

WBP EVALUATIE: KNELPUNTEN MET BETREKKING TOT DE WBP EN PRIVACY OP DE WERKPLEK

Gerrit-Jan Zwenne

Inleiding

In een van laatste bepalingen van de Wet bescherming persoonsgegevens (Wbp) staat dat de wet binnen vijf jaar na inwerkingtreding moet zijn geëvalueerd. Inmiddels, een paar jaar later dan had moeten, is het onderzoek naar de doeltreffendheid en de effecten van deze wet afgerond. Dit onderzoek is gedaan in twee fasen. De eerste fase betreft een literatuurstudie uitgevoerd door de privacyonderzoeksgroep van eLaw@Leiden.¹ De tweede fase is gedaan door Pro Facto, het bureau voor bestuurskundig onderzoek van de Rijksuniversiteit Groningen, en heeft een meer empirisch en praktijkgericht karakter.

In het in Leiden uitgevoerde ‘eerste fase evaluatieonderzoek’ is nagegaan hoe er in de juridische literatuur werd gedacht over de bijdrage die de wet heeft geleverd aan de beoogde doelstellingen.²

Reality check!

Juristen hebben de onhebbelijke gewoonte om zich voor van alles in te dekken en altijd voorbehouden te maken. In de literatuurstudie voor de WBP-evaluatie is dat niet anders. De lezer wordt erop gewezen dat het, enerzijds, niet is uitgesloten dat er zich in de praktijk toch ook knelpunten voordoen die niet in de literatuur zijn gesignaleerd. Ook wordt aangegeven dat het, anderzijds, mogelijk is dat er aan de knelpunten die wel in de literatuur zijn geïdentificeerd om wat voor reden dan ook in die literatuur onevenredig veel aandacht is gegeven.

In dit hoofdstuk wordt ingegaan op enige resultaten van het eerste faseonderzoek, vooral voorzover deze relevant zijn voor wat wel wordt genoemd ‘privacy op de werkvloer’. Vervolgens wordt, bij wijze van illustratie, heel kort nader ingegaan op rechtspraak over dit specifieke onderwerp.

Enige gesignaleerde knelpunten

Er worden, zo is gebleken, in de juridische literatuur talloze knelpunten gesignaleerd met betrekking tot de werking van de Wbp. Veel daarvan betreffen niet specifiek de bescherming van werknemers, maar raken daaraan wel. Een aantal van de gesignaleerde

¹ eLaw@Leiden, centrum voor recht in de informatiemaatschappij, is onderdeel van de faculteit der rechtsgeleerdheid van de Universiteit Leiden. eLaw@Leiden deed dit onderzoek in samenwerking met de Afdeling Staats- en Bestuursrecht van dezelfde universiteit en Duthler Associates.

² G-J. Zwenne et al, *Eerste fase evaluatie Wet bescherming persoonsgegevens*, Ministerie van justitie, december 2007. (www.wodc.nl)

knelpunten is vooral praktisch van aard. Zo bevat de wet allerlei procedurele voorschriften – meldplicht, vergunningplicht – terwijl niet altijd duidelijk is hoe en in hoeverre daaraan moet worden voldaan en/of wat deze bijdragen aan de bescherming van privacy. Voor dergelijke problemen worden vaak praktische oplossingen voorgesteld.

Maar daarnaast zijn er ook problemen met een fundamenteeler karakter. Wat op verschillende plaatsen wordt genoemd, is het probleem dat de wet erg veel gebruik maakt van heel open en vage normen en algemene begrippen. Als gevolg daarvan wordt de wet ingewikkeld gevonden en moeilijk toe te passen. Een ander fundamenteel probleem betreft de beperkte betekenis van de Wbp in de rechtspraak en de geringe bekendheid ervan.

OPEN EN VAGE NORMEN, ABSTRACTE EN ALGEMENE BEGRIPPEN

Zowel voor degenen die door de wet worden geadresseerd ('de verantwoordelijken' en 'de bewerkers') als de individuen die door de wet worden beschermd ('de betrokkenen') blijkt het in veel gevallen niet goed mogelijk om te bepalen of de wet van toepassing is, en zo ja, wat dat dan betekent. Ook toezichthouders en rechters hebben trouwens moeite daarmee.

Enkele auteurs stellen dan ook, soms met nauwelijks onderdrukte verontwaardiging, dat 'duidelijke antwoorden geven niet de sterkste kant is van de Wbp' en kenschetsen de wet als 'in dit bedje ziek'. Andere auteurs stellen dat het 'eenvoudigweg niet realistisch' is te verwachten dat degenen die met de wet moeten werken in staat zijn 'om handen en voeten te geven aan de vele open normen'. Ook wordt wel gesteld dat de Wbp 'meer van mensen vergt dan menselijk haalbaar is'. En ook dat de wet moet worden beschouwd als 'een onderwerp voor specialisten'.

De ingewikkeldheid en onduidelijkheid van de wet laat zich niet gemakkelijk oplossen. Het is het gevolg van de door de wetgever gemaakte uitdrukkelijke keuze om in de wet in vergaande mate uit te gaan van algemene en abstracte wettelijke begrippen en open en vage normen. Anders dan soms wordt gedacht, is deze keuze weloverwogen en met reden gemaakt. Open normen en abstracte, algemene begrippen zijn de middelen waarmee de wetgever regels stelt voor de situaties die hij nog niet of beperkt kan overzien. En juist als het gaat om zo iets dynamisch als het gebruik van geautomatiseerde gegevensverwerking is er veel voor te zeggen om gebruik te maken van normen en begrippen die al naar gelang de concrete situatie en feitelijke omstandigheden kunnen worden ingevuld. Wat de wetgever uitdrukkelijk wilde voorkomen is dat de Wbp, door een precisering van de

normen daarin, een keurslijf zou worden dat te weinig op de praktijk kan worden toegesneden.³

Een voorbeeld van een abstract, lastig in te vullen begrip is ‘het persoonsgegeven’. In de wet wordt dit gedefinieerd als ‘elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon’. Of er sprake is van identificatie of identificeerbaarheid wordt bepaald aan de hand van het criterium of het al dan niet een onevenredige inspanning kost om met behulp van de gegevens een individu te identificeren. Er moet worden vastgesteld of het in een concrete situatie al dan niet teveel moeite kost om met een bepaald gegeven iemand te identificeren.

Maar wat heeft te gelden als een ‘onevenredige inspanning’ is veranderlijk, onder andere als gevolg van technische of organisatorische of context-afhankelijke omstandigheden en ontwikkelingen. Een voorbeeld is een IP-adres of het internetadres van een computer. Of met zo een IP-adres een individuele werknemer kan worden geïdentificeerd hangt er vanaf welke softwaresystemen er door de werkgever worden gebruikt en/of de kundigheid van de systeembeheerder. In veel gevallen zal het weinig moeite kosten om een één-op-één relatie te leggen tussen IP-adres en werknemer. Maar lang niet altijd. Wat als het gaat om flex-plekken? Wat als de desbetreffende computers door verschillende werknemers worden gebruikt? Wat als werknemers elkaars *username* en *password* gebruiken? Of als een programmaatje is geïnstalleerd waarmee het IP-adres wordt gemaskeerd? In die en andere gevallen is het maar de vraag of er een werknemer kan worden geïdentificeerd met dit IP-adres. En dan is het dus ook de vraag of er wel sprake is van een persoonsgegeven, waarop de Wbp van toepassing is.

Een voorbeeld van een open en vage norm is het in de wet vastgelegde beginsel dat persoonsgegevens die voor het ene doel zijn verzameld niet zonder meer voor een ander daarmee onverenigbaar doel mogen worden gebruikt (zgn. ‘doelbinding’). In het kader van een klantenkaart kan een supermarkt vastleggen welke klanten wel eens een fles wijn kopen – bijvoorbeeld om deze klanten op enig moment een aanbieding te doen voor een nieuwe betaalbare Cabernet Sauvignon uit Australië. Maar het is niet de bedoeling dat supermarkten dergelijke gegevens doorverkopen aan zorgverzekeraars, die daarmee wellicht nauwkeuriger gezondheidsrisico’s kunnen inschatten en zo gedifferentieerde zorgpremies kunnen bepalen. Althans, zo wordt er nu over gedacht. Maar als de zorgkosten de pan uit rijzen valt misschien niet uit te sluiten dat het acceptabel wordt gevonden dat

³ *Kamerstukken II 1997/98*, 25 892, nr. 3, p. 5-6, 9, 12-13, 33.

er wordt gecontroleerd of verzekerden wel gezond genoeg leven. En dan zijn de gegevens over de dagelijkse boodschappen natuurlijk interessant.

Om de Wbp een wat langere houdbaarheidsdatum te geven moet de wet dus niet alleen voorbereid zijn op allerlei niet te voorziene nieuwe technologieën en toepassingen, maar ook op snel veranderende opvattingen over wat het belang is van privacy en privacybescherming, afgezet tegen andere belangen. In discussies over veiligheid blijkt dat wat vijf jaar geleden onbespreekbaar was (zeg: videocameratoezicht op het station) vandaag algemeen is geaccepteerd. En wat minder dan drie jaar geleden ondenkbaar was (zoals Youtube, LinkedIn, Hyves, Facebook, Twitter, enz.) is nu ingeburgerd. Om de privacywet niet voortdurend aan dergelijke ontwikkelingen te moeten aanpassen, moet de wet in staat zijn om daarop in te spelen. In het licht van dat allemaal is het niet onbegrijpelijk dat de wetgever ervoor heeft gekozen om de privacywet flexibel te maken en te vertrouwen op open en vage normen en abstracte, algemene begrippen.

TE WEINIG AANKNOPINGSPUNTEN VOOR CONCRETISERING

Een wet met veel open normen en abstracte begrippen hoeft niet per se onduidelijk te zijn, of niet toepasbaar of onuitvoerbaar, of anderszins problematisch. Waar het om gaat is dat er bruikbare instrumenten zijn om de normen en begrippen te concretiseren. De wetgever had daar indertijd, toen de wet tot stand kwam, oog voor. Hij ging er vanuit dat de normen van de Wbp op verschillende manieren zouden moeten worden geconcretiseerd. Dit zou, zo dacht de wetgever erover, kunnen door zelfregulering en of in sectorale wetgeving, of in de rechtspraak.

Acht jaar later is duidelijk dat deze concretisering maar in beperkte mate heeft plaatsgevonden. Over de hele linie hebben zowel zelfregulering als sectorale regels en rechtspraak er niet voor kunnen zorgen dat verantwoordelijken, betrokkenen en anderen, het gevoel hebben dat zij voldoende in staat zijn om de wettelijke normen en begrippen te concretiseren.

BEPERKTE BETEKENIS EN BETREKKELIJKE ONBEKENDHEID VAN DE PRIVACYWET

Ongeveer een jaar na de inwerkingtreding van de Wbp stelt de FNV aan de orde dat de wet betrekkelijk weinig betekenis heeft in civielrechtelijke procedures, en dat maar in beperkte mate gevolgen verbonden zijn aan een schending van deze wet bij het verzamelen van bewijsmateriaal. Ook geeft de werknemersorganisatie aan dat kantonrechters uiteenlopende oordelen geven over vergelijkbare zaken. Als gevolg daarvan stagneert de rechtsontwikkeling en worden privacynormen niet geconcretiseerd.

Anderen wijzen erop dat ‘de logica achter de Wbp’ niet of nauwelijks is doorgedrongen in andere rechtsdomeinen, zoals met name het arbeidsrecht. Ook wordt er wel op gewezen dat een inbreuk op de Wbp door een werkgever heel vaak alleen een betekenis heeft bij het bepalen van de uiteindelijk vast te stellen ontslagvergoeding voor de werknemer. Een en ander leidt ertoe dat de wet niet de bescherming biedt die de wetgever voor ogen had.⁴

Privacy op de werkvloer – in de rechtspraktijk

Waar het gaat om verhoudingen van werkgevers en werknemers moet het in de vorige paragraaf geschetste beeld worden genuanceerd, in zoverre dat er in deze verhoudingen nou juist wel de nodige initiatieven zijn genomen om de privacynormen – en begrippen te concretiseren. Tegelijkertijd zijn er verschillende praktijkgevallen, met name ontslag- en ontbindingszaken, waarin de Wbp niet wordt toegepast waar dat wel had gekund en gemoeten.

Hoewel is gebleken dat ook in de verhoudingen tussen werkgevers en werknemers nog veel vragen over de toepassing van de wet niet eenduidig kunnen worden beantwoord, hebben verschillende *stakeholders* op dit gebied al in een vrij vroeg stadium de moeite genomen om invulling te geven aan de wettelijke privacynormen. Wat kan worden genoemd zijn de model privacygedragscodes die door werkgevers- en werknemersorganisaties zijn opgesteld. Aan de hand daarvan hebben veel werkgevers, al dan niet samen met de ondernemingsraad, vastgesteld onder welke voorwaarden op de werkvloer gebruik mag worden gemaakt van e-mail en internet, en in hoeverre dat door de werkgever mag worden gemonitord en gecontroleerd.

Ook kan worden gewezen op de activiteiten van het College Bescherming Persoonsgegevens. De privacytoezichthouder heeft verschillende adviezen, rapporten en brochures over dit specifieke onderwerp opgesteld, zij het dat daarover niet door iedereen even positief wordt gedacht, getuige deze wat narrige opmerking in een wetenschappelijke publicatie:⁵

‘In Nederland treft ons dan de ogenschijnlijk drukke activiteit van het CBP rond controle door de werkgever van e-mails, maar de adviezen van het CBP worden door geen enkele arbeidsrechter gevolgd of gebruikt en in die adviezen wordt ten onrechte een onduidelijk antwoord gegeven op

⁴ Zie Zwenne et al. 2007, p. 87, 110.

⁵ P. de Hert & S. Gutwirth, ‘Veiligheid en grondrechten. Het belang van een evenwichtige privacypolitiek’, in E.R. Muller (red.), *Veiligheid. Studies over inhoud, organisatie en maatregelen*, Alphen aan den Rijn 2004, p. 587-631.

de essentiële vraag ‘of een werkgever zonder enige individuele of collectieve kennisgeving e-mails mag controleren.’

Verder, *last but not least*, is er enige rechtspraak over het e-mail en internetgebruik op de werkvloer, waarin weldegelijk invulling wordt gegeven aan de open privacynormen. Deze rechtspraak betreft ontslag- en ontbindingszaken waarin kantonrechters of rechtbanken de Wbp bij de beoordeling hebben betrokken. Maar, zoals gezegd, er zijn ook de nodige zaken aan te wijzen waarin de Wbp niet of nauwelijks betekenis had.

In het vervolg van deze paragraaf volgt, ter illustratie van het in het voorgaande uiteen-gezette probleem, een korte bespreking van enkele van deze uitspraken.⁶

PRIVACY IN ONTSLAG EN ONTBINDINGSZAKEN

Een veelvoorkomende en herkenbare situatie is het geval waar een werkgever op minder zorgvuldige wijze belastende informatie (persoonsgegevens) over een ontslagen werknemer blijkt te hebben verzameld. Bijvoorbeeld door heimelijk zijn e-mail en surfgedrag in te zien of te monitoren. In zo een geval ligt het voor de hand dat de werknemer een beroep doet op de Wbp en dat de rechter toetst of de werkgever zich bij het verzamelen van de persoonsgegevens heeft gehouden aan deze wet, en zo niet, welke gevolgen daaraan worden verbonden.

Wat opvalt bij een analyse van dergelijke zaken is dat rechters op uiteenlopende wijze omgaan met de Wbp en de normen en begrippen daarvan op heel eigen wijze invullen en toepassen. En dus dat er nog geen helder en eenduidig beeld lijkt te zijn van of en hoe deze privacynormen moeten worden toegepast.

In een aantal uitspraken gebruikt de rechter de term ‘privétisering van de werkplek’. Daarmee wordt beoogd aan te geven dat werknemers aanspraak maken op enige privacybescherming op de werkplek. Een voorbeeld is deze overweging van de kantonrechter te Haarlem in een uitspraak van 16 juni 2000:

“In het huidige tijdsgenricht is aanvaard dat er een zekere “privétisering” op de werkplek optreedt. Dat heeft tot gevolg dat ook een werkgever binnen zekere grenzen heeft te aanvaarden dat er onder werktijd privé-contacten worden onderhouden.

⁶ Zie voor een uitgebreider overzicht en diepgaander analyse: M. van Pelt *Houd werk en privé gescheiden! Of toch niet? Monitoren van e-mail en internetgebruik op de werkvloer*, (master afstudeerscriptie Universiteit Leiden), februari 2009.

Ook op de werkvloer hebben werknemers dus een zeker recht op privacy. Een werkgever moet dat respecteren. Hij kan niet zomaar, zonder goede reden, e-mailberichten van werknemers inzien of surfgedrag monitoren. In een enkel geval worden er wel beperkingen toegestaan op dit recht op privacy op de werkvloer. De kantonrechter in Amsterdam zegt bijvoorbeeld in een uitspraak van 26 april 2001 dat de werkgever weliswaar binnen zekere grenzen moet toestaan dat er privécontacten worden onderhouden op de werkvloer, maar dat hij daartoe alleen is gehouden:

“indien en voor zover daarvan geen concrete, aanwijsbare nadelige invloed op het werk en/of de werksfeer uitgaat”

In een enkel geval wordt de bescherming van de privacy van werknemers op de werkvloer in verband gebracht met het goed werkgeverschap, soms zonder dat de Wbp wordt genoemd. De kantonrechter in Haarlem doet dit in een uitspraak van 4 juli 2003 zo:

“de wijze waarop [werkgever] is omgesprongen met de privacy van [de werknemer] bij het onderzoek [getuigt] op zijn minst niet van goed werkgeverschap. [de werkgever] heeft in deze gehandeld zonder ook maar enigszins met de belangen van [de werknemer] rekening te houden.”

Als een werkgever te weinig rekening heeft gehouden met de privacy van de werknemer op de werkplek, bijvoorbeeld doordat hij heimelijk e-mails van hen heeft ingezien of surfgegevens heeft vastgelegd, kan dat betekenen dat de aldus verzamelde informatie niet mag worden gebruikt in de ontslagprocedure. Een voorbeeld daarvan biedt deze overweging in de reeds genoemde uitspraak van 16 juni 2000 van de kantonrechter in Haarlem:

Een werkgever behoort de privacy van die [privé]contacten te waarborgen. De persoonlijke inhoud van het e-mailverkeer van [de werknemer] met derden [...] zal hier daarom buiten beschouwing worden gelaten.”

Maar niet alle rechters zijn bereid zo ver te gaan. Zo komt het, in afwijking van de zo even genoemde rechtspraak, ook wel voor dat kantonrechters weinig boodschap hebben aan de ‘privetisering’ van de werkplek. Een voorbeeld biedt deze overweging van de kantonrechter in Almelo in een al wat oudere uitspraak:

“dat [de werkgever] mogelijkwijs de privacy van [de werknemer] heeft geschonden, mag werknemer niet aan haar tegenwerpen. In het kader van het onderzoek naar misbruik van het internet bij werkgever, valt niet te ontkomen aan een onderzoek naar het persoonlijk gebruik dat van het internet is gemaakt.”

In rechtspraak van recentere datum wordt een vergelijkbare redenering gevolgd. Een voorbeeld is een zaak van 27 juni 2008, waarin de kantonrechter in Arnhem geen betekenis toekende aan de schending van de privacy van de werknemer op de werkplek. Waar het hem om gaat is of de door de werkgever heimelijk onderschepte e-mails juist en betrouwbaar zijn:

“In deze zaak heeft [de werkgever] haar vordering gegrond op schending van het tussen haar en [de werknemer] overeengekomen geheimhoudingsbeding, en heeft zij de onderschepte e-mailwisseling tussen [de werknemer] en [persoon A] als bewijs van die schending opgevoerd. Ook indien en voor zover zou moeten worden aangenomen dat het recht van [de werknemer] op eerbiediging van haar persoonlijke levenssfeer is geschonden, is niet in geding dat het door [de werkgever] gepresenteerde bewijsmateriaal betrouwbaar is. [de werknemer] heeft zowel in als buiten rechte alle gelegenheid gehad om de authenticiteit ervan ter discussie te stellen, maar zij heeft dat nagelaten. Dit brengt met zich mee dat het gebruik van de onderhavige e-mailberichten door [de werkgever] niet in strijd wordt geacht met het recht van [de werknemer] op een eerlijk proces.”

In een uitspraak van 13 maart 2008 komt de kantonrechter in Groningen tot eenzelfde uitkomst, maar dan na een belangenafweging, waarin privacy op de werkvloer ondergeschikt is aan het belang van ‘materiële waarheidsvinding’. De aanleiding voor het ontslag in deze zaak waren feiten die bekend waren geworden door gebruikmaking van heimelijk videocameratoezicht. In deze zaak stond vast dat de videobeelden wederrechtelijk waren verkregen – want in strijd met de Wet heimelijk cameratoezicht en in het verlengde daarvan toch ook de Wbp. En hoewel de kantonrechter het recht op privacy op de werkvloer wel erkende, stelt hij dat daarop inbreuk mocht worden gemaakt, omdat de werkgever anders in bewijsnood zou komen. Hij overweegt:

“...In een civiele procedure heeft de rechter een grote vrijheid in de waardering van het bewijs. Materiële waarheidsvinding staat voorop. In dit kader zal een belangenafweging moeten worden gemaakt, waarbij enerzijds het belang van de werkgever speelt om onrechtmatigheden in de onderneming te kunnen opsporen, en anderzijds het belang van de werknemer om beschermd te zijn tegen inbreuken op zijn privacy, ook op de werkplek.”

En ook:

“Uit de inspanningen en onderzoeken die [de werkgever] heeft gedaan, zoals in de vaststaande feiten omschreven, blijkt wel hoe moeilijk het is geweest de dader op te sporen. [...] Nu deze ingezette middelen geen resultaat hadden opgeleverd en het verspreiden van briefjes door is gegaan

en daarmee de onrust binnen [de werkgever] groter werd, mocht [de werkgever] in deze situatie van bewijsnood concluderen dat het opsporen van de dader dringend nodig was en niet anders dan met gebruikmaking van een verborgen camera kon slagen. Daarbij overweegt de kantonrechter dat het gebruik van de verborgen camera beperkt is gebleven tot de ruimte van de kleedkassen en dus niet verder is gegaan dan strikt noodzakelijk. Daarmee heeft [de werkgever] gehandeld met inachtneming van de beginselen van proportionaliteit en subsidiariteit en acht de kantonrechter het verkregen bewijs bruikbaar in deze procedure”

Wat opmerkelijk is aan deze zaak, behalve de uitkomst ervan, is dat de rechter volledig voorbij gaat aan de Wbp. En dit terwijl hij zonder meer aan de hand van de normen van de wet had kunnen redeneren:

- op grond van de Wbp geldt er voor de werkgever een informatieplicht ten aanzien van het verzamelen van videobeelden (d.w.z. persoonsgegevens) van werknemers (art. 33 Wbp);
- er zijn uitzonderingen mogelijk op deze informatieplicht, zoals in het geval het voldoen daaraan een onevenredige aantasting betekent van de gerechtvaardigde belangen van de werkgever (art. 43, onder e, Wbp).

Deze uitspraak kan dan ook worden gezien als een bevestiging van de onbekendheid van de Wbp bij de rechter en de rechtshulpverleners die de werkgever en werknemer bijstonden.

Er is nog wel meer interessante rechtspraak over de Wbp en privacy op de werkvloer. Op deze plaats wordt evenwel volstaan met de vaststelling dat het beeld zeer divers is. Als het gaat om ontslag en ontbindingszaken zijn er rechters die de Wbp toepassen waar het kan (en zou moeten). Maar ook dat er veel rechters zijn die er geen moeite mee hebben om aan de wet voorbij te gaan. Als rechters de Wbp toepassen doen zij dat op uiteenlopende en soms heel eigen en eigenaardige wijze.

Ter afsluiting

Natuurlijk, een handvol uitspraken is niet representatief. Maar het illustreert wel een belangrijk en klemmend knelpunt dat in de literatuurstudie ten behoeve van de wetsevaluatie naar voren kwam: de wet is ingewikkeld, vaag en onduidelijk en daardoor lastig toe te passen. Ook bevestigen deze uitspraken dat de wet betrekkelijk onbekend en onbemind is. Daardoor biedt de wet, als het erop aankomt, veel minder bescherming dan de wetgever voor oog had.

De verwachting is dat de wetgever, wellicht met de toezichthouder en andere *stakeholders*, nu gaat bedenken hoe de gesignaleerde knelpunten kunnen worden opgelost. Het is, zoals altijd, afwachten wat dat gaat opleveren. Aangenomen mag worden dat het opstellen en formuleren van privacywetgeving niet veel minder lastig is dan het toepassen of uitvoeren daarvan.