De meldplicht voor datalekken in de Telecommunicatiewet

Zuiderveen Borgesius, F.J.

Publication date
2011
Document Version
Author accepted manuscript
Published in
Computerrecht

Mr. F.J. Zuiderveen Borgesius[1]

De meldplicht voor datalekken in de Telecommunicatiewet

99

Het Wetsvoorstel wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen introduceert een meldplicht voor inbreuken in verband met persoonsgegevens. Aanbieders van openbare elektronische communicatiediensten moeten zulke datalekken voortaan melden aan OPTA, de Onafhankelijke Post en Telecommunicatie Autoriteit. Als een datalek waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van degene wiens persoonsgegevens het betreft, moeten aanbieders ook deze inlichten. In dit artikel wordt deze regeling besproken. Daarbij zal blijken dat er nog een aantal onduidelijkheden zijn. Ook wordt ingegaan op de vraag in hoeverre de meldplicht geschikt is om de doelen die de Europese regelgever nastreeft te bereiken. Geconcludeerd wordt dat een meldplicht nut kan hebben, maar dat de effectiviteit van de meldplicht aanzienlijk wordt beperkt doordat hij slechts geldt voor aanbieders van openbare elektronische communicatiediensten. Zelfs als een bredere meldplicht ingevoerd zou worden, zijn meer maatregelen nodig om alle genoemde doelen te bereiken.

1. Inleiding

Moderne communicatiemiddelen en steeds goedkoper wordende digitale opslagmethoden maken het leven een stuk aangenamer, maar stellen ons ook voor nieuwe uitdagingen. De enorme toename van de verwerking van persoonsgegevens brengt een aantal gevaren met zich mee. De media berichten voortdurend over datalekken en mogelijke gevolgen zoals identiteitsdiefstal.[2] Zo kregen hackers onlangs toegang tot de creditcardgegevens van tientallen miljoenen klanten van SONY.[3]

Dit artikel behandelt de meldplicht voor datalekken in het Wetsvoorstel wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen ('wetsvoorstel').[4] Voortaan moeten aanbieders van openbare elektronische communicatiediensten ('aanbieders') inbreuken in verband met persoonsgegevens melden aan OPTA.[5] Als een dergelijk datalek waarschijnlijk ongunstige gevolgen zal hebben voor degene wiens persoonsgegevens het betreft, moet ook deze worden ingelicht.[6] Op 25 mei 2011 dienden de lidstaten de nieuwe richtlijn geïmplementeerd te hebben,[7] maar Nederland heeft net als veel andere lidstaten deze deadline gemist.[8] Ten tijde van het schrijven van dit artikel ligt het wetsvoorstel ter behandeling bij de Eerste Kamer.

Hierna wordt na enige achtergrondinformatie over de meldplicht (2.1) besproken voor wie de meldplicht in de praktijk geldt (2.2). Vervolgens wordt behandeld waar aan gedacht moet worden bij 'inbreuken in verband met persoonsgegevens' (2.3) en in welke gevallen zulke datalekken gemeld moeten worden (2.4). Daarna wordt aandacht besteed aan de uitzondering voor technische beschermingsmaatregelen (2.5), de procedure van de melding en de verplichting voor aanbieders om een register met datalekken bij te houden (2.6). In paragraaf 2 blijkt dat de regeling nog een aantal onduidelijkheden bevat. In paragraaf 3 worden de doelen die de Europese regelgever nastreeft met het invoeren van de meldplicht behandeld, en wordt nagegaan in hoeverre de meldplicht geschikt is om die doelen te bereiken. De meldplicht zou bijdragen aan de privacybescherming van degene wiens persoonsgegevens het betreft, omdat deze maatregelen kan nemen naar aanleiding van een melding (3.1) en kan overstappen naar een andere dienstverlener (3.2). Ook zou het vertrouwen in elektronische communicatiediensten toenemen door de meldplicht (3.3). Verder zou een meldplicht aanbieders stimuleren om gepaste beveiliging na te streven, wat zou leiden tot veiliger communicatiediensten (3.4). Tevens zou de meldplicht nuttig zijn om informatie te vergaren over beveiligingsproblemen en datalekken (3.5). Tot slot zou de meldplicht uiting

1 Mr. F.J. Zuiderveen Borgesius is promovendus bij het Instituut voor Informatierecht van de Universiteit van Amsterdam en doet onderzoek naar behavioural targeting en het Europese privacyrecht.

2 De digitale burgerrechtenorganisatie Bits Of Freedom houdt op haar website een Zwartboek Datalekken bij (www.bof.nl/category/zwartboek-datalekken). Buiten Nederland worden dergelijke lijsten onder meer bijgehouden op de websites van Office of Inadequate Security (www.databreaches.net) en Privacy Rights Clearing House (www.privacyrights.org). Alle in dit artikel genoemde websites zijn geraadpleegd op 12 juli 2011.

3 Brief van Kazuo Hirai aan US Congress, 3 mei 2011, http://graphics8.nytimes.com/packages/pdf/technology/20110504-sony-letter.pdf.

4 *Kamerstukken I* 2010/11, 32 549, A (Wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen, gewijzigd voorstel van wet, 22 juni 2011). In deze publicatie wordt verwezen naar de geconsolideerde versie van de geamendeerde e-Privacyrichtlijn, en naar de geconsolideerde tekst van de Telecommunicatiewet, zoals gewijzigd door het wetsvoorstel.

5 Nu de richtlijn spreekt over *"bevoegde nationale instanties"?* zijn de lidstaten vrij om te kiezen aan welke instantie de bevoegdheden worden toegekend. Indien de Europese regelgever de nationale 'OPTA's' had willen aanwijzen zou gebruik zijn gemaakt van het begrip 'nationale regelgevende instantie' (art. 2(f) Kaderrichtlijn).

6 Zie voor een uitgebreide bespreking van de meldplicht in art. 4 e-Privacyrichtijn: R. Barcelo en P. Traung, 'The Emerging European Union Security Breach Legal Framework: The 2002/58 ePrivacy Directive and Beyond', in: S. Gutwirth, Y. Poullet en P. de Hert (red.), *Data Protection in a Profiled World*, Dordrecht: Springer 2010, p. 77-104 (verder: Barcelo en Traung 2010).

7 Art. 4 lid 1 Richtlijn burgerrechten (Richtlijn 2009/136/EG).

8 Artikel 29 werkgroep, *Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments* (WP 184), Brussel: 5 april 2011, p. 6 (verder: Artikel 29 werkgroep 2011, WP 184).

geven aan de beginselen die ten grondslag liggen aan het gegevensbeschermingsrecht (3.6).
De conclusie luidt dat een meldplicht nuttig kan zijn. De effectiviteit van de meldplicht wordt echter aanzienlijk beperkt doordat hij slechts geldt voor aanbieders van openbare elektronische communicatiediensten. Zelfs als een bredere meldplicht ingevoerd zou worden, zijn meer maatregelen nodig om alle genoemde doelen te bereiken.

2. Meldplicht voor datalekken in de Telecommunicatiewet

2.1. *Achtergrond van de meldplicht voor datalekken*

De eerste wet die een meldplicht voor datalekken voorschrijft, was de California Security Breach Information Act uit 2003. Directe aanleiding voor de wet was een groot datalek in 2002, waarbij hackers zich toegang hadden verschaft tot de salarisadministratie van de staat Californië, met daarin de gegevens van 250 000 werknemers, waaronder leden van de wetgevende macht. Een datalek in 2005 bij de data broker ChoicePoint was voor andere Amerikaanse staten de aanleiding voor het invoeren van een meldplicht. (Data brokers zijn bedrijven die gespecialiseerd zijn in de handel in persoonsgegevens; een bloeiende bedrijfstak in de Verenigde Staten.) ChoicePoint bleek de gegevens van meer dan honderdduizend mensen aan criminele bendes te hebben verkocht, maar weigerde betrokkenen in te lichten die niet in Californië woonden.[9] Het voornaamste doel van de Amerikaanse meldplichtwetten is het tegengaan van identiteitsdiefstal.[10] Inmiddels zijn in de meeste Amerikaanse staten en 25 landen meldplichtwetten ingevoerd.[11]
In Europa is pas weinig ervaring met een meldplicht voor datalekken. In 2006 presenteerde de Europese Commissie een voorstel voor een meldplicht,[12] in het kader van de herziening van de telecommunicatierichtlijnen.[13] In de bijbehorende Impact Assessment wees de Europese Commissie in verband met de kwetsbaarheid van moderne communicatiemiddelen onder meer op botnets en denial of service-aanvallen. Als voorbeelden van bedreigingen voor de privacy en voor de openbare elektronische communicatiediensten worden onder meer spyware, virussen, worms, adware en phishing genoemd. Volgens de Commissie richten criminelen zich voorts steeds meer op eindgebruikers, telecommunicatiebedrijven en internet service providers.[14]
De Richtlijn Burgerrechten,[15] die eind 2009 de e-Privacyrichtlijn heeft geamendeerd,[16] introduceert in Europa een meldplicht voor de telecommunicatiesector.[17] De e-Privacyrichtlijn zet de beginselen van de Richtlijn Bescherming Persoonsgegevens[18] om in specifieke voorschriften voor de sector elektronische communicatie. Als nadere uitwerking in de e-Privacyrichtlijn ontbreekt, geldt de Richtlijn bescherming persoonsgegevens. Partijen die persoonsgegevens verwerken die buiten het bereik van de e-Privacyrichtlijn vallen, dienen wel te voldoen aan de eisen die de Richtlijn bescherming persoonsgegevens stelt.[19]
De e-Privacyrichtlijn is in Nederland geïmplementeerd in de Telecommunicatiewet. Art. 11.3 Telecommunicatiewet bevat al de eis dat aanbieders van openbare elektronische communicatiediensten passende veiligheidsmaatregelen treffen.[20] Aanbieders moeten een passend beveiligingsniveau garanderen dat in verhouding staat tot het risico, en hoeven niet de zwaarst mogelijke veiligheidsmaatregelen te treffen.[21] Tevens moeten aanbieders abonnees informeren over bijzondere veiligheidsrisico's en over maatregelen die abonnees kunnen nemen.[22] Het wetsvoorstel voegt drie specifieke eisen toe in art. 11.3. Aanbieders moeten er in ieder geval voor zorgen dat alleen gemachtigd personeel toegang heeft tot persoonsgegevens, dat opgeslagen en verzonden persoonsgegevens worden beschermd en dat een veiligheidsbeleid wordt ingevoerd.[23] De meldplicht voor datalekken wordt opgenomen in een nieuw art. 11.3a, dat hierna wordt behandeld.

9 N.S. van der Meulen, 'Fertile grounds: the facilitation of financial identity theft in the United States and the Netherlands' (diss. Universiteit van Tilburg), Nijmegen: Wolf Legal Publishers 2010, p. 76-77; 206-209 (verder: Van der Meulen 2010). Choicepoint is inmiddels een afdeling van Reed Elsevier.
10 S. Romanosky, R. Telang en A. Acquisti, 'Do Data Breach Disclosure Laws Reduce Identity Theft?', *Journal of Policy Analysis and Management* 2005, Vol. 30, Issue 2, p. 256-286 (verder: Romanosky e.a. 2011).
11 A. Maurushat, 'Data Breach Notification Law Across the World from California to Australia' (University of New South Wales research paper 2009-11), *Privacy Law and Business International* 2009 (februari).
12 Europese Commissie, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on the Review of the EU Regulatory Framework for Electronic Communications Networks and Services, Brussels: 28 Jun 2006 (SEC(2006)816), par. 7.2 (verder: Europese Commissie, SEC(2006)816).
13 Richtlijn 2002/19/EG (Toegangsrichtlijn), Richtlijn 2002/20/EG (Machtigingsrichtlijn), Richtlijn 2002/21/EG (Kaderrichtlijn), Richtlijn 2002/22/EG (Universeledienstrichtlijn) en de e-Privacyrichtlijn. Al deze richtlijnen zijn eind 2009 geamendeerd.
14 Europese Commissie, *Impact Assessment*, Brussel: 13 november 2007 (SEC(2007)1472), p. 102-103 (verder: Impact Assessment).
15 Richtlijn 2009/136/EG.
16 Zie voor een bespreking van alle amendementen: B. Van der Sloot en F.J. Zuiderveen Borgesius, 'De amendementen van de Richtlijn Burgerrechten op de e-Privacyrichtlijn', *Privacy & Informatie* 2010-4, p. 162-172.
17 In Duitsland, Ierland, Spanje en het Verenigd Koninkrijk is al ervaring opgedaan met meldplichten (ENISA, *Data breach notifications in the EU*, Heraklion: ENISA: 2011, www.enisa.europa.eu, p. 12-13 (verder: ENISA 2011)).
18 Richtlijn nr. 95/46/EG. In Nederland is de Richtlijn bescherming persoonsgegevens geïmplementeerd in de Wet bescherming persoonsgegevens.
19 Art. 1 lid 2 en overweging 10 van de e-Privacyrichtlijn.
20 Anders dan de e-Privacyrichtlijn (art. 4 lid 1), legt de Telecommunicatiewet deze plicht ook op aan de aanbieder van een openbaar elektronisch communicatienetwerk.
21 Uit overweging 20 van de e-Privacyrichtlijn blijkt dat de beveiliging beoordeeld dient te worden in het licht van art. 17 Richtlijn bescherming persoonsgegevens (vgl. art. 13 Wet bescherming persoonsgegevens).
22 OPTA, Beleidsregels informatieplicht voor aanbieders over internetveiligheid (Art. 11.3 lid 2 Telecommunicatiewet), Den Haag: *Staatscourant* 2009, nr. 585, 14 januari 2009.
23 Art. 11.3 lid 2 Telecommunicatiewet.

2.2. ***Voor wie geldt de meldplicht?***

Art. 11.3a Telecommunicatiewet neemt de meldplicht in art. 4 e-Privacyrichtlijn zonder ingrijpende wijzigingen over. Art. 11.3a legt verplichtingen op aan aanbieders van openbare elektronische communicatiediensten; diensten die geheel of hoofdzakelijk bestaan uit het overbrengen van signalen.[24] Het gaat met andere woorden om een transmissiediensten. Typische voorbeelden daarvan zijn internet acces providers en bedrijven die telefonie aanbieden. Art. 13a geldt derhalve niet voor alle aanbieders van een dienst van de informatiemaatschappij, *"elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten verricht wordt."*[25] De meldplicht is dus niet van toepassing op bijvoorbeeld aanbieders van hosting diensten, online forums, social network sites, webwinkels, online banken, besloten gebruikersgroepen en bedrijfsnetwerken.[26] Het is voor de toepasselijkheid van art. 11.3a niet van belang of een aanbieder op grond van de Wet bescherming persoonsgegevens als verantwoordelijke of als bewerker gekwalificeerd moet worden.[27]

Het Europees Parlement vindt dat de meldplicht in de e-Privacyrichtlijn voor alle aanbieders van diensten van de informatiemaatschappij zou moeten gelden.[28] De Europese Toezichthouder voor gegevensbescherming (EDPS)[29] en de Artikel 29 werkgroep, het advies- en overlegorgaan van Europese privacytoezichthouders, zijn dezelfde mening toegedaan.[30] De Europese Commissie nam deze suggestie echter niet over, omdat zij vond dat een meldplicht voor aanbieders van diensten van de informatiemaatschappij de werkingssfeer van de e-Privacyrichtlijn zou overstijgen.[31] Hiertegen valt echter een aantal argumenten in te brengen. Ten eerste bevat de e-Privacyrichtlijn reeds bepalingen die niet slechts van toepassing zijn op aanbieders van openbare electronische communicatiediensten, zoals bijvoorbeeld het geval is bij de regels ten aanzien van spam en cookies.[32] Ten tweede staat niets er aan in de weg om de werkingssfeer van de e-Privacyrichtlijn uit te breiden.[33]

Bij wijze van compromis spoort de preambule van de Richtlijn burgerrechten de Europese Commissie aan spoedig passende maatregelen te nemen om de reikwijdte van de meldplicht uit te breiden. Volgens overweging 59 *"moet de Commissie, in overleg met de Europese Toezichthouder voor gegevensbescherming, onverwijld passende maatregelen nemen ter bevordering van de beginselen inzake melding van inbreuken betreffende gegevens uit [de e-Privacyrichtlijn], ongeacht de sector of het soort gegevens."* Hierbij moet waarschijnlijk gedacht worden aan een 'soft law'-maatregel zoals een aanbeveling.[34] De Richtlijn bescherming persoonsgegevens wordt momenteel herzien; daarin zal waarschijnlijk een algemene meldplicht voor datalekken worden opgenomen.[35] Naar verwachting zal dit proces echter een aantal jaar in beslag nemen.

In Nederland waren de Minister van Justitie en de Consumentenbond in 2005 nog van mening dat een wettelijke meldplicht voor datalekken niet nodig was.[36] Inmiddels is echter het juridische klimaat veranderd. De digitale burgerrechtenorganisatie Bits of Freedom voert campagne voor een brede meldplicht en heeft zelfs een wetsartikel voor de Wet bescherming persoonsgegevens voorgesteld.[37] Het huidige kabinet geeft in het regeerakkoord aan met een voorstel voor een meldplicht te komen, die echter alleen zou gelden voor aanbieders van een dienst van de informatiemaatschappij.[38] Veel organisaties zouden buiten deze meldplicht vallen, zoals een ziekenhuis dat medische dossiers laat rondslingeren of een bank die een USB-stick met gevoelige gegevens kwijtraakt.[39]

In de memorie van toelichting bij het Wetsvoorstel ter wijziging van de Telecommunicatiewet wordt vermeld dat een brede meldplicht voor datalekken toegevoegd zal worden aan de Wet bescherming persoonsgegevens. Het College be-

24 Zie voor de definitie van electronische communicatiediensten: art. 1.1 (f) Telecommunicatiewet en art. 2(c) Kaderrichtlijn.

25 Zie voor de definitie van dienst van de informatiemaatschappij: art. 3:15d lid 3 BW en art. 1 lid 2 Richtlijn informatieprocedure II (Richtlijn 98/34/EG).

26 Art. 3 e-Privacyrichtlijn en overweging 55 van de Richtlijn burgerrechten.

27 Zie art. 1(d) en 1(e) Wet bescherming persoonsgegevens en art. 2(d) en 2(e) Richtlijn bescherming persoonsgegevens.

28 Europees Parlement, amendement 136, Brussel: 24 september 2008.

29 Europese Toezichthouder voor gegevensbescherming, *Advies van de Europese Toezichthouder voor gegevensbescherming over het voorstel voor een richtlijn van het Europees Parlement en de Raad tot wijziging van met name Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie)*, Brussel: 18 juli 2008 (*PbEG* 2008, C 181/01), par. II.2 (verder: EDPS 2008, Eerste advies); Europese Toezichthouder voor gegevensbescherming, *Tweede advies van de Europese toezichthouder voor gegevensbescherming over de herziening van Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (Richtlijn betreffende privacy en elektronische communicatie)*, Brussel: 6 juni 2009 (*PbEG* 2009, C 128/28), par. II.22 (verder: EDPS 2009, Tweede advies).

30 Artikel 29 werkgroep, *Advies 8/2006 over de herziening van het regelgevingskader voor elektronische communicatienetwerken en -diensten, met bijzondere aandacht voor de ePrivacy-richtlijn* (WP 126), Brussel: 26 september 2006, par. 3; Artikel 29 werkgroep, *Advies 2/2008 over de herziening van Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie (e-Privacyrichtlijn)* (WP 150), Brussel: 15 mei 2008, par. 2; Artikel 29 werkgroep, *Advies 1/2009 over de voorstellen tot wijziging van Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie* (e-Privacyrichtlijn) (WP159), Brussel: 10 februari 2009, par. 2.1 (verder: Artikel 29 werkgroep 2009, WP 159).

31 Europese Commissie, Amended proposal, Brussel: 6 november 2008 (COM(2008)723 final), p. 20.

32 Art. 5 en art. 13 e-Privacyrichtlijn. Zie ook Artikel 29 werkgroep 2009, WP 159, par. 2.1, noot 7.

33 EDPS 2009, *Tweede advies*, kantlijnnummer 26.

34 Barcelo en Traung 2010, p. 103.

35 European Commission, *A comprehensive strategy on data protection in the European Union*, Brussels: October 2010 (COM(2010) 609 final), p. 6.

36 *Handelingen II* 2004-2005/105, p. 6363-6366, behandeling van motie Gerkens en Van Dam. Zie voor een overzicht van de discussie in Nederland: L. Boer en T.K. Grimmius, *Melding maken? Internationale quick scan meldplicht gegevensverlies, Een onderzoek in opdracht van het Ministerie van Economische Zaken*, Zoetermeer: Research voor beleid 2009, p. 55-61.

37 Bits of Freedom, *Position Paper Meldplicht Datalekken*, Amsterdam: 25 januari 2010, www.bof.nl.

38 Regeerakkoord VVD-CDA, *Vrijheid en verantwoordelijkheid*, Den Haag: 30 september 2010, p. 42.

39 Beide voorbeelden zijn ontleend aan het Zwartboek Datalekken van Bits of Freedom.

scherming persoonsgegevens zal worden belast met het toezicht op die meldplicht. Het toezicht op datalekken bij aanbieders van elektronische communicatiediensten wordt dan wellicht ook bij het College bescherming persoonsgegevens ondergebracht.[40] In april 2011 hebben de Staatssecretaris van Veiligheid en Justitie en de Minister van Binnenlandse Zaken en Koninkrijksrelaties een wetsvoorstel ter wijziging van de Wet bescherming persoonsgegevens aangekondigd. Daarin zal een meldplicht worden opgenomen voor elke voor de verwerking van persoonsgegevens verantwoordelijke.[41]

2.3. *Wat is een inbreuk in verband met persoonsgegevens?*

Wat in het dagelijks spraakgebruik wel een datalek wordt genoemd, heet in het wetsvoorstel een *"inbreuk in verband met persoonsgegevens"*. Het wetsvoorstel neemt de definitie nagenoeg ongewijzigd over uit de e-Privacyrichtlijn. Art. 11.1 sub j Telecommunicatiewet luidt als volgt:

> "inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die resulteert in een onbedoelde of onwettige vernietiging, verlies, wijziging, niet geautoriseerde toegang tot persoonsgegevens die zijn verstuurd, opgeslagen of anderszins verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de Europese Unie."[42]

Waar moet in de praktijk aan gedacht worden bij een *"inbreuk in verband met persoonsgegevens"*? Het lijkt voor de hand te liggen om bijvoorbeeld te denken aan de situatie dat er door hackers wordt ingebroken op de internetverbinding van een abonnee. Deze interpretatie zou aansluiten bij art. 4 e-Privacyrichtlijn en art. 11.3 Telecommunicatiewet, waarin aanbieders verplicht worden passende maatregelen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden diensten te treffen. De Nederlandse wetgever lijkt blijkens de memorie van toelichting ook voornamelijk aan inbreuken op de veiligheid van elektronische communicatiediensten te denken: *"De meldplicht geldt (…) alleen voor inbreuken op het netwerk dat door de aanbieder van de openbare elektronische communicatiedienst wordt gebruikt voor het leveren van zijn dienst."*[43] Het is niet evident hoe een aanbieder er bijvoorbeeld achter zou moeten komen dat een phishing attack plaatsvindt.[44] De aanbieder moet immers de privacy en het communicatiegeheim respecteren, en zal doorgaans het internetverkeer niet (mogen) inspecteren.[45] In de nota naar aanleiding van het verslag wordt dan ook opgemerkt: *"Wanneer aan deze zorgplicht [van artikel 11.3 Telecommunicatiewet] is voldaan, dat wil zeggen wanneer de beveiliging op orde is, en een inbreuk wordt niet opgemerkt, dan kan en hoeft de internet service provider de inbreuk niet te melden."*[46] Als een aanbieder echter een inbreuk op de beveiliging constateert en het mogelijk is dat persoonsgegevens zijn gelekt, zal hij de betrokkenen moeten inlichten.[47]

Een andere interpretatie van het begrip 'inbreuk in verband met persoonsgegevens' is ook mogelijk. De definitie spreekt over persoonsgegevens die zijn verwerkt "*in verband met* de levering van een openbare elektronische communicatiedienst". De woorden *"in verband met"* geven ruimte voor een brede interpretatie.[48] ENISA, de European Network and Information Security Agency, heeft onder meer achttien bevoegde nationale instanties geïnterviewd om een beeld te krijgen van waar zij aan denken bij datalekken. De instanties blijken veel situaties als datalekken te beschouwen die niet direct te maken hebben met de beveiliging van de communicatiedienst of het netwerk zelf. Zo wordt de situatie genoemd waarin een aanbieder een laptop of een USB-stick met persoonsgegevens kwijtraakt. Andere genoemde voorbeelden zijn het verkeerd adresseren van een brief of e-mail die persoonsgegevens bevat en het bij het vuilnis zetten van gevoelige dossiers. Eén toezichthouder noemt ook het gebruik van persoonsgegevens voor direct marketing zonder toestemming van de betrokkene als voorbeeld van een datalek.[49] Kortom, het rapport van ENISA suggereert dat de meldplicht voornamelijk ziet op het lekken van persoonsgegevens die de aanbieder zelf verwerkt in verband met de levering van zijn diensten.

Het kan dan bijvoorbeeld gaan om klantgegevens of verkeersgegevens, gegevens die worden verwerkt voor het overbrengen van communicatie of voor de facturering ervan.[50] Voorbeelden van verkeersgegevens zijn een opgeroepen telefoonnummer en de duur en het tijdstip van een telefoongesprek.[51] Veel aanbieders verwerken en bewaren ook locatiegegevens, zoals gegevens die verwijzen naar de plaats waar een mobiele telefoon zich bevindt op een bepaald tijdstip.[52] Bovendien moeten aanbieders op grond van de Dataretentierichtlijn grote hoeveelheden verkeers-

40 *Kamerstukken II* 2010/11, 32 549, nr. 3, p. 23-24 en 42.
41 Ministerie van Veiligheid en Justitie, Kamerbrief voornemens voorstel van wet tot wijziging van de Wet bescherming persoonsgegevens, 29 april 2011 (kenmerk: 5688920/11/6).
42 Art. 11.1 sub j Telecommunicatiewet.
43 *Kamerstukken II* 2010/11, 32 549, nr. 3, p. 41-42.
44 Phishing is het oplichten van mensen door ze te verleiden hun gegevens te verstrekken door bijv. op een valse website in te loggen of een webformulier in te vullen.
45 N.A.N.M. van Eijk et al., *Op weg naar evenwicht: een onderzoek naar zorgplichten op het internet*, WODC/Universiteit van Amsterdam: 2010, p. 34.
46 *Kamerstukken II* 2010/11, 32 549, nr. 7, p. 23. Zie ook: *Kamerstukken II* 2010/11, 32 549, nr. 3, p. 42.
47 Omwille van de leesbaarheid wordt in het navolgende ook het woord 'de betrokkene' gebruikt; in de artikelen over de meldplicht in de e-Privacyrichtlijn en de Telecommunicatiewet wordt dit woord echter niet gehanteerd. In sommige gevallen zou de terminologie relevant kunnen zijn. Een 'betrokkene' kan alleen een natuurlijk persoon zijn. Een abonnee (de term die de e-Privacyrichtlijn gebruikt in de regeling van de meldplicht) kan ook een rechtspersoon zijn (art. 2(k) Kaderrichtlijn). Kortom, de richtlijn laat de mogelijkheid open dat ook rechtspersonen ingelicht moeten worden over een datalek.
48 Barcelo en Traung 2010, p. 90.
49 ENISA 2011, p. 16-17.
50 Art. 2(b) e-Privacyrichtlijn en art. 1.1(b) Telecommunicatiewet.
51 Overweging 15 van de e-Privacyrichtlijn.
52 Art. 2(c) en overweging 14 van de e-Privacyrichtlijn en art. 11.1(d) Telecommunicatiewet.
53 Richtlijn 2006/24/EG.

gegevens bewaren,[53] in Nederland voor een periode van twaalf maanden.[54] Het is nog niet duidelijk hoe OPTA het begrip 'inbreuk in verband met persoonsgegevens' zal interpreteren.

Naast de meldplicht voor datalekken bevat het wetsvoorstel nog een meldplicht, gebaseerd op de Kaderrichtlijn. Aanbieders moeten de Minister van Economische Zaken in kennis stellen van elke inbreuk op de veiligheid of elk verlies van integriteit die een belangrijke impact had op de exploitatie van netwerken of diensten.[55] Hierbij kan gedacht worden aan het uitvallen van een netwerk ten gevolge van graafwerkzaamheden, stroomuitval of een cyberaanval. Deze meldplicht, die ook geldt ook als er geen persoonsgegevens in gevaar zijn, wordt hier verder niet behandeld.

2.4. *Twee drempels*

Er is tijdens de totstandkoming van de Richtlijn burgerrechten veel gediscussieerd over de vraag wat voor drempel (of 'trigger') er moet gelden voor het melden van een datalek. Ook buiten Europa speelt deze discussie. Als ieder datalek aan de betrokkenen zou worden gemeld, zouden zij de overvloed aan meldingen wellicht negeren.[56] Hierbij dient wel bedacht te worden dat een overvloed aan meldingen kan duiden op een structureel beveiligingsprobleem.[57] Als de drempel echter te hoog ligt, bestaat de kans dat betrokkenen niet gewaarschuwd worden in ernstige gevallen. De Europese regelgever heeft getracht dit dilemma op te lossen door twee verschillende meldplichten voor datalekken in te voeren. Ten eerste moeten aanbieders ieder datalek aan de bevoegde nationale instantie melden. Ten tweede moet de aanbieder de betrokkene onverwijld in kennis stellen als een datalek *"waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer"*.[58]

In Nederland moeten aanbieders datalekken voortaan melden aan OPTA. In art. 11.3a lid 1 Telecommunicatiewet is dit als volgt verwoord:

> "De aanbieder van een openbare elektronische communicatiedienst stelt het college onverwijld in kennis van een inbreuk op de beveiliging, bedoeld in artikel 11.3, die nadelige gevolgen heeft voor de bescherming van persoonsgegevens die zijn verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de Europese Unie."[59]

Art. 11.3a lid 1, gebruikt niet de woorden 'inbreuk in verband met persoonsgegevens' en verwijst daardoor niet naar de definitiebepaling in art. 11.1 sub j Telecommunicatiewet. Aannemelijk is dat wel gedoeld wordt op de 'inbreuk in verband met persoonsgegevens'.

Een aanbieder moet degene wiens persoonsgegevens het betreft onverwijld in kennis stellen van een inbreuk in verband met persoonsgegevens, als de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Een relevante vraag is dus wat verstaan moet worden onder 'waarschijnlijk ongunstige gevolgen'. Volgens de Richtlijn burgerrechten moet een datalek *"als schadelijk voor de persoonsgegevens of het privéleven van een abonnee of persoon worden beschouwd, wanneer er bijvoorbeeld identiteitsdiefstal of -fraude, lichamelijke schade, ernstige vernedering of aantasting van de reputatie, met betrekking tot de levering van openbare communicatiediensten in de Gemeenschap het gevolg ervan kan zijn."*[60] Het is in eerste instantie de aanbieder die moet bepalen of een datalek waarschijnlijk ongunstige gevolgen zal hebben. Als een aanbieder een inbreuk niet heeft gemeld aan de betrokkenen omdat hij van mening was dat ongunstige gevolgen niet waarschijnlijk waren, kan OPTA dat alsnog opdragen.[61]

Op grond van de e-Privacyrichtlijn kunnen de bevoegde nationale instanties richtsnoeren en instructies uitvaardigen over de *"omstandigheden waarin de kennisgeving van de inbreuk in verband met persoonsgegevens door aanbieders noodzakelijk is"*.[62] Deze bepaling is niet expliciet geïmplementeerd in het wetsvoorstel, maar OPTA kan wel beleidsregels vaststellen.[63] Hoe OPTA de open term 'waarschijnlijk ongunstige gevolgen' zal interpreteren is nog niet bekend. De e-Privacyrichtlijn noch het wetsvoorstel zijn erg helder over de vraag of OPTA kan beslissen dat triviale datalekken niet aan OPTA gemeld hoeven te worden.[64] Wil OPTA altijd ingelicht worden als er één brief met persoonsgegevens aan een verkeerd adres wordt gestuurd?

2.5. *Uitzondering in geval van gepaste technische beschermingsmaatregelen*

Een aanbieder hoeft een datalek niet aan de betrokkenen te melden als hij *"naar het oordeel van [OPTA] gepaste technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft, versleuteld of anderszins onbegrijpelijk zijn voor een ieder die geen recht heeft op toegang tot die gegevens."*[65] Als een aanbieder alle gegevens onleesbaar heeft gemaakt door middel van bijvoorbeeld encryptie, hoeft hij een datalek dus mogelijk niet aan de betrokkenen te melden. OPTA kan echter beslissen dat niet is aangetoond dat de beveiligingsmaatregelen afdoende zijn. De aanbieder

54 Art. 13.2a Telecommunicatiewet.
55 Art. 11a.2 Telecommunicatiewet en art. 13bis lid 3 Kaderrichtlijn.
56 Fred H. Cate, 'Information Security Breaches: Looking Back and Thinking Ahead', *The Centre of Information Policy Leadership. Hunton & Williams LLP* 2008, p. 10-11.
57 EDPS 2009, Tweede advies, par. 35.
58 Art. 11.3a lid 2 Telecommunicatiewet.
59 Art. 11.3a Telecommunicatiewet. "College"? is gedefinieerd in art. 1.1 (b) Telecommunicatiewet jo. art. 2 Wet Onafhankelijke post- en telecommunicatieautoriteit.
60 Overweging 61 van de Richtlijn burgerrechten. Zie voor de mening van nationale instanties: ENISA 2011, p. 17.
61 Art. 11.3a lid 4 Telecommunicatiewet.
62 Art. 4 lid 4 e-Privacyrichtlijn.
63 *Kamerstukken II* 2010/11, 32 549, nr. 3, p. 41-42.
64 Barcelo en Traung concluderen dat alle datalekken aan de bevoegde nationale instanties gemeld moeten worden (Barcelo en Traung 2011, p. 91). Men zou echter in art. 4 lid 4 e-Privacyrichtlijn kunnen lezen dat bevoegde nationale instanties wel kunnen beslissen dat niet alle datalekken gemeld hoeven te worden; zij kunnen *"instructies uitvaardigen betreffende de omstandigheden waarin de kennisgeving van de inbreuk in verband met persoonsgegevens door aanbieders noodzakelijk is"*.
65 Art. 11.3a lid 5 Telecommunicatiewet en art. 4 lid 3 e-Privacyrichtlijn.

moet dan alsnog de betrokkenen inlichten.[66] Anders dan in bijvoorbeeld veel Amerikaanse meldplichtwetten is geen sprake van een 'encryption safe harbour'.[67] Het enkele feit dat encryptie is toegepast maakt nog niet dat een datalek niet gemeld hoeft te worden aan de betrokkenen. Encryptie is slechts een van de factoren waar rekening mee wordt gehouden bij de beoordeling of een datalek waarschijnlijk ongunstige gevolgen zal hebben.
In de e-Privacyrichtlijn staat te lezen: *"Dergelijke technologische beschermingsmaatregelen maken de gegevens onbegrijpelijk voor eenieder die geen recht op toegang daartoe heeft."*[68] Deze zin lijkt waterdichte encryptie of andere beschermingsmaatregelen te eisen en geen ruimte te laten voor een proportionaliteitstoets zoals in art. 11.3 Telecommunicatiewet.[69]

2.6. *Procedure van de melding*

De kennisgeving aan de betrokkenen moet in ieder geval bevatten: de aard van de inbreuk in verband met persoonsgegevens, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.[70] Er mogen geen kosten in rekening worden gebracht voor het verschaffen van deze informatie.[71] De kennisgeving aan OPTA moet naast deze gegevens ook de gevolgen van de inbreuk op de persoonsgegevens en de maatregelen die de aanbieder voorstelt of heeft getroffen om de inbreuk aan te pakken bevatten.
Een inherent probleem van een meldplicht is dat aanbieders geneigd zouden kunnen zijn om datalekken niet te melden, om te ontsnappen aan negatieve publiciteit.[72] Om OPTA en het College bescherming persoonsgegevens[73] de mogelijkheid te geven te controleren of de meldplicht wordt nageleefd, zijn aanbieders verplicht een overzicht bij te houden van datalekken, met daarin onder meer de gevolgen van deze datalekken en de herstelmaatregelen die zijn genomen.[74] Uit de richtlijn blijkt dat dit overzicht uitsluitend de voor dit doel noodzakelijke gegevens mag bevatten.[75]
Het rapport van ENISA suggereert dat veel nationale autoriteiten verschillende media zullen accepteren om een datalek aan de betrokkenen te melden, zoals brieven, persberichten of een melding op de website. Als de aanbieder geen contactgegevens (meer) heeft van de betrokkenen, zal een advertentie in de krant wellicht voldoen.[76] OPTA kan beleidsregels uitvaardigen over de *"het voor deze kennisgeving toepasselijke formaat, alsmede de manier waarop de kennisgeving geschiedt."*[77] Het is nog niet bekend wat de mening van OPTA is in dit verband.
Aanbieders dienen de melding niet direct aan OPTA te richten, maar aan een nog op te richten centraal meldpunt. Bij dat meldpunt moeten aanbieders behalve datalekken ook veiligheidsinbreuken op netwerken melden.[78] Het meldpunt zal de meldingen dan doorgeven: in het geval van inbreuken op netwerken aan de Minister van Economische Zaken, en in het geval van datalekken aan OPTA.[79] De Europese Commissie kan technische uitvoeringsmaatregelen aannemen in verband met onder meer de omstandigheden en de procedures die gelden voor de informatieverstrekking en de meldplicht.[80] Deze uitvoeringsmaatregelen kunnen bij of krachtens algemene maatregel van bestuur geïmplementeerd worden.[81] Samenvattend is de procedure van de melding nog niet helemaal duidelijk.

3. Doelen van de meldplicht

De Nederlandse wetgever heeft voor een strikte implementatie van de regeling van de meldplicht gekozen en in de memorie van toelichting worden geen argumenten toegevoegd aan de argumenten die de Europese regelgever noemt voor het invoeren van de meldplicht.[82] De Europese regelgever streeft meerdere doelen na. De meldplicht zou bijdragen aan de privacybescherming van de betrokkene, omdat deze maatregelen kan nemen naar aanleiding van een melding en kan overstappen naar een andere dienstverlener die betere beveiliging biedt. Ook zou het vertrouwen in elektronische communicatiediensten toenemen. Verder zou een meldplicht aanbieders stimuleren om gepaste beveiliging na te streven. Tevens zou de meldplicht nuttig zijn om informatie te vergaren over beveiligingsproblemen en datalekken. Tot slot zou de meldplicht passen bij de beginselen van behoorlijk gegevensbeheer. Hierna worden de argumenten becommentarieerd.

3.1. *Privacybescherming, betrokkenen kunnen maatregelen nemen*

Volgens de Europese regelgever kan een meldplicht nuttig zijn omdat de betrokkenen na een datalek voorzorgsmaat-

66 Art. 11.3a lid 4 Telecommunicatiewet en art. 4 lid 3 e-Privacyrichtlijn.
67 Zie uitgebreid over dit onderwerp: M. Burdon e.a. 'Encryption Safe Harbours and Data Breach Notification Laws', *Computer Law & Security Review* 2010, p 520-534.
68 Art. 4 lid 3 e-Privacyrichtlijn.
69 Barcelo en Traung 2010, p. 94-95. Zie ook art. 13 Wet bescherming persoonsgegevens en art. 17 Richtlijn bescherming persoonsgegevens.
70 Art. 11.3a lid 3 Telecommunicatiewet.
71 Overweging 20 van de e-Privacyrichtlijn.
72 P.M. Schwartz en E.J. Janger, 'Notification of data security breaches', *Michigan Law Review* 2007, p. 913-984, p. 931 (verder: Schwartz en Janger 2007).
73 *Kamerstukken II* 2010/11, 32 549, nr. 3, p. 75.
74 Art. 11.3a lid 6 Telecommunicatiewet. De verhouding tussen het nemo tenetur-beginsel en de verplichting voor aanbieders om bewijs te verzamelen dat later tegen hen zou kunnen worden gebruikt valt buiten het bestek van dit artikel.
75 Art. 4 lid 4 e-Privacyrichtlijn.
76 ENISA 2011, p. 19; Artikel 29 werkgroep 2011, WP 184, kantlijnnummer 38.
77 Art. 4 lid 4 e-Privacyrichtlijn. Zie ook *Kamerstukken II* 2010/11, 32 549, nr. 3, p. 41-42.
78 *Kamerstukken II* 2010/11, 32 549, nr. 2, art. 11a.2.
79 *Kamerstukken II* 2010/11, 32 549, nr. 3, p. 23-24.
80 Art. 4 lid 5 e-Privacyrichtlijn.Op 14 juli 2011 is de Europese Commissie in dit verband een consultatieronde gestart (Europese Commissie, *ePrivacy Directive: circumstances, procedures and formats for personal data breach notifications Public consultation*, Brussel: 14 juli 2011, http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/data_breach/ePrivacy_databreach_consultation.pdf).
81 Art. 11.3 lid 7 Telecommunicatiewet; *Kamerstukken II* 2010/11, 32 549, nr. 3, p. 75.
82 *Kamerstukken II* 2010/11, 32 549, nr. 3, p. 22-27, 42-43 en 72-75.

regelen kunnen treffen om bijvoorbeeld economisch verlies of sociale schade tot een minimum te beperken.[83] Zo kunnen betrokkenen hun bankpassen blokkeren, hun bankrekening in de gaten houden of hun wachtwoorden veranderen. Dit wordt wel het hoofddoel van de meldplicht genoemd.[84]

Van der Meulen wijst er in haar proefschrift op dat men niet al te veel moet verwachten van de maatregelen die betrokkenen kunnen nemen om identiteitsdiefstal tegen te gaan, ook al zijn zij ingelicht over een datalek. De gegevens zijn immers al gelekt. Ook laat zij zien dat het verband tussen datalekken en identiteitsdiefstal moeilijk is aan te tonen.[85] Romanosky e.a. komen tot de voorzichtige conclusie dat invoering van meldplichtwetten in de Verenigde Staten heeft geleid tot een vermindering van het aantal gevallen van identiteitsdiefstal van rond de 6%. Zij benadrukken echter dat harde cijfers moeilijk te achterhalen zijn.[86] Dit betekent niet dat hier eenzelfde effect zal optreden. De situatie in Nederland is niet goed te vergelijken met die in de Verenigde Staten. Zo zijn in Nederland data brokers zoals ChoicePoint geen wijdverspreid fenomeen. Ook kent de Verenigde Staten een geheel ander wettelijk regime met betrekking tot de bescherming van privacy en persoonsgegevens.[87]

Mogelijk draagt een meldplicht ertoe bij dat mensen zich het belang van goede beveiliging realiseren.[88] Het is echter de vraag in hoeverre zij in staat zijn effectieve maatregelen te nemen. Ook computers met compleet up to date beveiligingssoftware blijken bijvoorbeeld geïnfecteerd te worden met malware.[89] Nu de meldplicht alleen voor aanbieders van elektronische communicatiediensten geldt, helpt de meldplicht consumenten niet in te schatten in welke situaties de grootste risico's spelen. Datalekken komen zeker niet alleen voor in de telecommunicatiesector. Uit het rapport van ENISA blijkt dat nationale instanties van mening zijn dat aanbieders van elektronische communicatiediensten de bescherming van persoonsgegevens goed op orde hebben. Nationale instanties vermoeden dat de grootste risico's spelen in de financiële sector, de gezondheidssector en bij het midden- en kleinbedrijf.[90] Samenvattend zou een meldplicht nuttig kunnen zijn voor degene wiens persoonsgegevens zijn gelekt, omdat deze enige maatregelen kan treffen. Dit zou voor een bredere meldplicht pleiten.

3.2. *Privacybescherming, betrokkenen kunnen overstappen naar concurrent*

Volgens de Europese regelgever draagt een meldplicht ertoe bij dat aanbieders hun beveiliging op orde zullen brengen, om klachten of negatieve publiciteit te voorkomen.[91] Een meldplicht zou zorgen voor een transparante markt en aanbieders zouden gaan concurreren op beveiligingsbeleid. Consumenten krijgen op die manier de kans aanbieders mede op grond van hun beveiligingsbeleid te kiezen.[92]

Het is echter de vraag of veel abonnees van aanbieder zouden wisselen naar aanleiding van een datalek. Het overstappen naar een concurrent brengt kosten (tijd en moeite) met zich mee. Verder kan men alleen overstappen naar een concurrent die een beter beveiligingsbeleid heeft, als aanbieders concurreren op het gebied van beveiliging. Bovendien is het moeilijk te beoordelen of een andere aanbieder betere beveiliging biedt, ook al worden er af en toe datalekken gemeld. Sinds de jaren '70 van de vorige eeuw is er onder economen veel aandacht voor markten waarin de afnemers niet goed in staat zijn de kwaliteit van diensten of producten te beoordelen. Dit wordt wel een markt met asymmetrische informatie genoemd. Nobelprijswinnaar Akerlof signaleerde het zogenoemde *lemons*-probleem.[93] Als afnemers niet kunnen beoordelen of een bepaalde kwaliteit geleverd wordt, zullen zij alleen op de prijs letten. In een markt die gekenmerkt wordt door asymmetrische informatie wordt daarom vaak niet geconcurreerd op kwaliteit. Dit kan leiden tot producten en diensten van lage kwaliteit. Nu veel abonnees niet voldoende technische kennis hebben om het beveiligingsbeleid van aanbieders te beoordelen, zou sprake kunnen zijn van een *lemons*-probleem.[94]

Het voorgaande schetste de problemen die een hypothetische rationele consument tegenkomt. Een tweede aandachtspunt is dat mensen niet altijd rationeel (in de economische zin van het woord) beslissen. In de literatuur over consumentenrecht klinkt de laatste jaren kritiek op het grote vertrouwen van de Europese regelgever in informa-

83 Overweging 61 van de Richtlijn burgerrechten.
84 Barcelo en Traung 2010, p. 81.
85 Van der Meulen 2010, p. 79-80.
86 Romanosky e.a. 2011.
87 Van der Meulen 2010, p. 51 en 205-212.
88 EDPS, *Eerste advies*, par. II.2.
89 T. Moore, 'The law and economics of cyber security', Harvard: 2011, p. 19, http://people.seas.harvard.edu/~tmoore/ijcip10.pdf (verder: Moore 2011); M. van Eeten, 'Gedijen bij onveiligheid: Afwegingen rond de risico's van informatietechnologie', in: D. Broeders, M.K.C. Cuijpers en J.E.J. Prins (red.), *De staat van informatie*, Amsterdam: Amsterdam University Press 2011, p. 133-163 en 145 (verder: Van Eeten 2011).
90 ENISA 2011, p. 21-22.
91 Europese Commissie, SEC(2006)816, par. 7.2; Impact Assessment, p. 114-115.
92 Impact Assessment, p. 118.
93 Akerlof gebruikte de markt voor tweedehands auto's als voorbeeld van een markt met asymmetrische informatie. Stel: er worden goede en slechte tweedehands auto's ('lemons') te koop aangeboden. De verkoper weet of hij een slechte of een goede auto te koop aanbiedt, maar een aspirant koper kan verborgen gebreken niet vaststellen. Een rationele aspirant koper kan niet veel beter doen dan de prijs bieden die overeenkomt met de gemiddelde kwaliteit van alle tweedehands auto's die op de markt zijn. Dat betekent echter dat iemand die een goede tweedehands auto wil verkopen te weinig geboden krijgt. Veel verkopers van goede auto's zullen daarom hun auto's niet te koop aanbieden. Het gevolg is dat de gemiddelde kwaliteit van tweedehands auto's op de markt daalt. Kopers zullen daarom nog lagere prijzen bieden. Dit heeft weer tot gevolg dat steeds minder mensen hun auto te koop aan te bieden. De kwaliteit van aangeboden auto's daalt op die manier steeds verder (G. A. Akerlof, 'The Market for 'Lemons': Quality Uncertainty and the Market Mechanism', *Quarterly Journal of Economics* 1970, p. 488-500).
94 Zie voor een toepassing van Akerlof's theorie op de beveiliging van communicatienetwerken: Moore 2011, p. 6-7.
95 G. Howells, 'The Potential and Limits of Consumer Empowerment by Information', *Journal of Law and Society* 2005 (vol. 32, nr. 3), p. 349-370.

tieverstrekking als middel om consumenten te beschermen.[95] Veel consumenten zijn bijvoorbeeld niet snel geneigd van dienstverlener te wisselen.[96] Mogelijkerwijs vrezen abonnees bijvoorbeeld enige tijd zonder internetaansluiting te zitten bij een overstap naar een andere aanbieder. Dit alles neemt niet weg dat een meldplicht nuttig kan zijn voor consumenten die naar aanleiding van een datalek zouden willen overstappen naar een andere access provider of telefoonaanbieder.[97] Nu de meldplicht alleen geldt in de telecommunicatiebranche, wordt hen echter niet de kans gegeven dergelijke keuzes te maken ten aanzien van andere dienstverleners. Van Eeten vat de kritiek samen: *"Als een meldingsplicht al helpt, dan zeker niet in de smalle variant."*[98] Tot slot is het de vraag of de bescherming van persoonsgegevens — een fundamenteel recht[99] — wel overgelaten dient te worden aan marktwerking.

3.3. *Het vergroten van het vertrouwen in communicatiediensten*

De meldplicht zou ook bijdragen aan het vertrouwen in communicatiediensten.[100] Dit vertrouwen is van belang, want het succes van die diensten *"hangt gedeeltelijk af van het vertrouwen van de gebruikers dat hun persoonlijke levenssfeer zal worden geëerbiedigd"*, aldus de e-Privacyrichtlijn.[101] Het is echter ook mogelijk dat het vertrouwen van consumenten daalt na meldingen. De Europese Commissie realiseerde zich dit ook, maar voegde hier meteen aan toe dat dit negatieve effect kan worden gecompenseerd door het feit dat consumenten het idee hebben dat ze meer controle hebben over hun eigen persoonsgegevens. De Commissie wees er verder op dat de meeste Europese burgers op de hoogte gebracht willen worden als het misgaat met hun persoonsgegevens.[102]

3.4. *Stimulans voor bedrijven om gepaste beveiliging na te streven*

De Europese regelgever hoopt dat een meldplicht aanbieders stimuleert om beveiliging te verbeteren omdat bekend geworden datalekken zorgen voor negatieve publiciteit. Dit zou bijdragen aan de veiligheid van communicatiediensten.[103]

Het argument dat bedrijven gestimuleerd worden gepaste beveiliging na te streven klinkt aannemelijk. Ook de vrees voor kosten zou aanbieders ertoe kunnen bewegen te investeren in beveiliging. Het melden van een datalek aan misschien wel duizenden mensen kost immers tijd en geld. Amerikaans onderzoek suggereert dat organisaties meer aandacht kregen voor beveiliging na het invoeren van een meldplicht voor datalekken.[104]

Een meldplicht garandeert echter niet dat communicatiediensten optimaal beveiligd worden. Moore & Van Eeten behandelen de beveiliging van communicatienetwerken vanuit een economisch perspectief. Zij wijzen op het probleem dat degenen die mogelijk iets zouden kunnen doen aan beveiliging, niet altijd degenen zijn die de kosten van gebrekkige beveiliging dragen.[105] Zo hebben mensen van wie de computer deel uitmaakt van een botnet daar zelf vaak geen weet en geen last van. Een botnet is een netwerk van soms miljoenen computers die op afstand aangestuurd kunnen worden. De geïnfecteerde computers kunnen bijvoorbeeld worden gebruikt om spam of phishing e-mails te versturen.[106] Anderen dragen daar de lasten van. Internet access providers kunnen signalen krijgen dat bepaalde computers van hun abonnees deel uitmaken van een botnet, bijvoorbeeld omdat veel spam verstuurd wordt. Ook access providers dragen echter niet alle schade. De kosten worden grotendeels afgewenteld op anderen. Kortom, voor computergebruikers en access providers is de beveiliging van communicatienetwerken een externaliteit.[107] Milieuschade is het klassieke voorbeeld van een externaliteit.[108] Doorgaans wordt aangenomen dat problemen met externaliteiten niet worden opgelost met marktwerking, ook niet als marktwerking wordt gestimuleerd met transparantievergrotende maatregelen zoals een meldplicht. Dergelijke situaties kunnen ingrijpen van de overheid rechtvaardigen.[109] (Het is overigens niet in alle gevallen zeker dat de overheid effectieve maatregelen kan nemen.) Samengevat, hoewel een meldplicht ertoe zou kunnen leiden dat aanbieders meer aandacht geven aan beveiliging, zijn waarschijnlijk meer maatregelen nodig voor optimaal beveiligde communicatiediensten.

3.5. *Statistieken*

Volgens de Europese regelgever moeten de bevoegde nationale instanties beschikken over betrouwbare gegevens over datalekken en veiligheidsincidenten voor nadere analyse. Mede daarom moeten aanbieders alle datalekken aan de bevoegde nationale instanties melden en een overzicht bijhouden.[110]

96 W. Samuelson and R. Zeckhauser, 'Status Quo Bias in Decision Making', *Journal of Risk and Uncertainty* 1988, p. 7-59.

97 Mogelijk zullen consumentenorganisaties wel onderzoek doen naar het beveiligingspeil van verschillende leveranciers, en de resultaten vervolgens verspreiden.

98 Van Eeten 2011, p. 155.

99 Art. 8 Handvest van de grondrechten van de Europese Unie.

100 Impact Assessment, p. 105 en 115.

101 Overweging 5 van de e-Privacyrichtlijn.

102 Impact Assessment, p. 114-115. 64% van de ondervraagde burgers in Europa wil op de hoogte gebracht worden van hen betreffende datalekken bij bedrijven zoals telecommunicatieaanbieders (Europese Commissie, *E-Communications Household Survey* (Special Eurobarometer 274), Brussel: 2007, p. 110).

103 Europese Commissie, SEC(2006)816, par. 7.2; Impact Assessment, p. 114-115.

104 Samuelson Law, Technology & Public Policy Clinic, University of California, Berkeley School of Law, 'Security Breach Notification Laws: Views from Chief Security Officers', *Berkeley School of Law* December 2007, www.law.berkeley.edu/files/cso_study.pdf.

105 Moore 2011, p. 7.

106 Van Eeten 2011, p. 143-145.

107 Moore 2011, p. 8.

108 De vergelijking van milieuschade met beveiliging van netwerken is niet helemaal zuiver, omdat criminelen de schade van botnets veroorzaken; het is echter moeilijk om de schade op hen te verhalen (Van Eeten 2011, p. 142).

109 Moore 2011, p. 8 en 12; Van Eeten 2011, p. 144-145.

110 Overweging 58 van de Richtlijn burgerrechten.

Tegen dit argument valt niets in te brengen. Een van de grootse problemen bij de aanpak van bijvoorbeeld datalekken, virussen en botnets is het gebrek aan gegevens. Er worden hierover veel cijfers en rapporten gepubliceerd, maar het is niet altijd duidelijk waarop de schattingen en aannames gebaseerd zijn. Beveiligingsexperts en leveranciers van beveiligingssoftware schatten schade mogelijk aan de hoge kant. Zonder dat de problemen rond veiligheidsinbreuken en datalekken in kaart zijn gebracht kan geen goed beleid worden ontwikkeld. Informatievergaring is dus essentieel.[111]

Hoewel in de Verenigde Staten meldplichtwetten vooral zijn ingevoerd om identiteitsdiefstal tegen te gaan, bleken de wetten een onverwacht maar welkom neveneffect te hebben en een schat aan informatie op te leveren.[112] De verzamelde informatie wordt echter alleen optimaal benut als de informatie niet alleen bij de nationale bevoegde instanties wordt opgeslagen maar ook openbaar wordt gemaakt. Voor onderzoek naar de grootte van het probleem zou het wellicht niet noodzakelijk zijn dat alle organisaties waar data zijn gelekt ook met naam genoemd worden. Nu alleen gegevens over datalekken verzameld worden in de telecommunicatiesector zullen verzamelde gegevens niet duidelijk maken bij wat voor organisaties de grootste risico's spelen. Een brede meldplicht zou ongetwijfeld meer nuttige gegevens opleveren.

3.6. *Beginselen die ten grondslag liggen aan de bescherming van persoonsgegevens*

Een laatste argument is dat de meldplicht voortvloeit uit de beginselen die ten grondslag liggen aan de bescherming van persoonsgegevens.[113] Het gaat bij de meldplicht om *"het algemene belang van het feit dat burgers ingelicht worden over beveiligingstekortkomingen"*.[114] Dit argument is — anders dan de hiervoor vermelde argumenten — niet alleen gebaseerd op een bepaald doel dat nagestreefd wordt.[115]

De bepalingen van de e-Privacyrichtlijn vormen een specificatie van en een aanvulling op de Richtlijn bescherming persoonsgegevens. Goed verdedigbaar is dat een juiste lezing van de Richtlijn bescherming persoonsgegevens al met zich meebrengt dat een datalek aan de betrokkenen gemeld moet worden. Een van de kernbeginselen van de Richtlijn bescherming persoonsgegevens is dat gegevensverwerking transparant dient te zijn.[116] Volgens Gutwirth & De Hert is transparantie zelfs het hoofddoel.[117] Verder moeten verantwoordelijken persoonsgegevens eerlijk en rechtmatig verwerken en voldoende beveiligen.[118] Er kan moeilijk van een transparante en eerlijke verwerking gesproken worden als een aanbieder betrokkenen niet inlicht als hun persoonsgegevens gelekt zijn.

Verder volgen uit Europese jurisprudentie hoge eisen aan de beveiliging van persoonsgegevens. Art. 8 EVRM kan ook positieve plichten met zich meebrengen voor staten. Uit het arrest *I. tegen Finland* blijkt dat een staat tekort kan schieten in die positieve verplichtingen als de nationale wetgeving er niet voor zorgt dat private partijen gevoelige persoonsgegevens afdoende beveiligen.[119]

Uit het bovenstaande volgt eigenlijk al dat datalekken aan de betrokkenen gemeld moeten worden. Het kan echter geen kwaad deze meldplicht expliciet te maken. Nu alle hiervoor genoemde beginselen ook buiten de telecommunicatiesector gelden, is het minder logisch om de meldplicht alleen voor die sector te laten gelden.

4. Conclusie

In dit artikel is de meldplicht voor datalekken in het Wetsvoorstel wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen besproken. Voortaan moeten aanbieders van openbare elektronische communicatiediensten 'inbreuken in verband met persoonsgegevens' melden aan OPTA. Als een dergelijk datalek waarschijnlijk ongunstige gevolgen zal hebben voor de privacy, dienen aanbieders ook degene wiens persoonsgegevens het betreft in te lichten.

In paragraaf 2 is de regeling tegen het licht gehouden. In de praktijk is de regeling vooral relevant voor internet access providers en bedrijven die telefonie aanbieden. In Nederland en in Europa zijn echter plannen om de meldplicht ook van toepassing te verklaren op andere partijen die persoonsgegevens verwerken. De regeling blijkt nog een aantal onduidelijkheden te bevatten. Zo is er discussie mogelijk over wat precies onder een 'inbreuk in verband met persoonsgegevens' verstaan moet worden. Ook is bijvoorbeeld niet helemaal duidelijk in welke gevallen de betrokkenen ingelicht moeten worden. Nadere uitleg in een algemene maatregel van bestuur of beleidsregels van OPTA is dus wenselijk.

In paragraaf 3 is nagegaan welke doelen met de meldplicht worden nagestreefd. De meldplicht zou bijdragen aan de privacybescherming van de betrokkene, omdat deze maatregelen kan nemen naar aanleiding van een datalek en kan overstappen naar een andere dienstverlener. Voorts zou het

111 Moore 2011, p. 6 en 20-22; Van Eeten 2011, p. 137 en 155.
112 Schwartz en Janger 2007, p. 917.
113 Barcelo en Traung 2010, p. 81-85. Het grondrecht op bescherming van persoonsgegevens is onder meer neergelegd in art. 8 Handvest van de grondrechten van de Europese Unie.
114 Overweging 59 van de Richtlijn burgerrechten.
115 M. Burdon, 'Contextualizing the tensions and weaknesses of information privacy and data breach notification laws', *Santa Clara Computer and High Technology Law Journal* 2011, vol. 27 nr. 1, p. 64-130.
116 Art. 10 en 11 Richtlijn bescherming persoonsgegevens.
117 S. Gutwirth en P. de Hert, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in: E. Claes, A. Duff en S. Gutwirth (red.), *Privacy and the criminal law*, Antwerpen: Intersentia 2006, p 61-104.
118 Art. 6 lid 1 (a) Richtlijn bescherming persoonsgegevens en art. 17 Richtlijn bescherming persoonsgegevens.
119 EHRM, *I v. Finland*, appl. no. 20511/03, 17 July 2008, par. 38-48. Zie uitgebreid over het arrest *I. v. Finland* in de context van de informatiemaatschappij: P. de Hert, 'Systeemverantwoordelijkheid voor de informatiemaatschappij als positieve mensenrechtenverplichting', in: D. Broeders, M.K.C. Cuijpers en J.E.J. Prins (red.), *De staat van informatie*, Amsterdam: Amsterdam University Press 2011, p. 33-96. Uit het arrest *Malone* volgt dat ook verkeersgegevens worden beschermd door art. 8 EVRM (EHRM 2 augustus 1984, *NJ* 1988/534 (*Malone v. Verenigd Koninkrijk*), par. 84).

vertrouwen in elektronische communicatiediensten toenemen en zou een meldplicht aanbieders stimuleren om gepaste beveiliging na te streven. Bovendien zou de meldplicht nuttig zijn om informatie te vergaren over beveiligingsproblemen en datalekken. Tot slot is goed verdedigbaar dat een juiste lezing van de Richtlijn bescherming persoonsgegevens al met zich meebrengt dat een datalek aan de betrokkenen gemeld zou moeten worden.

De conclusie luidt dat een meldplicht nut kan hebben, maar dat de verwachtingen niet al te hooggespannen moeten zijn. De effectiviteit van de meldplicht wordt aanzienlijk beperkt doordat hij slechts geldt voor aanbieders van openbare elektronische communicatiediensten. Zelfs als een bredere meldplicht ingevoerd zou worden, zijn meer maatregelen nodig om alle genoemde doelen te bereiken.