tijdschrift voor sociologie

PRIVACY OP HET INTERNET: REËEL OF VIRTUEEL?

Een onderzoek naar de bescherming van de persoonlijke levenssfeer in Belgische commerciële websites

Michel Walrave

1. INLEIDING: DE INDIVIDUALISERING VAN DE MARKETINGCOMMUNICATIE

Een groeiend aantal organisaties uit zowel de profit als de non-profit sector communiceren met hun doelpublieken door middel van directe en interactieve media. Niet alleen direct mailing en de telefoon, maar ook het internet en andere online en off line media worden door menig marketeer in het communicatieplan opgenomen. Dat direct marketing (1) steeds meer gebruikt wordt, is verklaarbaar vanuit verschillende socio-culturele, economische en technologische ontwikkelingen. In de profit sector, bijvoorbeeld, zouden ontwikkelingen als individualisering binnen de consumentenmarkt, een geringer onderscheid tussen producten, merkverwarring en een overload aan massamediale reclame er onder meer toe geleid hebben dat klanten minder trouw blijven aan fabrikanten of distributeurs. Daarom probeert de bedrijfswereld niet alleen om zijn producten- en dienstenaanbod te individualiseren, maar ook zijn communicatiepogingen te personaliseren (Hoekstra 1994, 14-15; Molenaar 1992, 17-19; Patterson 1998, 69-71).

Tijdens deze communicatieprocessen worden vaak persoonsgegevens (naam, adres, koop- en andere gewoonten) verzameld, die daarna verwerkt worden om een beter inzicht te krijgen in kenmerken en (koop)gewoonten van het doelpubliek. De consumenten die deelnemen aan deze communicatieprocessen blijven dus geen anonieme massa, zoals meestal het geval is bij massamediale reclame, maar ze worden persoonlijk identificeerbaar. Hun koopgedrag wordt traceerbaar en het

uitvoeren van analyses op deze persoonsgegevens maakt het ontwerpen van consumentenprofielen mogelijk. Daarbij komt dat bedrijven en organisaties door middel van directe communicatie en de verzamelde informatie over consumenten, de gewonnen klanten proberen te behouden. Via loyaliteitsprogramma's door middel van elektronische klantenkaarten en promoties wil men de trouw van de klanten stimuleren en belonen. Deze fidelisseringstechnieken worden bovendien ook voor consumentenonderzoek ingezet. Door het snel en accuraat verzamelen en verwerken van persoonsgegevens komt men tot steeds gedetailleerdere consumentenprofielen en evolutieschetsen van het consumptiegedrag. Deze zijn noodzakelijk om de volgende communicatiepogingen preciezer te richten op specifieke doelgroepen, waarvan men onderzocht heeft of ze een zekere affiniteit hebben met het product of de dienst die men wil aanbieden.

2. DIRECT MARKETING EN PRIVACY: KLIKT HET OF BOTST HET?

Als conclusie bij de voorgaande situatieschets wordt steeds vaker geponeerd dat het commerciële gebruik van directe en interactieve media en het verwerken van persoonsgegevens belangrijke gevolgen heeft voor de bescherming van de privacy van de consument. Maar wat verstaan we onder privacy en hoe kunnen we nieuwe vormen van marketing hiermee in verband brengen?

Sinds de ontwikkeling van de informatiemaatschappij, hebben auteurs uit verschillende disciplines gepoogd om het begrip "privacy" te ontleden en te definiëren (Gavison, 1984; Guldix, 1986; Merton, 1967; Prosser 1984; Rachels, 1984; Warren & Brandeis 1890; Westin 1970) (2). Uit deze verschillende onderzoeken kunnen we twee nauw met elkaar verwante dimensies van de privacy onderscheiden, namelijk de ruimtelijke en de informationele privacy. Met ruimtelijke of relationele persoonlijke levenssfeer wordt in deze context het zelfbeschikkingsrecht van een individu bedoeld met betrekking tot de vraag met wie, wanneer, waar, hoe en waarover hij of zij (tele)communiceert. Respect voor de relationele privacy betekent dat men de consument de kans geeft om zich af te schermen tegen bepaalde vormen van directe communicatie, maar ook om een bedrijf mee te delen welke typen van communicatie wel welkom zijn.

Informationele privacy verleent ieder individu het recht om zelf te beslissen aan wie hij of zij persoonsgegevens vrijgeeft en voor welke doeleinden die gegevens gebruikt mogen worden. Het spanningsveld tussen direct marketing en de informationele en relationele privacy is verscherpt omwille van de snelle evolutie van de informatie- en communicatietechnologie (ICT). Enerzijds heeft de ontwikkeling van de ICT de mogelijkheden om persoonsgegevens te verzamelen, te registreren en te koppelen aanzienlijk verbeterd. Anderzijds levert informatie- en communicatietechnologie ook *privacy enhancing technologies (3)* (*PET*'s): privacybevorderende technologieën, die beide dimensies van de persoonlijke levenssfeer op het internet kunnen beschermen.

Parallel met deze technologische evolutie is het economisch en sociaal belang van gegevensverwerking toegenomen. In alle openbare en private sectoren worden

persoonsgegevens verwerkt om de efficiëntie van de organisatie te verhogen. Hiermee gaat de stijging van de mate van afhankelijkheid van een organisatie van die gegevensverzameling en -verwerking gepaard. Het verzamelen en verwerken van persoonsgegevens is daarom ook een belangrijke economische activiteit geworden. Het commercieel belang groeit van hen die de nieuwe technologische mogelijkheden kunnen gebruiken om het gedrag van de consument doorzichtiger te maken. De handel in persoonsgegevens is namelijk *big business* geworden in het informatietijdperk. Dit heeft ertoe geleid dat van iedere persoon inmiddels een aantal 'dataklonen' bestaan: digitale evenbeelden van mensen van vlees en bloed.

Een eerste evolutie van het creëren van een virtuele burger in databases ontstond in de publieke sector. Deze 'klonen' hebben reeds lang de grens tussen het publieke en het private overgestoken. De digitalisering van gedrag en meningen van individuen zet zich voort in de bedrijfswereld. Daar waar efficiëntie en het maken van winst de hoogste prioriteit worden verleend, moeten potentiële risico's steeds exacter berekend kunnen worden. Ook wenst men vanuit de profielen, die men van consumenten maakt, steeds meer de marketingcommunicatie te kunnen toespitsen op persoonlijke kenmerken en wensen en op die manier de slaagkansen van de communicatie te verhogen.

De 'datahonger' van bedrijven, die hiermee gepaard gaat, wordt echter getemperd door bepaalde wetgeving en zelfregulering. De kern van dit beleid is dat de klant of prospect een aantal 'privacykeuzen' kan maken. Dit geldt zowel voor de informationele als voor de relationele privacy. Wat de informationele privacy betreft kan men bij het voorleggen van een formulier aangeven welke gegevens noodzakelijk zijn voor het verstrekken van een bepaalde dienst en welke informatie optioneel is. Daarnaast bepaalt Europese en nationale privacywetgeving dat volledige transparantie gewaarborgd moet worden door de communicatie van de doelstellingen van de verwerkte data. Bovendien kan een consument zich verzetten tegen het gebruik van zijn of haar gegevens voor direct marketingdoeleinden.

Wat de relationele privacy betreft kan men aan de consument de keuze laten welke communicatiekanalen gebruikt kunnen worden om met hem te communiceren. Één concrete maatregel is bijvoorbeeld de Robinsonlijst. Consumenten, die net als een Robinson Crusoe op zijn eiland afgezonderd willen zijn van bepaalde vormen van commerciële communicatie, die dus geen reclamepost wensen te ontvangen, die niet telefonisch benaderd willen worden voor commerciële doeleinden of geen commerciële e-mails wensen te ontvangen, hebben in verschillende landen de mogelijkheid om zich van bepaalde typen direct marketing af te sluiten. Iedere consument die het wenst, kan namelijk zijn naam en enkele andere data plaatsen op een lijst van personen, die bijvoorbeeld geen reclamepost of telemarketingoproepen wensen. Organisaties, die lid zijn van een nationale direct marketing koepelorganisatie, hebben hun handtekening geplaatst onder een code van zelfregulering, die in deze mogelijkheid voorziet. De databestanden van de organisaties, die lid zijn van een dergelijke koepelorganisatie, moeten, vooraleer ze gebruikt worden voor een direct marketingcampagne, vergeleken worden met deze Robinsonlijsten. Wanneer zowel in het bestand van de onderneming als in de Robinsonlijst dezelfde persoonsgegevens voorkomen, worden deze gegevens geblokkeerd, opdat die consumenten niet benaderd zouden worden. Wie geen

mailings meer wenst te ontvangen laat zich opnemen in de Mail Preference Service (MPS) (4), ook wel de Robinsonlijst voor direct mail genoemd. Wie geen telemarketing-oproepen meer wenst, deelt zijn of haar wens mede aan de verantwoordelijke van de Telephone Preference Service of de Robinsonlijst voor telemarketing. Ook werd de e-MPS gelanceerd: de e-Mail Preference Service (5). Dit is een samenwerkingsverband tussen verschillende landen, omdat juist e-mailmarketing vaak over de grenzen heen gevoerd wordt. De Robinsonlijsten hebben echter enkele nadelen. Het is namelijk de consument zelf, die het initiatief moet nemen om zijn gegevens op deze lijst(en) te plaatsen. Hij moet dan ook eerst geïnformeerd zijn omtrent deze mogelijkheid (6). Bovendien zijn niet alle bedrijven aangesloten bij een beroepsvereniging, die deze Robinsonlijsten beheert. Tenslotte stellen sommigen zich vragen omtrent de controle op de naleving van deze afspraken en de mogelijke sancties, die kunnen volgen bij overtredingen.

Het alternatief voor de Robinsonlijsten is wat men een opting-in systeem noemt: de consument moet alvorens hij in dit direct marketingsysteem participeert uitdrukkelijk zijn of haar toestemming geven aan een bedrijf, dat zijn persoonsgegevens voor direct marketingcommunicatie wenst te gebruiken (7). In een opting-out systeem daarentegen mogen bedrijven persoonsgegevens voor direct marketing gebruiken zolang de consument zich hiertegen niet verzet. Momenteel vindt in Europa en de Verenigde Staten een geanimeerd debat plaats tussen de aanhangers van de Robinsonlijsten (het opting-out systeem) en de aanhangers van opting-in (ook nog permissiemarketing genoemd). Vooral met de opkomst van het gebruik van e-mail en Short Message Service (SMS) voor reclamedoeleinden komen stemmen op voor een opting-in regime (8).

Kortom, de gevolgen van direct marketing voor de privacy kunnen dubbelzijdig zijn: enerzijds wordt de consument door middel van directe media en een specifieke commerciële retoriek soms ongevraagd aangeschreven of aangesproken door organisaties, waarvan de consument soms niet weet hoe deze aan hun adres en andere persoonsgegevens zijn gekomen. Anderzijds betekent direct marketing in principe dat bedrijven dankzij databasetechnieken profielen schetsen om hun aanbiedingen preciezer te richten op vermeende of geobserveerde noden en wensen van consumenten.

3. DIRECT MARKETING OP HET INTERNET: OP ZOEK NAAR SPOREN

Deze mogelijkheden van profilering en het individueel aanbieden van producten en diensten zijn bijzonder scherp op het internet. Dit wereldwijd vertakte netwerk biedt vooreerst bedrijven de mogelijkheid om interactief te communiceren met individuele prospecten en klanten door middel van reclamebanners, internetcommercials - zogeheten intermercials - en andere vormen van elektronische marketing. Bijzonder is wel dat deze reclameboodschappen kunnen aangepast worden aan het surfgedrag van individuele websitebezoekers en dat tijdens het navigeren iedere klik van de bezoeker zijn profiel verder gaat verfijnen. In tegenstelling tot de off-linewereld zijn

er in cyberspace twee manieren om data over individuen te verzamelen: een expliciete en een impliciete manier.
De expliciete manier betreft het bewust en vrijwillig vrijgeven van informatie in elektronische formulieren: dus het eigenhandig invullen door een internetgebruiker van een elektronische bestelbon of een coupon om informatie over producten en diensten te ontvangen en dergelijke meer. Hierbij heeft de bezoeker van een website zelf een zekere controle over persoonsgegevens die hij aan bedrijven meedeelt. Om deze controle te kunnen uitoefenen moet de internetgebruiker natuurlijk volledig geïnformeerd worden over de gebruiksdoeleinden van zijn persoonsgegevens en het eventueel doorgeven van deze data aan andere organisaties. Slechts in deze omstandigheden kan een consument een beslissing nemen omtrent het al dan niet toevertrouwen van bepaalde informatie.
Bij een impliciete verzameling van data ligt dit moeilijker. Impliciet worden vaak zonder dat een internetgebruiker het opmerkt ook data tijdens het surfen gegenereerd louter door de omgang met de technologie. Ook deze data worden door steeds meer bedrijven geanalyseerd en als basis gebruikt voor onderzoek, prospectie en gesegmenteerde of zelfs individueel gerichte webvertising (9).
Alle sporen, die internetgebruikers in cyberspace achterlaten, worden opgevangen en bewaard in logfiles. Een logfile is een bestand, waarin de historiek van datacommunicatiesessies vermeld staat. In dit bestand staat bijvoorbeeld de intermediair vermeld, via dewelke de bezoeker toegang heeft tot het internet (Internet Service Provider of een bedrijf of organisatie, waarvan hij deel uitmaakt), het tijdstip en de duur van het bezoek en bepaalde kenmerken van de computer, die hij gebruikt. Bovendien wordt bijgehouden welke pagina's opgevraagd worden en welke bestanden (bijvoorbeeld afbeeldingen) aangeklikt worden. Dit kan onder meer gebruikt worden om anonieme statistieken op te stellen van de meest bezochte webpagina's, maar ook van de domeinen en landen, waarvan de meeste bezoekers afkomstig zijn, en de piek- en daluren van het verkeer naar de website enzovoorts. Hiermee kunnen webmasters en -marketeers achterhalen hoeveel internetgebruikers hun website bezoeken en waar zij vandaan komen, maar nog niet wie deze individuen precies zijn.
Hoe kan men dan precies te weten komen wie bepaalde informatie op de website raadpleegt? Daarvoor zijn andere technieken ontworpen, waarvan de cookies ondermeer de belangrijkste en meest gebruikte zijn. Cookies zijn informatiepakketjes, die door de HyperText Transport Protocol-server (HTTP- of webserver) automatisch worden verstuurd naar een cliëntmachine (de personal computer van de gebruiker) en op de harde schijf van de computer geplaatst worden op het moment dat de gebruiker de website bezoekt. Een dergelijk bestandje bevat de naam van de cookie, de waarde van de cookie (dit kan een unieke code zijn), de vervaldatum (het einde van de surfsessie of soms een zeer afgelegen datum) en de domeinnaam, waarnaar de cookie (bij herhaalbezoek) gestuurd kan worden (Bazsalisca e.a. 2001, 249; Dinant 1999, 296-297). Men kan het onderscheid maken tussen sessie-cookies en permanente cookies. Sessie-cookies onthouden bepaalde voorkeuren van de websitebezoeker enkel tijdens één surfsessie. Permanente cookies blijven bewaard op de harde schijf van de internetgebruiker (tot de gebruiker zelf het bestandje uitwist of de einddatum van de cookie bereikt wordt). Dergelijke cookie kan bij een herhaalbezoek het raadplegen van informatie versnellen en

vergemakkelijken, omdat bepaalde gegevens vanaf het tweede bezoek automatisch worden ingevuld. Eén van de oorspronkelijke functies van cookies, die nog steeds veelgebruikt is en die bijzonder nuttig is voor websitebezoekers, bestaat erin om de taal die een surfer tijdens zijn eerste bezoek aan een website koos, automatisch bij een tweede bezoek op te roepen, omdat de server de bezoeker en de taalkeuze via de cookie herkent. Ook het invullen van formulieren kan vergemakkelijkt worden dankzij een cookie, omdat de server automatisch het formulier invult (in een bestelformulier van een e-shop) met de persoonsgegevens van de bezoeker die herkend wordt. Kortom, het surfen kan hiermee versneld en vergemakkelijkt worden. Een cookie kan echter ook fungeren als een soort barcode. Telkens wanneer een bezoeker naar de website terugkeert, stuurt zijn browser de cookie naar de server door en herkent de server de computer dankzij deze cookie. Het individu wordt pas identificeerbaar, wanneer de websitebezoeker in een elektronisch formulier persoonsgegevens heeft ingevoerd en deze data gekoppeld worden aan een unieke code, die in de cookie steekt. Cookies kunnen in dit geval een commerciële functie hebben: ze kunnen bijvoorbeeld het navigatiepad (*clickstream*) van de gebruiker van de betreffende site volgen (*tracking*). Op die manier kan de exploitant van de website bijvoorbeeld nagaan in welke informatie (producten en diensten) een gebruiker geïnteresseerd is en aan de hand daarvan bepaalde aanbiedingen doen. Ook de trefwoorden, die een bezoeker in de zoekmachine heeft ingevoerd, kunnen opgeslagen worden en het profiel van de bezoeker verfijnen.
De kritiek die ontstaan is omtrent deze heimelijke bestandjes die op de PC worden opgeslagen, zonder de gebruiker hierover in te lichten, hebben browser-producenten geïnspireerd om een optie in te bouwen die (indien door de gebruiker geactiveerd) waarschuwt wanneer een server een cookie verzendt. De gebruiker kan dan beslissen om het bestandje te aanvaarden of te weigeren. Het surfen wordt echter bemoeilijkt, soms onmogelijk, wanneer men cookies niet aanvaardt. Bepaalde websites verlenen dan geen toegang. Het surfen wordt ook bemoeilijkt wanneer men, telkens een cookie gestuurd wordt, aan zijn browser een verwittiging vraagt om geval per geval te beslissen of men de cookie aanvaardt of niet. Om het cookie-vrij surfen comfortabeler te maken bestaan daarom pakketten waarmee cookies uitgeschakeld worden (10).

De verschijning van bepaalde content in een website of van een reclameboodschap kan ook afhangen van een profielendatabase. Men vraagt de websitebezoeker om een formulier in te vullen, waarin hij gepolst wordt naar kenmerken en interesses. Dit profiel linkt men aan de cookie. Op die manier kan men bij een herhaalbezoek inhoud en reclame aanpassen aan het individu.
Bovengenoemde mogelijkheden (11) beperken zich echter niet tot het scannen van het surfgedrag in één website. Bepaalde marketingbedrijven hebben netwerken aangelegd van websites, waarmee ze het surfgedrag en de zoekorders van bezoekers doorheen verschillende sites kunnen analyseren en op die manier ook de reclamebanners de internetgebruiker kunnen laten volgen op basis van de interesses die hij in één of meerdere sites heeft getoond.
Zoals hierboven geschetst, is de mogelijke koppeling van de expliciete gegevens en de impliciet verzamelde data weliswaar een krachtig marketinginstrument, maar vormt het ook een uitdaging voor de bescherming van de privacy van de

internetgebruiker. In de off-linewereld worden natuurlijk ook gegevens verzameld via een antwoordcoupon, een bestel- of wedstrijdformulier, tijdens een gesprek met een callcenter-operator enzomeer. De dataverzameling gebeurt echter bijna exclusief op een expliciete manier. Een consument vult zelf een coupon in, biedt zijn of haar elektronische klantenkaart aan de kassabediende aan, antwoordt op vragen van een operator: allemaal momenten, waarop een consument gegevens verstrekt. Wat hij vóór en na het invullen van het bestelformulier doet, komt een marketeer strikt genomen niet te weten. Enkel de informatie, die een consument zelf prijsgeeft, komt in de bestanden terecht. Deze bestanden worden daarbij echter ook verrijkt met gegevens van andere databases. Er worden profielen gedistilleerd en conclusies getrokken op basis van de input, die de consument zelf gaf. Het verkeer en de handel van gegevens tussen verschillende bedrijven verscherpt het profiel van de consument, met als uiteindelijk doel bepaalde communicatiekansen niet te missen om gepersonaliseerde en op tijd geleverde aanbiedingen te kunnen doen en om op die manier een klant te winnen en te behouden.

Op het internet echter kan een marketeer niet alleen informatie over internetgebruikers verwerven dankzij de data, die zij bewust aan bedrijven toevertrouwen. Vooraleer en nadat het elektronisch bestelformulier of coupon is ingevuld, kan de verzameling en analyse van data verdergaan. De technologie, waarop het internet berust, genereert namelijk van nature allerlei data, die de marketeer van het internet kan plukken en kan analyseren om het profiel van zijn doelpubliek te verfijnen, wat zijn communicatie hiermee kan verbeteren. Met de groei van de on-linetransacties en de koppeling van on-linesurf- en consumptiegegevens met het off-lineconsumptiegedrag wordt de foto van de consument niet alleen scherper. Het blijft niet bij een momentopname, maar de stroom gegevens, die bijgehouden wordt, inspireert een film over de relatie van de consument met het bedrijf. Het verzamelen en gebruiken van deze persoonsgebonden informatie kan echter niet zonder het verlenen van een aantal rechten aan de betrokkenen waarvan de data verwerkt en gebruikt worden. Of deze rechten worden verleend in Belgische commerciële websites, is de globale onderzoeksvraag van de analyse die hierna wordt weergegeven.

4. E-PRIVACY IN BELGIË: DE BESCHERMING VAN DE PRIVACY IN BELGISCHE COMMERCIËLE WEBSITES

4.1. De Belgische privacywet: gerespecteerd?

Hierboven stipten we reeds aan dat iedere persoon waarvan gegevens verwerkt worden, bepaalde rechten heeft die neergeschreven werden in de Europese dataprotectierichtlijn (12), omgezet in de Belgische privacywet die op 1 september 2001 van kracht werd (13). Daarvoor, sinds 1992, had België reeds een privacywet. Een aantal verschillen tussen de oorspronkelijke Belgische wet en de richtlijn, heeft de Belgische wetgever genoodzaakt de wet te herzien en aan te vullen met bepaalde

wetgever genoodzaakt de wet te herzien en aan te vullen met bepaalde supplementaire rechten voor het individu.

Bij het uitvoeren van dit onderzoek over privacybescherming in Belgische websites, was het uitvoeringsbesluit van de 'nieuwe' privacywet nog niet gepubliceerd in het Staatsblad. Daarom hebben we bestudeerd aan welke plichten van de oorspronkelijke privacywet (van 1992) de websites voldeden, maar ook welke websites hun privacybeleid reeds hebben aangepast aan de nieuwe privacywet (van 1998). Volgens deze nieuwe wet moet de verantwoordelijke voor een verwerking van persoonsgegevens aan onder meer volgende plichten voldoen:

- de betrokkene waarvan data verzameld worden moet geïnformeerd worden over de identiteit van de verantwoordelijke (en zijn adres);
- hij moet op de hoogte gebracht worden van de doeleinden waarvoor de data gebruikt zullen worden;
- indien de gegevens voor direct marketingdoeleinden gebruikt worden, dan moet de betrokkene geïnformeerd worden over zijn recht om, kosteloos en op verzoek, zich te verzetten tegen dit gebruik van zijn gegevens;
- verder verneemt de persoon dat hij het recht heeft om zijn eigen gegevens in te kijken (recht op inzage) en eventuele fouten te (laten) verbeteren (recht op correctie);
- wanneer de data ook aan één of verschillende andere organisaties worden doorgegeven, dan deelt de verantwoordelijke de ontvangers of categorieën van ontvangers van de data mee;
- de verantwoordelijke deelt ook het al dan niet verplichte karakter van het meedelen van de persoonsgegevens en de eventuele gevolgen van een weigering om bepaalde informatie mee te delen.

Eén van de nieuwe verplichtingen waaraan een verantwoordelijke voor een gegevensverwerking zich moet voldoen, is het recht op verzet bij het gebruik van persoonsgegevens voor direct marketing. Dit recht is normaalgezien van kracht sinds 1 september 2001. Volgens bepaalde juristen echter waren de bepalingen van de nieuwe privacywet reeds vroeger van kracht, aangezien België de termijn voor de omzetting van de Europese richtlijn in Belgische wet, niet gerespecteerd had (namelijk 24 oktober 1998).

Naast de privacywet zijn er nog andere nationale wetten en Europese richtlijnen die aspecten van de bescherming van de persoonlijke levenssfeer regelen. In dit onderzoek beperken we ons tot de toepassing van de privacywet in Belgische websites en dus de bescherming van de informationele privacy. Concreet trekken we na hoe en in welke mate de privacyrechten van websitebezoekers gerespecteerd worden en hoe ze over hun rechten geïnformeerd worden in een privacystatement. Hiermee bedoelen we een tekst (bij een elektronisch formulier of in een aparte webpagina) waarin een organisatie die persoonsgegevens opvraagt, zijn privacybeleid meedeelt. Conform de privacywetgeving, vermeldt zo'n statement idealiter de verantwoordelijke voor de verwerking, de doeleinden van de gegevensverwerking en de privacyrechten van de betrokkenen.
We gaan niet alleen na hoeveel websites de noodzakelijke informatie meedelen en hoe ze dit doen, maar ook hoe volledig deze informatie is.

4.2. Selectie van de websites

In totaal werden 250 websites gedetailleerd onderzocht door middel van een gestandaardiseerd analyse-instrument. Iedere website werd op 93 kenmerken onderzocht. De constructie van het onderzoeksinstrument is gebaseerd op enerzijds de wetgeving en anderzijds op een aantal adviezen weergegeven in de Memorie van Toelichting van de wet, het Advies van de Commissie ter Bescherming van de Persoonlijke Levenssfeer omtrent e-commerce (14) en eigen onderzoek over het meedelen en toepassen van een privacybeleid in direct marketing en marketing op het internet (Walrave 1999; Walrave 2001).
Vooraleer in te gaan op de resultaten van deze analyse, willen we even stilstaan bij de gebruikte methode om de websites te selecteren. Aangezien er geen volledige en betrouwbare lijst van alle websites in België beschikbaar of raadpleegbaar is, zijn we de samenstelling van de steekproef off line moeten starten. We hebben de officiële databank van Belgische bedrijven geraadpleegd en hieruit een toevalssteekproef genomen. Daarbij werd uit verschillende NACE-categorieën een gelijk aantal bedrijven genomen, met dien verstande dat enkel business-to-consumer bedrijven geselecteerd werden en niet de pure business-to-business ondernemingen. Met andere woorden, deze analyse van websites beperkt zich tot bedrijven die zich met hun producten en diensten richten tot een consumentenpubliek. De volgende stap bestond erin om één voor één na te gaan of de geselecteerde bedrijven daadwerkelijk ook over een website beschikten. Meer precies, moest dit een website zijn die zich tot consumenten richt en in één of meerdere van onze officiële landstalen en/of het Engels is opgesteld. Van het totale aantal websites konden een aantal eenheden niet in de steekproef opgenomen worden, gezien deze websites niet meer toegankelijk waren tijdens het onderzoek. Uiteindelijk voldeden 250 websites van bedrijven uit de oorspronkelijke steekproef aan bovenstaande selectiecriteria. We hebben deze selectiemethode verkozen boven het lukraak selecteren van websites door middel van zoekmachines of online indexen of webgidsen. Aangezien het universum, het totale aantal websites van bedrijven die in België gevestigd zijn (met een .be en/of een .com of andere domeinnaam) niet exact nagegaan kan worden, kunnen we geen uitspraak doen over de representativiteit van deze steekproef. De methode die wij gebruikten garandeert wel een evenredige verdeling van de steekproefeenheden over de verschillende economische sectoren die zich richten tot consumenten.

4.3. Het scannen van de websites

Eerst wordt nagegaan in welke mate en op welke wijze expliciet persoonsgegevens gevraagd worden aan websitebezoekers. Daarna focussen we op één vorm van impliciete gegevensverwerking door middel van cookies.

4.3.1. Het scannen van de websites

Wat de expliciete verzameling van gegevens betreft, vraagt 93% van de onderzochte websites op één of andere manier persoonsgegevens van bezoekers. Dit gebeurt door middel van een elektronisch formulier om zich te abonneren op een e-zine, een bestelformulier, een gastenboek of een formulier om meer informatie over producten en diensten aan te vragen. Ook de mogelijkheid om bijvoorbeeld de webmaster of de klantendienst te e-mailen is een verwerking van persoonsgegevens, aangezien het bedrijf in het bezit komt van het e-mailadres (eventueel coördinaten en andere informatie van de afzender in de e-mail zelf). Concreet worden de gegevens op de volgende manieren verzameld:

Tabel 1. Wijze waarop gegevens online verzameld worden

Enkel een elektronisch formulier	34%
Enkel een bestelformulier	9%
Enkel feedback via e-mail	9%
Verschillende typen formulieren	48%

Na de vraag of er online daadwerkelijk persoonsgegevens verzameld worden, is het interessant om na te gaan welke gegevens het meest of het minst gevraagd worden. In 96% van de gevallen wordt het e-mailadres gevraagd. Enkele websites (4%) verzamelen dus wel andere informatie, maar vragen blijkbaar niet het e-mailadres. De andere data die opgevraagd worden, met hun respectievelijke frequentie, worden weergegeven in Tabel 2. Vooral naam, adres en telefoonnummer worden gevraagd. Het valt op dat de restcategorie uitgebreid is. Onder de restcategorie verstaan we vooral taal, land, nationaliteit, geslacht, eigen websiteadres en naam van de werkgever. Soms wordt informatie gevraagd over de gezinstoestand (aantal gezinsleden, burgerlijke staat) of wordt ruimte voorzien om opmerkingen en wensen te formuleren over de inhoud en vorm van de website. Enkele websites die zich tot minderjarigen richten vragen zowel gegevens over de websitebezoekers als over hun ouders. Eén onderzochte website gaat nog verder door te informeren naar de vrije tijdsbesteding, de levensstijl en enkele persoonsgegevens. Onder deze laatste categorie wordt informatie gevraagd die door de privacywet bestempeld wordt als "gevoelige gegevens". Dit zijn data waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook de verwerking van persoonsgegevens die het seksuele leven betreffen. Dergelijke persoonsgegevens zijn onderworpen aan een zeer streng regime, namelijk een principieel verbod op verwerking van deze data, met enkele uitzonderingen. Hoewel dus bepaalde gevoelige gegevens opgevraagd worden, geeft deze website geen enkele informatie over privacyrechten en het doel van de verwerking. Evenmin worden de specifieke regels voor de verwerking van deze gevoelige data gerespecteerd.

Bovenstaande voorbeelden vormen in onze steekproef echter de uitzonderingen. De meeste websites vragen een beperkt aantal identificatiegegevens.

Tabel 2. Welke gegevens worden online verzameld

Naam	98%
E-mail	96%
Adres	90%
Telefoon	82%
Geboortedatum	25%
Beroep	22%
Kredietkaart	21%
GSM	10%
Studies	7%
Andere data	34%

Hierbij werd ook onderzocht of in het elektronisch formulier een onderscheid gemaakt wordt tussen noodzakelijke data voor het bereiken van een doel en bijkomende gegevens. Het is namelijk opvallend hoe sommige websites bepaalde gegevens verzamelen die, strikt genomen, niet nodig zijn voor het expliciet meegedeelde doel van de verwerking. Zo is voor een gratis abonnement op een e-zine eigenlijk enkel het e-mailadres noodzakelijk. We stellen echter vast dat verschillende organisaties dit abonnement koppelen aan het (soms verplicht) invullen van andere persoonsgegevens. Deze bijkomende gegevens zijn zeker een interessante bron van informatie over de websitebezoekers en kunnen gebruikt worden om (gesegmenteerd) contacten te onderhouden met geïnteresseerde consumenten. Dergelijke bijkomende doeleinden moeten echter expliciet vermeld worden. De consument moet de keuze krijgen om bijkomende gegevens al dan niet mee te delen. Ten slotte moet de consument ook enige controle in handen hebben over het beheer en gebruik van zijn data. Aan deze drie voorwaarden wordt echter in bepaalde Slechts 46% van de websites maakt in de lijst gegevens die zij opvragen, het onderscheid tussen noodzakelijke data en facultatieve gegevens. Deze keuze wordt soms aangegeven door een asterisk (*) bij de noodzakelijke data of door het onderlijnen van de verplichte vragen.

Behalve via elektronische (bestel)formulieren, verwerkt een websitebeheerder ook persoonsgegevens wanneer hij gewoonweg een e-mail ontvangt van een prospect of klant. In 86% van de gevallen staat op een website een e-mailadres waar men terechtkan voor vragen of feedback. Deze minimale verwerking van persoonsgegevens zou dus ook gepaard moeten gaan met de nodige uitleg over het

zou dus ook gepaard moeten gaan met de nodige uitleg over het doel van de verwerking, de identificatie van de verantwoordelijke en de privacyrechten.

De wet stelt dat de betrokkene geïnformeerd moet worden over bepaalde kenmerken van de gegevensverwerking, de verantwoordelijke en over zijn privacyrechten ten laatste wanneer de gegevens verkregen worden. In een website is dit dus vooraleer een elektronisch formulier ingevuld wordt. Idealiter neemt deze informatie de vorm aan van een privacystatement bovenaan het formulier. Ook kan men bovenaan het formulier een korte tekst of symbool plaatsen die gelinkt is met het privacystatement in, bijvoorbeeld, een pop-up venster. Het KB van de nieuwe privacywet preciseert bovendien dat het recht op verzet bij direct marketing moet verleend worden op het formulier waar de consument schriftelijk data invoert (art. 34).
In de bestudeerde websites die persoonsgegevens verzamelen (93% van de volledige steekproef), vinden we bij 43% van deze websites een privacystatement. Dus nog niet de helft van de websites die uitdrukkelijk persoonsgegevens verzamelen, hebben ergens in hun site een tekst geformuleerd waarin de sinds de privacywet van 1992 opgelegde informatieplicht wordt nageleefd. We zien dat de onderzochte webwinkels op dit vlak beter scoren dan de websites van bedrijven. 54% van de e-shops verleent informatie over hun privacybeleid tegenover 40% van de corporate websites. Het privacystatement van de e-shops is vaak ook verbonden aan andere informatie die een webwinkelier aan de consument op basis van, bijvoorbeeld, de Belgische wet op de handelspraktijken moet verschaffen.

De websites die wel een privacystatement hebben, geven er in 47% van de gevallen een ereplaats aan door er een aparte pagina aan te wijden. 53% integreert de privacyrechten in een globaler geheel. In deze laatste categorie vinden we 28% die de privacyrechten opneemt in de algemene voorwaarden. 11% neemt deze informatie op in de klantendienst, een webpagina waar consumenten (soms in de vorm van een FAQ-pagina, Frequently Asked Questions) informatie vinden over hun rechten. 45% vermeldt de privacyrechten enkel bij het elektronisch formulier. 16% heeft alternatieven bedacht, zoals een disclaimer. In enkele gevallen verschijnt het privacystatement pas in een volgende webpagina, nadat de persoonsgegevens zijn ingevoerd en doorgestuurd. De informatieplicht is echter bedoeld om individuen de mogelijkheid te bieden om een geïnformeerde beslissing te nemen omtrent het al dan niet toevertrouwen van persoonsgegevens. Dit betekent dat zij op de hoogte gebracht moeten worden van hun rechten en van het privacybeleid van de organisatie in het algemeen, vooraleer de verantwoordelijke voor de verwerking hen om persoonsgegevens verzoekt.
Iets minder dan de helft van de websites met een privacystatement, neemt dit op in een aparte webpagina. Maar is deze webpagina gemakkelijk bereikbaar voor de websitebezoeker? In 30% van de gevallen is de privacypagina toegankelijk via de homepage. Dus bij de start van het bezoek aan de website kunnen consumenten zich informeren over het privacybeleid. 23% van de websites met een aparte privacypagina, maken die toegankelijk door middel van een hyperlink (eventueel symbool) die blijvend in de inhoudstafel van de website staat. Op die manier kan een bezoeker, zelfs na het verlaten van de homepage nog gemakkelijk terecht bij het privacystatement. Slechts 21% van de sites leggen een link tussen het elektronisch formulier, waarin gegevens ingetypt kunnen worden, en het aparte privacystatement. Ten slotte gebeurt de link tussen de website en de privacypagina op een andere

de link tussen de website en de privacypagina op een andere manier bij 26% van de websites, namelijk door een woord of logo onderaan iedere webpagina. Soms is dit woord ("beleid", "disclaimer", "voorwaarden", "site policy") in een bijzonder klein lettertype weergegeven. Bovendien moet de bezoeker scrollen naar de bodem van de webpagina om een link naar deze informatie te vinden. Soms moet men verschillende niveaus van de site doorklikken vooraleer informatie te vinden over het privacybeleid. Opvallend is ook dat bepaalde multinationals met een website in het .be-domein, een link leggen met een in het Engels opgesteld privacystatement dat wel voldoet aan enkele Fair Information Practices (enkele principes van zelfregulering omtrent beheer van persoonsgegevens, cf. infra), maar niet aan de Europese of Belgische regelgeving. Ook het gebruik van Engelse termen als "legal disclaimer" bijvoorbeeld is niet echt consumentvriendelijk in een website gericht tot (onder meer) Belgische consumenten.

Een stap verder is het analyseren van de inhoud van het privacystatement. Beantwoordt het aan de wettelijke vereisten? Gaan sommige bedrijven verder dan hun wettelijke plichten? Hoe scoren de privacystatements qua duidelijkheid en volledigheid? Het antwoord op deze en andere vragen laat ons toe om de kwaliteit van de privacystatements te beoordelen.

Eerst en vooral gaan we na of de verantwoordelijke voor de verwerking meegedeeld wordt. Krijgen websitebezoekers te lezen aan wie ze hun gegevens eigenlijk toevertrouwen?

45% van de websites die gegevens verzamelen en die een privacystatement hebben, identificeren de verantwoordelijke voor de verwerking. Hoeveel bedraagt dit percentage echter wanneer we alle websites bekijken die persoonsgegevens verzamelen, los van het feit of ze een privacystatement hebben of niet? Van alle onderzochte websites die gegevens verzamelen, vinden we in totaal slechts 21% die de verantwoordelijke identificeert. Een vijfde geeft dus deze basisinformatie. Vooraleer een persoon kan oordelen of hij/zij persoonsgegevens wenst toe te vertrouwen, is het echter noodzakelijk om te weten bij welke organisatie(s) deze gegevens terechtkomen. Hoe gedetailleerd is deze informatie over de verantwoordelijke in het privacystatement opgenomen? 90% vermeldt de naam van de organisatie, 23% zelfs een specifieke afdeling en 4% een contactpersoon. De privacywet bepaalt ook dat een verantwoordelijke voor de verwerking zijn adres moet meedelen: dit is in 65% van de privacystatements het geval.

10% vermeldt een telefoonnummer van de verantwoordelijke voor de verwerking. 19% neemt een e-mailadres op, wat het de bezoeker gemakkelijk kan maken om contact op te nemen voor eventuele bijkomende informatie. 8% vermeldt verschillende contactgegevens.

Naast de identificatie van de verantwoordelijke, moet men de consument informeren over de doeleinden van de verwerking.

85% van de websites met een privacystatement, delen de doeleinden van de verwerking mee. 15% van de privacystatements bevat dus deze essentiële informatie niet. We kunnen ons hier niet uitspreken over de volledigheid en de kwaliteit van deze informatie. We kunnen in deze analyse van websites namelijk niet nagaan of de meegedeelde doeleinden overeenstemmen met de eigenlijke concrete gebruiksdoeleinden van de data binnen het bedrijf of de verschillende organisaties die de gegevens verwerken.

Wat wel opvalt, is dat 37% van alle onderzochte websites die online persoonsgegevens verzamelen (dus zowel de sites met als zonder privacystatement) meedeelt waarvoor die gegevens gebruikt zullen worden. Een meerderheid van de websites verzamelt dus persoonsgegevens, zonder duidelijk mee te delen waarvoor deze persoonsgegevens gebruikt zullen worden.

Welke doeleinden worden in de websites meegedeeld? 34% van de privacystatements deelt mee dat de data nodig zijn om een bestelling goed af te handelen. 8% spreekt van een abonnement waarvoor de betrokkene zich inschrijft. 60% meldt dat ze met de verzamelde gegevens de consument op de hoogte willen houden van hun producten en diensten. Met andere woorden, wordt in 60% van de privacystatements meegedeeld dat de data voor direct marketing gebruikt zullen worden. 15% deelt mee dat de gegevens ook door derden voor direct marketingdoeleinden gebruikt kunnen worden. 59% van de privacystatements vernoemt daarnaast andere doeleinden, die meestal zeer vaag geformuleerd zijn en eigenlijk volstrekt onduidelijk zijn voor de websitebezoeker. Het gaat om uitdrukkingen als "intern gebruik", "commerciële en contractuele acties", "administratie van de website", "website gebruiksvriendelijker maken", "afstemmen van informatie op kenmerken van de bezoekers" en "een zo goed mogelijke webervaring aanbieden". Voor het vernieuwen van de website door het aanpassen van de inhoud aan kenmerken van de bezoekers, heeft men overigens meestal geen persoonsgegevens nodig. Men kan geïnteresseerd zijn in de leeftijd, de taal, het geslacht en andere kenmerken van bezoekers, maar daarom moeten deze kenmerken nog niet noodzakelijk gekoppeld worden aan individuele persoonsgegevens (zoals naam, adres, etc.). Soms wordt het vage doel "intern gebruik" gekoppeld aan "contractueel verbonden organisaties", waarbij de consument niet wijzer wordt over de eigenlijke gebruiksdoeleinden van de persoonsgegevens.

Aangezien een ruime meerderheid van de onderzochte websites gegevens verzamelt (namelijk 93%) en daarvan een minderheid (43%) een privacystatement heeft, vragen we ons af of in het statement ook de essentiële privacyrechten van de betrokkenen worden meegedeeld. Meer nog, worden er ook (laagdrempelige) procedures voorgesteld om die rechten uit te oefenen?

In 68% van de privacystatements wordt meegedeeld dat de betrokkene een recht op inzage heeft, met name dat de consument zijn gegevens bij de verantwoordelijke kan inkijken. Een derde van de websites met een privacystatement vermeldt dit recht dus niet, hoewel het sinds de privacywet van 1992 moet verleend worden.

Als we nu alle onderzochte websites die persoonsgegevens verzamelen (zowel diegene met en zonder een privacystatement) scannen op het inzagerecht, dan verleent slechts één derde (33%) het recht om de eigen gegevens in te kijken.

En hoe kunnen consumenten dit recht op inzage dan concreet uitoefenen? 54% van de privacystatements deelt geen procedure mee om de eigen gegevens in te kijken. Slechts 25% vermeldt hiervoor een postadres waar de consument dit recht kan uitoefenen. 4% voegt op deze plaats in het privacystatement uitdrukkelijk een specifiek e-mailadres toe. 15% verleent de betrokkene de mogelijkheid om online, dankzij een loginnaam en een paswoord, zijn eigen gegevens in te kijken. We merken dus op dat, hoewel het internet bijzonder laagdrempelige procedures mogelijk maakt om zijn eigen gegevens online in te kijken (en eventueel te verbeteren) een groot aantal websites geen online procedure voorstellen of bepaalde drempels inbouwen om

websites geen online procedure voorstellen of bepaalde drempels inbouwen om het recht op inzage uit te oefenen.

71% van de privacystatements schenkt aandacht aan de mogelijkheid om zijn eigen gegevens te verbeteren indien er fouten in voorkomen. Van alle onderzochte sites die data verzamelen, vermeldt 33% deze mogelijkheid (wat overeenstemt met het percentage websites dat het recht op inzage vernoemt).

Hoe kan een consument nu zijn eigen data verbeteren? Gebeurt dit door een brief te sturen naar de verantwoordelijke of kan men dit online doen? 50% verleent geen informatie over de manier waarop men foute gegevens kan verbeteren. Het recht op verbetering is dan slechts een vaag principe dat niet geconcretiseerd wordt in een laagdrempelige en consumentvriendelijke procedure. 26% geeft de consument de kans om per post het recht op verbetering uit te oefenen. 4% vermeldt een specifiek e-mailadres, al kan natuurlijk elders op de website een e-mailadres staan waar consumenten terecht zouden kunnen met dit verzoek. In 16% van de gevallen moet een consument pen noch papier gebruiken, noch een e-mail sturen. Hij of zij kan rechtstreeks online, dankzij een loginnaam en paswoord, de eigen data verbeteren.

Ten slotte gaan we na in welke mate het recht op verzet verleend wordt. Van zij die in hun privacystatement expliciet vermelden dat de gegevens voor direct marketing gebruikt zullen worden (namelijk 60%), meldt 73% dat de betrokkene het recht heeft om zich hiertegen te verzetten. Hoewel dit recht op verzet nog niet officieel van kracht was op het moment dat deze eerste inhoudsanalyse is uitgevoerd, wordt dit door een meerderheid toegepast. Drie vierden van de websites die gegevens verzamelen en die in hun privacystatement vermelden dat deze data ook voor direct marketing gebruikt zullen worden, vermelden het recht op verzet.

Hoe krijgt een consument nu de kans om zich te verzetten tegen het gebruik van zijn gegevens voor direct marketing? 26% preciseert niet hoe men zijn recht op verzet kan uitoefenen. 30% meldt dat de consument het bedrijf moet contacteren indien hij geen reclame wenst te ontvangen. Hierbij worden geen verdere details van de procedure bekendgemaakt. 13% verleent de betrokkene de mogelijkheid om een vakje aan te kruisen waarmee hij uitdrukkelijk de toestemming verleent dat zijn gegevens voor direct marketing gebruikt mogen worden (d.i. opting-in). Hierbij valt het soms wel eens voor dat het vakje reeds aangekruist is. Er wordt, met andere woorden, vanuit gegaan dat men zich op de mailinglijst van het bedrijf wenst te plaatsen. 30% kiest voor een opting-out procedure: de consumenten kunnen een vakje aankruisen indien zij zich wensen te verzetten tegen het gebruik van hun data voor direct marketing. Slechts één website verwijst naar de bestaande Robinsonlijst voor direct marketing.

Indien de gegevens worden doorgegeven voor direct marketing doeleinden, krijgt men in de helft van de gevallen de mogelijkheid zich te verzetten (52%). We benadrukken dat slechts 15% van de onderzochte websites (die gegevens verzamelen) uitdrukkelijk meedeelt de verzamelde gegevens aan derden door te geven. Het gaat dus om een klein aantal websites binnen de steekproef. Daarom worden deze resultaten met de nodige voorzichtigheid meegedeeld. Dit recht van verzet gebeurt in 33% van de gevallen door het bedrijf te contacteren. 9% verleent een opting-in en 38% verleent een opting-out dankzij een zin en een vakje die de internetgebruiker kan aanvinken. 19% geeft geen nadere toelichting over de te ondernemen stappen.

Een mogelijk interessante bijkomende dienst die aan de consument verleend zou kunnen worden, is dat er één contactpunt zou zijn waar hij geïnformeerd kan worden over het privacybeleid van de onderneming. 49% van de privacystatements biedt op één of andere wijze de uitdrukkelijke mogelijkheid om contact op te nemen met de onderneming (via post, e-mail of telefoon) voor vragen over het privacybeleid. In ongeveer de helft van de gevallen betreft het een algemeen e-mailadres. 36% vermeldt het e-mailadres van een dienst en niet het algemeen e-mailadres van de onderneming. In 22% van de gevallen is er een telefoonnummer van een dienst. De helft draagt een postadres waar men schriftelijk vragen kan stellen. Geen enkel privacystatement vermeldt een 'privacy officer', een werknemer die verantwoordelijk is voor de implementatie van het privacybeleid en vragen hierover beantwoordt.

Samenvattend kunnen we zeggen dat bepaalde websites minimalistische privacyformules hanteren, zoals "Wij respecteren de privacywet", "De privacy van de bezoeker wordt beschermd", "Uw privacy is 100% gewaarborgd" of nog "Wij respecteren de wet van 08.12.92". Sommige privacystatements zijn hiervan de tegenpool. Ze zijn namelijk nogal formeel, langdradig en zeer detaillistisch. Ze roepen eerder verveling op dan interesse en vertrouwen. Bepaalde statements verdrinken soms in de webpagina over de algemene voorwaarden. Ze stellen privacybescherming niet voor als de filosofie van het huis en geven er geen ereplaats aan op hun site. In deze websites gaat het slechts om een noodzakelijke wettelijke formule die ergens wel op de website moet staan. Dergelijke, soms moeilijk verstaanbare, formules geven een erg consumentonvriendelijke indruk. Soms worden de rechten van de consument boudweg genegeerd en wordt het privacystatement eigenlijk enkel geschreven vanuit het standpunt van het bedrijf, niet van de consument. Het wordt dan een 'disclaimer', waarin zoveel mogelijk verantwoordelijkheid wordt afgewimpeld. Het 'privacystatement' wordt dan herleid tot een 'vrijwaring'.

Het is aan te bevelen om een volledig privacystatement op of bij een formulier te plaatsen waar de bezoeker gegevens invoert. Meer details en antwoorden op concrete vragen kan men kwijt in een FAQ-pagina (i.e. antwoorden op veelgestelde vragen). Privacy kan een thema zijn binnen een algemene FAQ-pagina of men kan een aparte webpagina wijden aan zowel het privacybeleid als de beveiliging van de data en de transactie, maar ook aan andere consumentenrechten.
Indien een website in verschillende talen is opgesteld, moet men er ook voor zorgen dat het privacystatement in de verschillende talen is geformuleerd. De stijl van het statement en de woordenschat, spitst men best toe op de kenmerken van de eigen doelgroep(en).

4.3.2. De impliciete gegevensverwerking

Tot nu toe hebben we onze analyse toegespitst op het expliciet verzamelen van persoonsgegevens in elektronische formulieren. Er bestaan echter ook andere technieken om meer te weten te komen over websitebezoekers, bijvoorbeeld door middel van cookies.
51% van de onderzochte websites gebruikt cookies. De afzender van de cookie is in 76% van de gevallen de server van de website zelf. 16% van de cookies zijn afkomstig van één of meerdere derden (bijvoorbeeld marketingbedrijven) die cookies

stig van één of meerdere derden (bijvoorbeeld marketingbedrijven) die cookies sturen. In 7% van de gevallen worden zowel van de website als van externe bedrijven cookies gestuurd.
Een derde van de cookies (34%) zijn sessie-cookies. Deze zijn enkel actief tijdens een bezoek aan een website. Wanneer het bezoek afgelopen is, verdwijnen deze bestandjes. 66% van de cookies kunnen echter gebruikt worden bij herhaalbezoeken (tot soms een verafgelegen datum in 2030, bijvoorbeeld).
Indien een bezoeker zijn browser zo instelt dat cookies niet automatisch aanvaard worden, maar er eerst een waarschuwingsvenster verschijnt, krijgt de bezoeker dan toegang indien de cookies verworpen worden? In 33% van de gevallen krijgt men zonder problemen toegang tot de site, zelfs indien men de cookies dus niet aanvaardt. In 55% van de websites blijft de cookie of blijven de cookies herhaaldelijk verschijnen, wat storend is bij het surfen. Men krijgt in dit geval wel toegang tot de site, maar herhaaldelijk verschijnen opnieuw cookies die de gebruiker kan aanvaarden of verwerpen. In 11% van de gevallen krijgt men geen toegang tot de website indien men op de homepage de cookies niet aanvaardt. Er verschijnt dan soms een webpagina waarin de bezoeker aangeraden wordt om de cookies te aanvaarden. In 12% van de gevallen informeert men de bezoeker over het doel van de cookies in het privacystatement of op een aparte pagina waarin juridische aspecten of algemene voorwaarden uiteengezet worden. 88% van de websites die cookies gebruiken, geven echter nergens op de website informatie over het doel en gebruik van de cookies. De e-shops scoren beter: 20% ervan geeft informatie over cookies in het privacystatement.

4.3.3. De e-mail response test

Het e-mailadres in bepaalde privacystatements heeft ons aangespoord om na te gaan in welke mate een bedrijf een eenvoudige vraag over het privacybeleid kan beantwoorden. Niet alleen waar een privacystatement aanwezig was, hebben we per e-mail een vraag gesteld. Bij iedere website waarin persoonsgegevens gevraagd werden, hebben we een eenvoudig verzoek gericht met betrekking tot, bijvoorbeeld, de doeleinden waarvoor de data gebruikt zullen worden. We hebben voor dit deel van het onderzoek geen K.U.Leuven e-mailadres gebruikt, aangezien dit de antwoorden zou kunnen vertekenen.
Ons e-mailverzoek werd door 57% niet beantwoord. Zij die antwoordden, hadden er enkele minuten voor nodig of beantwoordden de mail soms pas tien dagen later. 78% van zij die antwoordden, hebben binnen de 24 uur feedback gegeven.
Wat is nu de kwaliteit van het antwoord? Wordt specifiek en persoonlijk geantwoord op het verzoek? 65% beantwoordt de vraag concreet en persoonlijk. 18% geeft een gestandaardiseerd antwoord. 17% ten slotte bedankt de consument voor het verzoek, maar gaat niet concreet in op de vraag. Sommige e-mailantwoorden zijn zeer informatief over het uiteindelijke doel van de gegevensverwerking. In een bepaald privacystatement staat bijvoorbeeld dat de data enkel voor "intern gebruik" benut zullen worden. Wanneer men daar in een e-mail op ingaat, komt men te weten dat het eigenlijk om "eigen direct marketingacties" gaat. In sommige e-mails stapt men daarentegen vlug over de vraag heen en stelt men meteen voor om de gegevens uit het bestand te wissen. De vraag van de consument bleef echter beperkt tot informatie over de doeleinden van het bestand en het recht op inzage. Sommige bedrijven

doeleinden van het bestand en het recht op inzage. Sommige bedrijven associëren de vraag rond privacy onmiddellijk en uitsluitend met beveiliging. Ze antwoorden dan ook dat de gegevens adequaat beveiligd worden, maar geven geen informatie over de doeleinden waarvoor de data gebruikt worden. Hoewel het veilig stockeren van persoonsgegevens absoluut noodzakelijk is, moeten we benadrukken dat de bescherming van de privacy echter ook het (conform o.m. wetgeving) beheren en gebruiken van persoonsgegevens inhoudt volgens afspraken die uitdrukkelijk met de consument gemaakt zijn.

Bepaalde antwoorden van bedrijven stemmen tot nadenken, aangezien men aanstipt dat de gegevens momenteel niet voor direct marketing gebruikt worden. Sommigen voegen daaraan toe dat ze niet kunnen voorzien wat er in de toekomst met die persoonsgegevens gedaan zal worden. Hierbij is het echter noodzakelijk om de betrokkene op de hoogte te brengen op het moment dat het privacybeleid wijzigt en de gegevens voor, bijvoorbeeld, direct marketing zouden gebruikt worden. In deze e-mail zou de consument dan de mogelijkheid moeten krijgen zijn keuze aan te geven. De betrokkene heeft namelijk op een bepaald tijdstip zijn gegevens aan het bedrijf toevertrouwd. Indien de doeleinden van de data wijzigen, stemt dit niet meer overeen met de voorwaarden die de consument tijdens het meedelen van zijn gegevens aanvaard heeft. De betrokkene moet dus opnieuw geraadpleegd worden en de mogelijkheid krijgen om deze nieuwe gebruiksvoorwaarden van zijn gegevens, al dan niet te aanvaarden.

Er bestaat een sterk contrast in de resultaten van deze e-mail response test tussen de bedrijven die snel, beleefd en volledig antwoorden op de gestelde vraag en de bedrijven die niet antwoorden of soms zelfs een kort en bot berichtje terugzenden. Bijvoorbeeld, in de trant van "alle informatie vindt u bij het bestelformulier" wat dan uiteindelijk niet klopt gezien er met geen woord gerept wordt over privacyrechten.

Bij meer dan de helft van de websites wordt dus niet geantwoord op een eenvoudig verzoek met betrekking tot de verwerking van de persoonsgegevens. Dit kan op verschillende hiaten wijzen binnen de organisatie. Ten eerste mogen we niet vergeten dat meer dan de helft van de sites geen privacystatement heeft. De informatie over deze materie zal dan waarschijnlijk ook niet intern meegedeeld zijn aan personen die de e-mails moeten beantwoorden. We zien ook dat naargelang de kwaliteit en de volledigheid van het privacystatement stijgt, de kwaliteit van het antwoord en de snelheid van de response toenemen.

Kortom, een privacybeleid mag niet louter een accessoire zijn in het elektronische uitstalraam om vertrouwen op te roepen. Het privacystatement moet intern beleefd worden. Dit kan enkel indien de personeelsleden, die omgaan met persoonsgegevens en e-mails (maar ook brieven, telefoontjes) van klanten en prospecten beantwoorden, ook zelf geïnformeerd worden over de wet en de toepassing van de wet binnen de eigen organisatie. Duidelijke interne communicatie van het privacybeleid moet dus de externe communicatie ervan voorafgaan.

4.4. Besluit bij de analyse van websites

Ter afsluiting van de analyse van privacystatements geven we een overzicht van het percentage websites dat voldoet aan enkele wettelijke verplichtingen. Op basis van de oorspronkelijke privacywet moet minstens informatie gegeven worden over de verantwoordelijke, de doeleinden en eventueel ook het recht van inzage en verbetering. De nieuwe privacywet voegt er nog het recht van verzet bij, wanneer data voor direct marketing gebruikt zullen worden. Op basis van de puur legale aspecten, scoren de onderzochte websites die persoonsgegevens verzamelen als volgt.

Tabel 3. Percentage websites die persoonsgegevens verzamelen en verplichtingen van de privacywet respecteren

Identificatie van de verantwoordelijke	21%
Informatie over de doeleinden	37%
Informatie over het recht op inzage	33%
Informatie over het recht op verbetering	33%
Informatie over het recht op verzet	20%

Hierbij benadrukken we dat het gaat om het percentage van alle onderzochte websites die online persoonsgegevens verzamelen. We herhalen dat van de volledige steekproef 93% op één of andere wijze data van bezoekers verzamelt. Daarvan heeft minder dan de helft (43%) een privacystatement waarin de wettelijk verplichte informatie kan opgenomen worden.

Een meerderheid van de websites scoort dus ruim onvoldoende voor het informeren van de bezoekers over hun privacyrechten en het verlenen van procedures om deze rechten desgewenst uit te oefenen.

Naast deze minimale informatie die door de wet is opgelegd, zijn we nagegaan in welke mate de sites eventueel ook andere informatie meedelen. 21% van alle sites die data verwerken, vermeldt expliciet de privacywet, terwijl in 12% van de sites de Privacycommissie vernoemd wordt. 3% van de onderzochte sites draagt ook een privacylabel (meestal op de homepage) of verwijst naar een ethische code waarop hun privacybeleid gebaseerd is. Hoewel reeds enkele jaren professionele organisaties aan bedrijven de mogelijkheid bieden om een deontologische code te onderschrijven, zich te onderwerpen aan controles en bijgevolg een privacylabel op de website te mogen plaatsen, is een bijzonder klein aantal Belgische sites hierop ingegaan.

Als conclusie van deze eerste analyse, wensen we even na te gaan hoe België scoort ten opzichte van andere landen, waar dergelijk onderzoek al plaatsvond. Indien we deze resultaten vergelijken met buitenlands onderzoek, met name in Frankrijk en de VS, komen we tot de volgende vaststellingen.

In Frankrijk is een verantwoordelijke voor een verwerking van persoonsgegevens sinds 1978 aan een aantal verplichtingen onderworpen (15). Momenteel wordt deze

wet aangepast aan de Europese dataprotectierichtlijn. Naar aanleiding van de twintigste verjaardag van deze wet, nam de CNIL (de Franse Privacycommissie) het initiatief om honderd Franse websites te onderzoeken en na te gaan of ze aan de wettelijke verplichtingen voldeden (cf. http://www.cnil.fr). De CNIL heeft zich beperkt tot e-commerce sites waar bezoekers aankopen kunnen doen. Men stelde vast dat 69% van deze sites informatie over de privacywet bevat. In ons onderzoek in België geeft 43% informatie over het privacybeleid. We hebben gemerkt dat dit voor e-shops hoger ligt, namelijk 54%. Wat toch nog 15% lager is dan in Frankrijk.
81% van de Franse ecommerce sites die cookies gebruiken, geeft geen enkele informatie over de cookies. Dit bedraagt in België 88%. Opnieuw ligt de score voor e-shops hoger. Namelijk 20% van de e-shops die cookies gebruiken geven er informatie over.
52% verleent geen informatie over de manier waarop het recht op inzage uitgeoefend kan worden. 54% van de Belgische sites verleent geen informatie over de te volgen procedure, hoewel 60% van de Belgische e-shops dit wel doet.
We merken bij deze korte vergelijking van enkele resultaten uit het Franse onderzoek met de eerste analyse van Belgische websites, dat Frankrijk hoger scoort wat betreft het integreren van een privacystatement in de website. Op andere vlakken scoren zowel Belgische als Franse e-commerce sites op eenzelfde niveau.
In de Verenigde Staten heeft de Federal Trade Commission ook onderzoek verricht naar de mate waarin privacystatements aanwezig zijn op websites en wat dit privacybeleid precies inhoudt (cf. http://www.ftc.gov). Uit de analyse van een toevalssteekproef van 335 Amerikaanse websites blijkt dat 88% een privacystatement heeft. De inhoud van deze statements is echter moeilijk vergelijkbaar met de informatie die in de Europese Unie aan websitebezoekers meegedeeld moet worden. Wanneer de onderzoekers echter de kwaliteit van deze privacystatements nagaan, zijn de resultaten minder positief. 20% van de privacystatements bevatten alle vier principes van de Fair Information Practices. Dit zijn gedragsregels aanbevolen door bepaalde internationale organisaties (OESO en andere), koepelorganisaties van bedrijven en (Amerikaanse) privacyorganisaties. Het gaat om:

1. Notice: informatie over welke gegevens verzameld worden, hoe (zowel expliciet als impliciet, d.m.v. cookies bijvoorbeeld) dit gebeurt, voor welke doeleinden de data nodig zijn en of gegevens aan derden worden doorgegeven. Verder moet de websitebezoeker geïnformeerd worden over de drie andere richtlijnen.
2. Choice: De betrokkenen moeten de keuze krijgen op welke manier hun persoonsgegevens gebruikt mogen worden, buiten het gebruik van de data voor het doel waarvoor de gegevens oorspronkelijk verzameld worden. Het betreft intern secundair gebruik (bijvoorbeeld, eigen direct marketing campagnes) en extern secundair gebruik (bijvoorbeeld verhuur van gegevens aan derden voor direct marketing).
3. Access: Consumenten moeten ook toegang krijgen tot hun data en mogelijke fouten kunnen corrigeren.
4. Security: De websitebeheerder moet de nodige procedures ontwikkelen om de verzamelde persoonsgegevens te beveiligen.

41% van de onderzochte websites bevatten de principes "notice" en "choice". Op 8% van de websites prijkt een privacylabel (in België 3%). Deze initiatieven van zelfregulering worden dus nog maar zelden gevolgd. Wanneer gegevens voor direct

gulering worden dus nog maar zelden gevolgd. Wanneer gegevens voor direct marketing gebruikt worden, stellen we vast dat 50% in dit verband een keuze aanbiedt (in België 73%). 25% van de sites stellen een opting-in voor (in België 13% een online opting-in). 71% verleent een opting-out (30% een online opting-out in België). 18% van de onderzochte Amerikaanse sites verleent het recht op inzage en correctie (in België 33%).
De Commissie besluit dan ook dat, hoewel er reeds vorderingen geboekt werden, de initiatieven van zelfregulering onvoldoende navolging krijgen. Het onderzoek wijst, volgens de auteurs, aan dat zelfregulering onvoldoende is voor de garantie van een algemene implementatie van een aantal fundamentele principes. De Commissie benadrukt de belangrijke rol die deontologie nog kan spelen, maar adviseert het Amerikaanse Congres wetgevende initiatieven te nemen om, in samenwerking met deontologie, een toereikend niveau van online privacybescherming te kunnen verzekeren (FTC 2000).

Ten slotte vermelden we een internationaal vergelijkend onderzoek, verricht door Consumers International in samenwerking met 13 nationale consumentenorganisaties (cf. http://www.consumersinternational.org). In totaal werden 751 websites onderzocht in de VS en de EU (waaronder 9 Belgische sites). Het onderzoek maakt een onderscheid tussen de algemene toevalssteekproef, de meest populaire websites en enkele categorieën (retail, financiële websites, gezondheidssites). In dit algemeen overzicht beperken we ons tot de resultaten van de algemene steekproef.
67% van de onderzochte websites verzamelt persoonsgegevens van de bezoeker. Naam, e-mailadres en postadres zijn de meest gevraagde persoonsgegevens.
Voor het raadplegen van 7% van de websites moet men persoonsgegevens vrijgeven vooraleer de site bezocht kan worden. Eén derde van de sites tracht een cookie te plaatsen op de computer van de bezoekers.
58% van alle onderzochte sites die persoonsgegevens verzamelen beschikken over een privacystatement. Slechts 32.5% biedt de internetgebruiker de mogelijkheid om het privacystatement te raadplegen op de plaats waar gegevens verzameld worden (dus bij een elektronisch formulier). In 63% van de gevallen was het privacystatement op een gemakkelijke manier te bereiken vanaf de homepage. Indien de privacy policy op de website niet gevonden werd, dan moest de onderzoeker naar de betrokken organisatie e-mailen om uitleg te vragen over het privacybeleid. Op 177 e-mails antwoordde slechts 17%. Dit wijst, volgens de onderzoekers, op een gebrek aan interesse en betrokkenheid van vele bedrijven voor privacy.
Wat het gebruik van data voor direct marketing betreft, stellen de onderzoekers vast dat slechts 20% van de sites het uitdrukkelijk aan de consument overlaat om al dan niet op de mailinglist opgenomen te worden. 9.5% geeft de keuze wanneer het om direct marketing van derden gaat. Wat de inhoud van het privacystatement betreft, is het meest meegedeelde gegeven het doel van de database waarin de gegevens worden opgenomen (52%). 42.5% deelt mee met wie de gegevens gedeeld worden en voor welke doeleinden. 17.5% biedt de consument bepaalde keuzes met betrekking tot de eigen persoonsgegevens. 14% informeert de consument hoe hij zich kan laten schrappen uit een mailinglist van de onderneming. 18% geeft een mogelijkheid om toegang te krijgen tot de eigen data en 31% biedt de mogelijkheid om data te laten verbeteren. 16% biedt daarenboven de mogelijkheid om zijn gegevens uit de database te laten schrappen. 22% van de privacystatements informeert de consument

se te laten schrappen. 22% van de privacystatements informeert de consument over de beveiliging van persoonsgegevens. Ten slotte informeert 6% de consument over de bewaartermijn van de gegevens.
De onderzoekers besluiten hier ook dat, ondanks wettelijke initiatieven van Europese en nationale overheden, de privacy van de consument op het internet nog niet adequaat beschermd wordt. Zowel websites in Europa als in de Verenigde Staten falen in het toepassen van de fundamentele internationale richtlijnen omtrent privacybescherming (Consumers International 2001).

5. BESLUIT: BIG BROTHER OF BIG BUTLER?

Hierboven werden enkele mogelijkheden van internetmarketing aangestipt, waarbij benadrukt werd dat niet alleen op een expliciete, zichtbare manier gegevens over internetgebruikers verzameld kunnen worden. De koppeling met informatie over het surfgedrag van de websitebezoeker, die soms zonder zijn medeweten gevolgd wordt, vormt een scherp profiel, dat soms aanleiding geeft tot het aanbieden van individueel gerichte reclameboodschappen. Daarna gaven we een overzicht van enkele resultaten uit een eerste analyse van Belgische websites omtrent de toepassing van de Belgische privacywet bij het online verzamelen van persoonsgegevens. Consumentendata zijn voor de nieuwe economie namelijk een belangrijke grondstof geworden, maar ook de bescherming van de privacy van consumenten heeft onder meer ook een economische waarde. Het gebruik van nieuwe diensten kan namelijk afgeremd worden, indien niet duidelijk en geloofwaardig genoeg verzekerd kan worden dat bepaalde verwachtingen omtrent de vertrouwelijkheid en de veiligheid en andere aspecten van de persoonlijke levenssfeer van de consument niet geschonden zullen worden. Dit leidt natuurlijk ook tot de vraag of deze verwachtingen ook leven bij de consumenten. Uit de resultaten van Europees, maar ook Amerikaans onderzoek blijkt dat de toekomstmogelijkheden van direct marketing (via directe of interactieve media) sterk samenhangen met de toepassing van een privacybeleid in iedere organisatie, die direct communiceert met prospecten en klanten. Dit privacybeleid moet er niet alleen komen om conform bepaalde wetgeving te handelen. In diverse onderzoeken over direct marketing en privacy wijzen consumenten op een gebrek aan transparantie in de verzameling en het gebruik van persoonsgegevens en een gebrek aan controle over direct marketingcommunicatie, waarvan ze het doelwit zijn. Indien deze negatieve attitude zich verder ontwikkelt en zich ook geleidelijk aan vertaalt in negatief gedrag van consumenten, kan dit leiden tot onder meer een vertrouwenscrisis, die de effectiviteit van directe en interactieve marketing sterk zou kunnen aantasten.

Maar misschien is het al zover? Onderzoek wijst uit dat de groei van elektronische handel en dienstverlening onder meer afhankelijk is van de vraag of de consument erop vertrouwt dat zijn of haar persoonsgegevens bij elektronische aanbieders in goede handen zijn. Het vertrouwen van de consument kan enkel gewonnen worden door hem of haar duidelijk mee te delen waarvoor gegevens nodig zijn - voor bijvoorbeeld de zorg voor een betere en persoonlijkere dienstverlening - waarbij men

de zorg voor een betere en persoonlijkere dienstverlening - waarbij men ook bepaalde garanties geeft omtrent het gebruik van de gegevens en het individu steeds een controlemogelijkheid verleent. Op die manier kan men geloofwaardig aantonen dat men als bedrijf een Big Butler is, die gegevens nodig heeft om persoonlijke dienstverlening te verzorgen, maar geen vermomde Big Brother. Zolang men de consument echter in het ongewisse laat, voedt men zelf (voor)oordelen, vrees en doemscenario's.

Het informeren van de consument is echter onvoldoende. Het betrekken van en voorleggen van keuzes aan de consument leidt tot wat men permissiemarketing is gaan noemen: het vragen van de toestemming van de betrokkene voor het gebruik van persoonsgegevens en het direct communiceren met de consument.

Kortom, de uitdaging, waarvoor de nieuwe economie staat, is om niet alleen dankzij interactieve communicatie prospecten en klanten te polsen naar hun voorkeuren wat producten en diensten betreft om hen persoonlijke dienstverlening te kunnen aanbieden. Men moet hen ook garanties bieden wat betreft de verwerking en het gebruik van hun persoonsgegevens en hen meer controle in handen geven omtrent de manier waarop hun gegevens gebruikt worden, en de wijze waarop met hen gecommuniceerd wordt. Slechts op die manier kan men evolueren naar langdurige, loyale en evenwichtige relaties tussen bedrijven en consumenten, gebaseerd op een dialoog tussen gesprekspartners op voet van gelijkheid.

VOETNOTEN

(1) Direct marketing definiëren we als iedere marketingactiviteit waarbij de intentie van de opdrachtgever erin bestaat direct contact te leggen en/of een duurzame relatie op te bouwen, door middel van voornamelijk directe communicatiemedia, met individuen uit één of meerdere doelgroepen die men door middel van databasetechnieken gesegmenteerd en geïdentificeerd heeft, om uiteindelijk een product of dienst te promoten, aan te bieden, informatie te verstrekken of een andere service te bezorgen (gebaseerd op: Albert, e.a., 1992: 398; Belch, 1993: G6; Bird, 1993: 30; Desjardins, 1992: 27; Hoekstra en Raaijmaakers, 1993: 21; Molenaar, 1996: 4; Pilon, 1993: 11).

(2) Een evolutieschets van het onderzoek over privacy vindt u bij Schoeman, 1992; Walrave, 1999.

(3) PET's kunnen gedefineerd worden als "technical devices organizationally embedded in order to protect personal identity by minimizing or eliminating the collection of data that would identify an individual or, if so desired, a legal person" (Burkert, 1997: 92). Naast het minimaliseren of uitschakelen van de verwerking van persoonsgegevens (door encryptie of anonymiseringstechnieken op het internet) kan men ook de relationele privacy beschermen door software die bijvoorbeeld de toegang tot de eigen mailbox ontzegt aan elektronische post die vanuit bepaalde bedrijven verstuurd wordt of die bepaalde begrippen inhoudt. Dit noemt men anti-spamsoftware, waarmee men ongevraagde en ongewenste (reclame)post kan weren uit het eigen elektronisch postvakje (Walrave, 2001: 87).

postvakje (Walrave, 2001: 87).

(4) De Belgische Mail/Telephone en Fax Preference Service vindt u in de Robinson Service van het Belgisch Direct Marketing Verbond: http://www.bdma.be.
Een overzicht van de Robinsonlijsten in Europa vindt u op http://www.fedma.org/code/page.cfm?id_page=103#liens06.

(5) Meer informatie over dit initiatief vindt u op http://www.e-mps.org.

(6) Uit onderzoek in Vlaanderen blijkt dat 4% van de populatie de Robinsonlijst voor direct mail kan situeren, hoewel deze lijst al 10 jaar bestaat (Walrave, 1999: 364-368). Uit het onderzoek van Schwartz in de V.S. blijken een aantal problemen bij het toepassen van zelf-regulering en de Robinsonlijsten (Schwartz, 1996: 309).

(7) Uit een onderzoek in opdracht van de Europese Commissie blijken onder meer de kosten van ongevraagde commerciële e-mails voor de consument en de internet Service Providers. Ook wordt kritisch het functioneren van de opting-out-bestanden onder de loep genomen en wordt een opting-in-regime aanbevolen:
http://europa.eu.int/comm/internal_market/fr/media/dataprot/studies/spam.htm.

(8) Reeds vijf landen in de Europese Unie hebben voor commerciële e-mails een opting-in systeem aangenomen namelijk Duitsland, Oostenrijk, Denemarken, Finland en Italië. Tijdens de redactie van dit artikel werd op Europees niveau gedebatteerd omtrent de toepasssing van een opting-in systeem voor e-mailmarketing in de gehele Unie in het voorstel van richtlijn omtrent de bescherming van de persoonlijke levenssfeer in elektronische communicatie. De e-commerce richtlijn laat momenteel aan de lidstaten van de Unie de keuze om zelf te beslissen of zij reclame e-mail en SMS, bijvoorbeeld, onderwerpen aan een opting-in of opting-out. Voor twee media laat Europa geen keuze: reclamefaxen en automatische belmachines zonder menselijke tussenkomst zijn reeds aan een voorafgaande toestemming van de ontvanger (opting-in) onderworpen. Intussen keurde de Belgische Ministerraad een voorontwerp van wet goed die de e-commerce richtlijn (van 8 juni 2000) moet omzetten in Belgische wet. Deze omzetting in nationale wet moet ten laatste gebeuren in januari 2002. Naast de verplichtingen waaraan elektronische commerciële transacties moeten voldoen is in dit voorontwerp ook de keuze gemaakt voor een opt-in systeem bij het gebruik van e-mail voor commerciële doeleinden.

(9) Webvertising of internetreclame is iedere (betaalde) boodschap, die een adverteerder via het internet verspreidt om bij de ontvanger een bepaald gedrag uit te lokken (bijvoorbeeld een aankoop) en/of de ontvanger bepaalde kennis bij te brengen over producten, diensten en/of de organisatie en/of zijn of haar houding op een gunstige manier te beïnvloeden.

(10) Meer informatie over cookies en de opties in browsers om cookies uit te schakelen, maar ook de mogelijkheden van anti-cookie software, vindt u op: http://www.cookiecentral.com.

(11) Naast logfiles en cookies, vindt men ook een groeiend aantal andere technieken (b.v. web bugs) die men onder de noemer "spyware" onderbrengt, met name software die door bedrijven maar ook de overheid gebruikt kan worden om het surfgedrag van internetgebruikers te volgen en hieruit profielen te distilleren (Walrave: 2001).

(12) De Europese Dataprotectierichtlijn (95/46/EG) behandelt de bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens.

(13) Wet tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, 11 december 1998. Deze wet vervangt de oorspronkelijke wet van 8 december 1992 (B.S. 18 maart 1993).

(14) Avis N° 34 du 22 Novembre 2000 Avis d'initiative relatif à la protection de la vie privée dans le cadre du commerce électronique (cf. http://www.privacy.fgov.be).

(15) Loi N° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, cf. http://www.cnil.fr/textes/index.htm

BIBLIOGRAFIE

Albert, W. P., e.a. (1992), *Moderne Marketing. Naar het jaar 2000*. Deventer: Kluwer Bedrijfswetenschappen.

Allen, C. (1998), *Internet World Guide to One-to-One Web Marketing*. New York: Wiley Computer Publishing.

Bathelot, B. & S. Carpentier (2001), *La publicité sur Internet*. Paris: Micro Application e-business.

Bazsalisca, M. & P. Naïm (2001), *Data mining pour le Web. Solutions d'Entreprise*. Paris: Editions Eyrolles.

Bird, D. (1993), *Commonscense Direct Marketing*. London: Kogan Page.

CNIL (1998), *Protection des données personnelles et e-commerce en France*. (http://www.cnil.fr).

Consumers International (2001), *Privacy @ net. An international comparative study of consumer privacy on the internet* (http://www.consumersinternational.org).

Dinant, J.M. (1999), *Les Traitements invisibles sur internet*. CRID, FUNDP, Namur (http://www.droit.fundp.ac.be/crid).

FTC (2000), *Privacy on line: Fair information practices in the electronic market-place. A report to congress* (http://www.ftc.gov).

Gavison, R. (1984), Privacy and the Limits of Law in F. Schoeman (ed.), *Philosophical dimensions of Privacy. An Anthology*. Cambridge: Cambridge University Press, p. 346-402.

Gelman, R. (1998), *Protecting Yourself Online*. San Franciso: Harper Edge.

Guldix, E. (1986), *De persoonlijkheidsrechten, de persoonlijke levenssfeer en het privéleven in hun onerling verband*. *Doctoraatproefschrift.* Brussel : VUB.

Hoekstra, J. (1994), *Direct Marketing: van respons tot relatie*. Groningen: Wolterd-Noordhoff.

Janal, D. (1995), *Online marketing handbook*. New York: Van Nostrand Reinhold.

Louveaux, S. (2000), *Spamming: Etat de la question*. CRID, FUNDP, Namur (http://www.droit.fundp.ac.be/crid).

Mathiesen, M. (1996), *Marketing on the internet*. Gulf Breeze: Maximum Press.

Merton, R. (1967), *Social Theory and Social Structure*. New York: Free Press.

Molenaar, C. (1992), *Grondslagen van database marketing*. Alphen aan den Rijn/Zaventem: Samsom BedrijfsInformatie.

Patterson, M. (1998), Direct Marketing in Postmodernity: Neo-tribes and Direct Communications, *Intelligence and Planning, 1998*, Vol. 16(1), p. 68-74.

Peterson, C. (1998), *I love the internet, but I want my privacy too!* Prima Publishing.

Prosser, W. (1984), Privacy. A Legal Analysis in F. Schoeman (ed.), *Philosophical dimensions of Privacy. An Anthology*. Cambridge: Cambridge University Press, p. 104-155.

Rachels, J. (1984), Why Privacy is Important in F. Schoeman (ed.), *Philosophical dimensions of Privacy. An Anthology*. Cambridge: Cambridge University Press, p. 290-299.

Schoeman, F. (1984), *Philosophical dimensions of Privacy. An Anthology*. Cambridge: University Press.

Schwartz, P. (1996), *Data Privacy Law*. Charlottesville: Michie Law Publishers.

Walrave, M. (1999), *Privacy gescand?* Leuven: Universitaire Pers.

Walrave, M. (2001), *e-Marketing & Privacy*. Diegem: Kluwer.

Warren S. & L. Brandeis (1890), The Right to Privacy, *Harvard Law Review*, 15 december, p. 193-220.

Westin, A. (1970), *Privacy and Freedom.* New York: Atheneum N.Y.

Westin, A. (1991), *How the American Public views consumer privacy issues in the early 90's and why. Testimony before the subcommittee on Government Information, Justice and Agriculture*. Committee on Government Operations, US Government Printing Office, Washington D.C., April 10, 1991.