

Tilburg University

Tijd voor een nieuw punitief sluitstuk in de WBP?

Nouwt, J.

Published in:
Privacy & Informatie

Publication date:
2005

[Link to publication in Tilburg University Research Portal](#)

Citation for published version (APA):
Nouwt, J. (2005). Tijd voor een nieuw punitief sluitstuk in de WBP? *Privacy & Informatie*, 8(6).

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Tijd voor een nieuw punitief sluitstuk in de WBP?

Mr. J. Nouwt

[Sjaak Nouwt is werkzaam bij TILT – Centrum voor Recht, Technologie en Samenleving van de Universiteit van Tilburg en lid van de redactie van P&I]

Trefwoorden: strafrecht, bestuursrecht, WBP, misbruik, handhaving, heling

[Samenvatting]

Ervaringen uit de praktijk doen de vraag rijzen of de WBP wel altijd serieus wordt genomen. Beschikken bedrijfsleven, overheid en non-profit organisaties wel over voldoende kennis van de regels in de WBP? Staat vast dat alle meldingsplichtige verwerkingen van persoonsgegevens ook inderdaad zijn aangemeld bij het CBP? En als een verwerking is gemeld, houdt de naleving van de WBP daarmee dan op? Is het toelaatbaar dat ruim vier jaar na de inwerkingtreding van de WBP er nog altijd onrechtmatig met persoonsgegevens wordt omgegaan? Kortom: is het niet eens tijd voor uitbreiding van het strafrechtelijke sluitstuk in de WBP? Andere EU-landen gingen ons reeds voor.¹

1. Inleiding

In dit artikel wordt bepleit om bij de evaluatie van de Wet bescherming persoonsgegevens (WBP) aandacht te besteden aan de naleving en handhaving van de voorschriften voor het gebruik van persoonsgegevens. In het bijzonder zou daarbij moeten worden ingegaan op de vraag of misbruik van persoonsgegevens niet in ruimere mate strafbaar zou moeten zijn en ook vaker zou moeten worden bestraft. Vooruitblikkend op de evaluatie wordt in deze bijdrage in kort bestek gewezen op de mogelijkheden van strafrechtelijke en bestuursrechtelijke handhaving van de voorschriften in de WBP ter voorkoming van misbruik van persoonsgegevens.

Met ‘misbruik van persoonsgegevens’ wordt in feite bedoeld op het onrechtmatige gebruik van persoonsgegevens.² Voor de omschrijving van het begrip ‘gebruik’ kunnen we een onderscheid maken in de fase van het verzamelen van gegevens en die van het verder verwerken van eenmaal verzamelde gegevens. Dit verder verwerken kan uit vrijwel alle elementen bestaan, behalve ‘verzamelen’, die onder de definitie van het ‘verwerken van persoonsgegevens’ vallen. Het gaat dan in elk geval om: “(...) vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens”. Voor alle duidelijkheid zij er op gewezen dat het begrip ‘verwerken van persoonsgegevens’ in de WBP ook het verzamelen omvat.

Persoonsgegevens kunnen beschikbaar zijn gesteld door iemand die daar niet toe bevoegd is. Zo werden door een werknemer en de directeur van een handelsinformatiebureau andere personen tegen een financiële vergoeding opgedragen om veelal vertrouwelijke persoonsgegevens te verzamelen uit niet-openbare bronnen.³ Die gegevens werden op slinkse

¹ Dit artikel is geschreven naar aanleiding van een uitgebreid onderzoek van de auteur naar de vraag of vormen van gebruik van ongeautoriseerd ter beschikking gestelde bedrijfs- en persoonsgegevens strafbaar dienen te worden gesteld.

² Zie over het begrip “persoonsgegeven” in de WBP en het begrip “gegeven” in het Wetboek van Strafrecht de bijdrage van Jan Berkvens in dit nummer.

³ Rechtbank 's-Gravenhage, 29 september 2004, LJN: AR2979 en LJN: AR2973.

wijze verzameld, doordat personeelsleden en derden telefonisch andere instellingen benaderden. Zij gebruikten daarbij valse namen en gaven zich uit als collega van soortgelijke instellingen.

In gevallen als deze zijn de persoonsgegevens onrechtmatig verkregen. Het is dan logisch dat elke vorm van gebruik (verder verwerken) van deze gegevens ook onrechtmatig is.

In deze bijdrage wordt in overweging gegeven of het niet wenselijk en mogelijk is het bestaande strafrechtelijke sluitstuk in de WBP uit te breiden. Uitbreiding van het punitieve sluitstuk lijkt mogelijk via strafrechtelijke of bestuursrechtelijke handhaving.

2. Strafrechtelijke bescherming van persoonsgegevens

Het huidige Wetboek van Strafrecht biedt tot op zekere hoogte al strafrechtelijke bescherming tegen misbruik van persoonsgegevens door 'geheimen' te beschermen. Zo luidt artikel 272 WvSr (schending ambts-, beroepsgeheim) als volgt:

1. Hij die enig geheim waarvan hij weet of redelijkerwijs moet vermoeden dat hij uit hoofde van ambt, beroep of wettelijk voorschrift dan wel van vroeger ambt of beroep verplicht is het te bewaren, opzettelijk schendt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie.

2. Indien dit misdrijf tegen een bepaald persoon gepleegd is, wordt het slechts vervolgd op diens klacht.

Strafbaar is (slechts) degene die een geheim schendt dat hij uit hoofde van zijn ambt of beroep zou moeten bewaren. Tevens moet er sprake zijn van opzet. Als de schending van de geheimhoudingsplicht benadeling van een bepaalde persoon tot gevolg heeft, is de vervolging van het misdrijf uitsluitend mogelijk als die benadeelde persoon een klacht indient (lid 2).

Artikel 75 is het enige artikel in de WBP dat strafbepalingen bevat. Strafbaar is de verantwoordelijke die in strijd handelt met de artikelen 4, derde lid (geen vertegenwoordiger in Nederland aangewezen), 27, 28 (ten onrechte niet of onjuist gemeld), of 78, tweede lid, onderdeel a (verboden doorgifte naar derde land). Op overtreding staat een geldboete van de tweede categorie (ten hoogste € 2.500). Als de overtreding opzettelijk is begaan, kan een gevangenisstraf van ten hoogste zes maanden of een geldboete van de derde categorie (ten hoogste € 4.500) worden opgelegd.

Toch zou het niet vreemd zijn als de WBP op meer overtredingen, in het bijzonder overtreding van de materiële normen, een mogelijkheid tot strafvervolging zou stellen. Een vergelijking met strafbaarstellingen in de privacywetgeving van andere EU-lidstaten geeft zeker aanleiding om dat te overwegen.

In de meeste andere EU-landen is, evenals in ons land, het niet melden van een verwerking van persoonsgegevens strafbaar. Daarnaast is in een aantal landen het schenden van de geheimhoudingsplicht strafbaar (Oostenrijk, Finland, Spanje, Luxemburg), het verwerken van gevoelige gegevens (België, Denemarken, Italië, Spanje, Zweden) en het niet voldoen aan de beveiligingsplicht (Oostenrijk, België, Denemarken, Finland, Italië, Spanje, Luxemburg). Met name België en Denemarken kennen nog een groot aantal andere strafbaarstellingen voor misbruik van persoonsgegevens. In België kan bijvoorbeeld een maximale geldboete van maar liefst € 100.000 worden opgelegd als een verantwoordelijke persoonsgegevens niet eerlijk en rechtmatig verwerkt, die persoonsgegevens niet voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen heeft verkregen, die persoonsgegevens op onverenigbare wijze verder verwerkt, als de gegevens niet toereikend, ter zake dienend of juist overmatig zijn, als de gegevens niet nauwkeurig zijn, of als de gegevens in herleidbare vorm langer bewaard blijven dan noodzakelijk is voor de realisatie van het doel waarvoor ze

zijn verzameld (art. 39 Wet verwerking persoonsgegevens). Dezelfde boete kan worden opgelegd als bijzondere (gevoelige) persoonsgegevens in strijd met de wet worden verwerkt. Teneinde deze bijzondere persoonsgegevens beter te kunnen beschermen zou ook in ons land bijvoorbeeld gekozen kunnen worden voor handhaving via het strafrecht als het om misbruik van gevoelige gegevens gaat.

3. Jurisprudentie CBP

Het College bescherming persoonsgegevens (CBP) is het bestuursorgaan dat toezicht houdt op de naleving van wetgeving die het gebruik van persoonsgegevens regelt. Het CBP heeft ter handhaving daarvan de bevoegdheid om bestuurlijke boeten op te leggen en te besluiten tot het opleggen van dwangsommen en het toepassen van bestuursdwang. Deze bevoegdheden ontleent het CBP aan hoofdstuk 10 "Sancties" (artikel 65 e.v.) van de WBP.

Bestuursdwang en dwangsom kunnen in het algemeen als *situatieve sancties* worden beschouwd. Zij zijn er primair op gericht om een einde te maken aan de geconstateerde normovertreding en een situatie te bereiken die in overeenstemming is met het recht. De bestuurlijke boete daarentegen heeft meer het karakter van een *punitieve sanctie*. Kenmerken van een dergelijke sanctie zijn leedtoevoeging en vergelding. De bestuurlijke boete heeft daardoor het karakter van een strafsanctie.⁴

Veel uitspraken die op de website van het CBP zijn gepubliceerd gaan over de onrechtmatige verwerking (misbruik) van persoonsgegevens. Enkele voorbeelden daarvan zijn de volgende uitspraken:

- *Informatiehuishouding bij Het Bureau Jeugdzorg: intake teams en informatie-uitwisseling (14 januari 2002, z2001-1575);*
- *Verwerkingen persoonsgegevens teleco-aanbieder niet rechtmatig (5 juni 2002, z2001-1395);*
- *Mijn Zaken: online toegang tot handelsrol rechtbanken disproportioneel (27 februari 2003, z2002-1015);*
- *Relatiebestand Postbank en ING Bank (21 maart 2003, z2002-0881);*
- *Afschriften telefoonrekening als bewijs illegale bewoning vakantiehuisjes (7 april 2003, z2003-0369);*
- *Onrechtmatige mailing door apotheek op basis van centraal medicatiebestand (9 mei 2003, z2002-1085);*
- *Onrechtmatige verstrekking van gezondheidsgegevens door verzekeraars (15 juli 2003, z2003-0214);*
- *Onrechtmatige verificatie studentgegevens door Interpay (1 november 2004, z2004-1401).*

Het CBP brengt in bovenstaande uitspraken tot uitdrukking dat het gebruik van persoonsgegevens in de omstandigheden van deze gevallen onrechtmatig is.

Wat echter uit deze uitspraken niet volgt is wat de gevolgen zijn van het oordeel van het CBP voor de verantwoordelijke die de persoonsgegevens onrechtmatig verwerkt (misbruikt). Gaan die uitspraken wel ver genoeg of is een betere bescherming en handhaving nodig en kan de naleving van de WBP worden bevorderd door het onrechtmatige verwerken (misbruik) van persoonsgegevens strafbaar te stellen?

4. Strafrechtelijke aansprakelijkheid

⁴ Zie over deze bestuursrechtelijke handhaving H.D. van Wijk, *Hoofdstukken van bestuursrecht*. Elfde herziene druk door mr. Willem Konijnenbelt en mr. Ron van Male. Den Haag: Elsevier bedrijfsinformatie bv, 1999, p. 471-511 (nieuwste druk: 2002).

Is het strafrecht een geschikt instrument om bescherming te bieden tegen misbruik van persoonsgegevens? Onze samenleving heeft zich ontwikkeld van een nachtwakerstaat tot een veiligheidstaat. Criminaliteit is een normaal sociaal probleem dat de overheid moet zien te 'managen'. Veiligheid en normhandhaving staan hoog op de sociale en politieke agenda. Het strafrecht wordt minder 'ultimum remedium', maar krijgt steeds meer instrumentele betekenis. Het strafrecht wordt vaker toegepast als sturingsinstrument om opvattingen en gedragingen in de samenleving te beïnvloeden.

Ook burgers lijken een sterkere repressieve en instrumentele betekenis aan het strafrecht toe te kennen, zoals blijkt uit het Sociaal en Cultureel Rapport 2002 van het Sociaal Cultureel Planbureau.⁵ Van het begrippenpaar 'instrumentaliteit' en 'rechtsbescherming'⁶ lijken de bestaande opvattingen over strafrecht meer nadruk te leggen op instrumentaliteit, dat wil zeggen het strafrecht als instrument om de maatschappij te beveiligen tegen criminaliteit. Naast de instrumentele rol heeft het strafrecht tegelijkertijd de rol om burgers te beschermen tegen te grote willekeur van de overheid. Het lijkt vooral het spanningsveld tussen deze beide te zijn die bepalend is voor de vraag wanneer een gedraging strafbaar moet zijn. Het belangrijke ultimum remedium-beginsel (zie hierna) hoeft de eventuele strafbaarstelling van misbruik van persoonsgegevens niet in de weg te staan.

Strafrechtelijke aansprakelijkheid kent verschillende varianten en vloeit niet alleen voort uit het Wetboek van Strafrecht. Toezicht en handhaving van strafbare feiten hoeft ook niet altijd door het toch al overbelaste Openbaar Ministerie te gebeuren, maar is ook mogelijk door zelfstandige bestuursorganen. Bestuursorganen kunnen een bestuurlijke boete opleggen aan degenen die zich schuldig maken aan overtreding van een administratiefrechtelijk gebod of verbod. De bestuurlijke boete is een financiële punitieve sanctie met een leedtoevoegend karakter. Daardoor bestaat er een nauwe verwantschap met het strafrecht. De rechtsbescherming bestaat uit een beroep op de bestuursrechter tegen de boetebeschikking van het bestuursorgaan. Bekende voorbeelden van wetten op grond waarvan een bestuurlijke boete kan worden opgelegd zijn: Algemene wet inzake rijksbelastingen, Wet administratieve handhaving verkeersvoorschriften (Wet Mulder), de Telecommunicatiewet en de Mededingingswet. De Mededingingswet bijvoorbeeld kent bestuursrechtelijke handhaving door de NMa van voorschriften met een geringe normatieve lading, waarvan overtreding geen letsel aan personen of schade aan goederen toebrengt.⁷ Vrijheidsbeneming of andere dwangmiddelen zijn in dat verband niet nodig om de normen te kunnen handhaven. Tegelijkertijd bevat de Mededingingswet verbodsbepalingen die het beste door een gespecialiseerd bestuursorgaan kunnen worden gehandhaafd.

Het Wetboek van Strafrecht beschermt tegen commune criminaliteit (strafbare feiten uit dat Wetboek). Daarnaast bieden ook bijzondere strafwetten bescherming tegen criminaliteit, zoals de Wegenverkeerswet, de Opiumwet, de Wet economische delicten en de Wet wapens en munitie. De Wet economische delicten stelt bijvoorbeeld overtreding van art. 11.7, derde lid, van de Telecommunicatiewet (anonieme spam) strafbaar: ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden is alleen toegestaan met vermelding van de werkelijke identiteit van degene namens wie de communicatie wordt overgebracht, en een geldig postadres of nummer waaraan de ontvanger een verzoek tot beëindiging van dergelijke communicatie kan richten. Het opzettelijk niet vermelden van deze informatie is een misdrijf en in andere gevallen een overtreding.

⁵ Zie J. de Hullu, *Materieel strafrecht. Over algemene leerstukken van strafrechtelijke aansprakelijkheid naar Nederlands recht*. Deventer: Kluwer 2003 (tweede druk), p. 10.

⁶ R. Foqué, A.C. 't Hart, *Instrumentaliteit en rechtsbescherming*. Arnhem/Antwerpen 1990.

⁷ J.B.H.M. Simmelink, 'Over misdrijven, overtredingen en administratieve gedragingen', in: M.S. Groenhuijsen, J.B.H.M. Simmelink (red.), *Glijdende schalen. Liber Amicorum J. de Hullu*. Nijmegen: Wolf Legal Publishers, 2003, p. 527.

Eventuele strafbaarstelling van misbruik van persoonsgegevens hoeft dus niet perse in het Wetboek van Strafrecht te worden opgenomen, maar is ook mogelijk via bijzondere wetten. In beginsel lijkt het zelfs in de systematiek van het huidige strafrecht te passen om misbruik van persoonsgegevens strafbaar te stellen, bijvoorbeeld in bijzondere strafwetgeving. Het antwoord op de vraag of het strafrecht moet of kan worden ingezet, kan worden gebaseerd op de criteria voor strafbaarstelling.⁸

De wetgevingspraktijk (de landelijke politiek) die uiteindelijk bepaalt of een gedraging strafbaar moet worden gesteld, lijkt zich in de regel weinig van deze criteria aan te trekken. Politici maken er soms eerder uit politiek opportunisme een sport van wie als eerste strafbaarstelling eist als een verwarde tenenlikker in een Rotterdams park de pers heeft gehaald.⁹

Daarnaast speelt ook het opportuniteitsbeginsel van het Openbaar Ministerie een rol bij de strafrechtelijke handhaving van misbruik van persoonsgegevens. Tot nu toe heeft het Openbaar Ministerie daaraan duidelijk nog geen prioriteit toegekend, gelet op het geringe aantal strafzaken dat is gebaseerd op de artikelen 4, 27, 28 of 78 WBP. Een korte zoekactie op Rechtspraak.nl levert slechts twee strafrechtelijke vonnissen op.¹⁰

5. Heling van persoonsgegevens

Misbruik van persoonsgegevens kan bestaan uit het onrechtmatige gebruik van rechtmatig of te goeder trouw verkregen persoonsgegevens. Het is echter ook mogelijk dat de verkrijging van die persoonsgegevens al onrechtmatig was. Misbruik van persoonsgegevens laat zich vergelijken met de strafrechtelijke heling. De materiële norm ter bestrijding van heling bevat het strafrechtelijke verbod om gedragingen te verrichten die een (ander) misdrijf ondersteunen na afloop van dat misdrijf en daardoor dat misdrijf begunstigen. Heling is als misdrijf opgenomen in boek II, titel XXX, WvSr als een begunstigingsdelict. Niet alleen opzetheling is strafbaar (artikel 416 WvSr), maar ook de gewoonteheling (artikel 417 WvSr) en schuldheling (artikel 417bis WvSr). Zelfs een poging tot schuldheling is strafbaar. Met de helingbepalingen wordt beoogd te voorkomen dat iemand profiteert van het misdrijf van een ander, in het bijzonder van een goed dat door het misdrijf van een ander is verkregen. Tevens beschermt de strafbepaling van heling tegen het voortduren van een bijvoorbeeld door diefstal, oplichting, verduistering, valsheid in geschrifte, e.d. ontstane onrechtmatige vermogensrechtelijke toestand. Behalve natuurlijke personen kunnen ook rechtspersonen het delict plegen. Deze mogelijkheid maakt dat het niet onlogisch zou zijn om de ‘heling van persoonsgegevens’ strafbaar te stellen.

Alle delicten in titel XXX zijn gedragsdelicten, dat wil zeggen dat het verrichten van de strafbare gedragingen op zichzelf strafbaar is, zonder dat voor de strafbaarheid een bepaald gevolg moet intreden. De misdrijven van artikel 416, lid 1 en 2 WvSr zijn commissiedelicten. Dat wil zeggen dat zij feitelijke handelingen strafbaar stellen. Dat neemt overigens niet weg dat een gedraging, zoals het verwerven of voorhanden hebben van een goed door nalatigheid kan worden verricht. De begrippen ‘verwerven’, ‘voorhanden hebben’ en ‘overdragen’ impliceren feitelijke zeggenschap over een goed. Dit is vergelijkbaar met de ‘feitelijke macht’ die men over persoonsgegevens kan hebben.

⁸ Vgl. Th.A. de Roos, *Strafbaarstelling van economische delicten*, Arnhem: Gouda Quint 1987, p. 53 e.v.

⁹ Kamervragen van de leden Van Heemst en Wolfsen (beiden PvdA) en antwoorden van de minister van Justitie over een “tenenlikker” in Rotterdam. *Aanhangsel Handelingen II*, 2004/05, nr. 111.

¹⁰ Rechtbank 's-Gravenhage, 29 september 2004, LJN: AR2979, 09.755.095/03 en LJN: AR2973, 09.755.033/03 (o.a. schending art. 27 WBP).

Het begrip ‘goed’ in artikel 416 WvSr omvat alle materiële zaken, inclusief geld. Computergegevens vallen hier echter niet onder.¹¹ Bij de invoering van de Wet computercriminaliteit¹² zijn de gedragingen met betrekking tot door misdrijf verkregen computergegevens bewust beperkt tot die in het gewijzigde artikel 273 WvSr, dat het bekend maken en het uit winstbejag gebruiken van geheime gegevens (van bepaalde ondernemingen) die uit geautomatiseerde werken door misdrijf zijn verkregen, strafbaar stelt als daaruit enig nadeel kan ontstaan. Algemene strafbaarheid van heling van computergegevens werd destijds onwenselijk geacht. Omdat computergegevens niet als ‘goed’ worden beschouwd, kunnen ze ook niet in beslag worden genomen. Om dat te veranderen wordt in het thans bij de Eerste Kamer aanhangige wetsvoorstel Computercriminaliteit II de mogelijkheid ingevoerd om computergegevens die samenhangen met een gepleegd strafbaar feit ontoegankelijk te maken of door de rechter te laten vernietigen.¹³

Natuurlijke personen lopen het risico van maximaal vier jaar gevangenisstraf of geldboete van ten hoogste € 45.000 (opzetheling), een gevangenisstraf van maximaal zes jaar, een geldboete van ten hoogste € 45.000, of een combinatie van beide (gewoonteheling), of een gevangenisstraf van maximaal een jaar, een geldboete van ten hoogste € 45.000 of een combinatie van beide (schuldheling). Aan rechtspersonen kan zowel voor opzetheling, gewoonteheling als schuldheling een geldboete van ten hoogste € 450.000 worden opgelegd en verbeurdverklaring.

6. Is misbruik van persoonsgegevens altijd even erg?

Het ongeautoriseerd ter beschikking stellen en het misbruik maken van persoonsgegevens zouden dus niet misstaan als begunstigingsdelicten. Om het gebruik van onrechtmatig ter beschikking gestelde persoonsgegevens strafbaar te kunnen stellen, zal echter ook het onrechtmatig ter beschikking stellen van persoonsgegevens strafbaar moeten zijn.

Ter beantwoording van de vraag of deze beide handelingen ook werkelijk strafbaar gesteld zouden moeten worden, kan een aanvullende vraag worden gesteld. Die vraag luidt: hoe ernstig is het misbruik van persoonsgegevens? Men kan zich namelijk afvragen of het onrechtmatig verstrekken en gebruiken van naam, adres, postcode en woonplaats even ernstig is als het verstrekken en gebruiken van gevoelige gegevens, zoals gegevens over iemands ras, politieke opvattingen, religie, gezondheid, strafrechtelijk verleden of inkomen. Als tot strafbaarstelling wordt besloten, zal wellicht moeten worden gedifferentieerd naar de soorten van de gegevens die in het geding zijn: gewone persoonsgegevens of bijzondere persoonsgegevens. Financiële gegevens over iemands inkomen of ontvangen subsidies in het kader van het Gemeenschappelijk Landbouwbeleid – die vanaf 21 september 2005 openbaar zijn gemaakt op de webpagina van het ministerie van Landbouw, Natuur en Voedselkwaliteit – worden door de burger ook als gevoelige (bijzondere) gegevens ervaren.¹⁴ Of doet de soort van de gegevens er niet toe en is het de context waarbinnen de gegevens worden gebruikt die de mate van gevoeligheid ervan bepaalt?¹⁵

7. Handhaving

Naast de vraag of het strafrecht bescherming moet bieden tegen misbruik van persoonsgegevens dient ook de vraag te worden gesteld wie een dergelijk strafrechtelijk verbod zou moeten handhaven.

¹¹ HR 3 december 1996, *NJ* 1997, 574 m.nt.’tH.

¹² Wet van 23 december 1992, *Stb.* 1993, 33, in werking getreden op 1 maart 1993.

¹³ *Kamerstukken II*, 1998/99, 26 671, nr. 3, p. 19.

¹⁴ Bron: Brabants Dagblad, 23 september 2005. De GLB-subsidies zijn gepubliceerd op internet: <<http://www9.minlnv.nl/>>.

¹⁵ Zie ook de bijdragen van Jan Holvast en Peter Rodrigues over de bijzondere gegevens in dit nummer.

Juridische handhavingmogelijkheden zijn aanwezig in het burgerlijk recht, het bestuursrecht en het strafrecht. Het strafrecht is in deze ultimum remedium.

Civielrechtelijke handhaving heeft de voorkeur in horizontale verhoudingen. Maar dat is bij het verwerken van persoonsgegevens niet altijd mogelijk, bijvoorbeeld omdat de wederpartij niet bekend is; bovendien is er vaak sprake van ongelijke machtsverhoudingen. In dit geval zou daarom een keuze moeten worden gemaakt tussen bestuursrechtelijke of strafrechtelijke handhaving. Een voordeel van civielrechtelijke handhaving, bijvoorbeeld op grond van artikel 6:162 BW (onrechtmatige daad) is dat de betrokkene (consument, burger) zelf het initiatief heeft in een gerechtelijke procedure. Een voordeel van strafrechtelijke of bestuursrechtelijke handhaving is dat de betrokkene alleen maar aangifte hoeft te doen bij de politie of een klacht hoeft in te dienen bij een bestuursorgaan.

De keuze voor bestuursrechtelijke of strafrechtelijke handhaving wordt bepaald door:

- de symbolische waarde van de strafrechtelijke handhaving;
- de wenselijk geachte en feitelijk beschikbare handhavingcapaciteit bij de betrokken instanties;
- de beoogde effectiviteit van de handhaving (procesvormen, mogelijkheden tot buitengerechtelijke afdoening, 'lik-op-stuk'-effecten);
- de maatschappelijke waardering van het onrecht; en
- de wenselijk geachte waarborgen bij opsporing en bestraffing.¹⁶

In dit verband kan er op worden gewezen dat het toepassen van de bestuurlijke boete momenteel sterk in opmars is. De bestuurlijke boete kan worden ingezet bij het overtreden van regels met een geringe normatieve lading. De vraag is of de morele en juridische plicht tot vertrouwelijkheid van persoonsgegevens een geringe of juist een grote normatieve lading heeft. In het laatste geval ligt de bestuurlijke boete niet voor de hand, maar zou eerder naar strafrechtelijke middelen moeten worden gegrepen.

Daarnaast speelt echter ook de (on)deskundigheid van de handhavende autoriteiten een rol. Het is een feit van algemene bekendheid dat het openbaar ministerie overbelast is en de bescherming van persoonsgegevens heeft aldaar dan ook geen prioriteit. Er is echter een aantal gespecialiseerde toezichthouders (NMa, AFM, OPTA, CBP) met veel meer deskundigheid op de betreffende terreinen. In de praktijk wordt daarom de handhaving van steeds meer specialistische rechtsgebieden overgelaten aan bestuursorganen, zoals de NMa, AFM, OPTA en CBP.

Strafbare feiten kunnen na de inwerkingtreding van de Wet OM-afdoening ook worden gehandhaafd door bestuursorganen.¹⁷ Deze wet maakt buitengerechtelijke afdoening van strafzaken mogelijk. Bij algemene maatregel van bestuur kunnen bestuursorganen ("lichamen of personen, met een publieke taak belast") worden aangewezen die een strafbeschikking mogen opleggen. Een strafbeschikking, die ook door een officier van justitie kan worden opgelegd, kan bestaan uit een geldboete, een taakstraf, onttrekking aan het verkeer, betalen van een som geld aan het slachtoffer of ontzegging van de rijbevoegdheid. Bij deze bestuursrechtelijke handhaving van strafbare feiten handelen de bestuursorganen onder toezicht van en volgens richtlijnen op te stellen door het College van procureurs-generaal. De door de bestuursorganen op te leggen sancties zijn strafrechtelijk van aard, zodat de strafrechtelijke leerstukken en uitgangspunten van toepassing zijn.¹⁸ Wellicht dat er in de toekomst nog wel een strafrechtelijke taak is weggelegd voor het CBP.

¹⁶ J.B.H.M. Simmelink, *a.w.* 2003, p. 528-529.

¹⁷ *Kamerstukken I*, 2004-2005, 29 849 A (Gewijzigd voorstel van wet).

¹⁸ Zie ook J.B.H.M. Simmelink, *a.w.* 2003, p. 534-535.

8. Conclusie

Met een beroep op de theorie en de praktijk van het (straf)recht is het mogelijk om misbruik van persoonsgegevens strafbaar te stellen. De theorie zegt dat vertrouwelijkheid van persoonsgegevens best door middel van punitieve sancties (strafrechtelijk of bestuursrechtelijk) beschermd kan worden. De praktijk zegt dat de handhaving daarvan beter aan de deskundigheid van gespecialiseerde toezichthouders kan worden overgelaten dan aan het toch al overbelaste Openbaar Ministerie. De Wet OM-afdoening maakt handhaving van strafbare feiten door bestuursorganen mogelijk onder toezicht van het Openbaar Ministerie. In de systematiek van het (straf)recht is uitbreiding van het punitieve sluitstuk ter voorkoming en bestrijding van misbruik van persoonsgegevens dus mogelijk.

Het rechtsbelang dat in het geding is, te weten de vertrouwelijkheid van persoonsgegevens en daarmee het vertrouwen van burgers in de overheid, het bedrijfsleven en andere organisaties, alsmede de veronderstelling dat de naleving van de WBP wel beter kan, pleiten er voor om te overwegen het bestaande strafrechtelijke sluitstuk uit te breiden. De wetgever kan bijvoorbeeld kiezen voor uitbreiding van de reikwijdte van artikel 272 WvSr of voor uitbreiding van de strafbaarstellingen in de WBP. De handhaving van deze strafbare feiten kan vervolgens in bestuursrechtelijke handen worden gelegd.

Wellicht dat de Europese Commissie te zijner tijd, ingefluisterd door de Artikel 29 Werkgroep en door de Europese toezichthouder voor gegevensbescherming, bij een toekomstige wijziging van de Europese privacyrichtlijn 95/46/EG de lidstaten zal voorschrijven om bepaalde onderdelen van de richtlijn strafrechtelijk te handhaven. Sinds kort mag dat. Het Hof van Justitie EG oordeelde op 13 september 2005 in een uitspraak over de handhaving van milieubeschermingsbepalingen dat de EG de lidstaten mag verplichten om strafrechtelijke sancties op te leggen.¹⁹ Tot nu toe werd de keuze van de sancties voorbehouden aan de lidstaten afzonderlijk. Strafrechtelijke handhaving van richtlijnbevestigingen is niet langer voorbehouden aan de lidstaten of aan de intergouvernementele derde pijler. Op Europees niveau ontstaat aldus ook ruimte voor uitbreiding van het strafrechtelijk sluitstuk.

Het is aan te bevelen om in de evaluatie van de WBP het strafrechtelijk sluitstuk als een mogelijk verbeterpunt voor de naleving van de wet mee te nemen.

¹⁹ Orde van de dag, Nieuwsbrief Nederlandse Orde van Advocaten en Reed Business Information bv, 15 september 2005.