een heldere Engelstalig inleiding tot het Duitse grondwettelijke recht: S. Michalowski & L. Woods, *German constitutional law. The protection of civil liberties*, Ashgate: Brookfield 1999.

<sup>9</sup> Zie meer uitgebreid over de betekenis, werking en reikwijdte van het *Grundgesetz*: A. Koekkoek, P. Zoontjens, F. Vlemminx, G.-J. Leenknecht, S. Nouwt, B.-J. Koops, H. Schooten-van der Meer & R. Bos, *Bescherming van grondrechten in het digitale tijdperk. Een rechtsvergelijkend onderzoek naar informatie- en communicatievrijheid en privacy in Zweden, Duitsland, Frankrijk, België, de Verenigde Staten en Canada* (eindrapport WODC), KUB: Tilburg 2000, 72-107; T. Hoeren & A. Rodenhausen, "Constitutional Rights and New Technologies in Germany", in: R. Leenes, B.-J. Koops & P. De Hert (eds.), *Constitutional Rights and New Technologies. A Comparative Study* (Information Technology & Law Series, vol. 15), T.M.C. Asser Press: The Hague 2008, pp. 137-158.

<sup>10</sup> In de lente en zomer van 2009 werd in de Duitse media uitgebreid gedebatteerd over de status van het *Grundgesetz* in het huidige tijdsgewricht van steeds verdergaande Europese eenwording. Hoewel sommigen vrezen dat het *Grundgesetz* en de Duitse constitutionele rechtspraak aanzienlijk aan belang zullen inboeten door de inwerkingtreding van het Verdrag van Lissabon – er gaan zelfs stemmen op voor een volledig nieuwe Duitse grondwet die beter in overeenstemming zou zijn met de politieke realiteit van de Europese eenwording! – wordt over het algemeen toch aangenomen dat *Grundgesetz* en Verdrag van Lissabon met elkaar zullen kunnen co-existeren. (Zie o.a.: T. Darnstädt, "Glück des Neuanfangs. Kann die deutsche Verfassung von 1949 in einer globalisierten Welt noch bestehen?", *Der Spiegel*, nr. 13, 23 maart 2009, pp. 52-59; "Germany's Constitutional Court. Judgment days", *The Economist*, 26 maart 2009). Directe aanleiding voor deze polemiek was enerzijds het 60-jarige bestaan van het *Grundgesetz* en anderzijds de verrassende en complexe uitspraak van het *Bundesverfassungsgericht* over de grondwettelijkheid van de Duitse implementatiewet van het Verdrag van Lissabon. In dit arrest (BVerfG 30 juni 2009, 2 BvE 2/08) oordeelde het Hof dat slechts twee van de drie wetten ter implementatie van het Verdrag in overeenstemming zijn met het *Grundgesetz*. Het Hof preciseert dat het Europese parlement nog onvoldoende in staat is om het Duitse volk op democratische en constitutionele wijze te vertegenwoordigen, en daarom zal de gewraakte Geleidewet van het Verdrag van Lissabon een grotere rol aan het Duitse parlement moeten toebedelen om in overeenstemming met het *Grundgesetz* te zijn. De meningen zijn verdeeld over de vraag of het arrest als een nationalistisch-euroceptische mislag of als een constitutionele triomf moet worden geduid.

<sup>11</sup> Deze garantie verbiedt slechts principiële wijzigingen en geen 'systeem immanente' wijzigingen: *Abhörurteil*, BVerfG 15 december 1970, *BVerfGE* 30, 1.

tegen een al te ongebreidelde machtsuitoefening van de staat.<sup>12</sup> Zo heeft de burger bijvoorbeeld de mogelijkheid om zich na de gewone rechtsgang tot een constitutioneel Hof te wenden met een zogenaamde grondwetschendingsklacht (*Verfassungsbeschwerde*, art. 93 GG, lid 1, sub 4a) wanneer hij meent dat er sprake is van een inbreuk van de staat op zijn constitutionele rechten. Dat de mogelijkheid om een grondwetschendingsklacht neer te leggen een unieke constitutionele bescherming biedt voor elke individuele burger werd in 2008 op een symbolisch niveau prachtig naar voren gebracht in de massale *Sammel-Verfassungsbeschwerde* tegen de Duitse implementatiewet van de Europese Databetrouwbaarheidsrichtlijn waarin meer dan 34.000 burgers zich achter dezelfde klacht schaarden.<sup>13</sup> Naast deze primaire beschermende functie dienen de grondrechten ook als de fundamentele toetssteen voor het Duitse positieve recht. Om te beginnen is de wetgever gebonden aan de Grondwet (art. 20 GG, lid 3): wetgeving moet zowel formeel als materieel in overeenstemming zijn met de grondwet. Bovendien dient iedere Duitse rechter een grondwetsconforme uitleg te geven aan alle positiefrechtelijke normen die een rol spelen in de hem voorgelegde zaken.<sup>14</sup> Wanneer een rechter in een concreet rechtsgeeding meent dat een rechtsregel in strijd is met de grondwet, moet hij deze aan het *Bundesverfassungsgericht* voorleggen (“concrete normcontrole”, art. 100 GG, lid 1). Afgezien van deze toetsing die voortvloeit uit concrete gevallen is er ook de zogenaamde “abstracte normcontrole” (art. 93 GG, lid 1, sub 2) waarbij de Bondsdag<sup>15</sup>, de Bondsregering of een Landsregering zich los van een concreet geschil tot de constitutionele rechters van het *BVerfG* kunnen wenden voor een beoordeling van de grondwettelijkheid van een abstracte norm. Als “hoeder van de Grondwet” heeft het *BVerfG* bij elk van de bovengenoemde procedures de bevoegdheid om de grondwettelijkheid van normen te beoordelen en zo nodig nietig te verklaren. De rechters van dit hoogste constitutionele Hof schromen niet om van deze bevoegdheid gebruik te maken en zenden daarmee met vaste regelmaat grensoverschrijdende signalen uit.<sup>16</sup> De meeste grondrechten in het *Grundgesetz* zijn geen absolute rechten. Rond dit vrij eenduidige uitgangspunt heeft het *BVerfG* in zijn rechtspraak een doorwrocht gebied vol nuances ontwikkeld. Wie weinig bekend is met het Duitse constitutionele recht verdwaalt vrij makkelijk in dit gebied vol juridische dwaallichten. Zo kan een schijnbaar ondubbelzinnige absolute bescherming bij zorgvuldigere lezing toch tot op zekere hoogte proportioneel blijken te zijn en andersom. Wie zich hierdoor echter niet laat afschrikken ontdekt dat onder de complexe juridische verstrengelingen iets zit waar menige flauwe proportionaliteitstoets dan wel onwerkbaar rigide absolute bescherming nog iets van kunnen leren: proportionaliteitsafwegingen met haar op de tanden. Maar laten we bij het begin beginnen – zoals gezegd kan vrijwel elk grondrecht onder bepaalde omstandigheden beperkt worden. Vele grondrechten kunnen bijvoorbeeld vanuit het oogpunt van strafpreventie of binnen het kader van een opsporingsonderzoek ingeperkt worden. De voorwaarden onder welke een inperking op een grondrecht mogelijk is staan gespecificeerd bij elk afzonderlijk grondrechtartikel. Soms gaat het hierbij om heel specifieke gronden, soms om een ruim geformuleerd voorbehoud dat restricties toestaat voorzover zij op grond van een formele wet geschieden. Om grondwettelijk te zijn

<sup>12</sup> BVerfG 15 januari 1958, *BVerfGE* 7, 198, 204.

<sup>13</sup> BVerfG 11 maart 2008 (*Vorratsdatenspeicherung*) en BVerfG 28 oktober 2008, BvR 256/08.

<sup>14</sup> Hierdoor kent de Duitse Grondwet ook een horizontale werking: deze staat bekend als de uit art. 1 GG, lid 3, afgeleide “mittelbare Drittwirkung”.

<sup>15</sup> Voorwaarde is wel dat het constitutionele beoordelingsverzoek door tenminste een derde van de parlementsleden gesteund wordt.

<sup>16</sup> Zie voor Nederland bijv.: HR 15 april 1994, *NJ* 1994, 608 (*Valkenhorst*); HR 6 januari 1995, *NJ* 1995, 422 (*Van Gasteren*).

moeten deze beperkingen zelf echter ook weer aan een aantal algemene criteria voldoen – aan zogenaamde “Schraken-Schraken” (beperkingen op grondwettelijke inperkingen). Deze *Schraken-Schraken* dienen om te voorkomen dat een onbezonnen wetgever naar believen grondwettelijke inperkingen kan creëren. Zo is er bijvoorbeeld het met rechtszekerheid en rechtsstatelijkheid samenhangende *Gebot der Normenklarheit und Normenbestimmtheit* (met name afgeleid uit art. 20 GG) dat vereist dat de beperking voldoende begrijpelijk en kenbaar moet zijn voor de betrokken burgers.<sup>17</sup> Andere belangrijke *Schraken-Schraken* zijn onder meer het *Verbot des Einzelfallgesetzes* (art. 19 GG, lid 1, 1<sup>ste</sup> zin) en het *Zitiergebot* (art. 19 GG, lid 1, 2<sup>de</sup> zin), die respectievelijk vereisen dat de inperking niet discriminatoir van aard is en dat een wet alleen een inbreuk kan legitimeren wanneer deze wet het grondrecht dat in het geding is expliciet noemt. Alle *Schraken-Schraken* hebben in de jurisprudentie van het *BVerfG* nadere invulling gekregen. Met name de invulling van het *Grundsatz der Verhältnismäßigkeit* en de *Wesensgehaltsgarantie* (art. 19 GG, lid 2) vormen een goede illustratie van de wijze waarop het *BVerfG* worstelt met de al dan niet absolute status van de *Schraken-Schraken*. Om te beginnen is er dus de *Wesensgehaltsgarantie* die inhoudt dat elk grondrecht een met de menselijke waardigheid uit art. 1 GG, lid 1, samenhangend kernbereik heeft dat onder geen enkele omstandigheid mag worden aangetast. De bescherming van het *Wesensgehalt* blijkt in de praktijk echter minder absoluut dan men op grond van deze formulering zou verwachten. In de jurisprudentie van het *BVerfG* heeft zich namelijk een zogenaamde ‘relatieve’ *Wesensgehalts*-theorie ontwikkeld die stelt dat het kernbereik van een grondrecht pas wordt aangetast wanneer de inbreuk de reikwijdte van de *Eingriffsgrund* (wettelijke grondslag voor de inbreuk) overschrijdt.<sup>18</sup> Door deze relatieve en casuïstische bepaling van het *Wesensgehalt* van een grondrecht is de *Wesensgehaltsgarantie* steeds meer samen gaan vallen met de *Grundsatz der Verhältnismäßigkeit* (“Übermaßverbot”). Dit overmaatverbod garandeert dat grondwettelijke inperkingen proportioneel<sup>19</sup> zijn ten opzichte van het in de wettelijke grondslag beoogde doel. Sommige auteurs menen dat de relatieve uitleg van het *Wesensgehalt* de betekenis van art. 19 lid 2 heeft uitgehold.<sup>20</sup> Het *BVerfG* heeft tot nu toe echter vastgehouden aan een relatieve lezing. Hoewel het Hof ook in het recente *Großer Lauschangriff* arrest (BVerfG 3 maart 2004, 1 BvR 2378/98 en 1 BvR 1084/99) niet tornt aan de relatieve interpretatie van het *Wesensgehalt* stelt het daarin tegelijkertijd dat de menselijke waardigheid uit art. 1 GG, lid 1, j<sup>o</sup> art. 79 GG, lid 3, een onafhankelijke toetssteen vormt naast de *Wesensgehaltsgarantie*: “Een aantasting van de essentiële kern (*Wesensgehalt*) in de zin van art. 19 GG, lid 2, kan weliswaar in een individueel geval

<sup>17</sup> Zie ook paragraaf 208-209 van *Online Durchsuehung*, Bundesverfassungsgerichtshof 27 februari 2008, waarin het hof de betekenis van het *Gebot der Normenklarheit und Normenbestimmtheit* nader omschrijft. Voor een vrije vertaling van dit gedeelte van het arrest naar het Nederlands: Steenbruggen (2008), p. 234.

<sup>18</sup> Zie o.a. Steenbruggen (2008), p. 234; Koekoek e.a. (2000), pp. 77-8; O. Lepsius, “Human Dignity and the Downing of Aircraft: The German Federal Constitutional Court Strikes Down a Prominent Anti-terrorism Provision in the New Air-Transport Security Act”, *German Law Journal* 2006, vol. 7, nr. 9, p. 768, voetnoot 20; P. Lerche, *Übermaß und Verfassungsrecht: zur Bindung des Gesetzgebers an die Grundsätze der Verhältnismäßigkeit und der Erforderlichkeit*, Heymann: Köln 1961, p. 34, voetnoot 21 en 22; BVerfG 28 april 1952, *BHGS* 4, 385 (392); BVerfG 15 december 1965, *BVerfGE* 19, 343.

<sup>19</sup> In de Duitse jurisprudentie wordt het proportionaliteitsprincipe nader ingevuld door te toetsen of een inbreuk *geeignet* (geschikt voor de verwelkoming van het beoogde doel), *notwendig* (noodzakelijk) en *angemessen* (proportionele verhouding tussen inbreuk en doel) is. Zie voor een overzicht van relevante rechtspraak bijv.: D. Schmalz, *Grundrechte*, Nomos: Baden-Baden 1997, p. 72-75; Michalowski & Woods (1999), p. 83-85.

<sup>20</sup> Zie o.a. J. von Bernstorff, *Der Wesensgehalt der Grundrechte und das Verhältnis von Freiheit und Sicherheit im Grundgesetz* (stellingname-document, conferentie voor Duitstalige wetenschappelijk assistenten publiekrecht, Heidelberg, 27 februari 2008), [http://www.mpil.de/shared/data/pdf/tp\\_vonbernstorff.pdf](http://www.mpil.de/shared/data/pdf/tp_vonbernstorff.pdf); M. Koetter, “Freedom, Security and (the) Public(ity): Notes on the 2008 Heidelberg Conference of German-speaking Public Law Assistants”, *German Law Journal* 2008, vol. 9, nr. 5, pp. 750-51.

tevens een inbreuk vormen op de door art. 79 GG, lid 3, beschermde essentie van menselijke waardigheid (*Menschenwürdegehalt*) van een grondrecht. Het *Wesensgehalt* kan echter niet gelijkgesteld worden met de *Menschenwürdegehalt* van een grondrecht”.<sup>21</sup>

Op deze wijze spaart het Hof zowel de geit als de kool: de relatieve lezing van de *Wesensgehaltgarantie* kan gehandhaafd blijven, terwijl daarnaast aangeknoopt kan worden bij de *Menschenwürdegehalt* voor het bepalen van een meer in absolute zin beschermd kernbereik van een grondrecht.

### ***Digitale grondrechten binnen het Duits grondwetsysteem***

Voor *ICT & Law* juristen vertoont het Duitse grondwetsysteem opvallende kenmerken. Hoewel er geen afzonderlijke ‘digitale’ grondrechten zijn is er sprake van een breed scala van algemene grondrechten die bescherming kunnen bieden aan de vrijheid van het individu in de sfeer van ICT. *De facto* is er hierdoor een overdaad aan grondnormen in het *Grundgesetz* die in de sfeer van privacy en surveillance vallen. In de eerste plaats zijn er specifieke normen, die met regelmaat geactualiseerd worden, zoals het *huisrecht*<sup>22</sup> (art. 13), dat met name grenzen stelt aan het aftappen en afluisteren door middel van richtmicrofoons en andere afluisterapparatuur binnen de huiselijke sfeer, de *vrijheid van meningsuiting* (art. 5, lid 1 en 2), en het *telecommunicatiegeheim* dat het brief-, post-, telefoon- en telegraafgeheim omvat (art. 10, lid 1). Daarnaast zijn er de meer open normen die volgen uit het zogenaamde ‘algemeen persoonlijkheidsrecht’ zoals afgeleid uit de twee artikelen waarmee het *Grundgesetz* begint: art. 1 GG, lid 1 (bescherming van de menselijke waardigheid), en art. 2 GG, lid 1 (het recht om vrij de eigen persoonlijkheid te kunnen ontplooiën).<sup>23</sup> Een dergelijk algemeen persoonlijkheidsrecht bestaat niet in het Nederlandse recht, hoewel er veel over wordt gesproken in de juridische literatuur en het in navolging van het Duitse recht zelfs een enkele maal in de Nederlandse jurisprudentie is opgedoken.<sup>24</sup> Uit dit algemene persoonlijkheidsrecht heeft het *BVerfG* in een aantal baanbrekende arresten, vaak “getriggerd” door technologische ontwikkelingen, enkele nieuwe grondrechten afgeleid. Het algemene persoonlijkheidsrecht is daarmee voor de constitutionele rechter een handzaam instrument om gaten in de grondwet te vullen. Voorbeelden van zulke specifieke *Ausprägungen*<sup>25</sup> van het algemeen persoonlijkheidsrecht zijn het recht op bescherming van de privé-sfeer, dat voor het eerst erkend werd in *BVerfG* 15 januari 1970, *BVerfGE* 27, 344 (*Ehescheidungsakten*) en het recht op informationele zelfbeschikking, dat

<sup>21</sup> “Eine Antastung des Wesensgehalts im Sinne von Art. 19 Abs. 2 GG kann zwar im Einzelfall zugleich den von Art. 79 Abs. 3 GG geschützten Menschenwürdegehalt eines Grundrechts beeinträchtigen. Der Wesensgehalt ist aber nicht mit dem Menschenwürdegehalt eines Grundrechts gleichzusetzen”. (*BVerfG* 3 maart 2004, (*Großer Lauschangriff*)1 BvR 2378/98 en 1 BvR 1084/99, paragraaf 112).

<sup>22</sup> Art. 13 *Grundgesetz* werd in 1998 werd herzien ten einde het direct afluisteren in woningen (*Großer Lauschangriff*) bij verdenking van zeer ernstige misdrijven mogelijk te maken. Zie voor het oordeel van het *Bundesverfassungsgericht* over deze grondwetswijziging: *BVerfG* 3 maart 2004, 1 BvR 2378/98 en 1 BvR 1084/99.

<sup>23</sup> Artikel 1, eerste lid, luidt: “Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.” Artikel 2, eerste lid, luidt: “Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.”

<sup>24</sup> HR 15 april 1994, *NJ* 1994, 608 (*Valkenhorst*); R. Nehmelmann, *Het algemeen persoonlijkheidsrecht. Een rechtsvergelijkende studie naar het algemeen persoonlijkheidsrecht in Duitsland en Nederland* (diss. Utrecht), Deventer: W.E.J. Tjeenk Willink 2002; A.J. Nieuwenhuis, *Tussen privacy en persoonlijkheidsrecht. Een grondrechtelijk en rechtsvergelijkend onderzoek*, Nijmegen: Ars Aequi 2001.

<sup>25</sup> “Uitdrukkingen”: hierdoor is het in principe onjuist is om van *nieuwe* grondrechten te spreken. Het gaat immers slechts om nieuwe *uitdrukkingen* van een bestaand grondrecht. W. Hoffmann-Riem, “Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme”, *JuristenZeitung* 2008, vol. 63, nr. 21, p. 1014.

geformuleerd werd in *Volkszählungsurteil* (BVerfG 15 december 1983, *BVerfGE* 65, 1). Ook in het *Online-Durchsuchung* arrest gaat het Hof vrij uitgebreid in op deze in het algemene persoonlijkheidsrecht besloten liggende *lückenschließenden Gewährleistung* (“gatenstoppende garantie”) die met name nodig is “om nieuwsoortige bedreigingen het hoofd te bieden” welke meegebracht kunnen worden door “wetenschappelijk-technische vooruitgang en de veranderde levensverhoudingen” (paragraaf 169).

Bij de bepaling van de toelaatbaarheid van inbreuken op de bovengenoemde ‘digitale’ grondrechten is het, net zoals bij andere grondrechten, noodzakelijk om vast te stellen wat de onaantastbare kern (*Wesensgehalt*) van het recht is. En ook hier brengt dat complexe juridische constructies met zich mee waarin het vaak verre van evident hoe absoluut “absolute” bescherming eigenlijk is en waar absolute bescherming ophoudt en proportionele begint. Zo heeft het *BVerfG* in zijn rechtspraak van de afgelopen halve eeuw<sup>26</sup> uit o.a. de *Wesensgehaltgarantie* een “onaantastbaar kernbereik van de private inrichting van het eigen leven” (“*unantastbare*” en “*absolut geschützte Kernbereich privater Lebensgestaltung*”) gestedilleerd. Op het eerste gezicht lijkt het evident dat er aan dit *Kernbereich* onder geen enkel beding getornd mag worden. Maar voor wie in het achterhoofd houdt dat het *BVerfG* een relatieve lezing geeft aan de *Wesensgehaltgarantie* zal dit minder vanzelfsprekend zijn. In het eerder besproken *Großer Lauschangriff* arrest<sup>27</sup> hield het *BVerfG* een en ander op door duidelijk te maken dat dit *Kernbereich privater Lebensgestaltung*<sup>28</sup> niet alleen voortvloeit uit de *Wesensgehaltgarantie* maar ook direct uit de in art. 1 GG, lid 1, beschermde menselijke waardigheid (paragraaf 54). Het Hof onderstreept de speciale status van dit kernbereik: “Wanneer men in eigen huis, in de private en intieme sfeer, ja zelfs wanneer men met zichzelf praat, niet meer zeker kan zijn of men niet afgeluisterd wordt, dan blijft er van het grondrecht op de onschendbaarheid van de woning niets meer over. Van telefoneren en het schrijven van brieven kan men eventueel afzien –van een laatste terugtrekmogelijkheid in de eigen woning niet”.<sup>29</sup> Voor zover het *Kernbereich privater Lebensgestaltung* direct voortvloeit uit de bescherming van de menselijke waardigheid uit art 1 GG, lid 1, stelt het in principe een absolute grens aan grondwettelijke inbreuken en behelst dus geen proportionaliteitsafweging zoals dat bij de *Wesensgehaltgarantie* wel het geval is. “Tot de onaantastbaarheid van de menselijke waardigheid op grond van art. 1 GG, lid 1, behoort de erkenning van een absoluut beschermd kernbereik van de private inrichting van het eigen leven. In dit bereik mag geen inbreuk gemaakt worden door akoestische observatie van de woonruimte voor strafvervolgendoeleinden (art. 13 GG, lid 3). Een afweging naar de maatstaf van het proportionaliteitsbeginsel tussen de onschendbaarheid

---

<sup>26</sup> Deze jurisprudentiële tendens wordt ingezet door het *Elfe*-arrest (BVerfG 6,32, 16 januari 1957, 1 BvR 253/56) waarin onder meer uit de *Wesensgehaltgarantie* (art. 19, lid 2 j° art. 1, lid 3 j° art. 2, lid 1 GG) wordt afgeleid dat er een “unantastbarer Bereich menschlicher Freiheit besteht, der der Einwirkung der gesamten öffentlichen Gewalt entzogen ist” (paragraaf 32). Het meest recente belangwekkende arrest op dit gebied is BVerfG 3 maart 2004, (*Großer Lauschangriff*), 1 BvR 2378/98 en 1 BvR 1084/99.

<sup>27</sup> BVerfG 3 maart 2004, 1 BvR 2378/98 en 1 BvR 1084/99

<sup>28</sup> Onder het *Kernbereich privater Lebensgestaltung* kunnen bijvoorbeeld vallen: een gesprek met een zielsverzorger, een hoogst persoonlijk gesprek met een nauwe familieverwant, intieme gevoelsuitingen of uitdrukkingen van seksualiteit. BVerfG 3 maart 2004, (*Großer Lauschangriff*) 1 BvR 2378/98 en 1 BvR 1084/99, paragraaf 123 en 132.

<sup>29</sup> “Wenn man in seiner Wohnung nicht mehr sicher sein könne, im privaten und intimen Kreis, ja sogar bei Selbstgesprächen nicht belauscht zu werden, so bleibe vom Grundrecht der Unverletzlichkeit der Wohnung nichts mehr übrig. Auf das Telefonieren und Briefeschreiben könne gegebenenfalls verzichtet werden, auf eine letzte Rückzugsmöglichkeit in der eigenen Wohnung nicht.” (BVerfG 3 maart 2004, (*Großer Lauschangriff*) 1 BvR 2378/98 en 1 BvR 1084/99, paragraaf 54).

van de woning (art. 13 GG, lid 1 j° art. 1 GG, lid 1) en het strafvervolgingsbelang vindt in zoverre niet plaats [...]; ieder gebruik van zulke informatie is uitgesloten”.<sup>30</sup>

Op deze wijze werd in het *Großer Lauschangriff* arrest een grondwetswijziging van art. 13 GG (het huisrecht), die akoestische observatie in woonruimtes mogelijk maakte, gedeeltelijk ongrondwettelijk verklaard omdat geen specifieke waarborgen voor de bescherming van het *Kernbereich privater Lebensgestaltung* gespecificeerd waren. Deze specifieke waarborgen moeten garanderen dat de akoestische observatie onderbroken wordt zodra het *Kernbereich privater Lebensgestaltung* in het geding is en dat eventueel toch geregistreerde gegevens uit dit bereik onmiddellijk gewist<sup>31</sup> worden (paragraaf 135). Het *Kernbereich privater Lebensgestaltung* speelt niet alleen bij het huisrecht maar ook bij andere ‘digitale’ grondrechten een cruciale rol. Zo zal bij de bespreking van het *Online-Durchsuchung* (zie hieronder, paragraaf 2.2.) blijken dat voor de beoordeling van de toelaatbaarheid van inbreuken op het nieuwe IT-recht niet alleen de *Verhältnismäßigkeit* en het *Gebot der Normenklarheit und Normenbestimmtheit*, maar ook het *Kernbereich privater Lebensgestaltung* van belang was.

### ***De hybride Duitse samenleving: repressie en rechtsbescherming.***

In vergelijking met de andere Europese lidstaten vindt men in Duitsland zowel een aantal uitzonderlijk verstrekkende politiebevoegdheden met het oog op de handhaving van de binnenlandse veiligheid als ook een bijzonder hoog niveau van privacybewustzijn, zeer krachtige dataprotectie-autoriteiten en een wettelijk vastgelegde privacybescherming die tot de meest strikte van de wereld behoort. Vanuit het oogpunt van privacy is Duitsland dan ook een land van grote contrasten. In de *International Privacy Ranking*<sup>32</sup> van 2007 geeft Duitsland een gele kleur (“*enige waarborgen maar verzwakte bescherming*”) – hetgeen een redelijk goede score op privacygebied is. Tot enkele jaren terug behaalde Duitsland zelfs het zeer goede donker groen (“*significante bescherming en waarborgen*”). Ter vergelijking: België scoorde in 2007 zoals Duitsland geel, Nederland scoort al jaren rood (“*systemisch falen om de waarborgen te handhaven*”) en Frankrijk schoot in 2007 naar roze (“*samenleving met surveillance op grote schaal*”). Het Verenigd Koninkrijk en de VSA scoren net als China en Rusland zwart (“*endemische ‘surveillance society’*”). Tegelijkertijd stelt *Privacy International* vast dat er maar in weinig landen zoveel wordt afgetapt als in Duitsland. Dat Duitsland een lange traditie van verregaande

<sup>30</sup> “Zur Unantastbarkeit der Menschenwürde gemäß Art. 1 Abs. 1 GG gehört die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung. In diesen Bereich darf die akustische Überwachung von Wohnraum zu Zwecken der Strafverfolgung (Art. 13 Abs. 3 GG) nicht eingreifen. Eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes zwischen der Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und dem Strafverfolgungsinteresse findet insoweit nicht statt [...]; jede Verwertung solcher Informationen ist ausgeschlossen” (BVerfG 3 maart 2004, (*Großer Lauschangriff*)1 BvR 2378/98 en 1 BvR 1084/99, Leitsätze 2 en 5).

<sup>31</sup> Omdat vaak pas *achteraf* beoordeeld kan worden of er al dan niet sprake is van gegevens uit het *Kernbereich privater Lebensgestaltung* ontstaat een opmerkelijke paradox: in vele gevallen zal de status van “absoluut beschermd gebied” pas *na* een inbreuk verleend kunnen worden. Bovendien spelen bij de bepaling van of iets tot het *Kernbereich* behoort wel degelijk proportionaliteitsafwegingen een rol: een gesprek waarin intieme bekentenissen vermengd zijn met de planning van een terroristische aanslag zal daarmee dus buiten het kernbereik vallen (vgl. paragraaf 281, *Online Durchsuchung*, Bundesverfassungsgerichtshof 27 februari 2008). Wat blijft er nog over van de absolute bescherming van het *Kernbereich* als de inhoud van dat gebied op grond van proportionaliteitsafwegingen wordt vastgesteld? (Cf. M. Baldus, “Der Kernbereich privater Lebensgestaltung – absolut geschützt, aber abwägungs offen”, *JuristenZeitung* 2008, vol 63, nr. 5, pp. 218-227) Een manier om deze paradox op te lossen is door te stellen dat de absolute bescherming van het *Kernbereich* er in steekt dat men onder omstandigheden weliswaar grondwettelijke inbreuken kan plegen, maar dat deze *nooit en te nimmer* een mensonwaardige behandeling mogen beogen. Een andere, zij het wat omslachtige, oplossing zou zijn om, telkens wanneer men het risico loopt een inbreuk te maken op het *Kernbereich privater Lebensgestaltung*, een preliminaire beoordeling te laten maken of bepaalde gegevens al dan niet tot het absoluut beschermde gebied behoren door een dienst die niet betrokken is bij het lopende onderzoek. Zie: R. Poscher, “Menschenwürde und Kernbereichsschutz. Von den Gefahren einer Verräumlichung des Grundrechtsdenkens”, *JuristenZeitung* 2009, vol. 64, nr. 6, pp. 269-277.

<sup>32</sup> <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559597>

politiebevoegdheden heeft is onder andere een gevolg van het terrorisme in de jaren zeventig. In de zaak *Klass* (EHRM 6 september 1978) durfde Duitsland als eerste het Europees Hof te trotseren met een af luisterwet waarin rechterlijke controle ontbrak en vervangen werd door parlementaire controle.<sup>33</sup> Deze traditie van verregaande veiligheidsbevoegdheden is in Duitsland in de laatste jaren sterk naar voren gebracht door mensen als Wolfgang Schäuble. Schäuble, lid van de CDU en sinds 2005 minister van binnenlandse zaken, is de man die CIA-achtige ideeën in de EU binnenbracht en die de geestelijke vader is van het Verdrag van Prüm (ook bekend als het Schengen III Verdrag) dat op 27 mei 2005 ondertekend werd door zeven lidstaten waaronder Nederland en België. Grondgedachte achter dit verdrag is het zogenaamde *beschikbaarheidsprincipe* dat stelt dat op nationaal niveau opgeslagen DNA-profielen, vingerafdrukken en kentekens direct beschikbaar moeten zijn voor elke politiedienst in Europa. Hoewel het Verdrag van Prüm een iets afgezwakte versie van het zuivere *beschikbaarheidsprincipe* vorm geeft, is het op het gebied van informatie-uitwisseling een absoluut baanbrekend verdrag dat weinig bekommernis om privacyrechten behelst.

Aan de andere kant zijn de levendige Duitse hackerbeweging en de massale pro-privacy protesten in Duitsland absolute unica in Europa.<sup>34</sup> Na de grootschalige protesten in november 2007 onder het motto “Vrijheid in plaats van angst” (“*Freiheit statt Angst*”) tegen de steeds verdergaande informatiezucht van de overheid, volgden volgens de Duitse werkgroep Data Retentie (“*Arbeitskreis Vorratsdatenspeicherung*”) door het gehele land talloze andere gelijkgestemde initiatieven waaraan duizenden burgers deelnamen.<sup>35</sup> Reeds in juli 2008 hadden meer dan 10.000 mensen een petitie ondertekend tegen de zogenaamde BKA-wet die de federale politie (het *Bundeskriminalamt*) verregaande bevoegdheden zou verlenen om private computers van op afstand uit te kunnen lezen. Toen deze wet op 12 november 2008 door de *Bundestag* werd aangenomen en vervolgens twee weken later door een veto van de *Bundesrat* alsnog werd verworpen, werd dit door menigeen dan ook gezien als een grote overwinning voor het ‘vrijheidskamp’. Zo duidde de grote krant *Die Zeit* de afwijzing van het wetsvoorstel door de *Bundesrat* als het bewijs dat de Bondsrepubliek eindelijk uit de schaduw was getreden van 9/11.<sup>36</sup> Tegelijkertijd wezen voorstanders van de BKA-wet erop dat dit niet betekende dat de BKA-wet van tafel was. En inderdaad: op 19 december 2008 kwam men onder leiding van een uit zowel leden van de Bondsdag als Bondsraad samengestelde *Vermittlungsausschuss* (“bemiddelingscommissie”, art. 77 GG) alsnog tot overeenstemming. Na enige wijzingen (zoals het verplicht stellen van rechterlijk toezicht bij online doorzoekingen) werd de nieuwe BKA-wet alsnog met een nipte meerderheid van 35 tegen 34 stemmen aangenomen. De nieuwe BKA-wet is op 1 januari 2009 in

---

<sup>33</sup> Voorafgaand aan het *Klass*-arrest (EHRM 6 september 1978, AA 1979, 327) gaf ook het *Bundesverfassungsgericht* (*Abhörurteil*, BVerfG 15 december 1970, *BVerfGE* 30, 1) groen licht aan de af luisterwet die het mogelijk maakt om een inbreuk te maken op het grondwettelijk vereiste van rechterlijke controle (art. 19 GG, lid 4).

<sup>34</sup> Cf. “Call for worldwide protests against surveillance”, *EDRI-gram*, *Biweekly newsletter about digital civil rights in Europe*, nr. 6.16, 27 augustus 2008, en “German Protests in over 30 cities against surveillance On 31 May 2008, privacy activists organized new rallies in more than 30 cities across Germany”, *EDRI-gram*, *Biweekly newsletter about digital civil rights in Europe*, nr. 6.13, 2 juni 2008.

<sup>35</sup> Zie o.a.: Persbericht van de Duitse werkgroep Data Retentie (alleen in het Duits, 1 juni 2008), <http://www.vorratsdatenspeicherung.de/content/view/227/1/lang.de/>; Het “Pigeon Project” – artistieke, privacy bevorderende activiteiten door internationale artiesten van het Amsterdamse Sandberg Instituut, <http://www.pigeonproject.net/>; Opnames van onafhankelijk radio-uitzendingen (alleen in het Duits, 31 mei 2008), <http://wiki.vorratsdatenspeicherung.de/Radio/>; De petitie tegen de BKA-wet (alleen in het Duits), <http://www.bka-petition.de/>.

<sup>36</sup> H. Wefing, “Das Ende von 9/11”, *Die Zeit*, 20 november 2008, nr. 48 [<http://www.zeit.de/2008/48/01-Rechtspolitik>]: “Was sich hier abzeichnet, ist etwas Größeres: Die Bundesrepublik tritt heraus aus dem Schatten von 9/11”.

werking getreden en geeft de federale politie onder andere de bevoegdheid tot het uitlezen van private harde schijven op afstand. Minder dan een maand later, op 27 januari 2009, legde de journaliste Bettina Winseman een *Verfassungsbeschwerde* tegen de wet neer bij het *BVerfG*.<sup>37</sup> Op 23 april volgde een grondwettelijke klacht van het *Deutsche Journalisten-Verband*. Deze klacht werd bovendien onderschreven door een grote groep journalisten, politici, artsen en advocaten waaronder zich ook gerenommeerde namen bevinden zoals die van voormalig federaal minister van Binnenlandse Zaken, Gerhart Baum, en de uitgever van *Die Zeit*, Michael Naumann.<sup>38</sup> Nadat in mei 2009 ook de oppositiefractie *Bündnis 90/Die Grünen* en de *Republikanische Anwältinnen- und Anwälteverein*<sup>39</sup> elk afzonderlijk de gang naar het *BVerfG* aflegden, staat de teller voorlopig op vier *Verfassungsbeschwerden* tegen de BKA-wet. De worsteling tussen veiligheidswetgeving en de constitutionele rechten is dus nog niet ten einde. Net als de bewaarplicht van verkeersgegevens op grond van richtlijn 2006/24/EG<sup>40</sup> is de bevoegdheid van het *Bundeskriminalamt* om private computers op afstand uit te kunnen lezen vermoedelijk nog lang geen afgesloten hoofdstuk – en zal tot op de vierkante millimeter uitgevochten worden door de twee tegengestelde tradities die de Duitse samenleving zo kenmerken. Het is nu vooral wachten op *Online Durchsuchung-II*, waarin het *BVerfG* zich zal moeten buigen over de grondwettelijkheid van de per 1 januari 2009 in werking getreden BKA-wet. Zo verklaarde de Duitse Bondsminister van Justitie, Brigitte Zypries (*SPD*), onlangs dat zij al een ontwerpwijziging van het Wetboek van Strafrecht klaar heeft liggen die het gebruik van spionage-software sterk uit zou breiden<sup>41</sup>: waar de huidige BKA-wet ‘slechts’ de bevoegdheid tot het preventieve gebruik van *spyware* verleent aan het *Bundeskriminalamt* in geval van terroristische dreigingen, zou de nieuwe wetswijziging gewone rechercheurs de bevoegdheid verlenen om bij strafrechtelijk onderzoek naar reeds gepleegde zware misdrijven tot “Quellen-Telekommunikationsüberwachung” over te gaan (*Quellen-TKÜ*). *Quellen-TKÜ* houdt in dat door middel van heimelijk geïnstalleerde spyware het mogelijk wordt om Skype-gesprekken af te luisteren op de broncomputers zelf: dat wil zeggen vóór dat de berichten versleuteld verstuurd worden. Hoewel het officiële standpunt van de wetgever is dat een *Quellen-TKÜ* heel wat anders is dan een *Online-Durchsuchung* van een complete harde schijf, heeft de Minister van Justitie verklaard toch liever eerst *Online Durchsuchung-II* af te wachten alvorens verdere wetgevende activiteiten te ondernemen. En zo sleept de eindeloze precaire tango tussen veiligheidswetgeving en de bescherming van burgerrechten zich voort.

In afwachting van *Online Durchsuchung-II* is het interessant om het *Online Durchsuchung*-arrest van 27 februari 2008 nog eens in nader detail te bestuderen. In dit arrest nam het *BVerfG* een regionale wet, die men in zeker opzicht als een voorloper van de federale BKA-wet kan beschouwen, onder handen. En ook in deze zaak waren het de journaliste Bettina Winseman, in dit geval samen met politicus Fabian Brettel (*Die*

<sup>37</sup> De tekst van deze *Verfassungsbeschwerde* is te vinden op: <http://www.heise.de/tp/r4/artikel/29/29614/1.html>

<sup>38</sup> M. Naumann, “Verfassungsklage gegen neues BKA-Gesetz. Jeder ist verdächtig”, *Die Zeit*, 23 april 2009, nr. 18, <http://www.zeit.de/2009/18/BKA-Gesetz>

<sup>39</sup> Een samenvatting van de *Verfassungsbeschwerde* is te vinden op: [http://www.rav.de/fileadmin/user\\_upload/rav/Zusfassg\\_wesentl\\_verfassungsrtl\\_beanstandungen.pdf](http://www.rav.de/fileadmin/user_upload/rav/Zusfassg_wesentl_verfassungsrtl_beanstandungen.pdf)

<sup>40</sup> BVerfG 11 maart 2008 en BVerfG 28 oktober 2008, BvR 256/08.

<sup>41</sup> “Bosbach: Strafprozessordnung soll erweitert werden”, *Neue Osnabrücker Zeitung*, 21 maart 2009, [http://www.neue-oz.de/information/noz\\_print/interviews/20090321\\_spionage.html](http://www.neue-oz.de/information/noz_print/interviews/20090321_spionage.html); “SPD will heimliche Online-Durchsuchungen vorerst nicht zur Strafverfolgung”, *Heise Online*, 22 maart 2009, <http://www.heise.de/newsticker/SPD-will-heimliche-Online-Durchsuchungen-vorerst-nicht-zur-Strafverfolgung--/meldung/134968>

Linke), en de eerder genoemde voormalig minister van binnenlandse zaken Gerhart Baum (FDP), die een *Verfassungsbeschwerde* neerlegden bij het *BVerfG*.

## 2. Het arrest *Online Durchsuchung* (Bundesverfassungsgericht, 27 februari 2008)

### *Achtergrond*

Heimelijk geïnstalleerde bespiedingssoftware is een geliefd instrument onder internet-marketeers en criminelen die het voorzien hebben op persoonlijke gegevens. De installatie van bepaalde vormen van *spyware* en ‘Trojaanse paarden’ maakt het immers mogelijk om elke handeling op een computer in *real time* te monitoren of zelfs een harde schijf van op afstand uit te lezen. Zo maakte een recente uitzending van het tv-programma *Zembla*<sup>42</sup> duidelijk hoe op het internet opererende criminelen op deze wijze creditcardgegevens met bijbehorende persoonlijke informatie onderscheppen. De mogelijkheid om op afstand heimelijk een computer te bespieden is echter niet alleen interessant voor marketeers of criminelen maar heeft recentelijk ook de interesse gewekt van menige politiedienst. Reeds wezen we op de heftige politieke en juridische gevechten in Duitsland rond de vraag of de politie onder bepaalde omstandigheden computers van verdachten mag infecteren met software die een zogenaamde *Online-Durchsuchung*<sup>43</sup> mogelijk maakt. Hoewel het nog maar de vraag is of een Trojaans paard van de politie niet evengoed door anti-spyware programma’s onderschept zal worden als willekeurig welk ander Trojaans paard<sup>44</sup> en het onduidelijk is wat de gehanteerde methode voor ‘infectie’ is (bijv. met een geïnfecteerde aanhangsel aan een officiële email van de overheid?), is de juridische en politieke discussie er niet minder om geweest. Een ‘online-doorzoeking’ houdt volgens het arrest van 27 februari 2008 in dat een “geheime toegang op een informatietechnisch systeem door middel van technische infiltratie”<sup>45</sup> wordt gecreëerd “waardoor het gebruik van het systeem geobserveerd en diens opslagmedia uitgelezen kunnen worden”.<sup>46</sup> In de officiële documenten spreekt men van “Remote Forensic Software”,<sup>47</sup> maar in de volksmond zijn de heimelijk geïnstalleerde stukjes software beter bekend als *Polizeitrojaner* of –wanneer het om het gebruik gaat op federaal niveau door het *Bundeskriminalamt*– van zogenaamde *Bundestrojaner*. De juridische culminatie van het debat vond plaats op 27 februari 2008 in het arrest *Online-Durchsuchung*.<sup>48</sup> In dit arrest oordeelde het *Bundesverfassungsgericht* dat een in december 2006 in Noordrijn-Westfalen geamendeerde wet<sup>49</sup> die de inlichtingendiensten

<sup>42</sup> *Zembla*, “Wij weten alles van u”, 9 november 2008, [http://zembla.vara.nl/Voorpagina.1975.0.html?&tx\\_ttnews%5Btt\\_news%5D=7752&tx\\_ttnews%5BbackPid%5D=1974&cHash=01f858b8a6](http://zembla.vara.nl/Voorpagina.1975.0.html?&tx_ttnews%5Btt_news%5D=7752&tx_ttnews%5BbackPid%5D=1974&cHash=01f858b8a6)

<sup>43</sup> Zie voor de geschiedenis van deze ambigue term: T. Böckenförde, “Auf dem Weg zur elektronischen Privatsphäre”, *JuristenZeitung* 2008, vol. 63, nr. 19, p. 929.

<sup>44</sup> A. Grabenströer, “Anti-Viren-Spezialisten zu Späh-Programm-Plänen: Der Bundestrojaner ist nicht vorstellbar”, 29 augustus 2007, <http://www.tagesschau.de/inland/meldung488832.html>

<sup>45</sup> “..heimlicher Zugriff auf informationstechnische Systeme mittels technischer Infiltration” (paragraaf 7, *Online Durchsuchung*, Bundesverfassungsgerichtshof, 27 februari 2008).

<sup>46</sup> “heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können” (Leitsatz 2, *Online Durchsuchung*, Bundesverfassungsgerichtshof 27 februari 2008).

<sup>47</sup> <http://netzpolitik.org/2007/bka-proudly-presents-remote-forensic-software/>

<sup>48</sup> BVerfGE, 27 februari 2008 – 1 BvR 370/07, 1 BvR 595/07

<sup>49</sup> Amendement van §5 Abs. 2 Nr. 11 van het “Verfassungsschutzgesetz Nordrhein-Westfalen” (VSG-NRW), *Gesetz- und Verordnungsblatt für das Land Nordrhein-Westfalen*, 20 december 2006, , p. 620. Online beschikbaar op: [http://www.im.nrw.de/sch/doks/vs/vsg\\_nrw\\_2007.pdf](http://www.im.nrw.de/sch/doks/vs/vsg_nrw_2007.pdf)

in deze deelstaat verregaande bevoegdheden tot online-doorzoekingen<sup>50</sup> gaf, ongrondwettelijk was. Twee vragen stonden centraal in de beoordeling van de Noordrijn-Westfaalse wet. Ten eerste was er de vraag *welk* grondrecht mogelijkwijs door het amendement van de *Verfassungsschutzgesetz* werd aangetast en in de tweede plaats speelde de vraag of de inbreuken binnen de grenzen van het grondwettelijk toelaatbare bleven. Het Hof beantwoordde de eerste vraag verrassend met de formulering van een nieuw grondrecht. Bij de beantwoording van de tweede vraag sloot het Hof zich aan bij de lijn die was uitgezet in een aantal eerdere arresten. De antwoorden op deze twee vragen worden in wat volgt nader geanalyseerd.

### ***De inhoud van het nieuwe grondrecht***

Na uitgebreid uiteengezet te hebben waarom de online-doorzoekingswet geen inbreuk vormt op bestaande grondrechten zoals het *recht op het telecommunicatiegeheim* (art. 10 GG), het *huisrecht* (art. 13 GG) of een van de uit het algemene persoonlijkheidsrecht (art. 1, eerste lid, en art. 2, eerste lid, GG) afgeleide rechten (het *recht op bescherming van de privé-sfeer*<sup>51</sup>, dan wel het *recht op informatiele zelfbeschikking*<sup>52</sup>), schiept het *BVerfG* op basis van het algemene persoonlijkheidsrecht een geheel nieuw grondrecht dat “de vertrouwelijkheid en integriteit van informatietechnologische systemen” beoogt te beschermen. Het nieuwe ‘IT-grondrecht’ beschermt waar de andere grondrechten tekort schieten. Zo stelt het Hof dat het *recht op het telecommunicatiegeheim* (art. 10 GG) onvoldoende bescherming biedt bij online-doorzoekingen omdat het weliswaar de communicatie maar geen opgeslagen data beschermt (paragraaf 185-190). Het *huisrecht* (art. 13 GG) lijkt eveneens moeilijk toepasbaar te zijn bij online-doorzoekingen: vaak zal het voor de politie immers irrelevant zijn of een computer binnenshuis gebruikt wordt of in een publieke ruimte. Of een computer zich binnen de huiselijke muren bevindt of niet wordt daarmee een min of meer toevallige bijkomstigheid: de muur van een huis vormt geen ‘extra’ moeilijkheid die technologisch omzeild moet worden. Het oprekken van het huisrecht (waarbij men het gebruik van een draagbare computer, PDA of mobiele telefoon in een publieke ruimte zou zien als een soort mobiele en virtuele ‘huiselijkheid’) wijst het Hof resoluut van de hand (paragraaf 191-195): een firewall is geen woningsmuur.<sup>53</sup> En tot slot stelt het Hof dat ook de in 1970 en in 1983 geformuleerde *Ausprägungen* van het algemene persoonlijkheidsrecht<sup>54</sup> geen afdoende bescherming bieden. Zo is het recht uit 1970 toegespitst op bescherming van de privé-sfeer, terwijl elk persoonlijk IT-systeem vermoedelijk meer dan louter privé gegevens zal bevatten (paragraaf 197). Zo ook biedt ook recht op informatiele zelfbeschikking uit het arrest van 1983 geen soelaas omdat een online-doorzoeking meestal niet zal gaan om het verzamelen, opnemen, verspreiden of verwerken, maar slechts om het uitlezen van grote

---

<sup>50</sup> Artikel 5, lid 2, sub 11, VSG-NRW: “...heimelijke observaties en andere manieren om het Internet te verkennen, in het bijzonder het op verdeckte wijze deelnemen aan zijn communicatie-structuren dan wel het zoeken hiernaar, evenals het verwerven van heimelijke toegang tot informatietechnologische systemen waarbij ook technologische middelen worden ingezet”. Het *BVerfG* oordeelt in het *Online Durchsuehung* arrest dat zowel het “op verdeckte wijze deelnemen”, als het verwerven van “heimelijke toegang met technologische middelen” ongrondwettelijk is, maar het is alleen met betrekking tot de laatst genoemde praktijk (het “online doorzoeken”) dat een nieuw grondrecht geformuleerd wordt.

<sup>51</sup> BVerfG 15 januari 1970, *BVerfGE* 27, 344.

<sup>52</sup> BVerfG 15 december 1983, *BVerfGE* 65, 1.

<sup>53</sup> Cf. Böckenförde (2008), p. 926.

<sup>54</sup> Resp. BVerfG 15 januari 1970, (*Ehescheidungsakten*), *BVerfGE* 27, 344 en BVerfG 15 december 1983, (*Volkszählungsurteil*), *BVerfGE* 65, 1

hoeveelheden reeds georganiseerde gegevens (paragraaf 198-207): “Een derde die zich toegang verschafft tot een dergelijk systeem, kan zichzelf potentieel een uiterst groot en veelzeggend databestand verschaffen, zonder op verdere dataverzamelings- en dataverwerkingsmethoden aangewezen te zijn. Een dergelijke toegang weegt voor de persoonlijkheid van de gedupeerde vele malen zwaarder dan afzonderlijke dataverzamelingen, waartegen het recht op informatiele zelfbeschikking beschermt”.<sup>55</sup> Het Hof maakt aldus duidelijk dat geen enkel bestaand grondrecht het gebied van online-doorzoekingen afdoende beslaat. De vraag of een dergelijke lacune opvulling behoeft, beantwoordt het Hof bevestigend: “Uit de relevantie van het gebruik van informatietechnische systemen ten behoeve van de persoonlijkheidsontplooiing (*Persönlichkeitsentfaltung*) en uit de gevaren voor de persoonlijkheid die verbonden zijn aan dit gebruik, volgt een nood aan bescherming die belangrijk is voor de grondrechten. Het individu is er op aangewezen dat de staat, met het oog op de ongehinderde persoonlijkheidsontplooiing, de gerechtvaardigde verwachtingen wat betreft de integriteit en vertrouwelijkheid van dergelijke systemen respecteert”.<sup>56</sup> Hoewel het Hof in zijn arrest dus vrij uitgebreid ingaat op hoe het nieuwe grondrecht op “vertrouwelijkheid en integriteit van informatietechnologische systemen” zich onderscheidt van aanpalende grondrechten en wat de noodzaak van dit specifieke recht is, heeft de literatuur desalniettemin geoordeeld dat – hoe moedig en vooruitstrevend het oordeel op zich ook is – de argumenten van het Hof soms te wensen overlaten qua logica en coherentie.<sup>57</sup> Zo schrijft één auteur dat vertrouwelijkheid en integriteit persoonlijke deugden zijn die men niet van een systeem kan verwachten.<sup>58</sup> Het recht zou daarmee een onpersoonlijk en techniek georiënteerd grondrecht zijn:<sup>59</sup> wanneer men uit het oog zou verliezen dat dit recht begrepen moet worden in het licht van het algemene persoonlijkheidsrecht – waaruit het afgeleid is – kan het lijken alsof het recht louter een lijstje technologische vereisten stelt aan een bepaald informatieel medium. Ook was niet iedereen overtuigd dat de bestaande grondrechten tekortschoten.<sup>60</sup>

De waarde van het nieuwe grondrecht kan het beste worden beoordeeld op grond van een nadere analyse van zijn drie bestanddelen:

(1) *Vertrouwelijkheid*. Het Hof beschrijft vertrouwelijkheid als “het belang van de gebruiker dat de door een [...] systeem geproduceerde, verwerkte en opgeslagen gegevens vertrouwelijk blijven” (paragraaf 204). In zekere zin is hier weinig nieuws onder de zon<sup>61</sup> en lijkt de notie van “vertrouwelijkheid” vrij nauw aan te sluiten bij klassieke privacy principes en het recht op “informatiele zelfbeschikking”. Het *systeem*

<sup>55</sup> “Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus” (paragraaf 200, *Online Durchsuchung*, Bundesverfassungsgerichtshof 27 februari 2008).

<sup>56</sup> “Aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, folgt ein grundrechtlich erhebliches Schutzbedürfnis. Der Einzelne ist darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet” (paragraaf 181, *Online Durchsuchung*, Bundesverfassungsgerichtshof 27 februari 2008).

<sup>57</sup> Zie o.a.: T. Hoeren, “Was ist das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme?”, *Multimedia und Recht* 2008, nr. 6, pp. 365-366; Böckenförde (2008), p. 925.

<sup>58</sup> T. Hoeren (2008), p. 365.

<sup>59</sup> M. Eifert, “Informationelle Selbstbestimmung im Internet”, *Neue Zeitschrift für Verwaltungsrecht* 2008, pp. 521-522. Anders: Hoffmann-Riem (2008), p. 1012, voetnoot 34.

<sup>60</sup> Hoffmann-Riem (2008), p. 1015.

<sup>61</sup> Cf. G. Hornung, “Ein neues Grundrecht”, *Computer und Recht* 2008, p. 303.

zelf blijft hier louter het “vehikel van zowel de subjectieve als de individuele persoonlijkheidsontplooiing van de drager van het grondrecht”.<sup>62</sup> Aan de andere kant zou een achterliggende gedachte achter de notie van “vertrouwelijkheid” wellicht wel kunnen wijzen op een aandachtsverschuiving in de zin dat het geopponeerd kan worden aan individuele autonomie. Door naast het recht op informationele zelfbeschikking, dat het individu het recht geeft om zelf te beschikken over prijsgeving en gebruik van zijn persoonlijke data (paragraaf 198), ook een recht te formuleren op de vertrouwelijkheid van een systeem, worden de “verwachtingen ten opzichte van de staat, om zich te bekommeren om de betrouwbaarheid van informatie technologie, omhoog geschroefd”.<sup>63</sup> Het vertrouwelijk blijven van opgeslagen gegevens hangt immers ook samen met een vertrouwen van de gebruiker in het functioneren van zijn informatietechnische systeem – een vertrouwen dat daarmee verder gaat dan een vertrouwen in de mogelijkheid van een autonome beslissing over het gebruik van eigen data.<sup>64</sup> Nog duidelijker speelt dit bij het volgende element van het grondrecht:

(2) *Integriteit*. Integriteit wordt in het *Online-Durchsuchung* arrest slechts indirect beschreven: “Een inbreuk op dit grondrecht is bovendien dan aan te nemen, wanneer de integriteit van het beschermde informatietechnische systeem aangetast wordt, doordat er dusdanige toegang tot een systeem wordt verkregen (*zugegriffen*), dat diens prestaties, functies en opgeslagen bestanden door derden gebruikt kunnen worden; dan is de beslissende technische horde voor bespieding, observatie of manipulatie van het systeem genomen” (paragraaf 204). Interessant is dat de focus hier niet langer ligt op de bescherming van data *binnen* een systeem, maar op de bescherming van het *systeem zelf*.<sup>65</sup> Daarmee is de “integriteit” van een systeem op te vatten als een “verding-lijking” van het recht ten opzichte van bijvoorbeeld het grondrecht op informationele zelfbeschikking: “net zoals in art. 13 GG zou dan aan een zaak worden aangeknoopt (in het geval van art. 13 GG is dat de woning, in dit geval is dit het informatietechnische systeem)”.<sup>66</sup>

(3) *Informatietechnische systemen*. De informatietechnische systemen beschermd door het nieuwe grondrecht omvatten alle systemen die “op zich of in hun technische verbondenheid persoonlijke gegevens kunnen bevatten van de betreffende persoon met een reikwijdte en omvang die het mogelijk maken dat toegang tot het systeem een inzicht kan verschaffen in een wezenlijk deel van de levenswandel van die persoon, of zelfs een grondig beeld kan schetsen van diens persoonlijkheid” (paragraaf 203). Vereiste is daarbij wel dat ze over een grote functionele capaciteit beschikken en op verschillende wijzen persoonlijke gegevens kunnen opslaan. Op deze wijze zou bijvoorbeeld de ene mobiele telefoon wel onder de noemer “informatietechnologisch systeem” kunnen vallen, terwijl een andere eenvoudigere mobiele telefoon die niet aan de laatstgenoemde vereisten voldoet buiten de categorie zou vallen (paragraaf 203). Aangetekend moet worden dat er nog veel onduidelijkheden zijn over het begrip systeem.<sup>67</sup> Een van de struikelpunten is het afgrenzen waar een systeem begint en eindigt, vooral wanneer het gaat om een systeem op een externe server, een *thin client*<sup>68</sup>, een USB-stick die

---

<sup>62</sup> Böckenförde (2008), p. 928.

<sup>63</sup> Böckenförde (2008), p. 938.

<sup>64</sup> Hoffmann-Riem (2008), pp. 1012-1013.

<sup>65</sup> Böckenförde (2008), p. 928.

<sup>66</sup> Hornung (2008), p. 302.

<sup>67</sup> Zie bijv. Böckenförde (2008), p. 929; Hornung 2008, p. 303; Hoeren (2008), p. 366; Hoffmann-Riem (2008), p. 1012.

<sup>68</sup> Een ‘uitgekleed’ apparaat of programma waarbij een groot deel van de dataverwerking plaatsvindt op een externe server.

aangesloten wordt op een computer in een internet-café, een losse DVD die in een DVD-drive wordt gestoken, etc. Een ander conceptueel lastig punt is dat het moet gaan om een systeem dat de betrokkene “als zijn eigen” (paragraaf 206) gebruikt. Vallen daaronder ook IT-systemen op de werkplek en door hackers overgenomen computers?<sup>69</sup> En hoe zit dat als in de toekomst *cloud computing* alomvattend wordt of wanneer door middel van RFID-chips een vrijwel grenzenloos *Internet der Dingen* of een *Ubiquitous Computing*-omgeving tot stand gebracht wordt?<sup>70</sup>

Wat is nu de betekenis van het *Online-Durchsuchung* arrest en het daarin geformuleerde nieuwe grondrecht bovenop de al bestaande grondrechten? De meest voor de hand liggende bespiegelingen betreffen natuurlijk de vraag hoe het recht op “vertrouwelijkheid en integriteit van informatietechnologische systemen” verder uitwerking zal vinden binnen het strafrecht.<sup>71</sup> Er is nog veel onduidelijkheid over de reikwijdte en de exacte betekenis van het grondrecht.<sup>72</sup> Het is ook nog maar af te wachten hoe het nieuwe recht zich zal gaan verhouden tot klassiekere rechten zoals het huisrecht (art. 13 GG), het recht op telecommunicatiegeheim (art. 10 GG) of het recht op “informatieel zelfbeschikking”.<sup>73</sup> Maar zulks neemt niet weg dat vrij algemeen aangenomen wordt dat het recht een juridische mijlpaal is binnen het gebied van ICT en dat het een waardevolle aanvulling zal vormen op de bestaande grondrechten. Hoewel het grondrecht ‘geboren’ is binnen de context van het strafrecht, zou het door het principe van de derdenwerking naast verticale ook horizontale effecten kunnen bewerkstelligen en op deze wijze ook voor het dataproctierecht, het mededingingsrecht, het consumentenrecht en bij de uitleg van normen in het burgerlijk recht een rol kunnen spelen.<sup>74</sup> Wat geldt voor “*Bundestrojaner*” en overheids-*spyware*, zal dan ook de ‘klassieke’ *spyware* met commerciële en criminele doeleinden niet onberoerd laten. Op een nog meer fundamenteel niveau zou men zich kunnen afvragen of dit grondrecht er toe zal leiden dat naast de natuurlijke en de rechtspersoonlijkheid ook een ‘digitale’ persoonlijkheid erkend zal worden,<sup>75</sup> en of naast de ‘gewone’ private sfeer ook een ‘elektronische private sfeer’<sup>76</sup> bescherming zal vinden.

### ***Legitieme beperkingen van het nieuwe grondrecht***

Zoals de meeste andere grondrechten is ook de bescherming door het nieuwe recht “op de vertrouwelijkheid en integriteit van informatietechnologische systemen” niet absoluut. De vaststelling van het *BVerfG* dat online doorzoeken een inbreuk kunnen vormen op dit nieuwe grondrecht, betekent daarom nog niet dat de online doorzoeken zoals toegestaan in de Noordrijn-Westfaalse wet ook *per se ongrondwettige* inbreuken zijn. Het tweede aspect dat het Hof daarom moest onderzoeken was of de door de Noordrijn-Westfaalse wet toegestane inbreuken op het nieuwe IT-grondrecht binnen de

<sup>69</sup> Hoeren (2008), p. 366.

<sup>70</sup> Hornung (2008), p. 302; Hoffmann-Riem (2008), p. 1011.

<sup>71</sup> Zie bijv. Hornung (2008), pp. 305-306.

<sup>72</sup> Hoeren (2008), pp. 365-366.

<sup>73</sup> Zie voor eventuele overlapping tussen het nieuwe IT-recht enerzijds en het huisrecht en recht op telecommunicatiegeheim anderzijds: Hoffmann-Riem (2008), pp. 1021-1022.

<sup>74</sup> Zie uitgebreid: A. Roßnagel & C. Schnabel, “Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht”, *Neue Juristische Wochenschrift* 2008, vol. 61, nr. 49, pp. 3534-3538.

<sup>75</sup> W. Schulz, “Protecting the digital personhood. German constitutional Law”. Presentatie op de *ITechLaw 2008 European Conference*, Barcelona, 7 november 2008.

<sup>76</sup> Böckenförde (2008), p. 939.

grondwettelijke grenzen op inbreuken (*Schranken-Schranken*) vielen. In zijn beslissing komt het Hof tot de conclusie dat dit niet het geval is. Ten eerste is de wet niet in overeenstemming is met het *Gebot der Normenklarheit und Normenbestimmtheit* (paragrafen 208-217), omdat de omstandigheden waaronder inbreuken mogelijk zijn louter met een veel te vage verwijzing naar art. 10 GG (*telecommunicatiegeheim*) worden beschreven: de Noordrijn-Westfaalse wetgever heeft blijkbaar rekening gehouden met de mogelijkheid dat de nieuwe wet een inbreuk zou kunnen vormen op dit grondrecht maar werkt dit niet verder uit. Verder biedt de Noordrijn-Westfaalse wet geen garantie dat de *Grundsatz der Verhältnismäßigkeit* in acht wordt genomen (paragrafen 218-256) aangezien de wet geen clausule bevat die het gebruik van online-doorzoekingen beperkt tot die uitzonderlijke omstandigheden waarin een dergelijke inbreuk proportioneel is. Tot slot bevat de wet ook geen toereikende waarborgen die ervoor zorgen dat het kernbereik van de private inrichting van het eigen leven (*Kernbereich privater Lebensgestaltung*) zoveel mogelijk onaangetast blijft (paragrafen 270-285). Hoewel het Hof stelt dat preventieve doelen of onderzoek in het kader van de strafvervolging zeer zeker inbreuken op het nieuwe IT-recht zouden kunnen rechtvaardigen (paragraaf 207), mag dit alleen onder zeer uitzonderlijke omstandigheden gebeuren. Een eerste voorwaarde voor een inbreuk is de toestemming van een rechter (m.n. paragraaf 257 en 269) of een gelijkwaardige “onafhankelijke en neutrale instantie” (paragraaf 258). Daarnaast moeten er voldoende waarborgen zijn die het absoluut beschermde kernbereik van de private leefwijze, zoals mededelingen over innige gevoelens en diepgaande relaties, beschermen (m.n. paragraaf 273 en 277). Deze bescherming moet technische maatregelen omvatten die tot doel hebben het verzamelen van gegevens over dit kerngebied te vermijden. Het Hof vervolgt: “Indien er concrete indicaties zijn dat in een specifiek geval een bepaalde maatregel voor het verzamelen van gegevens inbreuk zal maken op de kern van het privéleven, dan mag deze principieel niet toegepast worden” (paragraaf 281). Indien gegevens van dit kerngebied per ongeluk toch worden verzameld, dan moeten deze onmiddellijk worden gewist en kunnen ze onder geen beding worden doorgestuurd of gebruikt (paragraaf 283). Bovendien is een inbreuk op de vertrouwelijkheid en integriteit van IT-systemen alleen toelaatbaar als er sprake is van “feitelijke aanwijzingen” van een “concreet gevaar”, waarbij het met name gaat om de bedreiging van “het lichamenlijk welzijn (lijf), leven en de vrijheid van personen”, of van maatschappelijke goederen waarop de grondvesten van de staat of het menselijk bestaan berusten (paragraaf 247). Het is daarbij echter niet vereist dat er een hoge mate van waarschijnlijkheid is dat dit gevaar zich in de nabije toekomst zal manifesteren (paragraaf 251). Al met al bieden al deze *Schranken-Schranken* een heldere richtlijn om te bepalen of een inbreuk op het nieuwe IT-recht al dan niet grondwettelijk gerechtvaardigd is. Het staat daarbij als een paal boven water dat het *BVerfG* het grondwettelijk ontoelaatbaar acht om online doorzoekingen in te zetten op grond van te vage wetgeving en voor routine onderzoeken in de sfeer van het strafrecht of het inlichtingenwerk. Niet duidelijk is hoe het Hof zal oordelen over de inzet van deze bevoegdheid in gewone strafrechtelijke onderzoeken met betrekking tot gemene misdrijven. We beklemtonen dat in het arrest verduidelijkt wordt dat Online Durchsuchung alleen ingezet mag worden bij terroristische dreiging. De huidige Duitse Minister van Justitie wil voor de opsporing van gemene misdrijven een beperkte vorm van Online Durchsuchung mogelijk maken (niet complete harde schijven uitlezen, maar ‘alleen’ Skype gesprekken van de harde schijf).

### 3. De relatie met overige rechtspraak inzake surveillance technologie

Interessant is dat de rechterlijke overwegingen rond de *Schranken-Schranken* van het nieuwe IT-grondrecht nauw aansluiten bij een reeks andere recente uitspraken van het *BVerfG*. Deze recente uitspraken betreffen telkens de grondwettelijke toelaatbaarheid van bepaalde surveillancetechnologieën die ofwel bijzonder ingrijpend zijn (bijv. het afluisteren van iemands private woonruimte<sup>77</sup>) ofwel uitzonderlijk grootschalig zijn (bijv. het geautomatiseerd scannen en natrekken van kentekens,<sup>78</sup> het massaal en langdurig opslaan van verkeersgegevens rond e-communicatie<sup>79</sup> en het systematisch doorzoeken van gegevensbestanden op bepaalde ‘verdachte’ of ‘risicovolle’ profielen<sup>80</sup>). Aan technologie met een buitengewoon uitgestrekte reikwijdte stelt het Hof paal en perk door proportionaliteits- en legaliteitsafwegingen in het geweer te brengen. Wanneer het gaat om hele intrusieve technologie speelt bovendien, naast het toetsen van de proportionaliteit en legaliteit, ook de bepaling van het kernbereik van de private inrichting van het eigen leven (*Kernbereich privater Lebensgestaltung*) een grote rol. Binnen dit kernbereik geldt een absolute bescherming en doen zelfs proportionaliteit en legaliteit niet meer ter zake. De *Online Durchsuehung*-zaak sluit in dit opzicht dus aan bij het reeds kort besproken *Großer Lauschangriff*-arrest van 3 maart 2004 over het afluisteren van woningen op afstand. Een harde schijf van een PC is net als iemands woning een gebied waarin bijzonder gevoelige informatie kan worden verkregen. In *Online Durchsuehung* maakt de rechter dan ook duidelijk dat een online doorzoeking toegang kan bieden tot een “potentiell äußerst großen und aussagekräftigen Datenbestand” (paragraaf 200) en dat het op afstand uitlezen van harde schijven daarom als een “Grundrechtseingriff von besonders hoher Intensität” (paragraaf 237) beschouwd moet worden.

Lang niet elke moderne surveillance technologie is zo intrusief. Zo deed het Hof een luttele twee weken na *Online-Durchsuehung*, op 11 maart 2008, twee uitspraken met betrekking tot grootschalig inzetbare surveillancetechnologie waarin alleen de proportionaliteit en legaliteit van de inbreuken aan de orde zijn en niet het kernbereik van de private levenswijze. In de eerste plaats wees Duitslands hoogste constitutionele Hof een arrest dat grenzen stelt aan het op grote schaal geautomatiseerd scannen en natrekken van nummerplaten.<sup>81</sup> Daarnaast doorkruiste het Hof in kort geding met een gedeeltelijk toegewezen voorlopige voorziening<sup>82</sup> ook de door de wetgever voorgenomen

<sup>77</sup> BVerfG 3 maart 2004, (*Großer Lauschangriff*), 1 BvR 2378/98.

<sup>78</sup> BVerfG 11 maart 2008, (*Automatisierte Erfassung von Kfz-Kennzeichen*) 1 BvR 2074/05, 1 BvR 1254/07.

<sup>79</sup> BVerfG 11 maart en 28 oktober 2008, (*Vorratsdatenspeicherung*), 1 BvR 256/08.

<sup>80</sup> BVerfG 4 april 2006, (*Rastererfassung*) 1 BvR 518/02.

<sup>81</sup> BVerfG (*Automatisierte Erfassung von Kfz-Kennzeichen*), 1 BvR 2074/05, 1 BvR 1254/07

<sup>82</sup> Omdat het definitieve vonnis in de *Vorratsdatenspeicherung*-zaak nog niet is geveld en het moeilijk te voorspellen is hoe dat oordeel zal uitvallen, zal deze zaak in dit artikel verder grotendeels buiten beschouwing gelaten worden. Het maken van voorspellingen over de uitkomst van de *Vorratsdatenspeicherung*-zaak wordt bovendien ook nog eens extra gecompliceerd door het feit dat het moeilijk te voorspellen is hoe de Duitse constitutionele rechter het recente arrest *Ierland / Europees Parlement* (HvJ EG 10 februari 2009, C-301/06) in zijn oordeel zal meewegen. In dit arrest oordeelde het Europese Hof van Justitie oordeelde dat richtlijn 2006/24/EG op de juiste rechtsgrondslag is gebaseerd en dus niet nietig is. Het Hof onderstreepte echter zelf dat zijn oordeel louter de procedurele grondslag betreft en dat geen substantiële toetsing aan fundamentele privacy-rechten heeft plaatsgevonden: “It must also be stated that the action brought by Ireland relates solely to the choice of legal basis and not to any possible infringement of fundamental rights arising from interference with the exercise of the right to privacy contained in Directive 2006/24”. (paragraaf 57) Digital Rights Ireland zat daarom niet bij de pakken neer en diende onmiddellijk een verzoekschrift in bij de *High Court* – de constitutionele rechter van Ierland – om het HvJ EG zich te laten uitspreken over de richtlijn op substantiële gronden (zie o.a.

implementatie van de Europese Dataretentierichtlijn 2006/24/EG.<sup>83</sup> In beide zaken wijst de rechter op de gevaren die schuilen in de grootschaligheid van de surveillance. In het kort geding met betrekking tot de Dataretentierichtlijn wees de rechter bijvoorbeeld op de mogelijkheid dat het langdurig bewaren van eenieders telecommunicatiegegevens “de onbevangenheid van de communicatiewisseling en het vertrouwen in de bescherming van de ontoegankelijkheid van telecommunicatiesystemen” (paragraaf 155) wel eens diepgaand zou kunnen aantasten. In het arrest rond het geautomatiseerd scannen van nummerplaten werkt de rechter bovendien nauwkeurig uit onder welke voorwaarden deze grondwettelijke inbreuk op het recht op informatiele zelfbeschikking desalniettemin grondwettelijk toelaatbaar is: één van de voorwaarden die de rechter stelt is dat wettelijk vastgelegd moet worden dat de gescande nummerplaten onmiddellijk nagetrokken worden en dat alle nummerplaten waar niks aan schort direct uit het surveillancesysteem verwijderd worden. Soortgelijke overwegingen speelden ook al een rol in het *Data Profiling*-arrest.<sup>84</sup> Ook hier maakte het Hof duidelijk dat het systematisch screenen en vergelijken van databestanden op profielen van potentiële criminelen niet als een ongebreideld visnet ingezet mag worden. Het Hof oordeelde het gebruik van de *Rasterfahndung*-methode dan ook alleen grondwettelijk toelaatbaar bij een concreet gevaar voor een zeer belangrijk rechtsgoed. In alle andere gevallen moet deze methode beschouwd worden als een ongrondwettelijke inbreuk op het recht op informatiele zelfbeschikking.

Concluderend kan men stellen dat één van de aspecten die de recente arresten zoals *Online Durchsuchung*, *Rasterfahndung*, *Großer Lauschangriff* of *Automatisierte Erfassung von Kfz-Kennzeichen* zo interessant maakt vervat ligt in het feit dat ze constitutionele bescherming combineren met het uitstippelen van een concrete richtlijn voor toelaatbare inbreuken. Het Hof stelt in elk van deze arresten dat bepaalde politiediensten gebruik zouden moeten kunnen maken van nieuwe technologische monitor- en opsporingsmethoden<sup>85</sup>, maar maakt eveneens keer op keer duidelijk dat dit mag niet ontaarden in bestuursrechtelijk, ongerichte, grenzeloze of disproportionele surveillance. De rechter geeft de wetgever hiermee een heldere richtlijn.<sup>86</sup> Zo is daarom

---

<http://www.digitalrights.ie/category/mass-surveillance/> en [http://www.theregister.co.uk/2009/02/11/data\\_retention/](http://www.theregister.co.uk/2009/02/11/data_retention/)). De verwijzing naar de mogelijkheid om het HvJ EG zich te laten uitspreken over de verenigbaarheid van richtlijn 2006/24/EG is ook in Duitsland niet ongemerkt voorbijgegaan. Onder verwijzing naar het arrest *Ierland / Europees Parlement* heeft de Duitse administratieve rechtbank van Wiesbaden (Besluit van 27 februari 2009, dossiernummer 6 K 1045/08.WI ) zich onlangs tot het HvJ EG gewend met de prejudiciële vraag of de Dataretentierichtlijn niet strijdig is met de uit art. 8 EVRM lid 2 voortvloeiende proportionaliteitsdoets [zie met name paragraaf 29 en 30; volledige tekst beschikbaar op: <http://www.vorratsdatenspeicherung.de/content/view/301/1/lang.de/>]: “De rechtbank is van mening dat dataretentie een inbreuk vormt op het grondrecht op privacy. In een democratische samenleving is zij [dataretentie] niet noodzakelijk” (“Das Gericht sieht in der Datenspeicherung auf Vorrat einen Verstoß gegen das Grundrecht auf Datenschutz. Sie ist in einer demokratischen Gesellschaft nicht notwendig”, paragraaf 29). Alles wijst er daarmee op dat het niet lang meer kan duren voor het HvJ EG zich ook op materiële gronden over de Richtlijn zal moeten uitspreken. In Nederland ligt het wetsvoorstel ter implementatie van richtlijn 2006/24/EG op het moment bij de Eerste Kamer (Wetsvoorstel 31.145, *Wet Bewaarplicht Telecommunicatiegegevens*). Zie voor de Nederlandse situatie met betrekking tot het bewaren van telecommunicatiegegevens o.a.: M.G.W. den Boer, H. Bosma, C. de Graaf, A.A.M. Horrevorts, J.N. van Lunteren & W.J.B.M. Stolwijk, *Data voor Daadkracht* (rapport Adviescommissie Informatiestromen Veiligheid), 2007, [www.bzk.nl/aspx/download.aspx?file=/contents/pages/89605/datavoordaadkracht.pdf](http://www.bzk.nl/aspx/download.aspx?file=/contents/pages/89605/datavoordaadkracht.pdf); A.H.Vedder, L. Van Der Wees, B.-J., Koops & P. De Hert, *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw*, Den Haag: Rathenau Instituut, 2007.

<sup>83</sup> BVerfG, (*Vorratsdatenspeicherung*) 1 BvR 256/08; uitspraak hernieuwd op 28 oktober 2008.

<sup>84</sup> BVerfG 4 april 2006, (*Rasterfahndung*) 1 BvR 518/02

<sup>85</sup> Zoals o.a. het online doorzoeken van harde schijven van PC's, het opvragen van over een langere periode opgeslagen verkeersgegevens met betrekking tot e-communicatie (bezoekte webadressen, wie heeft wanneer met wie gebeld of e-mails uitgewisseld, etc.) en het systematisch scannen en natrekken van kentekenplaten.

<sup>86</sup> Zie bijv. voor de effecten op de wetgeving in de deelstaat Beieren en de BKA-wet op federaal niveau: Böckenförde (2008), pp. 932-935.

onjuist om het *Online-Durchsuchung* arrest alleen maar te zien als een constitutionele berisping aan het adres van de wetgever in Noordrijn-Westfalen: eerder is het een vorm van ‘opbouwende kritiek’ die de wetgever een constitutionele leidraad kan bieden bij de formulering van wetgeving rond online doorzoekingen<sup>87</sup>. Toen de federale wetgever in de tweede helft van 2008 de online doorzoekings-bevoegdheden van het *Bundeskriminalamt* probeerde vast te leggen in de eerder genoemde BKA-wet (zie hierboven, sub 1), vormde het oordeel van het *BVerfG* over de grondwettigheid van de Noordrijn-Westfaalse *Online Durchsuchung*-wet een handige richtlijn waarmee de federale wetgever in principe de eerdere fouten van de Noordrijn-Westfaalse wetgever zou kunnen vermijden. Voorstanders van de nieuwe BKA-wet beschouwen deze als een perfecte beantwoording aan de beperkingen zoals opgelegd door het *Bundesverfassungsgericht*. Criticasters wijzen er echter op dat in het federale wetgevingsproces het *Online Durchsuchung* arrest vaak slechts voor de schone schijn aangehaald werd en dat de BKA-wet *de facto* als een grove negering van het oordeel van het *BVerfG* beschouwd moest worden. Nu Bettina Winseman op 27 januari 2009 opnieuw een *Verfassungsbeschwerde* heeft ingediend (zie hierboven, sub 1) tegen de federale BKA-wet<sup>88</sup> is het afwachten op het oordeel van de rechter in *Online Durchsuchung-II*: pas dan zal duidelijk worden in hoeverre het Hof de nieuwe BKA-wet in overeenstemming acht met zijn oordeel van 27 februari 2008.

#### 4. De betekenis van *Online Durchsuchung* buiten Duitsland

De politiediensten in Duitsland zijn niet de enige die de computer van een potentiële terrorist stiekem willen uitlezen. Zo verklaarde Glenn Audenaert, directeur van de Belgische federale gerechtelijke politie, dat hij graag een wetswijziging zou zien die het de politie toe zou staan om wettelijk computers te kunnen hacken.<sup>89</sup> Rond diezelfde periode stelde de Nederlandse Raad van Hoofdcommissarissen dat de Nederlandse politie op zoek naar belastend materiaal geregeld gebruik maakt van Trojaanse paarden om in te breken computers van verdachten.<sup>90</sup> In de herfst van 2008 bespraken de Amerikaanse minister van Buitenlandse Zaken en de ministers van Binnenlandse Zaken van de zes grootste EU-lidstaten (Frankrijk, Duitsland, Spanje, Italië, Polen en het Verenigd Koninkrijk) de mogelijkheden om tot een geharmoniseerde wetgeving te komen met betrekking tot de bevoegdheden van de recherche om harde schijven op afstand uit te lezen.<sup>91</sup> Op 27 november 2008 werd door de Raad van de EU het beleid op het gebied

<sup>87</sup> In juni 2008 presenteerde de oppositiefractie *Bündnis 90/Die Grünen* zelfs een wetsontwerp (BT-Drs. 16/9607, elektronisch beschikbaar op: <http://dip21.bundestag.de/dip21/btd/16/096/1609607.pdf>) waarin wordt voorgesteld om het nieuwe recht op de vertrouwelijkheid en integriteit van IT-systemen expliciet in het *Grundgesetz* op te nemen. Zie ook: M. Klopfer & F. Schärdel, “Grundrechte für die Informationsgesellschaft - Datenschutz und Informationszugangsfreiheit ins Grundgesetz?”, *JuristenZeitung* 2009, vol. 64, nr. 9, pp. 453-462.

<sup>88</sup> Ook tegen een soortgelijke *Online Durchsuchung*-wet in de deelstaat Beieren is inmiddels een *Verfassungsbeschwerde* ingediend door de *SPD*: [http://bayernspd.de/workspace/uploads/pdfs/VB\\_final\\_Schriftsatzvom18.9.2008\\_o.U.\\_o.A..pdf](http://bayernspd.de/workspace/uploads/pdfs/VB_final_Schriftsatzvom18.9.2008_o.U._o.A..pdf)

<sup>89</sup> “Federale politie wil computers van terroristen kraken”, *Het Laatste Nieuws*, 27 juni 2008.

<sup>90</sup> M. Proos, “Justitie enthousiast over hacken computers”, *BN De Stem*, 17 mei 2008, <http://www.bndestem.nl/algemeen/binnenland/3134803/Justitie-enthousiast-over-hacken-computers.ece>. Onduidelijk is in hoeverre dit wettelijk toelaatbaar is omdat een expliciete wettelijke bepaling hieromtrent vooralsnog ontbreekt. Het is wachten op een zaak waarin de rechter zich moet buigen over de wettelijke toelaatbaarheid van bewijs dat verkregen is door het op afstand uitlezen van een harde schijf. Merken we op dat de *Wet op de inlichtingen- en Veiligheidsdiensten 2002* (Wiv) een wettelijke basis geeft aan de AIVD om computers van verdachten te hacken (“het al dan niet met gebruikmaking van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheid, binnendringen in een geautomatiseerd werk”, art. 24 lid 1 Wiv).

<sup>91</sup> Naast nationale *remote searches* wordt ook gepleit voor transnationale doorzoekingen op afstand aan om bijvoorbeeld de Nederlandse politie toe te laten op afstand een Spaanse harde schijf uit te lezen: “De Ministers van Binnenlandse Zaken maken duidelijk dat bijna alle partnerlanden nationale wetgeving hebben of hieraan werken, die het toestaat om harde schijven en andere opslagmedia binnen de landsgrenzen te doorzoeken. Het juridische raamwerk met betrekking tot transnationale doorzoekingen van dit soort apparaten is nog niet goed ontwikkeld. De Ministers van Binnenlandse Zaken zullen daarom manieren zoeken om de problemen

van cybercriminaliteitsbestrijding vastgesteld voor de komende vijf jaar, waarin er sprake is van een expliciete aanmoediging van politiediensten om *remote searches* in te zetten.<sup>92</sup> Op 4 januari 2009 lekte uit dat in het Verenigd Koninkrijk zulke *remote searches* al vrij frequent door de politie ingezet worden en dat het ministerie van Binnenlandse Zaken vooruitlopend op het door de Raad uitgestippelde beleid alvast de bevoegdheid verleend aan rechteerteams en MI5 om ook zonder rechterlijk bevel computers van afstand te doorzoeken (*remote searching*).<sup>93</sup> De officiële lezing van het Home Office is dat de *Regulation of Investigatory Powers Act 2000* en de *Computer Misuse Act 1990* aan politiediensten reeds een dergelijke bevoegdheid verschaffen waardoor er eigenlijk niets nieuws onder de zon is. Vijf dagen na het uitgelekte beleid in het Verenigd Koninkrijk verklaarde ook de Belgische Minister van Justitie Stefaan De Clerck dat de regering de *Wet op de Bijzondere Opsporingsmethodes* (BOM) zo wil aanpassen dat de politie voortaan computers zal mogen hacken of afluisteren met keylogs<sup>94</sup> – hoewel het nog maar afwachten is of deze wetuitbreiding goedgekeurd zal worden.

Met de toenemende wetgevende activiteit met betrekking tot het verlenen van bevoegdheden aan politie- en veiligheidsdiensten om op afstand harde schijven uit te kunnen lezen wordt het ook steeds waarschijnlijker dat binnenkort een nationale rechter, het Europese Hof van Justitie of het Hof in Straatsburg zich over een *Online Durchsuchung*-achtige zaak uit zal moeten spreken. De jurist die geconfronteerd wordt met een dergelijke zaak zal zeker baat hebben bij bestudering van het Duitse grondwetssysteem, de Duitse rechtspraak in verband met *remote searches*, *datamining* en afluisteren op afstand. Hoewel deze Duitse elementen niet zomaar getransponeerd kunnen worden naar de jurisdicties van andere lidstaten of naar een Europees niveau – onder andere vanwege het zeer bijzondere Duitse grondwettelijke recht en de specifieke culturele spanningsvelden tussen privacy en veiligheid binnen de Bondsrepubliek – valt er toch veel van te leren.

Ten eerste is er het belang van het nieuwe grondrecht op de vertrouwelijkheid en integriteit van IT-systemen. Ook rechters buiten Duitsland<sup>95</sup> zouden wel eens kunnen meegaan in de redenering van hun Duitse collegae dat de klassieke grondrechten tekortschieten ten opzichte van de gevaren van de huidige informatietechnische systemen. Zoals blijkt uit het Duitse voorbeeld brengt de formulering van een nieuw grondrecht echter ook veel onduidelijkheid met zich mee. De Duitse rechter heeft een moedige aanzet gedaan. Door de lof en kritiek uit de Duitse juridische literatuur is duidelijk geworden waar een toekomstige rechter of wetgever – of het nu binnen of buiten de Duitse context is – mogelijkerwijs nog meer helderheid zal moeten scheppen.

---

op te lossen en het proces in de toekomst te versnellen” (paragraaf IV, 13). Zie voor het officiële verlag van het Anti-Terrorisme Symposium van de G6 en de VS (Bonn, Villa Hammerschmidt, 26.–27.09.2008): <http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2008/09/Conclusions.templateId=raw.pr.operty=publicationFile.pdf/Conclusions.pdf>

<sup>92</sup> Doc. 15569/08, 11 november 2008, *Draft Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime*: <http://register.consilium.europa.eu/pdf/en/08/st15/st15569.en08.pdf>; “Fight against cyber crime: cyber patrols and Internet investigation teams to reinforce the EU strategy”, IP/08/1827, persbericht *Rapid*, Brussel 27 november 2008, <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827>

<sup>93</sup> Zie o.a.: N. Morris, “New powers for police to hack your PC. Civil liberties groups raise alarm over extension of surveillance without warrant”, *The Independent*, 5 januari 2009, <http://www.independent.co.uk/news/uk/home-news/new-powers-for-police-to-hack-your-pc-1225802.html>

<sup>94</sup> “Als het van de regering afhangt, mag de politie straks informaticasystemen hacken”, *De Morgen*, 9 januari 2009.

<sup>95</sup> De invloed van de rechtspraak van het *Bundesverfassungsgericht* reikt over de Duitse grens. Zie bijv: “Germany’s Constitutional Court. Judgment days”, *The Economist*, 26 maart 2009.

Daarbij valt onder andere te denken aan de reikwijdte van wat een “als eigen” gebruikt informatietechnologisch systeem is, een nadere invulling van het begrip “systeem”, de verhouding ten opzichte van andere grondrechten, de eventuele horizontale werking van een dergelijk grondrecht, etc. Daarnaast zou bijvoorbeeld ook onderzocht kunnen worden in hoeverre (bij gebrek aan algemeen persoonlijkheidsrecht) art. 8 EVRM eventueel als een aanknopingspunt zou kunnen dienen voor een vergelijkbare bescherming als degene die door het nieuwe Duitse IT-grondrecht wordt verleend.

Ten tweede vormt ook de Duitse *Schranken-Schranken*-systematiek met betrekking tot intrusieve en grootschalige surveillancetechnologie een inspiratiebron. Het komt ons voor dat de Europese grondrechten-beperkingsystematiek wat mager uitvalt, zeker in vergelijking met het Duitse systeem.<sup>96</sup> Duitse rechters hebben de mantra over de nood aan proportionaliteit en het verbod op overmaat op een hoger niveau doorontwikkeld. Het feit dat ook binnen het Duitse recht vaak blijkt dat absolute bescherming een praktische onmogelijkheid is, is dan ook zeker geen reden om te kniesoren: de naar absolute aspirerende proportionele bescherming en de met proportionaliteit verluchtigde absolute bescherming staan in een verfrissend contrast tot de vaak weinig om het lijf hebbende proportionaliteitstoetsen in andere lidstaten. Hoewel het wat inspanning kost om inzicht te krijgen in de nuances van de Duitse proportionaliteitssystematiek is er in ieder geval geen sprake van een flauwe proportionaliteitstoets die er in de praktijk op neer komt dat alle technologische opsporingsmethoden grondrechtenconform worden verklaard. Door het hanteren van een ernstige proportionaliteitstoets geven de Duitse rechters het signaal mee te willen spreken in het debat over nieuwe opsporingstechnieken.<sup>97</sup> Via een doorgedreven legaliteitstoets heeft het Europees Hof van de Rechten van de Mens in het op 1 juli 2008 gewezen *Liberty*-arrest een hoopvolle aanwijzing gegeven ook mee te willen spelen bij de beoordeling van dit soort technologie.<sup>98</sup> Wie de juridische details even laat voor wat ze zijn, kan in het *Liberty* arrest parallellen zien met de benadering van het *BVerfG* in *Online Durchsuchung*.<sup>99</sup>

Waar het binnen de Duitse grenzen afwachten is wat *Online Durchsuchung-II* zal brengen, kan ondertussen buiten de Duitse grenzen het eerste *Online Durchsuchung* arrest alvast als een grote inspiratiebron dienen.

---

<sup>96</sup> P. De Hert, “Strafrecht en privacy. Op zoek naar een tweede adem”, *Rechtshulp. Maandblad voor de sociale praktijk*, 2003/10, 41-54.

<sup>97</sup> P. De Hert, “Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11”, *Utrecht Law Review*, 2005, vol. 1, nr. 1, 68-96.

<sup>98</sup> EHRM, 1 juli 2008 (*Liberty e.a. t. Verenigd Koninkrijk*), verzoekschrift nr. 58243/00. Zie ook: P. De Hert & A. Hoefmans, ‘Rechtspraak in kort bestek. EHRM juli 2008’, *Tijdschrift voor Strafrecht*, 2008, vol. 9, nr. 5, pp. 412-416.

<sup>99</sup> In de *Liberty*-zaak ging het erom dat het Britse Ministerie van Defensie tussen 1990 en 1997 door middel van een af luister technologie (‘Electronic Test Facility’) tienduizenden telefoongesprekken, faxen en e-mails vanuit en naar Ierland had onderschept en gescreend op bepaalde verdachte woorden. Enkele burgerrechtenorganisaties (*Liberty*, *British Irish Rights Watch* en de *Irish Council for Civil Liberties*) stapten naar het Europees Hof voor de Rechten van de Mens, dat oordeelde dat het Verenigd Koninkrijk met deze grootse af luister praktijk artikel 8 EVRM geschonden had. Net als het *BVerfG* onderwerpt het Straatsburg Hof de wet die de grondslag vormde voor de inzet van deze surveillancetechnologie aan een genuanceerde constitutionele toetsing en het concludeert unaniem dat de wettelijke grondslag voor de inbreuk op de rechten van de verzoekers niet overeenkomstig was met de drie voorwaarden van artikel 8 lid 2 EVRM (voorzien bij wet, nastreven van legitieme redenen en noodzakelijkheid in een democratische samenleving). Ook hier maakt de rechter korte metten met onheldere formuleringen en democratisch oncontroleerbare procedures.