JURISPRUDENTIE

Bodil Lindqvist / Koninkrijk Zweden
Noot bij Europees Hof van Justitie 6 november 2003 (Zaak C101/01)[1]

GERRIT-JAN ZWENNE* **Bodil Lindqvist werkt als vrijwilliger in een kerkgemeente van de Protestantse Kerk van Zweden. Eind 1998 heeft zij een computercursus gevolgd en met de daarmee verkregen kennis heeft zij op haar eigen computer een website gebouwd. Op deze website heeft zij allerlei, waarschijnlijk nuttige informatie voor aankomende gemeenteleden geplaatst, zoals voor en achternamen van haarzelf en achttien collega's. Verder heeft Lindqvist 'in licht humoristische bewoordingen' een beschrijving gegeven van de werkzaamheden van haar collega's en hun liefhebberijen. In een aantal gevallen werden hun gezinssituatie, hun telefoonnummer en andere gegevens vermeld. Over een collega merkte zij op dat deze haar voet heeft bezeerd en met ziekteverlof is.**

Lindqvist heeft de betreffende collega's niet van het bestaan van deze website op hoogte gesteld en heeft ook geen toestemming van hen verkregen voor het opnemen van hun gegevens. Evenmin heeft zij haar de gegevensverwerkingen op haar website aangemeld bij de Zweedse privacytoezichthouder ('Datainspektion'). Echter, toen zij hoorde dat enkele van de betreffende collega's er bezwaar tegen maakten dat hun gegevens waren opgenomen, heeft zij deze gegevens wel verwijderd.

Een en ander is voor het Zweedse openbaar ministerie aanleiding om over te gaan tot strafrechtelijke vervolging wegens schending van de Zweedse privacywetgeving ('Personupgiftslag' SFS 1998, nr. 204'). In de telastelegging wordt Lindqvist verweten dat zij in strijd met de privacywet heeft gehandeld doordat zij onder andere persoonsgegevens heeft verwerkt zonder dit vooraf schriftelijk aan de privacytoezichthouder te melden en ook doordat zij zonder toestemming van de betreffende collega's de persoongegevens heeft doorgegeven naar een land buiten de Europese Unie.

* Gerrit-Jan Zwenne is advocaat bij Bird & Bird in Den Haag. Daarnaast is als universitair docent verbonden aan het Centrum eLaw@Leiden van de Faculteit der Rechtsgeleerdheid van de Universiteit Leiden en fellow bij het E.M. Meijers Instituut van dezelfde faculteit. E-mail: gerrit-jan.zwenne@twobirds.com

De rechter ('Eksö tingsrätt') acht de feiten bewezen en Lindqvist schuldig, en legt haar een boete op van 4000 Zweedse kronen, een bedrag dat overeenkomt met ongeveer 450 euro.[2] Daarnaast moet zij 300 kronen, ongeveer 33 euro, betalen aan een fonds voor slachtofferhulp. Lindqvist is het daar niet mee eens. Zij erkent de feiten maar vindt dat zij de wet niet heeft overtreden en gaat in beroep. De beroepsrechter ('Göta hovrät') komt er niet uit en stelt het Europees Hof van Justitie zeven prejudiciële vragen over de uitleg en toepassing van de privacyrichtlijn 95/46[3] – de richtlijn waarop de Zweedse en andere nationale privacywetten van de lidstaten van de Europese Unie zijn gebaseerd. De antwoorden van het Hof zijn dan ook niet alleen van belang voor de uitleg en toepassing van de Zweedse privacywet, maar ook voor de andere nationale privacywetten, zoals in Nederland de Wet bescherming persoonsgegevens ("Wbp").

Aan het arrest van het Hof is in uiteenlopende juridische tijdschriften de nodige aandacht besteed. Dat is begrijpelijk. Het arrest is niet alleen van belang voor iedereen die wel eens een website bouwt of onderhoudt, maar ook in meer algemene zin voor iedereen die zich bezig houdt met Europees recht of met privacy- en andere mensenrechten.[4]

De zeven aan het Hof gestelde prejudiciele vragen zien *grosso modo* op drie onderwerpen die direct of indirect voor internet van belang zijn:

- Een eerste onderwerp betreft de reikwijdte of werkingssfeer van de richtlijn. Het betreft de vraag of de privacyrichtlijn van toepassing is op het opnemen van naam- en andere gegevens op een website moet worden aangemerkt als «een geautomatiseerde verwerking van persoonsgegevens». Als deze vraag bevestigend wordt beantwoord is er vervolgens de vraag of deze verwerking valt onder een van de uitzonderingen van de richtlijn, zodat deze toch niet van toepassing is.
- Een tweede onderwerp houdt verband met de strenge regels die richtlijn geeft voor het doorgeven van persoonsgegevens naar landen buiten de Europese Unie, in de richtlijn aangeduid als 'derde-landen'. De vraag is er sprake is van zo een doorgifte als persoonsgegevens worden opgenomen op een website die op een server in Zweden is opgeslagen, waardoor de gegevens in een derde-land toegankelijk worden.
- Een derde onderwerp, tenslotte, betreft de vraag of de richtlijn een beperking vormt die in strijd is met de algemene beginselen van vrijheid van meningsuiting of andere in de EU geldende vrijheden of rechten, die onder meer zijn neergelegd in artikel 10 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden ("EVRM").

Is de richtlijn van toepassing? De richtlijn, en dus ook de nationale privacy-wetgeving, is van toepassing op de geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens, maar niet als het gaat om (a) verwerkingen in het kader van activiteiten die niet binnen de werking van het gemeenschapsrecht vallen,

of om (b) activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden. Dit staat in artikel artikel 3, eerste en tweede lid, van de richtlijn, en in artikel 2, eerste lid en tweede lid, onder a, van de Wbp.
De op de website opgenomen gegevens hebben betrekking op geïdentificeerde of identificeerbare natuurlijke personen, en dat betekent dat deze gegevens inderdaad vallen onder het begrip persoonsgegevens, zoals gedefinieerd in artikel 2, onder a, van de richtlijn en artikel 1, onder a, Wbp. Het opnemen van deze gegevens op de website betekent dat deze gegevens worden verwerkt in de zin van artikel 2, onder b, van de richtlijn en artikel 1, onder b, Wbp, en dat gebeurt met geautomatiseerde middelen, nl. de computer waarop de betreffende webpagina's zijn gebouwd en de server waarop deze webpagina's worden aangeboden. En dat allemaal betekent dat het op een website opnemen van gegevens, zoals naam en telefoonnummer en gegevens over liefhebberijen en werksituaties, moet worden aangemerkt als een geautomatiseerde verwerking van persoonsgegevens, waarop de richtlijn en dus ook de nationale privacywetgeving van toepassing is.[5]
De vraag of deze gegevensverwerking onder één van de uitzonderingen van de richtlijn valt, is minder eenvoudig te beantwoorden. De eerste uitzondering die in aanmerking komt betreft de gegevensverwerkingen in het kader van activiteiten die niet binnen de werking van het gemeenschapsrecht vallen. Daarbij moet, zo blijkt uit de tekst van de richtlijn, worden gedacht verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de staat en de activiteiten van de staat op strafrechtelijk gebied. Anders dan Lindqvist (en de Zweedse regering en de Advocaat Generaal) vindt het Hof dat daaronder niet ook andere activiteiten moeten worden begrepen dan die van staten of de overheidsdiensten. Om deze reden vallen vrijwilligerswerk of religieuze activiteiten niet onder deze uitzondering.[6]
De reden waarom het Hof kiest voor een beperkte uitleg van deze uitzondering (en dus voor een brede werkingssfeer van de richtlijn) houdt verband met de rechtszekerheid. Volgens het Hof heeft iedere andere uitleg het risico dat de grenzen van de werkingssfeer bijzonder onzeker en vaag worden, wat in strijd zou zijn met de belangrijkste doelstelling van de richtlijn, namelijk het harmoniseren van wettelijke bepalingen van de lidstaten.[7]
De tweede in aanmerking komende uitzondering betreft die voor de verwerkingen die worden gedaan door een natuurlijk persoon ten behoeve van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden. Het Hof overweegt dat Lindqvist ook niet van deze uitzondering kan gebruik maken, en wel omdat deze uitzondering beperkt is tot activiteiten die tot het persoonlijke of gezinsleven van particulieren behoren. En daarvan was bij de website van Lindqvist geen sprake omdat zij de gegevens voor een onbepaald aantal personen toegankelijk had gemaakt. Dit was mogelijk anders geweest als Lindqvist haar website alleen had bekend gemaakt aan de leden van haar kerkgemeente, bijvoorbeeld door de website af te schermen met behulp van een wachtwoord. Maar dan nog was het de vraag geweest of deze gemeenteleden tot haar «persoonlijke leven» kunnen worden gerekend.

Een en ander betekent dat de richtlijn onverkort van toepassing is op opnemen van persoonsgegevens op de website.[8] Ik kan mij daar, met een enkele kanttekening, wel in vinden. Natuurlijk is de richtlijn, en dus ook de nationale privacywetgeving, van toepassing op het opnemen van persoonsgegevens op een website en de verwerkingen van persoonsgegevens in het kader daarvan. En inderdaad ligt het niet erg voor de hand dat deze verwerkingen onder een van de uitzonderingen van de richtlijn kunnen worden gebracht. Een andere uitleg zou de betekenis van de richtlijn wel heel erg marginaliseren. En dat kan niet de bedoeling zijn.
Daarbij past, zoals gezegd, een enkele kanttekening. Allereerst een kanttekening over de in artikel 27 Wbp neergelegde verplichting om gegevensverwerkingen aan te melden bij het College bescherming persoonsgegevens (" Cbp"). Omdat het veelal gaat om betrekkelijk ongevaarlijke verwerkingen, ligt het in de rede dat gebruik wordt gemaakt van de in artikel 30 Wbp geregelde mogelijkheid om voor dergelijke verwerkingen vrij te stellen van de meldplicht van artikel 27 Wbp. Dit kan door in het zogeheten Vrijstellingsbesluit een dergelijke vrijstelling op te nemen.[9]
Verder kan ik mij, evenals de Commissie,[10] voorstellen dat veel van de verwerkingen in het kader van een website kunnen worden gebracht onder de (beperkte) uitzondering die de richtlijn maakt voor verwerkingen voor journalistieke of voor artistieke of literaire doeleinden. Dat betekent dan dat een aantal bepalingen in de richtlijn, zoals onder andere die over de melding van verwerkingen bij de privacytoezichthouder en die over de doorgifte van persoonsgegevens naar derde-landen, niet van toepassing is. Over de doorgifte naar derde-landen meer in de volgende paragraaf.

Is er sprake van doorgifte? Een volgende, voor de rechtspraktijk belangrijke vraag die het Hof beantwoord, is of het beschikbaarstellen van persoonsgegevens op een website moet worden aangemerkt als doorgifte van persoonsgegevens naar een land buiten de Europese Unie. Als dat het geval is, betekent dat dat de extra strenge vereisten, neergelegd in artikel 25 en 26 van de richtlijn en artikel 76 en 77 Wbp, van toepassing zijn. In dat geal kan het zijn dat voor de doorgifte van de gegevens gebruik moet worden gemaakt van een door de Commissie goedgekeurd standaard gegevensexport-contract en/of dat daarvoor een exportvergunning van de Minister van Justitie moet worden verkregen, of dat degenen op wie de gegevens betrekking hebben eerst ondubbelzinnige toestemming moeten hebben gegeven voor de doorgifte. Deze strenge regels beogen te voorkomen dat de geharmoniseerde privacyregels in de Europese Unie worden ontdoken door de gegevens door te geven naar een land buiten de EU dat mogelijk niet eenzelfde beschermingsniveau biedt (zeg: China, India, de Fileppijnen of een ander land dat zich profileert door middel van uiteenlopende hoogwaardige outsourced IT-services).[11]

Als het het beschikbaarstellen van persoonsgegevens op een website gelijk zou worden gesteld met doorgifte naar zo een derde-land, zijn de implicaties

verstrekkend. Het zou betekent dat een website-aanbieder ofwel moet voldoen aan de genoemde extra strenge vereisten, of wel zijn website zo ingericht dat deze alleen kan worden opgevraagd vanuit EU-landen en landen met een passend beschermingsniveau. Het is duidelijk dat zowel het een als het ander zou leiden tot allerlei, gebruiksonvriendelijke beperkingen – als het al geen onbegonnen werk is. Veel gewone en onschuldige websites, zoals detelefoongids.nl en websites met uitslagen van studentenroeiwedstrijden of schoolschaakkampioenschappen, zouden beperkt toegankelijk moeten worden gemaakt. Of er zou op allerlei geconstrueerde manieren ondubbelzinnige toestemming moeten worden verkregen van degenen over wie de gegevens worden bekend gemaakt. Allemaal niet erg praktisch en, gelet op het belang van privacybescherming, ook niet nodig.
Het Hof ziet dat gelukkig ook en komt tot het oordeel dat het niet de bedoeling van de richtlijn is dat het plaatsen van gegevens op een website, die ook toegankelijk is voor personen uit derde landen, wordt gelijkgesteld met een doorgifte van gegevens naar een derde land. Het Hof komt tot deze conclusie na een analyse van de handelingen die een internetgebruiker moet doen om te kunnen beschikken over de persoonsgegevens op een website:

> *"…om toegang te krijgen tot de informatie op de internetpagina waarop Lindqvist gegevens over haar collega's had geplaatst, [dient een internetgebruiker] niet alleen een verbinding met internet te maken maar diende hij ook eigenhandig de voor het raadplegen van die pagina's nodige handelingen te verrichten. Met andere woorden, de internetpagina's van Lindqvist bevatten niet de technische middelen waardoor die informatie automatisch had kunnen worden verzonden aan personen die niet bewust toegang tot die pagina's hadden proberen te krijgen."*

Volgens het Hof is er dus geen sprake van een rechtstreekse doorgifte, maar van een 'niet-rechtstreekse doorgifte' via de informatica-infrastructuur van de hosting provider waar de website opgeslagen. Vervolgens gaat het Hof in op de bedoelingen van de gemeenschapswetgever met betrekking tot zo een niet-rechtstreekse doorgifte. Het stelt vast dat de gemeenschapswetgever niet ingaat op het het gebruik van internet, en dat deze geen criteria heeft vastgesteld om te bepalen of voor de door tussenkomst van de hosting provider verrichte handelingen moet worden uitgegaan van de plaats van vestiging van de provider dan wel van de plaats(en) waar zich de computers bevinden die de informatica-infrastructuur van de provider vormen. Het Hof leidt daar uit af dat de gemeenschapswetgever niet heeft stilgestaan bij de mogelijkheden die het internet biedt, en dat om deze reden het begrip 'doorgifte' niet betrekking heeft op het opnemen van persoonsgegevens op een website. Het Hof zegt het zo:

> "*Gezien de ontwikkeling van internet ten tijde van de opstelling van richtlijn 95/46 en het ontbreken van criteria voor het gebruik van internet in hoofdstuk IV [het hoofdstuk over doorgifte GJZ], kan niet worden aangenomen dat het de bedoeling was van de*

> *gemeenschapswetgever, vooruitlopend op latere ontwikkelingen, het begrip doorgifte van gegevens naar een derde land ook te laten gelden voor de handeling van een persoon in de situatie van Lindqvist die gegevens op een internetpagina plaatst, ook wanneer die gegevens daarmee toegankelijk worden gemaakt voor personen uit derde landen die de technische middelen hebben om zich toegang daartoe te verschaffen*.".

De strenge regels voor de doorgifte van persoonsgegevens zijn dus niet van toepassing op websites waar persoonsgegevens ter beschikking worden gesteld aan personen die zich mogelijk bevinden in zo een derde-land. Deze redenering is niet onbegrijpelijk, maar overtuigt toch ook niet. De richtlijn heeft inderdaad geen criteria voor het gebruik van internet en websites, maar evenmin voor het gebruik van e-mail of mobiele telefoons of sms-berichten of cd-roms en re writable dvd's, of de opslagmedia in mp3-spelertjes en digitale camera's, voor Napster en KazAa of andere P2P-achtige toepassingen, of wat dan ook. En toch komt het mij voor dat de doorgifteregeling zonder meer van toepassing als persoonsgegevens met behulp van deze middelen worden doorgegeven naar landen buiten de EU. Dat de gemeenschapswetgever indertijd daaraan niet heeft gedacht, doet daar niet aan af. Waarom dat voor webpagina's anders zou zijn, is mij niet duidelijk.
Andere redeneringen waren ook mogelijk geweest. In haar bij het Hof ingediende schriftelijke opmerkingen stelt de Nederlandse regering, in overeenstemming met de door het Cbp voorgestane uitleg,[12] zich op het standpunt dat moet worden uitgegaan van de bedoeling van degene die de gegevens al dan niet doorgeeft. De regering stelt dat het begrip doorgifte moet worden opgevat als een activiteit die bewust is gericht op het doorgeven van persoonsgegevens van het grondgebied van een lidstaat naar een derde land. Vervolgens houdt de regering vast aan een technologieneutrale uitleg en stelt zich op het standpunt dat er geen onderscheid kan worden gemaakt tussen de verschillende vormen waarin gegevens voor derden toegankelijk kunnen worden gemaakt. De conclusie is dan dat, in het onderhavige geval, het met behulp van een computer plaatsen van persoonsgegevens op een website niet kan worden beschouwd als een doorgifte van persoonsgegevens naar een derde land. Dit kan, zo begrijp ik onze regering, anders zijn als de website wél zou zijn gebouwd met de bedoeling om de gegevens door te geven.[13]
Deze uitleg van het doorgifte-begrip verhoudt zich niet goed met de omstandigheid dat de richtlijn uitgaat van gegevensbescherming ongeacht de relevantie in de context van de bescherming van de persoonlijke levenssfeer – de richtlijn geldt nadrukkelijk ook als er geen direct privacybelang is.[14] Toch komt mij de redenering van de Nederlandse regering als redelijk voor, en wel omdat daarmee in elk geval opzichtige ontduikingsconstructies kunnen worden aangepakt. Ik denk dan aan, bijvoorbeeld, een door middel van een wachtwoord afgeschermde website, waarop een internationaal opererend concern werknemers- of klantgegevens opneemt, die vervolgens met behulp van dat wachtwoord kunnen worden gedownload door dochtervennootschappen buiten de Europese Unie. Omdat het duidelijk is dat deze website bewust is gericht op het doorgeven van de gegevens, is er in de redenering

van de Nederlandse regering waarschijnlijk in dat geval wél sprake van doorgifte. En dat komt voor als alleszins verdedigbaar.
De regering van het Verenigd Koninkrijk gaat uit van een andere uitleg, namelijk een waarin onderscheid wordt gemaakt tussen enerzijds het terbeschikking stellen of toegankelijk maken van gegevens en anderszijds het verzenden daarvan. Alleen in het laatste geval is er volgens deze regering sprake van doorgifte. In deze uitleg hebben de doorgiftebepalingen in de richtlijn betrekking op de doorgifte van gegevens naar derde landen, maar niet op de vraag of zij vanuit derde landen toegankelijk zijn. Het begrip doorgifte houdt in dat een gegeven door een zich op een bepaalde plaats bevindende persoon wordt verzonden naar een zich op een andere plaats bevindende derde. Het opnemen van persoongegevens op een website is iets anders dan het verzenden van de gegevens en valt dus niet onder het doorgifte-begrip.[15] In het voorbeeld van het internationaal opererend concern, dat ik zo even noemde, zou deze uitleg vermoedelijk ertoe leiden dat er géén sprake is van doorgifte omdat er geen gegevens worden verzonden maar alleen beschikbaar gesteld. Daarmee staat de weg open voor allerlei ontduikingsconstructies en daarom is deze uitleg, hoewel begrijpelijk, niet goed verdedigbaar.

In het arrest heeft het Hof enerzijds onderkend dat het opnemen van persoonsgegevens op een website niet, zoals de Zweedse regering en de Commissie stelden, zonder meer als doorgifte kan worden aangemerkt. Maar anderszijds heeft het Hof ook niet willen laten gebeuren dat er een gat zou worden geschoten in de doorgifte-regeling, wat het geval zou zijn geweest als zou worden uitgegaan van de uitleg die Engelse regering geeft. Tegelijkertijd wilde heeft het Hof niet zover willen gaan, dat zou worden uitgaan van de bedoelingen van degene die de gegevens op een website heeft geplaatst. Ik heb de indruk dat het Hof, mogelijk om te voorkomen dat de werkingssfeer van de doorgifte-regeling onduidelijk wordt,[16] een specifieke uitzondering heeft geformuleerd die hij vervolgens zo beperkt mogelijk heeft omschreven, namelijk door aan te geven dat deze alleen geldt "voor de handeling van een persoon in de situatie van Lindqvist die gegevens op een internetpagina plaatst", dat wil zeggen voor de situatie waarin:

> "…*een persoon in een lidstaat persoonsgegevens plaatst op een internetpagina bij zijn in dezelfde of in een andere lidstaat gevestigde hosting provider, en deze persoonsgegevens aldus toegankelijk maakt voor eenieder die een internetverbinding tot stand brengt, met inbegrip van personen die zich in derde landen bevinden*".[17]

Om dat te kunnen doen moest het Hof wel uitgaan van de (veronderstelde) bedoelingen van de gemeenschapswetgever. Zoals gezegd, erg overtuigend is dat niet. Maar gegeven het voorgaande kon het Hof misschien ook niet anders.
Een van de gevolgen van deze uitleg is dat de richtlijn veel minder technologieneutraal blijkt te zijn dan wel werd aangenomen.[18] Het Hof heeft aan de hand van de bedoelingen van de gemeenschapswetgever een technologiespecifieke

uitzondering geformuleerd. De vraag is dan of er nog andere van dergelijke uitzonderingen denkbaar zijn. Zoals ik al eerder aangaf, zijn er nog wel meer toepassingen en technologische ontwikkelingen waarvoor de richtlijn geen criteria geeft en waarmee de gemeenschapswetgever geen rekening heeft kunnen houden. Waartoe dit gaat leiden is niet duidelijk. Ik sluit niet uit er nog meer afstand zal worden genomen van het uitgangspunt dat de regelgeving zoveel mogelijk technologieonafhankelijk moet zijn. De regelgeving wordt daardoor niet eenvoudiger, maar dat waren privacyregels toch al niet. Voor privacyjuristen is dat natuurlijk niet verkeerd.

Is de richtlijn in strijd met de vrijheid van meningsuiting? Om deze vraag te beantwoorden stelt het Hof vast dat er een spanning bestaat tussen de enerzijds doelstelling van het vrije gegevensverkeer en anderszijds de bescherming van persoonsgegevens. Echter, zowel de richtlijn als de omzetting daarvan in nationale privacywetgeving bieden de mogelijkheden om de betrokken rechten en belangen tegen elkaar te wegen. Het juiste evenwicht moet worden gevonden bij de toepassing van deze wetgeving. Daarbij komt onder andere betekenis toe aan de grondrechten, zoals de vrijheid van meningsuiting. Als zodanig bevatten dat de bepalingen van de richtlijn volgens het Hof dan ook geen beperking die in strijd is met de vrijheid van meningsuiting of met andere in de Europese Unie geldende rechten en vrijheden, zoals vastgelegd in artikel 10 EVRM.
Dit is niet verrassend. In de Nederlandse rechtspraktijk zijn er verschillende uitspraken waarin de rechter, bijvoorbeeld in het kader van de belangenafweging van artikel 8, onder f, van de Wbp, het belang bij het recht op uitingsvrijheid afweegt tegen dat van de bescherming van de persoonlijke levenssfeer en andere belangen. Een recent voorbeeld is een, door de betreffende voorzieningen rechter als schrijnend aangeduide procedure over het vermelden van persoonlijke gegevens van holocaust-slachtoffers op een website waarmee de Stichting Digitaal Monument Joodse Gemeenschap eer wilde betonen aan de Joodse gemeenschap.[19]

Ter afsluiting. Het Lindqvist-arrest is in verschillende opzichten belangrijk voor iedereen die iets van doen heeft met websites waarop persoonsgegevens worden opgenomen. Het opnemen van deze persoonsgegevens valt zonder meer onder de privacywetgeving. Er moet dus rekening worden gehouden met de voorwaarden die deze privacywet stelt, zoals de verplichting om de verwerkingen, behoudens de websites met uitsluitend journalistieke, artistieke of literaire doeleinden, aan te melden bij het CBP. Dat is, met het oog op de rechten en belangen van degenen over wie gegevens worden opgenomen, niet echt zinvol. Daarom ligt het in de rede dat de wetgever in Nederland daarvoor – liever vandaag dan morgen – een vrijstelling opneemt in het Vrijstellingsbesluit.
Dat het opnemen van persoongegevens op een website niet gelijk kan worden gesteld met doorgifte naar een derde-land, ligt voor de hand. Maar de redenering waarlangs het Hof daartoe is gekomen, doet wel af aan het uitgangspunt van

technologieonafhankelijkheid. De wetgeving wordt daardoor niet eenvoudiger. Dat de belangen bij het recht op bescherming van pesroonsgegeven moeten worden afgewogen tegen andere belangen, waaronder de belangen bij de vrijheid van meningsuiting, is niet nieuw.

Een niet helemaal onbelangrijke vraag, waar ik nog niet op ben ingegaan, is wat Bodil Lindqvist ervan vindt. Op haar website, die gelukkig nog steeds beschikbaar is,[20] doet zij de volgende triomfantelijke (?) mededeling: "Och rättvisans kvarnar mal långsamt! Men väl!". Dat betekent, vrij vertaald: "de molens van de rechtspraak draaien langzaam, maar zeker". Of daaruit kan worden opgemaakt, dat zij wel kan leven met het arrest is niet helemaal duidelijk.

De links bij deze jurisprudentiebespreking vindt u op www.javisite.nl.

[1] Het Lindqvist-arrest is te vinden op de website van het Europees Hof van Justitie: http://curia.eu.int
[2] In het randnr. 17 van het arrest wordt opgemerkt dat het door Lindqvist te betalen bedrag, gelet op haar financiele situatie, was berekend op 100 Zweedse kronen (ca. 11 euro). Dit bedrag is wegens de ernst van inbreuk (!) met een factor 40 verhoogt.
[3] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *PbEG* L 281 van 23/11/1995.
[4] Peter Blok, 'Inkomens, internet en informationele privacy' *NTER* 2004-1/2, p. 30-36; Jan Berkvens, 'De Lindqvist-case of de onbevlekte ontvangenis van persoons-gegevens', *Privacy en Informatie* 2004-1, p. 17-20; Herke Kranenborg, 'Pas op met wat je op je homepage zet! Publicatie van persoonsgegevens op Internet beschermd door Europese regelgeving' *NJCM-bulletin* 2004-3.
[5] Zie randnrs. 24 t/m 27 van het arrest.
[6] HvJEG van 20 mei 2003, C-465/00, C-138/01 en C-139/01 (Österreichiser Rundfunk e.a.)
[7] Zie randnrs. 41 en 42 van het arrest.
[8] Een andere, voor de rechtspraktijk minder interessante vraag is of er ook sprake is van 'bijzondere gegevens', zoals gezondheidsgegevens, waarvoor de richtlijn veel strengere eisen stelt dan voor 'gewone gegevens'. Dit begrip wordt ruim uitgelegd (vgl. *kamerstukken II* 1997-1998, 25892, nr. 3, p 102, 109 en 167) en daarom is het geen verrassing dat het Hof stelt dat daarvan inderdaad sprake is waar Lindqvist de voetblessure van haar collega noemt. Zie randnrs. 49 t/m 51 van het arrest.
[9] Besluit van 7 mei 2001, houdende aanwijzing van verwerkingen van persoonsgegevens die zijn vrijgesteld van de melding bedoeld in artikel 27 van de Wet bescherming persoonsgegevens ("Vrijstellingsbesluit"), *Stb.* 2001, 250.
[10] Zie randnr. 33 van het arrest.
[11] Zie Daniel H. Pink, 'The New Face of the Silicon Age', *Wired Magazine*, Februari

2004, p. 94-103.
[12] D. Alonso Blas, De doorgifte van persoonsgegevens naar derde landen in het kade van de Wbp, College bescherming persoonsgegevens, 2003, p. 7 en []
[13] Zie randnr. 54 van het arrest.
[14] Vgl. Jan Berkvens, 'De Lindqvist-case of de onbevlekte ontvangenis van persoonsgegevens', *Privacy en Informatie* 2004-1, p. 19
[15] Zie randnr. 55 van het arrest.
[16] Vgl. ook randnrs. 41 en 44 van het arrest en mijn opmerkingen daarover bij in de vorige paragraaf van deze annotatie.
[17] Resp. randnrs. 68, 70 en 71 van het arrest
[18] Vgl. bijv. *kamerstukken II* 1997-1998, 25892, nr. 3, p. 41; daarover Peter Blok, 'Inkomens, internet en informationele privacy' *NTER* 2004-1/2, p. 36
[19] Vzr. Rb. Den Haag 11 december 2003, LJN-nr. AN9893 (Zknr: KG 03/1363 AB)
[20] Zie http://biphome.spray.se/mors