Waken voor kenbaar maken. Over privacy, identiteit en anonimiteit in de informatiemaatschappij

Prins, J.E.J.

Published in:
Privacy

Publication date:
2002

Prins, J.E.J. (2002). Waken voor kenbaar maken. Over privacy, identiteit en anonimiteit in de informatiemaatschappij. In Titulaer-Meddens, J.M. (Ed.) *Privacy: ons een zorg! De betekenis van privacybescherming voor het V&W-beleid*. Ministerie van Verkeer en Waterstaat. pp.30-42

Waken voor kenbaar maken.

Over privacy, identiteit en anonimiteit in de informatiemaatschappij

J.E.J. Prins[1]

1. Inleiding

"Het systeem moet anoniem gebruik toestaan", aldus Roel Pieper in zijn advies 'Mobimiles'[2] over de elektronische kilometerheffing. De vraag die hier natuurlijk direct opkomt is: hoe anoniem is anoniem? Immers, in veel situaties waarin momenteel wordt gesproken van een anonieme toepassing is in feite geen sprake van daadwerkelijke anonimiteit: dat wil zeggen anonimiteit in de zin dat de betreffende persoon op geen enkele manier valt te achterhalen. Vele van de momenteel in omloop zijnde technieken om anonimiteit te bewerkstelligen werken op basis van het principe dat de in beginsel anonieme berichten onder omstandigheden toch tot de betrokken persoon kunnen worden herleid. Voorbeelden hiervan zijn de chipknip en andere virtuele betaalmiddelen. In feite is er dus geen sprake van echte anonimiteit, maar vaak alleen van pseudo-anonimiteit. Pieper is niet de eerste die het belang van anonieme handelingen en transacties aan de orde stelt. Het thema anonimiteit mag zich de laatste jaren in een grote belangstelling verheugen. Dit komt met name doordat anonimiteit volgens sommigen een sleutelrol speelt in de discussie over adequate privacybescherming. In diverse beleidsdocumenten is inmiddels aandacht besteed aan het thema. Er wordt zelfs wordt gesproken over een (grond)recht op anonimiteit. Welke zijn zoal deze beleidsdocumenten en welke visie valt hieruit te destilleren? Waar hebben we het eigenlijk over als we spreken over anonimiteit? Zijn anonieme handelingen en transacties wel te realiseren in onze huidige informatiemaatschappij? Want de informatiemaatschappij – de term zegt het al – wordt gekenmerkt door een zucht naar steeds meer informatie en achter deze informatie verborgen kennis.[3] Het zijn deze en andere vragen die in dit betoog centraal staan.

---

[1] Corien Prins is hoogleraar recht en informatisering, Centrum voor recht, bestuur en informatisering, Katholieke Universiteit Brabant (J.E.J.Prins@kub.nl).

[2] R. Pieper, *Mobimiles. Bewust op weg*, rapport in opdracht van de Minister van Verkeer en Waterstaat, 10 april 2001, p. 13. Het volledige rapport is beschikbaar via http://www.vananaarbeter.nl/kilometerheffing.

[3] Vgl. bijvoorbeeld de toenemende belangstelling voor zogenoemde datamining-technieken, welke beogen om op basis van profielen uit reeds verzamelde gegevens de verborgen kennis te destilleren. Men spreekt hier niet voor niets van 'schatgraven in informatie'. Zie hierover: E. Schreuders, *Datamining, de toetsing van beslisregels en privacy*, dissertatie Katholieke Universiteit Tilburg, online beschikbaar via:

2. Er is meer dan alleen identificatie

Zoals bekend, wilde het kabinet oorspronkelijk een heffingssysteem invoeren per gereden kilometer, waarvan het tarief afhankelijk was van tijdstip en plaats waar de automobilist rijdt.[4] Een dergelijke elektronische heffing kan niet functioneren zonder de registratie van verplaatsingen van personen. Dit betekent dat het systeem gevolgen kan hebben voor de privacy van de automobilisten. De bedoeling was om een systeem te introduceren waarbij uitsluitend de direct betrokken instanties - de Belastingdienst en de chipkaartaanbieder – de beschikking zouden krijgen over de met het systeem gegenereerde gegevens. Toch staat het natuurlijk vast dat deze gegevens ook gebruikt zouden kunnen worden voor andere (secundaire) doeleinden. Zoals opsporing en in de toekomst een scala aan (commerciële) voorzieningen met behulp van zogenoemde *in-car* telematica.
Het is daarom niet verbazingwekkend dat de Registratiekamer in haar advies over het wetsvoorstel kritisch oordeelt over dit kabinetsvoornemen. De Registratiekamer vraagt zich af waarom er niet wordt gekozen voor een heffingsalternatief waarbij geen sporen van de automobilist worden achtergelaten. Ze refereert daarbij aan de toezegging van de Minister van V&W om aandacht te hebben voor de ontwikkeling van anonimiteitswaarborgen.[5] Verder wijst de Registratiekamer op de noodzaak tot de introductie van anonieme elektronische betaalmiddelen, zoals de electronic purse die aan buitenlandse weggebruikers zal worden verkocht.[6]

De voorgaande discussie is een mooie illustratie van de vraag in hoeverre bepaalde toepassingen het noodzakelijk maken dat er persoonsgegevens worden verzameld. Het maakt ook duidelijk dat waar wordt gesproken over anonimiteitswaarborgen, zeker niet altijd sprake hoeft te zijn van volledige anonimiteit.
Vaak willen organisaties en bedrijven om een diversiteit aan redenen (zekerheid, traceerbaarheid, marketingoverwegingen, etc.) weten met wie ze van doen hebben. Daarom wensen ze dat de identiteit van iemand bekend is of dat diens identiteit gemakkelijk te achterhalen is aan de hand van sporen of identificerende persoonsgegevens. De meest betrouwbare vorm is de controle van de juistheid van de

---

http://www.privacydossier.nl; J. Holvast, *Het gebruik van persoonlijkheidsprofielen in de publieke sector*, ITeR-reeks no. 42, Sdu Den Haag 2001.
[4] Wetsvoorstel Bereikbaarheid en mobiliteit, *Kamerstukken II* 2000-2001, 27552, nrs. 1-3.
[5] Brief van de Minister van Verkeer en Waterstaat aan de Registratiekamer, maart 1998.
[6] Ambtshalve advies over het wetsvoorstel Bereikbaarheid en mobiliteit, Registratiekamer 6 maart 2001. Beschikbaar op: http://www.registratiekamer.nl/bis/top-1-1-5-8-5.html.

identificerende persoonsgegevens aan de hand van een officieel legitimatiebewijs. Deze controle gebeurt door een daartoe bevoegde derde partij. Dit kan een private of een publieke instantie zijn. Bijvoorbeeld een notaris, een ambtenaar van de burgerlijke stand en in de toekomst wellicht een (particuliere) organisatie die de status van TTP (Trusted Third Party)[7] heeft verworven.
In de praktijk blijkt echter ook bij een controle door een van deze partijen zelden iemands ware identiteit met volledige zekerheid vast te stellen. De controlerende instantie volstaat meestal met de vaststelling dat iemand dezelfde is als mag worden verwacht. Helaas is men zich meestal niet bewust van de beperking van de gebruikelijke vorm van persoonsherkenning. Daardoor wordt verificatie in de praktijk vaak gelijkgesteld met identificatie. Zelfs als een persoon ter plaatse kan worden vergeleken met een foto op een legitimatiebewijs, kan deze eenmalige en losstaande verificatie nooit absolute zekerheid verschaffen dat hij werkelijk degene is voor wie hij zich uitgeeft. Voor veel rechtshandelingen is een persoonsherkenning van het type "hij is *dezelfde* als…" echter goed genoeg. Dit zal bijvoorbeeld ook zo zijn bij het hiervoor beschreven systeem voor een kilometerheffing: vastgesteld moet worden dat degene bij wie de heffing in rekening wordt gebracht, ook degene is wiens auto zich op een specifiek moment op een bepaalde weg bevond.
De voorgaande constatering brengt ons bij het onderscheid tussen identificatie en verificatie. Identificatie is gericht op het vaststellen van iemands *ware* identiteit. Bij verificatie stelt men alleen vast of twee gegevens bij *dezelfde* persoon horen. In de meerderheid van de gevallen zal in ons maatschappelijk verkeer derhalve sprake zijn van niet meer dan verificatie. Dit maakt dat het in veel situaties het niet noodzakelijk is de identiteit van een persoon vast te stellen. We kunnen volstaan met vormen van pseudo-identiteit. Omdat pseudo-identiteit vaak wordt verward met anonimiteit, moeten we eerst stilstaan bij de grenzen van beide termen.

3. … maar er is ook meer dan anonimiteit

De term anonimiteit wordt vaak ten onrechte gebruikt in beleidsdocumenten of literatuur. Er is pas sprake van volstrekt anoniem handelen als herleidbaarheid van een rechtshandeling op een persoon volstrekt onmogelijk is omdat er geen aanknopingspunt is. De telefooncel is een bekend voorbeeld van volstrekte anonimiteit van de beller. Zodra

[7] De TTP krijgt als certificatiedienstverlener een rol bij de uitgifte van elektronische handtekeningen. Zie het wetsvoorstel ter implementatie van de Europese Richtlijn elektronische handtekeningen dat in mei 2001 bij de Tweede Kamer is ingediend: *Kamerstukken II* 2000-2001, 27743, nrs. 1-2.

tenminste één persoon of instantie weet of kan achterhalen wie de handelende partij precies is, is er geen volstrekte anonimiteit. We hebben dan te maken met semi-anonimiteit.
Bij een semi-anonieme rechtshandeling kunnen bepaalde instanties of tussenpersonen de juiste identiteit van de betrokkenen vaststellen wanneer omstandigheden daartoe aanleiding geven. Een voorbeeld van semi-anonieme handelingen zijn de remailerdiensten op internet. Postbussen, autokentekens en de mogelijkheid om op een veiling 'anoniem' te bieden, zijn andere voorbeelden van semi-anonimiteit. Bij tenminste één instantie zijn (onder meer of minder stringente voorwaarden en soms tegen betaling) nadere gegevens te verkrijgen over de ware identiteit van de gebruiker, houder of opdrachtgever.
Zoals gezegd is ook het begrip 'pseudo-identiteit' van belang. De belangrijkste reden om onder een pseudoniem handelingen en transacties te verrichten is dat de persoon die het pseudoniem hanteert zich daarmee (her)kenbaar maakt zonder zijn ware naam (identiteit) prijs te geven. Zo kan iemand met behulp van een pseudoniem op internet in discussiegroepen participeren. Hij wordt daar onder zijn of haar 'nym' herkend. Maar iemand kan zich ook middels de bij een chipkaart behorende PIN-code presenteren als de rechtmatige houder van de PIN-pas. Zoals hiervoor al gezegd kunnen bij een semi-anonieme rechtshandeling waarbij de betreffende persoon gebruik maakt van een pseudo-identiteit, bepaalde instanties of tussenpersonen de identiteit van de betrokkenen vaststellen wanneer omstandigheden daartoe aanleiding geven.
Ook nu kan de hiervoor besproken kilometerheffing tot voorbeeld dienen. De chipkaartaanbieder kreeg onder het voorgestelde systeem de beschikking over informatie over betalingen in het kader van de heffing. Deze informatie bevat geen identificerende gegevens over de achterliggende persoon. Echter, bij een eventuele betwisting van een rekening door de rekeninghouder is het (conform artikel 4 van het wetsvoorstel) op nadrukkelijk verzoek van deze houder mogelijk dat de chipkaartorganisatie gegevens beschikbaar stelt aan de Belastingdienst. In een dergelijk geval worden gegevens gecombineerd en is sprake van een herleiding van de oorspronkelijk anonieme gegevens tot gegevens welke iets zeggen over een individuele persoon. Kortom: gegevens die in eerste instantie voor een bepaalde organisatie anonieme gegevens zijn, blijken in bepaalde gevallen wel degelijk om te zetten in identificerende gegevens. Er is in dit geval dus sprake van semi-anonimiteit, waarbij gebruik wordt gemaakt van een pseudo-identiteit.
Een pseudo-identiteit schept dus de mogelijkheid om tegelijkertijd voor de één anoniem te blijven en bij een ander volledig bekend te zijn. Wanneer een bank een PIN-code verstrekt, kan de bank op het moment van de uitgifte van de PIN-pas nagaan wie de houder werkelijk is. Gebruikt de bezitter de PIN-pas later om te betalen, dan kan hij voor

de wederpartij anoniem blijven. De PIN-code dient dan als pseudo-identiteit (pseudoniem) en de PIN-pas als pseudo-identiteitsbewijs. De winkelier die met behulp van de PIN-betaling zijn geld krijgt, weet wel dat zijn klant volgens de bank de rechtmatige houder van de PIN-pas is. En dit zonder dat de bank hem hoeft te vertellen wie zijn klant precies is.

4. Waarom (pseudo-) anonimiteit?

De voorgaande analyse laat zien dat een keuze voor (een gedeeltelijke) anonimiteit mogelijk is zonder schade voor belangen als rechtszekerheid en traceerbaarheid. Immers, de tweekoppigheid van een pseudo-identiteit (voor de één anoniem blijven en bij een ander volledig bekend zijn) maakt het mogelijk anonimiteit zodanig in het rechtsverkeer te organiseren dat daarbij de gewenste rechtszekerheid wordt gecreëerd. Door aandacht te schenken aan deze keuze zou de overheid tegemoet kunnen komen aan de behoefte bij een bepaalde groep burgers aan enige vorm van anonimiteit in het maatschappelijk verkeer. De drang naar anonimiteit lijkt in de praktijk zeker toe te nemen. Dit ondanks dat sommigen beweren dat privacy een non-issue is en burgers bereid zijn hun gegevens zonder veel problemen af te staan dan wel 'te verkopen'.[8] In ieder geval kan deze drang naar anonimiteit worden waargenomen bij bepaalde ICT-toepassingen, zoals prepaid mobiel bellen en internet. Een van de achterliggende verklaringen hiervoor is dat de – over het algemeen meer kritisch ingestelde – burger zich steeds meer bezorgd maakt over wat er zal overblijven van de privacy in een informatiesamenleving. Wie dan besluit om anoniem aan het maatschappelijk verkeer deel te nemen, is vervolgens niet langer afhankelijk van de vraag of verwerkers van persoonsgegevens de privacywetgeving al dan niet naleven. Privacybescherming wordt dan dus bewerkstelligd via anonimiteit. Anders gezegd, de gebruiker van de anonimiseringstechniek legt privacy pro-actief en dwingend op.[9]
De wens tot anoniem handelen kan ook voortkomen uit een beroep op de vrijheid van meningsuiting. Zo kunnen bepaalde (groepen van) personen er belang bij hebben dat niemand hun naam in verband brengt met een bepaalde uiting of handeling.[10]

---

[8] Denk aan loyalty-systemen (zoals bonuspunten) en de internetbedrijven die gratis dienstverlening aanbieden in ruil voor persoonsgegevens en andere persoonsgebonden informatie (zoals informatie over aankoopgedrag).
[9] Zie over de toenemende tendens en mogelijkheden om pro-actief en dwingend rechten te kunnen uitoefenen: J.E.J. Prins, 'Privaatrecht: virtuele verkenningen', *WPNR*, april 2001, pp. 264 ev.
[10] Vgl. de positie van krakers en de jurisprudentie inzake het dagvaarden van anonieme krakers. Zie ook het Muurkrant-arrest, HR 24 juni 1980, NJ 1981, 659.

Overwegingen rondom de vrijheid van meningsuiting en de vrije publieke discussie kunnen een nieuwe dimensie krijgen vanwege het mondiale karakter van elektronische communicatie. Tenslotte kan de reden om anoniem op internet actief te zijn, nog zijn gelegen meer duistere overwegingen. Zoals het plaatsen van illegaal of onrechtmatig materiaal. Er zijn inmiddels een flink aantal uitspraken van Amerikaanse rechtbanken in zaken waar iemand claimt dat de anonieme gedaagde verantwoordelijk is voor illegale praktijken of misleidende uitlatingen op internet. De rechtbanken werden in deze zaken geconfronteerd met de vraag onder welke omstandigheden van de gedaagde mag worden verlangd dat deze zijn identiteit prijsgeeft.[11]
Een overweging van een geheel andere aard rapporteerde 'The Economist' in juli 2001: "Scientists and engineers at Xerox's Palo Alto Research Center (PARC), for instance, were discouraged from searching an online database of patents maintained by IBM. Xerox feared that if IBM tracked the pattern of inquiries made by its engineers at PARC, the computer giant could build a fairly accurate profile of the kind of research under way in the Palo Alto laboratories."[12]

Mede onder invloed van de maatschappelijke discussie, hebben zich op beleidsniveau en in de literatuur diverse voorstanders gemeld van de introductie van een recht op anonimiteit.[13] Minister Van Boxtel kwam hierop terug tijdens de parlementaire behandeling van de Wet bescherming persoonsgegevens (Wbp). Hij deed de toezegging te onderzoeken of het mogelijk is om burgers ten behoeve van de digitale communicatie met de overheid "anoniem of pseudo-certificaten beschikbaar te stellen waarbij gegevens van de persoon losgekoppeld worden van de persoon zelf."[14] De Raad voor het Openbaar Bestuur kwam in januari 2000 met het rapport 'ICT en het recht om anoniem te zijn'.[15]

---

[11] Zie: B.P. Keller, P. Johnson, 'Online Anonymity: Who is John Doe?', *BNA Electronic Commerce & Law Report*, 2000, nr. 3, pp. 70-74; Zie in het VK de zaak *Totalise plc v. Motley Fool Ltd and another*, High Court, 19 February 2001; Vgl. ook het Memorandum hierover van The American Civil Liberties Union op http://www.aclu-wa.org/issues/privacy/bb.securities.litigation.2.26.01.html. Tevens: http://www.eff.org/Legal/Cases/Jane_Doe_v_John_Hritz/20001017_eff_janedoe_pr.html.
[12] Zie: http://www.economist.com/science/tq/displayStory.cfm?story_id=662374.
[13] K. Spaink, Parool 28 juni 1999; L. Asscher, Niemand als consument. Naar een evenwichtig grondrecht op anonimiteit', in: *De e-Consument. Consumentenbescherming in de Nieuwe Economie*, Elsevier 2000, pp. 7-19. Zie ook de diverse bijdragen in de speciale editie *Anonymous Communication on the Internet* van het tijdschrift *The Information Society,* http://www.slis.indiana.edu/TIS/tables_of_contents/toc_15.html#15-2. Verder: J.E.J. Prins, 'What's in a name. De juridische status van anonimiteit', *Privacy & Informatie*, no. 4 2000, pp 153-157. Zie tenslotte het overzicht van diverse anonimiseringsdiensten op: http://www.infosyssec.net/infosyssec/anon1.htm.
[14] *Handelingen II* 1999-2000, nr. 24, pp. 24.1807-24.1824.
[15] Raad voor het Openbaar Bestuur, 'ICT en het recht om anoniem te zijn', Den Haag, januari 2000. Beschikbaar via: http://www.rfv.nl/rob.

Hoewel de titel veel suggereert, gaat de Raad in het rapport zelf helaas nauwelijks in op de problematiek van anonimiteit. Verder nam de Commissie Grondrechten in het digitale tijdperk een eventueel grondrecht op anonimiteit in haar overwegingen mee. Maar de Commissie kwam vervolgens tot de conclusie dat een dergelijk recht onhaalbaar is omdat het in vele uiteenlopende situaties in het dagelijks leven zal moeten worden prijsgegeven: absolute anonimiteit is een illusie, aldus de Commissie.[16]
Men heeft op internationaal niveau eveneens oog voor het belang van anonimisering.[17] Zo stelt de Raad van Europa dat anonimiteit essentieel is voor privacybescherming op de elektronische snelweg.[18] Ook interessant is Recommendation 3/97 van de artikel-29 werkgroep, getiteld 'Anonymity on the Internet'.[19] De werkgroep noemt in deze aanbeveling diverse voorbeelden van anonimiserende diensten: bijvoorbeeld anonimiserende servers en remailers. Wanneer een afzender van een e-mailbericht of een nieuwsgroepbericht van deze laatste optie gebruikmaakt, ontdoet de aanbieder van de remailerdienst het bericht van de identificerende gegevens. Pas daarna wordt het doorgezonden aan de beoogd ontvanger van het bericht. De werkgroep wijst ook op de mogelijkheden die chipkaarten met een bepaald internet-tegoed bieden: namelijk de mogelijkheid om anoniem voor bepaalde diensten of producten te betalen.
Er zijn natuurlijk ook tegenstanders van een recht op anonimiteit. Het bericht eind 1999 dat het VVD-kamerlid Cherribi anoniem surf- en communicatiegedrag op internet strafbaar wilde stellen, zorgde voor veel commotie in de media. Aanleiding voor de actie van het kamerlid vormde de introductie in Nederland, door internet provider XS4All, van de Freedom-software. Een gebruiker kan met deze software zelf een anonieme elektronische identiteit ('nym') aanmaken. Er bestaan geen mogelijkheden tot terugkoppeling tussen de werkelijke naam van de gebruiker en de gekozen elektronische identiteit. Ook de internet provider als tussenpersoon kan de link tussen de beide identiteiten niet leggen.[20]

---

[16] Rapport van de Commissie Grondrechten in het digitale tijdperk, Den Haag mei 2000, p. 125. Beschikbaar via: http://www.minbzk.nl/gdt.

[17] Zie bijvoorbeeld art. 8, lid 3, van de Richtlijn elektronische handtekening. PbEG 2000 L 13/12.

[18] Guidelines Raad van Europa, 1997: " Guidelines for the protection of individuals with regard to the collection and processing of personal data on the information highways, which may be incorporated in or annexed to codes of conduct", Project Group on Data Protection, Council of Europe, 17 October 1997, CJ-PD (97) rev. , II, nr. 3.

[19] XV D/5022/97 final, 1997. Te raadplegen op de site van DG XV http://europa.eu.int/comm/internal_market.

[20] http://www.zeroknowledge.com/media/freedom-fs.asp.

Inmiddels schaart ook Minister van Boxtel zich kennelijk niet langer tot de groep mensen die meent dat de burger anoniem in zijn of haar communicatie met de overheid kan zijn. Naar aanleiding van de aanslagen in New York en Washington van september 2001, propageerde Van Boxtel de introductie van een algemene identificatieplicht.[21]

5. Nut of noodzaak?

De keuze voor een maatschappij waarin ruimte is voor (semi-)anonieme handelingen en transacties, lijkt haaks te staan op de wijze waarop (overheids)organisaties en bedrijven onze informatiemaatschappij inrichten. Immers, de huidige maatschappij wordt gekenmerkt door het gemak waarmee deze partijen gegevens vergaren en bewaren. Noodzakelijk voor de beoogde applicatie zijn vele van de verzamelde gegevens meestal niet: nuttig of mogelijk in de toekomst nuttig, kunnen ze het in de ogen van de verzamelaars zeer zeker wel zijn. Daarom zullen ze deze gegevens niet snel weggooien. De mogelijkheden van de technologie blijken daarbij vaak een dominante factor. Maar laten we deze ontwikkeling op zijn beloop, dan staan we wel voor de vraag: “nuttig ten koste van wat?”. Is het noodzakelijk om bij de elektronische tripperpas (de proef met de openbaar vervoer-chipkaart in het noorden van ons land) te werken met een gepersonaliseerd systeem? De chipkaart is gekoppeld aan een bank- of girorekening van de betreffende houder van de kaart, waarmee een soort volgsysteem worden opgezet. Met alle privacyconsequenties voor de betrokkene en zijn of haar familie van dien. Met de huidige stand van de technologie zijn er toch zeker minder ingrijpende – (semi-)anonieme – applicaties te bedenken?
De informatiezucht blijkt vaak ook gewoon voort te komen uit onachtzaamheid of gemakzucht. Aandacht voor nut dan wel noodzaak is dan ook vooral een kwestie van bewustwording. Veel toepassingen worden immers bijna klakkeloos voorzien van identificerende mechanismen. Bij een virtuele discussie op internet om de mening van de burgers te peilen over een bepaalde beleidsbeslissing (bijvoorbeeld een regionale herindeling of een milieunota) is het zeker niet noodzakelijk de geplaatste reacties te voorzien van adresgegevens. Een surftocht over internet laat echter zien dat het wel gebeurt.

Afwegingen tussen nut en noodzaak hebben alles te maken met de in het privacyrecht verankerde normen van proportionaliteit en subsidiariteit. Belangrijk is in dit kader artikel 8 van het Europees Verdrag van de Rechten van de Mens (EVRM).

---

21 ‘Van Boxtel wil identificatieplicht’, NRC Handelsblad 26 september 2001, p. 1, p. 7.

Proportionaliteit vereist in dit verband dat de beperking die de voorgestane applicatie betekent voor de persoonlijke levenssfeer, niet onevenredig mag zijn in verhouding tot het doel wat wordt nagestreefd. Het vereiste van subsidiariteit houdt in dat moet worden onderzocht of er voor het beoogde doel geen alternatieve applicaties zijn die minder ingrijpend zijn voor de persoonlijke levenssfeer. Kijken we vanuit deze twee normen met een kritische blik naar de beoogde toepassing en naar de persoonsgegevens die daarmee worden verzameld, dan zal blijken of de gemaakte keuzes gerechtvaardigd zijn in het licht van privacybescherming. Bij deze afwegingen kan de keuze tussen identificatie en verificatie een rol spelen. Overwegingen rondom identificatie en verificatie moeten daarom in een vroeg stadium worden betrokken in de keuze voor een (technisch) concept of voorziening. Hetzelfde geldt voor de uitwerking daarvan.

6. Transparantie

Lang niet altijd zal de afweging in het licht van proportionaliteit en subsidiariteit er toe leiden dat de keuze valt op een volstrekt anonieme toepassing. Er zijn zeker situaties waarin toch enige vorm van verificatie noodzakelijk zal blijken te zijn. Zoals in het eerdergenoemde voorbeeld van de betwisting van een rekening door de rekeninghouder bij een systeem van kilometerheffing.
Nog afgezien van de concrete privacyafwegingen, zal het personen die weigeren hun identiteit prijs te geven niet altijd gemakkelijk worden gemaakt. Zo zullen aanbieders van internetdiensten niet staan te springen om hun transacties af te handelen met een anonieme wederpartij. Dit kan immers tot problemen leiden als er een geschil ontstaat over de transactie. Verder moet de identiteit van een persoon op internet te achterhalen zijn wanneer de openbare orde wordt verstoord. Bijvoorbeeld in situaties waarin kinderporno op internet is geplaatst of een systeem is gehackt. De keuze om anoniem te blijven kan ook zo zijn prijs hebben. De Hoge Raad heeft nog op 27 februari 2001 in een strafzaak beslist dat verdachten die weigeren hun identiteit prijs te geven, geen rechtsmiddelen kunnen aanwenden tegen een eindvonnis dat tegen hen is gewezen.[22]
Tenslotte zien we dat diverse nieuwe wetgevingsprojecten voorwaarden stellen aan de kenbaarheid van de identiteit van de handelende personen. Bijvoorbeeld het wetsvoorstel ter implementatie van de 'Europese Richtlijn elektronische handel'[23] en de 'Europese

[22] HR 27 februari 2001, nr. 00293/00 NN. Zie hierover ook *Nieuwsbrief Strafrecht*, nr. 4 2001, pp. 110-11. De uitspraak is beschikbaar via Jurisprudentie Online: http://pubsys.wknl.com/JOL/straf, JOL-nummer 2001/175 of via http://pubsys.wknl.com/JOL/uitspraken/straf/week-2001-09/2001_175.html.
[23] Dit wetsvoorstel werd op 6 juli 2001 door het kabinet goedgekeurd en naar de Raad van State doorgestuurd. Zie: http://www.minjust.nl/c_actual/persber/pb0791.htm.

ontwerprichtlijn ter aanpassing van de regels betreffende BTW op bepaalde via elektronische middelen geleverde diensten'.[24]

Kortom, in bepaalde gevallen zal de verwerking van persoonsgegevens gerechtvaardigd of gewenst zijn.[25] Vertalen we dit naar de specifieke privacydimensie van het onderwerp, dan betekent het dat het van belang is dat de betrokkene ook echt weet dat zijn anonimiteit wordt opgeheven onder bepaalde omstandigheden. Dit brengt ons bij het belang van transparantie: Het moet aan de betrokkene duidelijk zijn hoe hij een spoor van persoonlijke gegevens achterlaat (ondanks de claim van anonimiteit) en in welke situaties deze gegevens worden gebruikt.
Concreet betekent dit dat als iemand gebruik wil maken van een anonieme toepassing, duidelijk moet zijn of er sprake is van echte anonimiteit of van pseudo-anonimiteit. Dit laatste omdat in bepaalde situaties met behulp van technieken of koppelingen toch persoonsgegevens in beeld kunnen komen. Deze transparantie kan ook gevolgen hebben voor organisaties die via hun internetsite informatie beschikbaar stellen of communiceren met externe partijen. Als ze daarbij claimen dat dit op volstrekt anonieme basis gebeurt, terwijl ondertussen wel een IP-adres wordt geregistreerd[26], dan moeten ze duidelijk maken dat er wel degelijk gegevens worden verzameld. Verder moeten ze aangeven in welke gevallen deze gegevens worden gebruikt. Dergelijke informatie kunnen ze verschaffen met een zogenoemd *privacy-statement*. Dit gebeurt bijvoorbeeld op de site 'ministervanboxtel.nl'. Bezoekers van de site kunnen hier duidelijk lezen welke gegevens worden verzameld en waarom dat gebeurt. Een dergelijke vorm van transparantie is voor informatieverwerkers zeker geen vanzelfsprekendheid. Dat wordt wel duidelijk bij een zoektocht naar andere voorbeelden van overheidssites met een dergelijke privacy-statement. Zomer 2001 blijft het helaas bij een zeer schamele oogst.[27] Wat dat betreft loopt de private sector – overigens onder invloed van eerdere ontwikkelingen in de VS – duidelijk voorop. Het lijkt er zelfs op dat het gebruik van een privacy-statement en het aanhaken bij een privacy-keurmerk een vorm van reclame en profilering begint te worden. Uit steeds meer onderzoek blijkt immers dat burgers en consumenten er de voorkeur aan geven elektronisch te communiceren met bedrijven die werken met statements en keurmerken.[28] Natuurlijk blijft het altijd de vraag in hoeverre bij het

[24] Zie: COM(2000) 349 final, *PbEG* 2000 C337E/65, 28/11/2000, Notice *PbEG* C 337/E/07. Te vinden op: http://europa.eu.int/comm/taxation_customs/proposals/taxation/com349_2000/com2000_349nl.pdf.
[25] Afgezien overigens van de vraag of het inderdaad noodzakelijk is dat in de genoemde wetgevingsvoorstellen een plicht wordt opgenomen tot kenbaarheid van de identiteit.
[26] Aan de hand waarvan middels bepaalde koppelingen toch de achterliggende persoon herleidbaar is.
[27] Zie voor een ander voorbeeld de site van de Registratiekamer, http://www.registratiekamer.nl.
[28] Zie hierover: *Privacy Laws & Business International Newsletter*, mei 2001, pp. 20-21.

hanteren van een privacy-statement niet uitsluitend sprake is van een optische privacybescherming. Privacybescherming komt uiteindelijk dan ook neer op fatsoen en fatsoenlijke omgangsvormen. Er moet respect zijn voor de wederzijdse belangen en vanuit die gedachte moeten beide partijen elkaar ook de nodige duidelijkheid verschaffen.

7. Keuzevrijheid

Bij de afweging tussen nut en noodzaak kan het natuurlijk ook zo zijn dat de verzameling van de gegevens tevens in het voordeel van de betrokkene zelf is. Bijvoorbeeld bij applicaties op het terrein van de mobiliteit op de wegenverkeersinfrastructuur: voordelen voor de automobilist kunnen hier zijn gelegen in additionele *in-car* telematicafaciliteiten. Zoals informatie over files in de buurt, snelle service bij pech of een ongeval aan de hand van GPS-ontvangers of actuele informatie over aanbiedingen bij het te passeren tankstation van een bepaalde benzinemaatschappij. Het verzamelen van persoonsgegeven voor dergelijke applicaties is nuttig, maar is niet noodzakelijk voor de beoogde invoering van een systeem voor het verhogen van de verkeersmobiliteit.
Uitgangspunt bij deze 'nuttige' applicaties moet zijn, dat pas dan iets uit de gegevensverzameling wordt afgeleid als dit door de gebruiker zelf is aangegeven. Kortom, een systeem van opt-in. Zolang een persoon niet kenbaar heeft gemaakt dat deze prijs stelt op de (nuttige) informatie, mogen zijn persoonsgegevens daartoe niet worden gebruikt. Vervolgens geldt ook voor deze situaties dat transparantie een voorwaarde is: welke gegevens worden precies verzameld, voor welke gebruikers en voor welke doeleinden?

8. Tenslotte

In het voorgaande is al aangegeven dat privacybescherming meer is dan het naleven van een stelsel van wettelijke regelingen, zoals neergelegd in onder meer de Wbp. Privacybescherming komt voor een groot deel neer op maatschappelijk fatsoen en fatsoenlijke omgangsvormen. Hierbij is er respect voor de wederzijdse belangen. Vanuit die gedachte wordt aan elkaar ook de benodigde duidelijkheid verschaft om aan deze belangen recht te kunnen doen. Privacybescherming – en dus de afweging om al dan niet te kiezen voor een (semi-)anonieme vorm van gegevensverzameling – is daarom een maatschappelijk 'probleem'. Niet een aangelegenheid die uitsluitend op het bordje van individuele actoren (verwerker en betrokkene) ligt. Dit laatste wil overigens zeker niet

zeggen dat deze individuele actoren niet een eigen verantwoordelijkheid hebben om privacybescherming te realiseren in een concrete situatie.[29]
We moeten als maatschappij echter niet achteroverleunen in de veronderstelling dat de nieuwe wet (Wbp) per 1 september 2001 een ieder heeft voorzien van de noodzakelijke instrumenten en dat daarmee de klus is geklaard. Het maatschappelijk en economisch belang verdient nadrukkelijk aandacht. Dit blijkt onder andere uit de constatering dat elektronische handel en een elektronische overheid nooit echt van de grond zullen komen als consumenten en burgers niet voldoende vertrouwen hebben in privacybescherming op internet. Maar ook meer fundamenteel is privacybescherming een maatschappelijk punt van aandacht. We staan met afwegingen rondom identiteit, kenbaarheid, verifieerbaar en anonimiteit voor de centrale vraag welk soort samenleving we wensen en creëren: een maatschappij waarin 'kenbaarheid, tenzij …' het uitgangspunt is of een samenleving waarin 'anonimiteit, tenzij ….' het vertrekpunt is? Daarbij spelen vragen als waar leggen we het evenwicht van informatiemachten en hoe rusten we de diverse partijen toe om dit evenwicht te bereiken (transparantie, opt-in, etc.)? En: hoe organiseren en reguleren we vervolgens het vertrouwen van de partijen in een dergelijk samenleving? Dit mede met het oog op de vraag of het handelen van actoren inderdaad conform dit evenwicht plaatsvindt. In essentie raken we met deze vragen de centrale kwestie: wat is het *doel* van (technologische) keuzes die we maken, de applicaties die we daarmee vervolgens realiseren en de persoonsgegevens die we met behulp daarvan al dan niet verzamelen?

[29] Vgl. hierover: J.E.J. Prins, 'De bescherming van persoonsgegevens: de betrokkene betrokken', *Privacy & Informatie*, 1998/1, pp. 11-14.