Dr.ir. B.H.M. Custers is adviseur bij Capgemini en onderzoeker bij het Tilburg Institute for Law, Technology and Society, mr. G.J. Zwenne is advocaat bij Bird en Bird en werkt bij het Centrum voor recht in de informatiemaatschappij, Universiteit Leiden.

Aandachtspunten voor het College Bescherming Persoonsgegevens

In Nederland zijn er alleen al op rijksniveau ruim twintig grote toezichthouders op verschillende terreinen, waaronder de financiële sector, onderwijs en zorg. Voor de bescherming van de privacy is het College Bescherming Persoonsgegevens (CBP) opgericht. Maar is onze privacy er in goede handen?

De privacywaakhond moet erop toezien dat zowel de overheid als bedrijven persoonsgegevens volgens de daarvoor geldende regels verwerken. Dat toezicht lijkt op dit moment tekort te schieten, zo blijkt uit onderzoek. de naleving van de privacywetgeving laat te wensen over.[1] Niettemin lijkt de toezichthouder, het CBP, nauwelijks op te treden. Het is illustratief dat het CBP in 2007 voor iets meer dan 20.000 euro aan boetes binnenhaalde. Dit bedrag steekt mager af tegen de bedragen die bijvoorbeeld de OPTA (telecomsector) en de AFM (financiële sector) opleggen. Voor deze toezichthouders is 20.000 euro eerder het minimumbedrag van een boete dan de totale jaarinkomsten.

Er zijn verschillende oorzaken waarom we zo weinig van de handhavingsmaatregelen merken. Aan sommige daarvan kan het CBP weinig doen, aan andere wellicht wel. De regelgeving, bijvoorbeeld, is abstract en algemeen en daardoor moeilijk te handhaven. Dit is het gevolg van Europese wetgeving en daar kan het CBP niet veel aan veranderen. Andere Europese privacytoezichthouders hebben er ook moeite mee en er wordt gestudeerd op verbeteringen. Wat zou het CBP wel kunnen doen?

Ga uit van vertrouwen

De meeste organisaties zijn zich zonder meer bewust van het belang van privacy en de bescherming van persoonsgegevens. Er zijn altijd spelers die zich niet aan de regels houden, maar gelukkig hebben de meeste organisaties geen aansporing nodig om te voorzien in de waarborgen die nodig zijn om de privacy van hun klanten, werknemers, consumenten, studenten, abonnees of eindgebruikers te beschermen. In de meeste marktsituaties kunnen ondernemingen het zich niet veroorloven aan de privacyzorgen van hun klanten voorbij te gaan. Er zijn marktsituaties, waarin de marktwerking niet of in beperkte mate aanwezig is. Daar blijkt dan dat ondernemingen eerder geneigd zijn privacybelangen te negeren, een opzichtig voorbeeld zijn de voortdurende problemen bij het OV-chipkaart-project. Toch lijken de meeste ondernemingen zich bewust te zijn van het belang van een goede en adequate privacybescherming en zijn zij bereid in de waarborging daarvan te investeren.

In andere situaties, zoals bij de overheid, ligt dat anders, maar toch wordt ook daar meestal gelet op de naleving van privacywetgeving, al was het maar omdat men oog heeft voor de voorbeeldfunctie. Bij misstanden zijn Kamervragen te verwachten en is er media-aandacht. Door uit te gaan van het welbegrepen eigenbelang bij privacy, kan ook hier vertrouwen als uitgangspunt worden genomen. Dit uitgangspunt betekent, om te beginnen, dat bij het oplossen van privacyproblemen niet meteen om meer handhavingsbevoegdheden of hogere boetes moet worden geroepen.[2] Uitgaande van het welbegrepen privacybelang is een intelligentere en meer (zelf)kritische benadering nodig. Het betekent dat wordt nagegaan

1 Vedder, A.H. e.a. (2007). *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw.* Den Haag: Rathenau Instituut. P. 49. Privacy International (2007) The 2007 international privacy ranking, leading surveillance societies in the EU and the world 2007.

2 D. Tokmetzis, Bescherming privacy vereist meer sancties, *NRC Handelsblad* 15 mei 2006; L. Mommers & G-J. Zwenne, Privacywetgeving is zelf het probleem, *Financieele Dagblad* 31 mei 2006.

waarom problemen zich voordoen en wordt onderzocht of die mogelijk in de wetgeving zelf liggen, in plaats van bij degenen die geacht worden de wet na te leven.
Onze privacywetgeving kenmerkt zich door open normen en vage begrippen, die in veel gevallen niet eenduidig worden geïnterpreteerd en die zeker niet voor iedereen begrijpelijk zijn. Daarnaast bevat de wetgeving vooral veel procedurele en formele vereisten, die soms niets met privacybescherming te maken hebben. Een voorschrift waarover grote twijfels bestaan, is de verplichting om alle geautomatiseerde gegevensverwerkingen bij het CBP (art. 27 Wbp) te melden. Er zijn meer dan 30.000 verwerkingen opgenomen in het daarvoor bedoelde openbare register, maar het merendeel daarvan houdt niet veel meer dan een nietszeggende invuloefening in.[3]

Geef aan waarop wordt gecontroleerd

Veel bedrijven en organisaties klagen dat ze wel voor privacy willen zorgen, maar niet goed weten hoe dat moet. Het probleem is, dat de privacywetgeving erg vaag is en van open normen uitgaat die maar beperkt worden ingevuld. De vertaling naar de praktijk ontbreekt.[4] De privacytoezichthouder kan bij deze vertaling een belangrijke rol spelen, niet zozeer door zelf voor te schrijven hoe een begrip of regel moet worden uitgelegd (dat is uiteindelijk aan de rechter), maar door bereidheid te tonen in voorkomende gevallen over niet ingevulde open normen of oplossingenrichtingen (geschillenbeslechting, handhavingsverzoek) van gedachten te wisselen. Het CBP blijkt hierin terughoudend te zijn, hetgeen afwijkt van de praktijk in andere toezichtsdomeinen. Voor NMa of OPTA is het niet ongebruikelijk te overleggen, bijvoorbeeld over het indienen van een klacht of een geschillenbeslechtings- of handhavingsverzoek. Op deze wijze wordt zowel bij marktpartijen als de toezichthouder zelf veel onnodig werk voorkomen. Als bedrijven en organisaties bij het CBP aankloppen, krijgen ze geen reactie of een reactie die in hun beleving vaak te weinig concreet is. Daardoor is niet duidelijk waarop wordt gecontroleerd of wat wel en niet wordt gehandhaafd. Er wordt dan uitgegaan van eigen en onzekere interpretaties van wettelijke begrippen. Partijen die het belang van privacy wel inzien, kunnen er daardoor niet op vertrouwen dat het CBP tegen schendingen van de wet optreedt. Het is belangrijk duidelijk te zijn waarop wordt gecontroleerd en wat wordt gehandhaafd. Dat betekent overleg met sectoren waarop toezicht wordt gehouden. Een bijkomend voordeel daarvan is dat het CBP beter inzicht krijgt in de processen van bedrijven en organisaties. Daarmee worden misstanden eerder opgemerkt en kan de wetgeving beter worden gehandhaafd.
Overleg betekent iets anders dan advies. Een toezichthouder moet terughoudend zijn met adviseren, omdat er dan belangenverstrengeling kan ontstaan. De toezichthouder wordt dan mede voor de ontstane situatie verantwoordelijk. Een toezichthouder moet niet concreet adviseren wat er moet gebeuren, maar overleggen welke resultaten er geboekt moeten worden. Door aan te geven waarop bij een controle wordt gelet, ontstaat een *resultaatsverplichting*.
Recent heeft het CBP de 'zienswijze' ingevoerd. Bedrijven of organisaties kunnen het CBP vragen een standpunt in te nemen over nieuwe of onopgeloste vragen over de toepassing of uitleg van wetgeving waarop wordt toegezien. Dit neigt naar advies in plaats van overleg. Het CBP geeft vanaf een afstand schriftelijk reactie op de vraag hoe de bedrijfsprocessen eruit moeten zien, terwijl hij met de sector zou moet overleggen welke resultaten hij verwacht.

> Het CBP zet de beschikbare handhavingsmiddelen maar in beperkte mate in

Controleer risicogericht

Als er vanuit wordt gegaan dat de meeste organisaties en bedrijven hun zaken goed proberen te regelen, is duidelijk dat het niet veel zin heeft iedereen altijd te controleren, het toezichtsdomein is daarvoor ook te groot. De duizenden overheidsinstellingen, organisaties en bedrijven kunnen of moeten niet allemaal worden gecontroleerd. Uitgaande van vertrouwen controleren toezichthouders daarom niet alle organisaties waarop ze toezien, maar werken gericht (met aanwijzingen of meldingen) of steekproeven (controles waar risico's worden verwacht). Het voordeel van een risicogerichte aanpak is dat organisaties en personen die niets misdaan hebben, ook minder of geen last van controles hebben en dat de toezichthouder geen onnodige capaciteit verliest.

3 www.cbpweb.nl.
4 G-J. Zwenne e.a, *Eerste fase evaluatie Wet bescherming persoonsgegevens: literatuuronderzoek en knelpuntenanalyse*, Den Haag: WODC 2007, p. 63-64.

Doordat er een betere *'hit-rate'* wordt gerealiseerd, worden er bovendien meer vertrouwen en draagvlak gecreëerd. Het schrikt bovendien overtreders af zodra duidelijk wordt dat de pakkans groot is. Degenen die het vertrouwen schenden, komen snel in beeld van de toezichthouder en de goeden hoeven niet onder de kwaden te lijden.[5]

Gebruik handhavingsmiddelen

Zodra duidelijk is dat een organisatie zich niet aan de regels houdt, moet snel en adequaat worden ingegrepen. Het is belangrijk dat voor de gecontroleerde helder is wat die precies verkeerd doet. Maar als een verplichting op grond van privacywetgeving voldoende duidelijk is, kan en moet de naleving ervan worden gehandhaafd, zeker als het gaat om veel voorkomende verwerkingen.[6] Anders dan wel wordt beoogd, is het probleem niet dat het CBP daartoe niet over voldoende handhavingsmiddelen zou beschikken. Het CBP kan weliswaar maar in enkele gevallen een bestuurlijke boete opleggen, het strafrechtelijk instrumentarium is bovendien beperkt.[7] Daarnaast is het CBP bevoegd tot toepassing van bestuursdwang ter handhaving van de bij of krachtens de Wbp gestelde verplichtingen.[8] In plaats daarvan kan het CBP ook een last onder dwangsom opleggen, een effectief en door veel toezichthouders gebruikt instrument om de naleving van de wet af te dwingen.[9]

Het CBP zet de beschikbare handhavingsmiddelen maar in beperkte mate in waar daartoe wel aanleiding was. Bekend is het geval van de passagiersgegevens die, ook vanuit Nederland, aan de douaneautoriteiten in de VS werden verstrekt.[10] Het CBP stelde terecht, dat de grootschalige gegevensverstrekking in strijd met de Wbp is, maar zag geen aanleiding zijn handhavingsmiddelen in te zetten. Een vergelijkbaar voorbeeld is de Swift-zaak, die in de bancaire wereld speelt. Ter bestrijding van fraude, witwassen en terrorismefinanciering verlangde de Amerikaanse overheid dat elke bank een klantenidentificatieprogramma opstelde, wereldwijd verplicht, met als sanctie het intrekken van de bankvergunning in de Verenigde Staten.[11] Ook verlangden de Amerikaanse autoriteiten dat persoonsgegevens werden verstrekt. Ondanks het feit dat de gegevensverstrekking in strijd was met de Wbp, zag het CBP, behoudens dreigen met handhaving, geen aanleiding op te treden. De toezichthouder zegt daarover dat *'de banken er na dreiging van handhaving door het CBP alsnog toe over (zijn) gegaan hun klanten conform de wettelijke eisen te informeren over wat er met hun gegevens gebeurt.'*[12] Dat lijkt heel wat, maar wie ziet hoe de banken hun klanten hebben geïnformeerd, moet zich afvragen of het CBP in dit specifieke geval niet een aangepaste opvatting heeft over wat de wettelijke eisen verlangen. Uit mededeling van de banken blijkt niet welke gegevens worden verstrekt, naar welke landen ze worden doorgegeven of welke autoriteiten en andere partijen daarvan kennisnemen. De vraag is of daarmee alle informatie is verstrekt die de klanten van de banken nodig hebben om er zeker van te zijn dat tegenover hen een behoorlijke en zorgvuldige verwerking is gewaarborgd. Toch vond het CBP dat met deze mededeling aan de vereisten van de Wbp was voldaan.

Wees niet bang voor procedures

Bij het inzetten van handhavingsmiddelen zijn reacties te verwachten. De overtreders zullen zich tegen dwangmiddelen verzetten. Dat kan tot schikkingen leiden, maar ook tot rechtszaken, waarin wordt uitgevochten wie er gelijk heeft. Het is belangrijk rechtszaken niet uit de weg te gaan, maar zelfs bewust aan te gaan. In procedures worden begrippen en regels opgehelderd. Tot nu toe wordt er echter, op een enkele uitzondering na, in Nederland weinig over toepassing en uitleg van privacyregels geprocedeerd.[13] Een reden daarvoor kan zijn dat het voor veel betrokkenen niet de moeite loont om te procederen omdat de kosten niet tegen de baten opwegen. Voor de privacytoezichthouder ligt dat anders. Verondersteld mag worden dat deze het belang van privacy inziet en over de kennis en deskundigheid beschikt om dat belang onder de aandacht van de rechter te brengen. Rechtszaken winnen kan alleen wanneer vooraf de zaken goed

5 Custers, B.H.M. (2007), Privacy en risicoprofilering bij keteninformatisering, in J. Grijpink e.a., *Geboeid door ketens, werken aan keteninformatisering*, Den Haag: Platform Keteninformatisering, p. 181-190.

6 Custers, B.H.M. (2007), Bedrijven die privacy burgers schenden pakken we te slap aan, *Trouw*, 3 maart 2007.

7 Art. 66 en art. 75 Wbp.

8 Art. 65 Wbp.

9 Art. 5:32, eerste lid, Algemene wet bestuursrecht (Awb).

10 Tokmetzis, D. (2007) Het bedrijfsleven wordt oom agent, *Intermediair*, 2 november 2007.

11 Custers, B.H.M. (2007) Klanten identificeren leidt niet tot betere opsporing, *Maandblad voor Accountancy en Bedrijfseconomie*, Jrg. 81, nr. 4, april 2007, p. 146-150.

12 Persbericht 2 april 2008: Hardere lijn bij bescherming privacy succesvol; Persbericht 28 januari 2007, Straks niemand meer onbespied door het leven. Toezichthouder CBP koerst op stevige handhaving van de privacyregels.

13 G-J. Zwenne & J. Webbink, De WBP en de winsverdubbelaar, *P&I* 2006/6, p. 2-8.

voorbereid zijn en er goed ingeschat is dat er realistische winkansen zijn. Er moet echter ervaring met rechtszaken worden opgedaan en geen koudwatervrees te hebben. Wie procedeert, weet dat er een kans is dat er niet wordt gewonnen.

Focus op kerntaken

Het CBP doet veel onderzoek en publiceert jaarlijks een of meerdere omvangrijke onderzoeksrapporten. Op zichzelf is dat niet verkeerd, want het is belangrijk een strategie en langetermijnvisie te hebben. Toch is onderzoek niet de hoofdtaak van een toezichthouder. In een moderne bedrijfsvoering is het interessant te overwegen nevenactiviteiten uit te besteden, al was het maar omdat andere, meer gespecialiseerde, partijen dat mogelijk beter en goedkoper kunnen. In Nederland zijn talloze onderzoeksinstituten die op dit terrein actief zijn en hierin via openbare aanbestedingen kunnen worden betrokken.

Jaarlijkse speerpunten

De belastingdienst controleert leaserijders extra bij hun aangifte, de politie zet extra capaciteit in bij het bestrijden van openbare geweldpleging, de douane controleert speciaal op nepmerkartikelen. Door elk jaar een speerpunt te nemen, wordt bij een bepaalde sector de aandacht op relevante regels gevestigd en daarmee op het risico van boetes en reputatieschade bij overtreding ervan. In het verleden heeft ook het CBP aangegeven zich in een bepaald jaar op een bepaalde sector of branche te concentreren. Inmiddels lijkt deze aanpak niet meer te worden gevolgd. Vanuit een toezichtsperspectief is dat een gemiste kans, omdat daarmee bewustheid (*awareness*) voor privacyregels binnen de desbetreffende sector wordt vergroot en omdat een dergelijke aanpak jaarlijks de nodige media-aandacht met zich meebrengt. Aannemelijk is dat daarvan weer een zekere preventieve werking uitgaat.

Koester onafhankelijkheid

Het CBP valt onder het ministerie van Justitie. Het komt regelmatig voor dat belangen van het ministerie en het CBP niet dezelfde zijn. Een voorbeeld is het cameratoezicht boven de snelweg bij Zwolle. Het CBP noemt dit 'onaanvaardbaar'.[14] Vervolgens wordt niet tot handhaving overgegaan, maar wordt de zaak in de Tweede Kamer door de ministers van Binnenlandse Zaken en Justitie afgedaan. Het CBP belooft met richtlijnen te komen, maar gaat niet over tot handhaving van het 'onaanvaardbare'. Los van de inhoudelijke vraag of in deze kwestie handhaving nodig is, lijkt hier geen sprake te zijn van een onafhankelijke positie. Toch moet een toezichthouder onafhankelijk kunnen opereren, onafhankelijk van de minister en van de politiek. Andere toezichthouders, zoals de AFM en de DNB, zijn ook van hun minister afhankelijk. Daarbij hoort ook dat het CBP zich geen andere rol aanmeet dan die van toezichthouder, toezicht houden op de naleving van de wet.

> Een toezichthouder moet onafhankelijk kunnen opereren

Het CBP neemt besluiten, maar doet geen uitspraak en wijst geen vonnis. Een toezichthouder is geen wetgever en evenmin rechter. Het is dan ook verwarrend en misleidend te spreken van CBP-jurisprudentie of CBP-uitspraken.[15] Verder doet het CBP er goed aan terughoudend te zijn met uitlatingen over hoe de wet moet worden geïnterpreteerd als de rechter daarover nog geen uitspraak heeft gedaan. Een voorbeeld van hoe het niet moet, is het CBP-persbericht waarin wordt gesteld dat voor eens en altijd is uitgemaakt dat IP-adressen als persoonsgegevens moeten worden aangemerkt, omdat een overlegorgaan van toezichthouders dit in een opinie heeft verdedigd.[16] De bevoegdheid te bepalen wat rechtens heeft te gelden, komt aan de rechter toe en het laatste woord is aan het Europees Hof van Justitie.

Transparant beleid

Op de website van het CBP staat veel informatie over de visies en het beleid van de toezichthouder. Er zijn talrijke rapporten, oordelen, besluiten, richtsnoeren, informatiebladen, opinies, verkenningen, toespraken, visies, jaarverslagen te vinden. Het zou mogelijk moeten zijn daaruit eenvoudig te achterhalen wat het CBP vindt, wat het gedaan heeft en in de toekomst nog gaat doen. Helaas is dat niet goed mogelijk, de website is moeilijk toegankelijk, de structuur is ondoorzichtig en onoverzichtelijk, de zoekfunctie beperkt en onvolledig, de zoekresultaten soms onbegrijpelijk. ■

14 Schenk, W (2008). Politie registreert alle auto's bij Zwolle, *Volkskrant*, 7 mei 2008.

15 Uitgangspunten en beleidsregels werkwijze CBP, *Stcrt.* 2004, 190; B.M.A. van Eck e.a. *Persoonsgegevens beschermd. Uitspraken van de Registratiekamer,* Den Haag 1999.

16 WBP (2008) *Internetzoekmachines moeten privacy respecteren,* persbericht, 7 april 2008.