

e-Big Brother: gevreesd of niet?

Attitude & gedrag van internetgebruikers
t.o.v. e-commerce en de bescherming van hun privacy.

Prof. dr. Michel Walrave
K.U. Leuven - Communicatiewetenschap



Reeds beschikbaar in deze reeks:

Privacy Paper Nr. 1.:

e-Privacy in België: werk aan de e-winkel? De bescherming van de persoonlijke levenssfeer in Belgische websites.

Privacy Paper N° 1.:

Privacy and e-Commerce: mind the gap! Protection of consumers' privacy in Belgian websites (in production).

Info: <http://www.e-privacy.be>

Niets uit deze uitgave mag worden verveelvoudigd zonder voorafgaandelijke schriftelijke toestemming van de auteur.

Alle rechten voorbehouden. Michel Walrave © K.U. Leuven

ISBN 90-71047-16-4

D 2001/4140/1

SYNTHESE

Op 1 september werd de nieuwe Belgische privacywet van kracht. Deze wet verleent de consument een aantal rechten met betrekking tot de bescherming van z'n persoonsgegevens. Directe aanleiding om even na te gaan welke ervaringen Belgische internetgebruikers hebben met e-commerce en de bescherming van hun privacy op het Internet. Werden ze al benaderd met (ongevraagde) reclame e-mails en hoe reageren ze erop? Hoe gaan ze om met elektronische formulieren? Vullen ze die getrouw in of zijn bepaalde gegevens taboe? Vinden ze het aanvaardbaar dat hun surfgedrag gevolgd en geanalyseerd wordt of wensen ze een aantal garanties? Deze en andere vragen werden voorgelegd aan meer dan 1000 internetgebruikers.

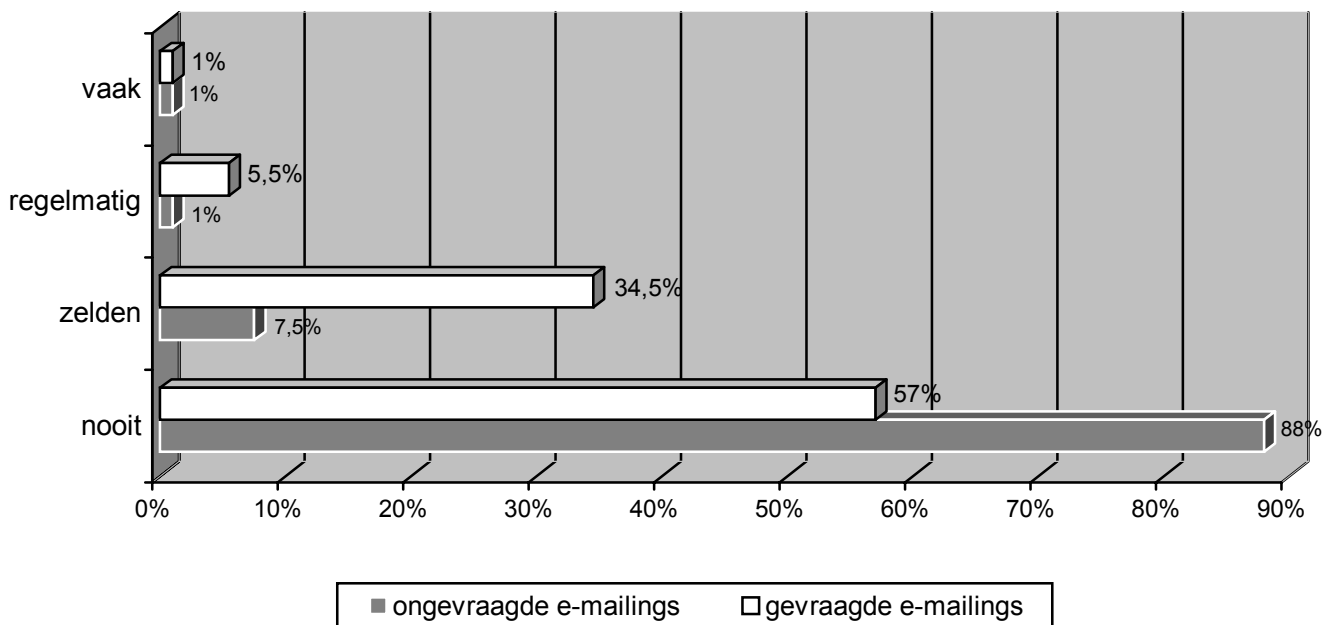
Al spam ervaren?

Hebben onze respondenten reeds (ongevraagde) elektronische reclamepost ontvangen? Zo ja, hoe reageren ze hierop? Is er een onderscheid naargelang ze de afzender kennen of niet?

80 % herinnert zich ooit al **ongevraagd reclame** ontvangen te hebben in zijn elektronisch postvakje. 17 % heeft dit nog nooit ervaren. 3 % gaf geen antwoord op deze vraag. Het percentage internetgebruikers dat ervaring heeft met ongevraagde e-mailings ligt lager dan de consumenten die per e-mail reclame ontvingen waar ze bij de afzender wél om verzocht hadden. 86 % herinnert zich reeds **gevraagde e-mailings** te hebben ontvangen. 13 % heeft dit nog nooit meegemaakt en 1 % gaf geen antwoord. Wat de ongevraagde reclamepost betreft, deelt 13 % mee dat ze dit eigenlijk vaak ervaren (8 % voor gevraagde e-mailings), 30 % regelmatig (37 % voor gevraagde e-mailings) en 37 % zelden (41 % voor gevraagde e-reclamepost).

Welke reactie op e-mailings?

Het gedrag ten aanzien van ongevraagde reclamemails blijkt minder positief dan bij gevraagde commerciële e-mails, zoals blijkt uit Figuur 1. 88 % verklaart nooit te zijn ingegaan op een aanbod van een bedrijf dat een reclame e-mail stuurde zonder dat de ontvanger dit gevraagd had. Het percentage personen die niet reageerden op dergelijk aanbod, ligt duidelijk lager voor gevraagde commerciële aanbiedingen per e-mail (57 %). In totaal ging 40 % ooit reeds in op een aanbod dat gedaan werd in een gevraagde commerciële mail, tegenover 9,5 % voor ongevraagde aanbiedingen per e-mail.



FIGUUR 1.: AL DAN NIET INGAAN OP EEN AANBOD VAN EEN GEVRAAGDE VERSUS ONGEVRAAGDE E-MAILING.

Opt-out of opt-in?

Op Europees niveau wordt discussie gevoerd omtrent de bescherming van de internetgebruiker bij e-mailmarketing. Momenteel geldt in de meeste landen van de Europese Unie een “opting-out regime” voor commerciële e-mails. Bij *opting-out* geeft men de mogelijkheid om zich te verzetten tegen het gebruik van het e-

mailadres (die men invoerde in een bestelformulier, bijvoorbeeld) voor e-mailmarketing. In enkele landen wordt echter *opting-in* toegepast. In dit geval vraagt men **uitdrukkelijk** aan de consument of hij/zij zich in de mailinglist wil laten registreren en dus e-mailings wenst te ontvangen.

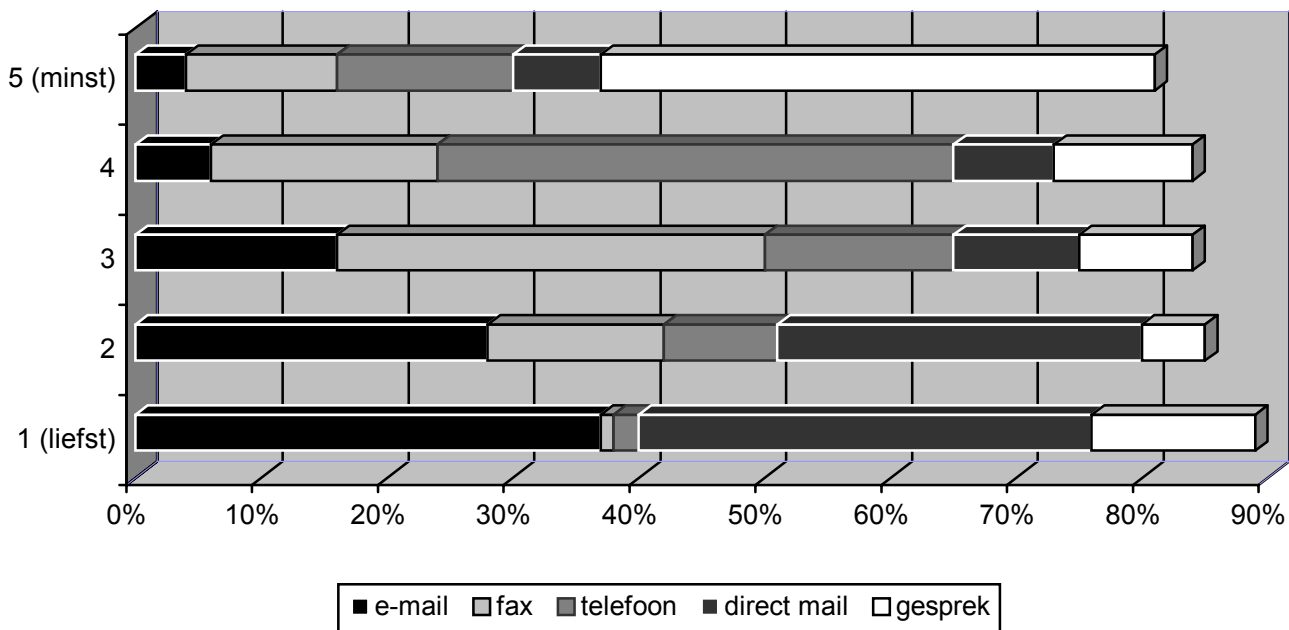
Wanneer we in dezelfde vraag de respondenten laten kiezen, dan verkiest 57 % een *opting-in* en 29 % een *opting-out*. 13 % verkiest andere methoden: ieder bedrijf mag reclame e-mails sturen, zonder meer (3 %) en enkel bedrijven waarbij men al klant is (10 %).

Ook via andere (controle)vragen peilden we naar de mening van de respondenten en kwamen we tot soortgelijke voorkeuren. Wanneer we beide opties neutraal en eenvoudig formuleren in stellingen die we voorleggen aan de respondenten, haalt *opting-in* het boven *opting-out*: 47 % is het eens met de stelling: "Een bedrijf mag mij reclame e-mails sturen zolang ik de mogelijkheid heb om, wanneer ik dit wens, geen e-mails van dit bedrijf meer te ontvangen" (20,5 % neutraal, 28 % niet akkoord en 4,5 % geen antwoord).

Daartegenover is 73 % een *opting-in* gunstig gezind en ziet meer in de stelling: "Een bedrijf mag mij reclame e-mails sturen, indien dit bedrijf mij vooraf de toestemming vraagt" (16 % neutraal, 7 % niet akkoord, 4 % geen antwoord).

Welk succes voor direct marketingmedia?

Wanneer internetgebruikers kunnen **kiezen** welk medium gebruikt wordt om hen op een directe en individuele manier te benaderen, dan scoort e-mail (37 %) en direct mail (36 %) het best. Een face-to-face gesprek met een vertegenwoordiger (13 %), telefonische commerciële communicatie (2 %) en faxreclame (1 %) scoren het laagst (cf. Figuur 2). 15 % van de respondenten verklaart echter via geen enkel van de opgesomde media, door bedrijven benaderd te willen worden. E-mailmarketing heeft dus blijkbaar een interessant potentieel, in vergelijking met bepaalde andere direct marketing media. Vraag is echter welke procedure consumenten verkiezen met betrekking tot het verzamelen en gebruiken van hun e-mailadres voor reclamedoeleinden.



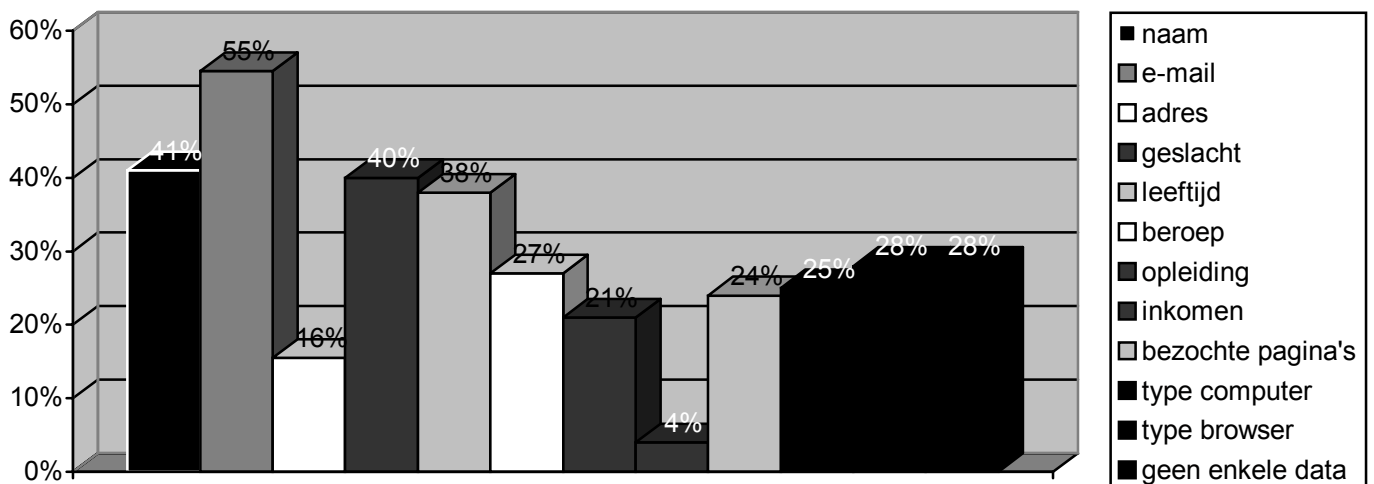
FIGUUR 2.: ATTITUDE TEN AANZIEN VAN DIRECTE RECLAMEVORMEN.

Informatie al geweigerd?

85 % van de ondervraagde internauten verklaart ooit al eens geweigerd te hebben om persoonsgegevens online mee te delen (11 % niet, 2 % geen mening en 2 % geen antwoord). Waarom heeft een meerderheid geweigerd? De hoofdredenen die aangegeven worden betreffen een gebrek aan **vertrouwen** (25 %) en een gebrek aan **informatie** over de eigenlijke doelstelling van de gegevensverwerking (27 %). Dit zijn, naar aanvoelen van onze respondenten, de redenen die hen gestimuleerd hebben om ooit persoonsgegevens online niet toe te vertrouwen. Een e-marketeer maakt dus best wat ruimte vrij in of bij een elektronisch formulier om duidelijk de doeleinden van de gegevensverwerking mee te delen en ook andere initiatieven te nemen om vertrouwen bij websitebezoeker in te boezemen. 15 % van onze populatie meldt toch dat ze gegevens geweigerd hebben, uit zorg om geen elektronische reclamepost te ontvangen.

In Figuur 3 vindt u een overzicht van de data die volgens de respondenten al dan niet 'taboe' zijn. Het elektronische adres scoort hoger (55 %) dan het geografische adres (16 %). Opvallend is dat het geslacht (40 %) en de leeftijd (38 %) en in mindere mate het beroep (27 %) en de opleiding (21 %) geen taboe zijn, vergeleken met het

inkomen (4 %). De respondenten zijn ook verdeeld wat betreft de verzameling van informatie over hun bezoek aan de website en hun computer (type computer: 25 %, type browser: 28 %). 24 % vindt dat een websitebeheerder te weten mag komen welke webpagina's een individuele surfer bezoekt. Vergeten we echter niet dat 28 % van de respondenten vinden dat de webmaster geen enkele gegevens over zijn bezoekers mag verzamelen.



FIGUUR 3: DATA DIE DE RESPONDENTEN BEREID ZIJN OM MEE TE DELEN.

Wanneer wel gegevens verstrekken?

Een ruim deel van onze respondenten ziet een economische ruilverhouding zitten, met name zijn ze bereid om persoonsgegevens te ruilen voor een korting in een webwinkel (11 %), data toe te vertrouwen in ruil voor de toegang tot interessante diensten of informatie (63%). 41,5 % vindt de **duidelijkheid** belangrijk van de gebruiksdoeleinden van het databestand waarin hun gegevens terecht komen. 55,5 % wordt gestimuleerd door het vertrouwen die ze hebben in de organisatie die de website beheert. 53,5 % koppelt het verlenen van persoonsgegevens aan de mogelijkheid om zelf te kunnen **beslissen** wanneer de data uit het bestand gewist moeten worden. Ten slotte wenst 26 % toegang tot de eigen data als voorwaarde tot het verlenen van persoonlijke informatie.

Hebben onze respondenten de ervaring dat ze gemakkelijker informatie toevertrouwen aan een bedrijf, wanneer in een website informatie gegeven wordt over de manier waarop de persoonsgegevens gebruikt zullen worden? 60 % beaamt dit (11 % volledig akkoord en 49 % akkoord) 23 % neemt geen standpunt en 4 % antwoordt niet op de vraag. Bij 13 % is dit niet het geval, zij geven niet gemakkelijker data prijs wanneer informatie verleend wordt over de gebruiksdoeleinden (5 % helemaal niet, 8 % niet).

Wanneer het internetgebruikers niet zint om in een website bepaalde data te moeten vrijgeven, zijn ze dan in staat om bewust foute informatie te verstrekken? Hebben onze respondenten al online een valse naam meegedeeld? 65 % geeft toe ooit wel eens een **valse naam** ingetypt te hebben in een elektronisch formulier (31 % heeft dit nog nooit gedaan, 4 % geeft geen antwoord).

60 % verklaart ons dat het hen al is voorgekomen om een ander e-mailadres mee te delen in een website dan hun regulier e-mailadres dat ze gewoonlijk gebruiken (36 % heeft dit niet gedaan, 4 % antwoordt niet op deze vraag). Deze resultaten roepen vragen op omtrent de kwaliteit van de gegevens die in databases terechtkomen. Om dergelijke foute data te voorkomen is het best om, ten eerste, het doel of de doeleinden van de gegevensverwerking duidelijk te formuleren om aan te tonen waarom de data nodig zijn. Ten tweede mag men geen overmatige gegevens eisen in een elektronisch formulier, namelijk data die eigenlijk in verhouding tot het meegedeelde doel van de database striktgenomen niet noodzakelijk zijn. Ten slotte geeft men de respondent best de mogelijkheid om het invoeren van bepaalde data, die niet noodzakelijk zijn voor het verlenen van de dienst, te weigeren.

Beveiliging van transacties.

Een delicaat aspect van online winkelen kan het meedelen zijn van de kredietkaartgegevens in een elektronisch formulier. Wanneer we de respondenten vragen welke methode zij verkiezen om online aankopen te **betalen**, dan antwoordt de grootste groep dat ze het liefst met een overschrijving zouden willen betalen, namelijk 45 %. 24 % wil de kredietkaartinformatie enkel in een beveiligd formulier intypen. Door gebruik te maken van een anoniem online betalingssysteem, elektronisch geld, is voor 5 % de methode die ze zouden verkiezen. Het meedelen van de data via een call center is voor 1 % de oplossing en het betalen van het

geleverde artikel aan de postbode (dus onder rembours) is voor 8 % de verkozen methode. Blijkbaar moeten vele internetgebruikers nog overtuigd worden van de inspanningen die online winkels doen om hun elektronische transacties te beveiligen.

Analyse surfgedrag: aanvaardbaar?

Hoe staan onze respondenten ten aanzien van het nagaan van het individuele surfgedrag van websitebezoekers? Vinden ze dit aanvaardbaar of niet? Indien dit wel door de beugel kan, stellen de internetgebruikers bepaalde garanties op prijs of niet?

*“Een websitebeheerder moet mij **informer**en wanneer mijn surfgedrag in zijn website gevolgd wordt”*. Deze stelling wordt gevolgd door 83 % van de respondenten (50 % volledig eens, 33 % eens). 9 % kiest geen kamp. 6 % is het hiermee niet eens (2 % helemaal niet, 4 % niet) en 2 % antwoordt niet.

Maar is informatie voldoende of willen consumenten meer zeggenschap? Bijvoorbeeld, dat een webmaster eerst hun toestemming vraagt vooraleer het surfgedrag te monitoren. *“Een websitebeheerder moet mijn **toestemming** vragen vooraleer in een website mijn surfgedrag te volgen”* Dat klinkt goed voor 74 % van de internetgebruikers. 7 % eist dit niet (2 % helemaal niet eens met de stelling, 5 % niet akkoord). 15 % neemt een neutrale positie in en 4 % antwoordt niet. Hebben internetgebruikers misschien meer begrip voor een analyse van hun surfgedrag, indien zij **anoniem** blijven in deze statistieken? Dit is aanvaardbaar voor een ruim deel van de internetgebruikers. 53 % is het hiermee eens (38 % akkoord en 15 % volledig akkoord). 20 % neemt geen standpunt in. 23 % ziet dit toch nog niet zitten (12 % helemaal niet eens met die praktijk, 11 % niet eens). 4 % gaf geen antwoord. Er is blijkbaar wel een begrip voor de voordelen die dergelijke analyses kunnen bijbrengen, maar een meerderheid van de respondenten wenst garanties: informatie, toestemming en eventueel anonieme verwerking van de data.

Een elektronisch schild gewenst?

We peilden ook naar de interesse voor privacybevorderende technologieën, de zogenoemde *PET's* of *privacy enhancing technologies*.

Blijkbaar bestaat er principieel nogal wat interesse voor **anti-spam software**. Dit zijn verschillende mogelijkheden van browsers of andere programma's die ongewenste reclame e-mails de toegang tot de e-mailbox kunnen ontzeggen. Slechts 7 % voelt hier niks voor (9 % spreekt zich hierover niet uit). 13 % verklaart deze mogelijkheden nu reeds te gebruiken. 71 % is geïnteresseerd om deze technologie ooit te gebruiken (19 % een beetje, 28 % nogal en 24 % zeer sterk).

Anonymisers, die het mogelijk maken om anoniem te surfen op het Net, worden door 5 % van de respondenten al gebruikt. 11 % voelt zich hierdoor echter helemaal niet aangesproken. 75 % toont interesse, gaande van ietwat interesse (17 %) naar nogal wat interesse (26 %) tot zeer veel interesse (32 %). 9 % heeft hier geen uitgesproken mening over.

Encryptie, of de versleuteling van telecommunicatie boodschappen, wordt door 9 % reeds benut. 10 % ziet hier niks in, terwijl 72 % interesse toont (20 % een beetje interesse, 22 % nogal wat interesse en 30 % zeer veel interesse). 9 % antwoordt niet op de vraag.

P3P, software die privacy statements automatisch scant en de internetgebruiker waarschuwt wanneer het niveau van privacybescherming niet beantwoordt aan de wensen van de gebruiker, is slechts in testfase (tijdens de afname van de enquête). 8 % is niet geïnteresseerd terwijl 79 % dergelijk hulpje bij het surfen belangrijk vindt (17 % is een beetje geïnteresseerd, 26 % nogal wat en 36 % zeer sterk geïnteresseerd). 13 % gaf geen antwoord.

De nieuwe privacywet: net op tijd?

Uit deze en andere resultaten van de 100 vragen die aan internetgebruikers werden voorgelegd, volgt dat een meerderheid van internauten bezorgd is om bepaalde aspecten van de bescherming van hun privacy online¹. Het gedrag ten aanzien van ongevraagde e-mailings, de attitude en het gedrag ten aanzien van elektronische formulieren en de interesse voor privacybevorderende technologieën zijn zoveel signalen naar de e-marketeers toe. Zij staan nu voor een dilemma: enerzijds helpt de analyse van het surfgedrag, het bijhouden van informatie over attitudes en (koop)gedrag bij het profileren van de wensen en noden van individuele websitebezoekers om hen gericht aanbiedingen te doen. Anderzijds reageren bepaalde internauten argwanend ten aanzien van het online verzamelen van gegevens en het gebruik hiervan om hen, b.v. via e-mail, een persoonlijk aanbod te doen. Hoe kan men nu dit spanningsveld ontladen? Persoonsgegevens zijn namelijk voor de nieuwe economie 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 betrouwbaarheid en de veiligheid en andere aspecten van de persoonlijke levenssfeer van de consument niet geschonden zullen worden. De toepassing van de nieuwe Belgische privacywet reikt hiervoor een aantal instrumenten aan. De wet legt niet alleen een transparantieplicht op, waarbij essentiële informatie over zowel de instantie die de gegevens verzamelt, maar ook over de doeleinden van de verwerking van de persoonsgegevens moet meegedeeld worden. De nieuwe wet verleent de consument een recht om zich gratis te verzetten tegen het gebruik van zijn gegevens voor direct marketing. Informatie hierover, maar ook het meedelen van de procedures waarmee een consument zijn rechten (recht op inzage in de eigen data, verbetering en onder meer verzet) kan uitoefenen, krijgt vorm in een privacystatement die in iedere website (waarin persoonsgegevens verzameld worden) zou moeten prijken. Dit privacybeleid moet er niet alleen – willens of onwillens– komen om conform de wet te handelen. Uit dit en andere

¹ Het eerste luik van dit «e-Privacy in België» onderzoek bestond uit een analyse van het privacybeleid van 250 Belgische websites (cf. <http://www.e-privacy.be>). Het volgende luik bestaat onder meer uit de samenstelling van een typologie van internetgebruikers volgens hun attitude en gedrag ten aanzien van e-commerce en verschillende vormen van e-marketing enerzijds en de graad van privacygevoeligheid anderzijds.

onderzoeken blijkt namelijk de wens van een ruim deel van de populatie om betrokken te worden bij het gebruik en het verkeer van hun persoonsgegevens. Dankzij een geloofwaardig privacybeleid, dat binnen de organisatie gerespecteerd wordt, kan de vrees omtrent een zogenoemde 'Big Brother' die op het Net in het geniep allerlei data zou verzamelen, bij consumenten plaats ruimen voor een 'Big Butler' die prospecten en klanten beter wil leren kennen, om hen volgens hun voorwaarden beter te kunnen bedienen.

Kortom, de uitdaging, waarvoor e-marketeers staan, 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 oprechte dialoog tussen beide gesprekspartners.

AUTEUR

Prof. dr. Michel Walrave is verbonden aan o.a. de K.U. Leuven. Hij verricht onderzoek, publiceert en doceert in binnen- en buitenlandse universiteiten over marketingcommunicatie, direct marketing, call centers, e-marketing en de bescherming van de privacy van de consument.

CONTACT

ADRES: Departement Communicatiewetenschap K.U. Leuven,
Van Evenstraat 2A, B-3000 Leuven.

E-MAIL: Michel.Walrave@soc.kuleuven.ac.be

WEBSITE: <http://www.e-privacy.be>

BOEK

«e-Marketing & Privacy. Zo geclickt?» Michel Walrave, Kluwer, Diegem, ISBN 90 5583 806 3, 160 pag., info: 0800-30 143, info@kluwer.be

Online info: <http://www.e-privacy.be> Online bestellen: <http://www.kluwer.be>