



Federale Overheidsdienst Economie,
KMO, Middenstand en Energie

Gids voor Internetgebruikers



2003

Grid

Nota van de uitgever

Dankwoord

De Federale Overheidsdienst Economie, KMO, Middenstand en Energie bedankt de auteurs van deze gids.

Waarschuwing

De redactie van dit werk werd afgerond in november 2002. Sedertdien kunnen de wetgeving of de tarieven wijzigingen hebben ondergaan. Deze gids is een vulgariserend werk. Voor bijkomende informatie kunt u steeds terecht bij technische of juridische adviseurs.

Vertaling

Dit werk werd oorspronkelijk in het Frans opgesteld. De Nederlandse versie werd verzorgd door de vertaaldienst van de Federale Overheidsdienst Economie, KMO, Middenstand en Energie.

Bestelling

De gids kan worden geraadpleegd (in html-formaat) of gedownload (in pdf-formaat) op de internetsite van de Federale Overheidsdienst Economie, KMO, Middenstand en Energie :

Franse versie :

http://mineco.fgov.be/information_society/consumers/consumers_internetguide/home_fr.htm

Nederlandse versie :

http://mineco.fgov.be/information_society/consumers/consumers_internetguide/home_nl.htm

Deze gids kan ook gratis met de post worden bezorgd, zolang de voorraad strekt. Wend u daartoe tot de Federale Overheidsdienst Economie, KMO, Middenstand en Energie met vermelding van uw naam, uw adres en de titel van het werk.

Federale Overheidsdienst Economie, KMO, Middenstand en Energie

Statistiek en Economische Informatie

Nijverheidsstraat 6

1000 Brussel

e-mail trefpunt@mineco.fgov.be

<http://mineco.fgov.be>

tel. 02 506 51 11

fax 02 513 46 57

Copyright

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm, of op welke andere wijze ook, zonder voorafgaande schriftelijke toestemming van de uitgever.

Verantwoordelijke uitgever

Hans D'HONDT, Leuvenseweg 44, 1000 Brussel

Wettelijk depot

D/2003/1226/07

Deze *Gids voor Internetgebruikers* werd opgesteld door het Centre de Recherches Informatique et Droit (FUNDP – Namen) in het kader van een onderzoekscontract gefinancierd door de Federale Overheidsdienst Economie, KMO, Middenstand en Energie.

Auteurs :

Marie Demoulin
Didier Gobert
Christophe Lazaro
Étienne Montero

Onder de leiding van professor Étienne Montero



Centre de Recherches Informatique et Droit
Facultés Universitaires Notre-Dame de la Paix
Rempart de la Vierge, 5
B - 5000 NAMUR

Tel. : 081/72.47.69.
Fax. : 081/72.52.02.

<http://www.crid.be>

Voorwoord

Deze gids wil, in zo duidelijk mogelijke taal, alles wat rond het internet draait van zijn geheimzinnigheid ontdoen en een antwoord bieden op heel wat vragen van potentiële surfers of andere belangstellenden.

Het is de bedoeling zowel de leek als de ingewijde vertrouwd te maken met een soms niet voor de hand liggende terminologie en zo tot een optimaal gebruik van het internetmedium te komen.

Gelet op het stijgend aantal internetgebruikers en op de mogelijke risico's die met dit nieuwe medium gepaard gaan, en om de sluier rond het internet op te lichten, vertrouwde de Federale Overheidsdienst Economie, KMO, Middenstand en Energie de verwezenlijking van dit werk toe aan het "Centre de Recherches Informatique et Droit" (CRID) van de "Facultés Universitaires Notre-Dame de la Paix" te Namen.

De gids behandelt eerst alles wat te maken heeft met de aansluiting op het internet. Vervolgens vindt de lezer tekst en uitleg over het raadplegen en verzamelen van informatie op het internet.

Wie internet zegt, zegt uitwisseling van informatie. Alle aspecten daarvan worden in deze gids uit de doeken gedaan.

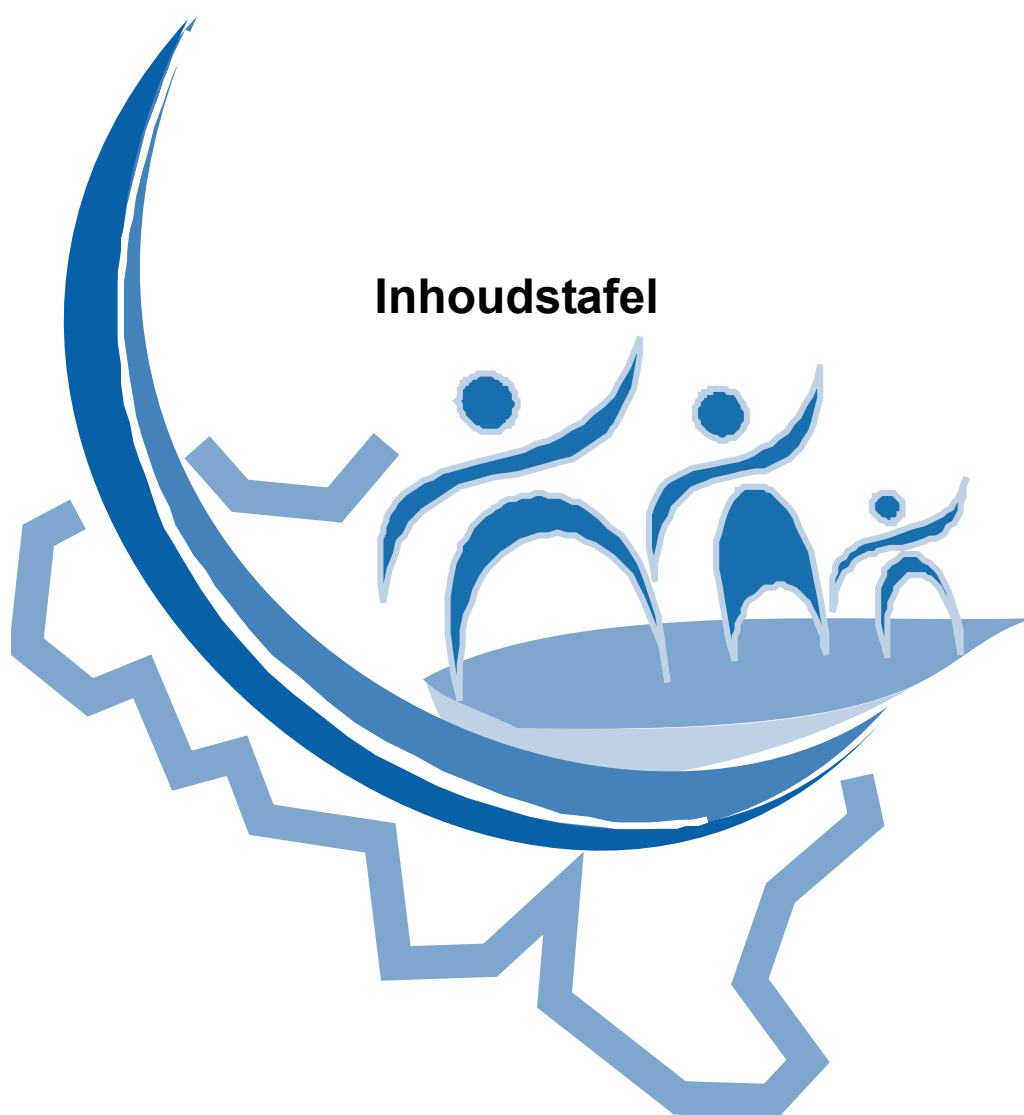
Aangezien het internet een multifunctioneel medium is, wordt de lezer eveneens wegwijs gemaakt in het kopen via het internet en wat daar rechtstreeks verband mee houdt, namelijk de elektronische handel of e-commerce, die een schitterende toekomst tegemoet lijkt te gaan.

Deze gids vertelt u tevens alles over het ontwerpen van een internetsite en over wat een verkoper zoal extra kan aanbieden.

Als afsluiter bevat de gids een uitgebreid glossarium met een aantal veelgebruikte termen uit het internetjargon.

Veel leesgenot !

Lambert VERJUS,
Voorzitter van het Directiecomité



Inhoudstafel

INHOUDSTAFEL

Nota van de uitgever	2
Auteurs	3
Voorwoord	5
Inhoudstafel	7
Deel 1. Zich aansluiten op het internet.....	15
Hoofdstuk I. Aansluiting op het internet.....	16
1. Wat kost een aansluiting op het internet ?	16
2. Welke hardware en software moet ik gebruiken ?	16
3. Welke communicatietechnologie moet ik kiezen ?	17
4. Verwisselbaar Telefonisch Netwerk (VTN).....	17
5. Integrated Services Digital Network (ISDN)	18
6. Televisiekabel	18
7. ADSL.....	19
8. Samenvattende tabel.....	21
Hoofdstuk II. Toegang tot het internet.....	22
9. Waarmee moet je rekening houden bij het kiezen van een internet service provider (ISP) ?	22
10. Wat moet ik denken van het "gratis internet" ?	23
11. Wordt mijn privé-leven geëerbiedigd ?	24
12. Wat zijn mijn verplichtingen tegenover de internetprovider.	24
13. Welke onrechtmatige bedingen zitten er soms in contracten van internet service providers ?	25
Deel 2. Op het internet communiceren	27
Hoofdstuk I. Informatie naslaan.....	28
Afdeling 1. Weg die de informatie volgt op het internet.....	28
14. Welke weg volgt de informatie die op het internet verstuurd wordt ?	28
15. Wat is het "cache(geheugen)" op je harde schijf ?	28
Afdeling 2. Zoeken naar informatie op het internet	29
16. Wat is een URL ?	29
17. Wat is een zoekmachine ?	29
18. Hoe kan mijn site in een zoekmachine worden opgenomen ?	30
19. Wat is een webgids ?	31
20. Wat is een hypertextlink ?	31
21. Welke soorten hypertextlinks bestaan er ?	31
Hoofdstuk II. Informatie verzamelen	33
22. Mag ik alles wat op het internet staat downloaden ?	33
Hoofdstuk III. Informatie uitwisselen	34
Afdeling 1. Elektronische post	34
23. Wat is elektronische post ?	34

24. Wat zijn de zwakke punten van e-mail ?	34
25. Hoe weet ik zeker dat de geadresseerde mijn e-mailbericht heeft ontvangen ?	35
26. Wat is een <i>hoax</i> ?	36
Afdeling 2. "Chatten"	37
27. Wat is " <i>chatten</i> " ?	37
28. Hoe kan ik " <i>chatten</i> " ?	37
29. Welke risico's houdt het chatten in ?	37
Afdeling 3. Discussiefora	38
30. Wat is een discussieforum ?	38
31. Hoe krijg ik toegang tot een discussieforum ?	38
32. Welke risico's zitten er aan een discussieforum ?	39
33. Wat is <i>netiquette</i> ?	39
Deel 3. Mijn website ontwerpen	41
Hoofdstuk I. Een domeinnaam reserveren	42
34. Wat is een domeinnaam ?	42
35. Ben ik verplicht een domeinnaam te hebben ?	43
36. Waaruit bestaat een domeinnaam ?	43
37. Welke uitbreidingen zijn mogelijk ?	43
38. Tot wie moet ik mij richten om een domeinnaam te laten registreren ?	44
39. Moet ik aan voorwaarden voldoen om een domeinnaam te bekommen ?	44
40. Kan ik om het even welke domeinnaam bekommen ?	45
41. Waar kan ik terecht indien ik de reservatie van een domeinnaam door een derde betwist ?	46
Hoofdstuk II. Wat kan ik op mijn site plaatsen zonder de rechten van derden te schenden ?	47
Afdeling 1. Grondbeginselen van het auteursrecht	47
42. Wat is beschermd door het auteursrecht ?	48
43. Moet ik nog aan andere voorwaarden voldoen om door het auteursrecht te worden beschermd ?	48
44. Welke rechten heeft een auteur op zijn werk ?	49
45. Hoe lang is een werk beschermd ?	50
46. Wat is niet door het auteursrecht beschermd ?	50
47. Mag ik een werk dat door het auteursrecht is beschermd nooit reproduceren ?	51
48. Van wie krijg ik toestemming ?	51
Afdeling 2. Concrete vragen die je stelt !	53
49. Heb ik het recht om software voor de aanmaak van een webpagina te gebruiken ?	53
50. Mag ik een foto scannen en in mijn webpagina invoegen ?	53
51. Mag ik een beeld (tekening) scannen en in mijn webpagina invoegen ?	54
52. Mag ik een tekst scannen en in mijn webpagina invoegen ?	54
53. Mag ik een werk (beeld, logo, icoon, foto, tekst, videosequens, muziekbestanden) van een andere site kopiëren of downloaden en op mijn site plaatsen ?	54

54. Mag ik een beeld of foto van een analoge informatiedrager scannen of een beeld of foto van een digitale informatiedrager kopiëren en op mijn website plaatsen, zelfs als ik er vooraf wijzigingen in aanbreng ?	55
55. Mag ik muziekbestanden (bijvoorbeeld mp3's) op mijn site ter beschikking stellen van internetters ?	55
56. Mag ik hyperlinks aanbrengen die verwijzen naar sites met mp3-bestanden ?	57
57. Mag ik een werk zonder <i>copyright</i> -vermelding vrij kopiëren ?	57
58. En wat met de werken met de vermelding “zonder auteursrechten” (copyright free) of de zogenaamde “freewares” of “sharewares” ?	57
59. Als ik met hyperlinks verwijs naar een andere website, moet ik dan de toestemming vragen van de eigenaar van die site ?	58
60. Kan ik mij verzetten tegen het leggen van een hyperlink naar mijn site ?	58
61. Welke sancties worden er getroffen als ik het auteursrecht niet eerbiedig ?	59
62. Is mijn site beschermd door het auteursrecht of door een ander recht ?	59

Deel 4. Zich beschermen tegen “aanvallen” op het internet61

Hoofdstuk I. Inbreuken op het privé-leven62

Afdeling 1. Indringingstechnieken62

63. In hoever wordt mijn privé-leven bedreigd als ik op het internet surf ?	62
64. Wat is een <i>cookie</i> ?	63
65. Waartoe dient een <i>cookie</i> ?	63
66. Moet ik op mijn hoede zijn voor cookies ?	64
67. Hoe kan ik mij beschermen tegen cookies ?	64
68. Hoe kan ik mij juridisch beschermen ?	65
69. Wat is spionagesoftware ?	66
70. Waartoe dient spionagesoftware ?	66
71. Hoe kan ik mij beschermen tegen spionagesoftware ?	67

Afdeling 2. Bescherming van de persoonlijke levenssfeer en verwerking van persoonsgegevens67

72. Wat is verwerking van persoonsgegevens ?	67
73. Hoe kan ik weten wie voor de verwerking van mijn gegevens verantwoordelijk is ?	68
74. Over welke rechten beschik ik om mijn privacy te beschermen ?	69
75. Welke mogelijkheden tot beroep heb ik als mijn rechten niet worden geëerbiedigd ?	70
76. Zijn mijn persoonsgegevens beschermd buiten de Europese Unie ?	70

Afdeling 3. Cybercontrole op het werk71

77. Wat zijn de grote principes ?	71
78. Kan ik in de arbeidsovereenkomst afstand doen van mijn recht op privé-leven ?	72
79. Mag mijn werkgever de inhoud van mijn e-mails controleren ?	73
80. Mag mijn werkgever mijn internetgebruik controleren ?	73

Hoofdstuk II. spamming74

81. Wat is spamming ?	74
82. Hoe komen adverteerders aan mijn elektronisch adres ?	74
83. Kan spamming mij schade toebrengen ?	74

84. Hebben adverteerders het recht mij via e-mail ongewenste reclame toe te sturen ?	75
85. Heb ik het recht om reclame via e-mail te weigeren ?	75
86. Wat moet ik in de praktijk doen om gebruik te maken van mijn recht op verzet ?	75
87. Geldt dit alles ook voor sms-berichten ?	76
88. Bestaan er technische middelen om je tegen spamming te beschermen ? ...	76
Hoofdstuk III. Illegale en nadelige sites	78
89. Mag ik een illegale site op het web straffeloos raadplegen ?	78
90. Wat moet ik doen als ik kinderpornografisch materiaal aantref op het internet ?	78
91. Hoe kunnen minderjarigen worden beschermd tegen ongewenste informatie ?	79
92. Welke filtersystemen zijn thans beschikbaar ?	80
93. Zijn filtersystemen efficiënt ?	80
94. Wat moet ik doen als ik op het web een illegale of nadelige site aantref ?	80
95. Wie kan ik voor het gerecht dagen om schadeloosstelling te krijgen ?	81
Hoofdstuk IV. Cybercriminaliteit.....	82
Afdeling 1. Informaticavervalsing	82
96. Wat is informaticavervalsing ?	82
97. Voorbeelden van informaticavervalsing	82
98. Is informaticavervalsing strafbaar ?	82
99. Kan ik informaticavervalsing plegen zonder dat ik mij daarvan bewust ben ?	82
Afdeling 2. Informaticabedrog.....	83
100. Wat is informaticabedrog ?	83
101. Voorbeelden van informaticabedrog.....	83
102. Is informaticabedrog strafbaar ?	83
103. Kan ik informaticabedrog plegen zonder dat ik mij daarvan bewust ben ?	83
Afdeling 3. Hacking.....	83
104. Wat is hacking ?	83
105. Is ongeoorloofde toegang tot gegevens voor de lol, als uitdaging of om de veiligheid van een systeem te testen strafbaar ?	84
106. Zijn er omstandigheden die de strafmaat kunnen verzwaren ?	85
107. Kan ook ik het slachtoffer zijn van hacking ? Hoe kan ik mij daartegen beschermen ?	85
Afdeling 4. Verzending/ontvangst van virussen.....	85
108. Wat is een computervirus ?	85
109. Welke levensloop heeft een computervirus ?	86
110. Hoe krijg ik een virus ?	87
111. Hoe kan ik weten of mijn computer besmet is ?	87
112. Hoe kan ik mij tegen virussen wapenen ?	87
113. Is het verzenden van virussen strafbaar ?	88
114. Mag ik voor de lol of als grap een "sympathiek" virus versturen ?	88
115. Kan ik worden gestraft als ik buiten mijn weten een virus verspreid dat mijn adressenbestand besmette ?	89
116. Wat moet ik denken van e-mails die mij waarschuwen dat er een gevaarlijk virus in omloop is ?	89

Afdeling 5. Andere vragen die je je stelt.....	89
117. Mag het gerecht of de politie bij mij binnenvallen en mijn informaticamaterieel in beslag nemen ?.....	89
118. Mogen zij gegevens van mijn harddisk of mobiele informatiedragers kopiëren ?.....	89
119. Mogen zij mij beletten toegang te hebben tot sommige gegevens of die gegevens wissen ?.....	90
120. Mogen zij mij verplichten informatie te verschaffen over de manier waarop ik toegang kreeg tot beveiligde gegevens ?.....	90
121. Worden mijn oproep- en identificatiegegevens bij gebruik van het internet geregistreerd en bewaard door sommige netwerk- en dienstenoperators ?	91
Deel 5. Een overeenkomst sluiten op het web.....	93
Hoofdstuk I. Informatie	94
122. Met wie heb ik te maken ? Welke inlichtingen over de verkoper en zijn activiteiten moet ik kunnen vinden ?.....	94
123. Hoe kan ik op netwerken het verschil zien tussen reclame en andere informatie ?.....	95
124. Wat met promotieaanbiedingen, wedstrijden en promotiespelen op de netwerken ?.....	95
125. Over welke informatie moet ik beschikken voor ik een bestelling plaats ?.....	95
126. Moeten de algemene voorwaarden mij worden meegedeeld vóór het sluiten van de overeenkomst ?.....	96
127. Welke informatie moet ik krijgen na mijn bestelling ?	97
128. Kan ik het verloop van mijn bestelling volgen na het sluiten van de overeenkomst ?.....	98
Hoofdstuk II. Het sluiten van een overeenkomst op het internet	99
129. Hoe kan ik iets bestellen op een website ?	99
130. Hoe kan ik weten of ik geen fouten heb gemaakt in mijn bestelling ?	99
131. Vanaf wanneer ben ik contractueel verbonden ?.....	100
132. Hoe ben ik zeker dat de verkoper mijn bestelling gekregen heeft ?.....	100
Hoofdstuk III. Bewijs en elektronische handtekening.....	101
133. Hoe kan ik bewijzen dat ik iets op het internet heb besteld ?	101
134. Hoe kan de verkoper bewijzen dat ik iets via het internet heb besteld ?	101
135. Wordt een gewone e-mail als bewijs erkend ?.....	102
136. Is een elektronisch ondertekend document een afdoend bewijsmiddel ?	102
137. Wat is een geavanceerde elektronische handtekening ?	103
138. Wat is een certificatedienstverlener ?.....	105
139. Wat is een gekwalificeerd digitaal certificaat ?.....	105
140. Wat is een veilig middel voor het aanmaken van een elektronische handtekening ?.....	106
141. Hoe kan ik een digitaal certificaat bekomen ?.....	107
142. Hoe werkt een digitale handtekening in de praktijk ?.....	108
143. Wordt de elektronische aangetekende brief in het Belgisch recht erkend ?.....	109
Hoofdstuk IV. Verzakingsrecht	110
144. Wat is het verzakingsrecht ?	110
145. Voor welke soort aankopen beschik ik over een verzakingsrecht ?	110
146. Hoe kan ik weten of ik over een verzakingsrecht beschik ?	111

147. Wat kan ik doen als ik niet werd ingelicht over mijn verzakingsrecht ?	111
148. Binnen welke termijn mag ik aan een overeenkomst verzaken ?	111
149. Mag ik aan de overeenkomst verzaken indien ik de prijs reeds betaalde ?	112
150. Moet ik een vergoeding betalen om aan de overeenkomst te kunnen verzaken ?	112
151. Mag ik aan de aankoop van een product of dienst verzaken wanneer ik een lening aanging om de betaling te financieren ? Wat gebeurt er met mijn kredietovereenkomst bij verzaking ?	113
152. Hoe moet ik de verkoper laten weten dat ik aan de overeenkomst verzaak ?	113
153. Welke zijn mijn verplichtingen als ik aan de overeenkomst verzaak ?	113
154. Welke verplichtingen heeft de verkoper wanneer ik aan de overeenkomst verzaak ?	114
Hoofdstuk V. Betaling	115
155. Ben ik verplicht te betalen vóór de levering ?	115
156. Welke betaalmiddelen kan ik op de netwerken gebruiken ?	116
157. Kan ik met een kredietkaart betalen ?	116
158. Welke risico's zitten er aan het gebruik van een kredietkaart op de netwerken ?	116
159. Met welke technische middelen worden kredietkaartbetalingen op de netwerken beveiligd ?	117
160. Moet ik de gevolgen dragen van het feit dat iemand met mijn kredietkaart bedrog pleegt op de netwerken ?	118
161. Wat moet ik doen als iemand mijn kredietkaart met bedrieglijk opzet gebruikt ?	119
162. Wat moet ik doen als ik vooraf betaalde met mijn kredietkaart en de verkoper de overeenkomst niet nakomt ?	119
163. Mag ik met mijn debetkaart van Bancontact / Mister Cash betalen ?	120
164. Kan ik rechtstreeks op de site betalen met een elektronische overschrijving ?	120
165. Kan ik met een bankoverschrijving betalen ?	121
166. Kan ik met een cheque betalen ?	121
167. Kan ik bij de levering betalen ?	121
Hoofdstuk VI. Levering van het product of dienstverlening	123
168. Wanneer moet de verkoper de overeenkomst uitvoeren ?	123
169. Wat moet ik doen wanneer de verkoper draait om mijn bestelling uit te voeren ?	123
170. Wordt de overeenkomst <i>online</i> of <i>offline</i> gesloten ?	123
171. Moet ik betalen als het product zoek raakt of bij de levering beschadigd is ?	123
172. Wat moet ik doen indien het geleverde product niet beantwoordt aan de beschrijving op de site ?	124
173. Op welke informatie heb ik recht bij de levering ?	124
174. Welke gevolgen heeft de levering ?	125
Hoofdstuk VII. Terugbetaling en Klantenservice	126
175. In welke gevallen mag ik terugbetaling van mijn aankopen eisen ?	126
176. Welke formaliteiten moet ik vervullen om terugbetaald te worden ?	126
177. Als ik aan de overeenkomst verzaak, binnen welke termijn moet de verkoper me dan terugbetalen ?	126

178. Geldt er voor de producten en diensten die ik op het internet koop een waarborg of klantenservice ?	126
Hoofdstuk VIII. Gedragscodes en labeling	127
179. Wat is een gedragscode ?	127
180. Kan ik vertrouwen hebben in een gedragscode ?	127
181. Kan ik mij beroepen op een gedragscode ?	127
182. Wat is labeling ?	128
183. Kan ik een op een website aangebracht label vertrouwen ?	128
Hoofdstuk IX. Wisselmechanismen voor de regeling van onlinegeschillen	130
184. Wat is een wisselmechanisme voor de regeling van onlinegeschillen (ADR) ?	130
185. Wanneer en hoe kan ik een beroep doen op dat soort mechanisme ?	130
186. Wat zijn de voordelen van ADR ?	131
187. Kan ik een elektronisch bemiddelings- of arbitragemechanisme vertrouwen ?	131
188. Mag men mij dit soort mechanisme opleggen bij het sluiten van een overeenkomst ?	131
189. Welke waarde heeft een ADR-beslissing ?	132
Deel 6. Regeling van grensoverschrijdende geschillen op het internet..	133
Hoofdstuk I. Bevoegde rechtbank bij grensoverschrijdende geschillen.....	134
190. Mag ik een buitenlandse persoon of vennootschap in België dagvaarden ?	134
191. Kan ik voor een buitenlandse rechtbank worden gedaagd ?	135
192. Mag men in een overeenkomst bepalen dat een buitenlandse rechtbank bevoegd is bij eventuele conflicten ?	135
Hoofdstuk II. Toepasselijk recht bij grensoverschrijdende geschillen.....	136
193. Wat zijn de grote principes ?	136
194. Bevat het Verdrag van Rome beschermingsregels voor de consumenten ?	136
195. Kan ik "onderhandelen" over het recht dat toepasselijk is op de overeenkomst ?	137
196. Welk recht is toepasselijk als de partijen geen keuze maken ?	138
197. Welk recht is toepasselijk in geval van misdrijf ?	138
Glossarium.....	139
Nuttige teksten en adressen.....	155
Index.....	161

Deel 1. Zich aansluiten op het internet



HOOFDSTUK I. AANSLUITING OP HET INTERNET

Het internet is een communicatiemiddel geworden waardoor je trefzeker de meest diverse informatie kunt opzoeken en raadplegen. Via dit communicatiemiddel kun je ook in contact komen of handel drijven met een heleboel mensen, organisaties, besturen en handelaars in alle uithoeken van de wereld.

De relaties die via het internet ontstaan, wisselen volgens de gebruikte toepassing. De raadpleging van websites (met informatie in de vorm van teksten, al dan niet bewegende beelden, klanken, enz.) en de verzending van elektronische post (eventueel met een aangehecht bestand) zijn de twee meest gebruikte toepassingen. Daarnaast kun je ook deelnemen aan discussieforums (*newsgroups*), virtueel discussiëren in *real time* (chatten) of snel bestanden verzenden (*FTP*). Welke sleutels heb ik nodig om toegang te krijgen tot die fantastische mogelijkheden ?

1. Wat kost een aansluiting op het internet ?

Aan de prijs van een computer of een *interface box* moet je de volgende vaste kosten toevoegen :

Prijs van een modem : VTN-modem (zie hieronder nr. 4) vanaf 50,00 EUR, ADSL-modem (zie hieronder nr. 7) vanaf 69,00 EUR, ISDN-modem (zie hieronder nr. 5) vanaf 130,00 EUR, kabelmodem (zie hieronder nr. 6) vanaf 219,00 EUR.

Abonnement bij een internetprovider : internetproviders bieden verschillende abonnementsformules aan tegen zeer uiteenlopende prijzen. Let vooral op de tarieven bij aansluiting buiten de in het contract vastgelegde uren. Sinds enkele jaren wordt in België gratis toegang tot het internet verleend (met name door Belgacom.Net, TELonline, FreeWorld, Planet Internet, SwinG, Tiscali, enz.).

Ook moet je rekening houden met eventuele **communicatiekosten** (die verschillen volgens de duur, het tijdstip en de gebruikte technologie). Voor internetgebruikers worden speciale tarieven toegepast (tussen 1,00 EUR en 2,50 EUR per uur, naargelang van het tijdstip van de aansluiting). Online vind je programma's waarmee je de communicatiekosten kunt uitrekenen (zoals : <http://www.kri-soft.be/timer> en <http://www.timeupsoft.com>).

2. Welke hardware en software moet ik gebruiken ?

Doorgaans heb je een computer nodig om op het internet te kunnen surfen. Momenteel kun je je met alle op de markt beschikbare computers op het internet begeven. De minimumconfiguratie is een processor met een snelheid van minstens 100 – 120 MHz, 16 MB vluchtig geheugen (RAM-geheugen) en een grafische kaart van 2 MB. Surfen op het internet is wel een heel stuk aangenameer als je over een snel apparaat beschikt, zodat je niet eindeloos moet zitten wachten op beelden of animaties.

Je hoeft je geen zorgen te maken over het computertype (PC of MAC) of over het besturingssysteem (Windows, Mac OS, Linux of Unix) om op het internet te surfen.

Er zijn verschillende programma's nodig om toegang te krijgen tot de diverse diensten die het internet aanbiedt. Over het algemeen worden ze gratis aangeboden door de internetprovider of hardwareverkoper. Enkele van de meest verspreide programma's zijn *Outlook*, om elektronische post te verzenden en te ontvangen, en *Internet Explorer* of *Netscape Navigator*, om op het internet te surfen. Maar het zijn niet de enige. Er zijn er veel meer.

Van het internet kun je ook een heleboel programma's van uiteenlopende aard downloaden. Dat is onder meer het geval op de volgende sites : <http://www.tucows.com>, <http://www.anshare.com> en <http://www.logicielscenter.com>. Die programma's zijn vaak gratis. Soms worden ze kosteloos aangeboden als demoversie en moet je betalen om ze verder te kunnen gebruiken. Kijk uit en download enkel die programma's waarvan je de oorsprong kent. Anders loop je het risico een virus binnen te halen (zie hierna nr. 108 en volgende).

3. Welke communicatietechnologie moet ik kiezen ?

De telecommunicatiebedrijven bieden momenteel verschillende technologieën aan :

- VTN (zie hieronder nr. 4) ;
- ISDN (zie hieronder nr. 4) ;
- televisiekabel (zie hieronder nr. 6) ;
- ADSL (zie hieronder nr. 7).

Wat de “modems” betreft, bestaan er voor elke categorie verschillende normen, technologieën en merken. Het is bijgevolg belangrijk de raad te volgen van een professional bij een dergelijke aankoop.

4. Verwisselbaar Telefonisch Netwerk (VTN)

Wat is dit ?

Het Verwisselbaar Telefonisch Netwerk is een gewone telefoonlijn. Theoretisch kunnen met deze technologie gegevens tegen een maximumsnelheid van 56.000 bits per seconde worden verstuurd. In de praktijk ligt de transfersnelheid echter niet altijd zo hoog.

Beantwoordt dit aan mijn behoeften ?

Momenteel gebruikt een particulier meestal een klassieke telefoonlijn om op het internet te surfen. Deze is gewoonlijk reeds geïnstalleerd en een beroep op de telecommunicatiediensten hoeft dus niet. Als je gebruik maakt van een dergelijke lijn samen met een gratis internetabonnement, dan zit je goed om voor weinig geld je eerste stappen te doen op het internet. Er zijn wel twee grote nadelen. Ten eerste monopoliseert de toegang tot het internet de telefoonlijn (als ze geactiveerd is) : tijdens het surfen kun je dus geen telefoontjes krijgen. Ten tweede gebeurt de overdracht van informatie nogal traag. Aangezien de internetsites hoe langer hoe meer omvangrijke gegevens bevatten, kan het downloaden van beelden, geluid of andere bestanden soms vrij moeizaam verlopen.

Welke hardware moet ik aanschaffen ?

Als je ervoor kiest je via het klassieke VTN aan te sluiten op het internet, heb je een computer en een modem nodig. Meestal is de modem reeds ingebouwd in de computer (aartzel niet ernaar te vragen als je een computer koopt). Je kunt je vanzelfsprekend ook een aparte modem aanschaffen.

Ben je minder kapitaalkrchtig of wens je geen computer te kopen, dan heeft een van de operatoren voor jou een andere oplossing in petto : de *Netbox*. Dit is een vereenvoudigde

console, die minder duur uitvalt dan een computer en via de scart-ingang op je TV wordt aangesloten en verbonden met je vaste-telefoonlijn. Voor de prijs van een klassieke internetcommunicatie verschaft ze toegang tot de meeste diensten die via het web worden aangeboden. Meestal moet je wel een toetsenbord aankopen.

5. Integrated Services Digital Network (ISDN)

Wat is dit ?

Het *Integrated Services Digital Network* (kortweg ISDN) is een volledig digitaal netwerk dat een snelle en vlotte overdracht van gegevens biedt. Met een basistoegang beschik je over twee kanalen van 64.000 bits per seconde elk. Als je de twee lijnen samen gebruikt, kun je met deze technologie theoretisch data versturen tegen een maximumsnelheid van 128.000 bits per seconde, in beide richtingen van de communicatie.

Beantwoordt die technologie aan mijn behoeften ?

Een ISDN-verbinding is stabiel en minder gevoelig voor analoge storingen dan een VTN-verbinding. Zo'n verbinding is ook sneller (je kunt er viermaal vlugger mee surfen dan met een klassieke lijn). Ze biedt dus meer gebruiksgemak tijdens het internetten. Het nadeel is echter dat je voor de installatie van een dergelijke lijn een beroep moet doen op een telecommunicatiebedrijf, uiteraard tegen betaling. Bovendien is deze oplossing duurder dan een klassieke telefoonlijn, ook al kun je - naast bovenvermelde voordelen - tegelijk surfen op het net en telefoneren, aangezien er twee communicatiekanalen zijn. Doch, in wat volgt zal blijken dat ADSL interessanter is dan ISDN voor particulieren die zich op het internet willen begeven. De overdrachtssnelheid ligt namelijk nog hoger en de kosten zijn forfaitair (dus niet gebonden aan de duur van de verbinding).

Welke hardware moet ik aanschaffen ?

Om via ISDN op het internet te surfen, moet je beschikken over een interface tussen je telefoonlijn en je computer, nl. een "ISDN-modem".

6. Televisiekabel

Wat is dit ?

In steeds meer Belgische steden verschaffen internetproviders toegang via de televisiekabel. Een kabelmodem werkt stukken sneller dan een VTN-modem. De overdrachtssnelheid hangt echter grotendeels af van het tijdstip van de verbinding, m.a.w. van de bezetting van het netwerk.

Beantwoordt die technologie aan mijn behoeften ?

Het belangrijkste voordeel van deze technologie is dat je een reëel comfort hebt bij gebruik van het internet. De verbinding is uitermate snel, je kunt 24u op 24u aangesloten blijven en je kabeltelevisieontvangst wordt niet gestoord. De overdrachtssnelheid kan echter sterk variëren volgens het tijdstip van de verbinding. Ook wordt je telefoonlijn niet belast. Het nadeel van een kabelverbinding is de gebruiksonvriendelijkheid. Als je (met een draagbare computer) het internet op verschillende plaatsen wilt gebruiken, heb je een klassieke modem nodig, die je in alle uithoeken van de wereld moet meenemen.

De kosten zijn forfaitair ; er zijn geen telefoonkosten meer. De prijs van een kabelmodem is daarentegen vrij hoog en het abonnement bij de provider is duurder dan bij de klassieke

internetproviders. Deze technologie is voornamelijk aangewezen voor personen die het internet intensief gebruiken en een groot aantal gegevens downloaden. Het is een interessant alternatief voor ADSL (zie hieronder nr. 7). Wij raden de grote internetgebruikers dus aan beide technologieën en de commerciële aanbiedingen aandachtig te vergelijken. Uiteraard is de kabel de ideale én enige oplossing voor surfers die afgestapt zijn van hun klassieke telefoonlijn ten voordele van hun GSM !

Hou er wel rekening mee dat deze technologie niet in heel België beschikbaar is, ook al stijgt het aanbod met de dag. Deze dienst wordt momenteel aangeboden door Brutélé, tv@blenet, Pandora (Telenet), Coditel, enz.

Welke hardware moet ik aanschaffen ?

Om het internet te gebruiken via de kabel heb je een kabelmodem nodig. Ondanks die benaming zijn kabelmodems niet vergelijkbaar met de standaardmodems die worden aangesloten op het verwisselbaar telefonisch netwerk. De verschillen zijn aanzienlijk, zowel inzake intrinsieke technologie als inzake prestaties. De (externe) kabelmodem wordt gewoonlijk ingeplugd in een vrije poort van de PC via een gewone Ethernet-kaart (die je eventueel moet kopen als er geen in de computer aanwezig is).

7. ADSL

Wat is dit ?

De ADSL-technologie (*Asymmetric Digital Subscriber Line*) maakt gebruik van je klassieke telefoonlijn en zorgt via een modem van de nieuwe generatie voor zeer hoge transfersnelheden (zowat 10 keer sneller voor het downloaden van gegevens en 2 maal sneller voor het verzenden van data). ADSL gebruikt namelijk de twee traditionele koperdraden van de telefoonkabel, maar op hogere frequenties, waardoor je 24 uur op 24 uur op het internet aangesloten kunt blijven en kunt surfen zonder dat je telefoonlijn bezet raakt. Momenteel worden de ADSL-diensten in België aangeboden door Belgacom TurboLine. Die technologie is zeer krachtig (1.000.000 bits per seconde van het netwerk naar je computer en 128.000 bits van je computer naar het netwerk).

Beantwoordt die technologie aan mijn behoeften ?

Zoals de TV-kabel is ADSL eerder geschikt voor relatief grote websurfers. Algemeen kun je stellen dat deze keuze interessant wordt als je met een VTN-verbinding meer dan 30 uur per maand surft tijdens de daluren of meer dan 15 uur tijdens de piekuren.

Hiervoor betaal je een forfaitair maandabonnement. Je telefoonrekening is dus niet meer gelinkt aan de duur van je internetverbinding. Wel moet je, naast je abonnement op je klassieke telefoonlijn, een abonnement betalen voor je ADSL-lijn plus een bijhorend abonnement bij een internetprovider.

Een forfaitair ADSL-abonnement biedt je meestal een maximaal overdrachtsvolume (tussen 10 en 15 gigabyte per maand, afhankelijk van de provider). Bij overschrijding van die grens wordt een meerprijs aangerekend. Weet echter dat een doordeweekse internaut dat volume slechts heel zelden bereikt.

Om technische redenen kan momenteel slechts 90% van de bevolking gebruik maken van ADSL, wat sowieso heel wat meer is dan het aantal mensen dat zich via de televisiekabel toegang tot het internet kan verschaffen. Een goede raad dus : informeer of ADSL beschikbaar is in je streek.

Welke hardware moet ik aanschaffen ?

Buiten de filters die je op je telefoonstekker moet aansluiten om ruis te voorkomen, moet je een ADSL-modem kopen. Over het algemeen wordt al dit materieel als pakket aangeboden tegen een gezamenlijke prijs die schommelt tussen 100,00 en 250,00 EUR.

8. Samenvattende tabel

(prijzen bij benadering in september 2002)

	Klassieke lijn (VTN)	Digitale lijn (ISDN)	Kabel	ADSL
Theoretische transfersnelheid in kbps (ontvangst/verzending)	56/33,6	128/128	1000/128	1000/128
Soort facturatie	op tijdsbasis	op tijdsbasis	forfaitair	forfaitair
Nodige hardware	modem (± 50,00 EUR)	modem (± 120,00 EUR)	kabelmodem (± 200,00 EUR)	ADSL-modem (± 100,00 EUR)
Activeringskosten	in principe geen, want de lijn is bij de meeste gezinnen reeds geïnstalleerd	± 100,00 EUR	50,00 tot 200,00 EUR	25,00 tot 220,00 EUR
Maandabonnement	voor een analoge lijn : 16,19 EUR	voor een digitale lijn : 36,29 EUR	vanaf 30,00 EUR	buiten het klassieke telefoonabonnement (16,19 EUR), ADSL-abonnement : ± 30,00 EUR
Maandabonnement(en) bij internetprovider	0 tot 15,00 EUR en meer	0 tot 15,00 EUR en meer	inbegrepen in het kabelabonnement	± 8,00 tot 10,00 EUR
Verzendings- en ontvangstvolumen	onbeperkt	onbeperkt	toeslag bij overschrijding van het in het abonnement vermelde maximum	toeslag bij overschrijding van het in het abonnement vermelde maximum

Opmerking : de aangeduide prijzen zijn vatbaar voor wijzigingen. Hou ook de vele promotieaanbiedingen van de operatoren in de gaten.

HOOFDSTUK II. TOEGANG TOT HET INTERNET

9. Waarmee moet je rekening houden bij het kiezen van een internet service provider (ISP) ?

Om het internet te kunnen gebruiken, moet je een beroep doen op een internet service provider (ISP), ook wel *internet access provider* (IAP) genoemd. Neem schriftelijk, telefonisch, per fax of via het internet contact op met een van de vele verschaffers van internettoegang. Als je voor een VTN- of ISDN-lijn kiest, dan stuurt de ISP je een installatie-cd-rom alsook de aansluitingsprocedure en alle nodige technische informatie (o.m. het telefoonnummer waarmee je modem op de ISP wordt aangesloten). Als je een gratis abonnement krijgt van een of ander tijdschrift of bij de aanschaf van een computer, dan zit daar meestal ook een installatie-cd-rom bij. Je ontvangt ook een gebruikersnaam en een paswoord waarmee de ISP je kan identificeren. Telkens je je op het internet aansluit, vormt de modem het telefoonnummer van je ISP, deelt hij je gebruikersnaam en paswoord mee, waardoor een lijn wordt 'geopend' tussen jou en de ISP. Vanaf dan kun je op het internet surfen en jouw elektronische post inkijken door middel van de passende software. Ook als je gekozen hebt voor een ADSL-lijn of voor een tv-kabel, verlopen de zaken nauwelijks anders. Voor de installatie heb je misschien de hulp van een technicus nodig als je je niet in staat acht het zelf te doen.

De markt puilt uit van de internetproviders die allerhande abonnementsformules aanbieden, hetzij gratis of tegen betaling. Naar gelang van je behoeften raden wij je aan alle aanbiedingen van een en dezelfde ISP en de aanbiedingen van een aantal andere ISP's te vergelijken, om uit te maken welke oplossing het best overeenstemt met jouw wensen en het best scoort qua kwaliteit/prijsverhouding. Let niet alleen op de prijs, maar ook op de kwaliteit van de aangeboden diensten (overdrachtssnelheid, aantal e-mailadressen, ruimte om je eigen website te hosten, *helpdesk* gratis of tegen betaling, veiligheidspakket inbegrepen of niet, enz.).

Lees aandachtig de abonnementsvoorwaarden die in het contract staan : zo ken je je rechten en verplichtingen. Een goede internetprovider verschaft je niet alleen de bovenvermelde algemene voorwaarden, maar tevens een handleiding met technische informatie over de installatie, de nodige software om je aan te sluiten en te surfen op het internet, een op de klant afgestemde technische dienst (*helpdesk*), een verbinding van goede kwaliteit (hoge snelheid, laag foutenpercentage, weinig onderbrekingen, enz.), een abonnement en een toegang die beantwoorden aan je behoeften, één of meer e-mailadressen en een ruimte om je eigen webpagina's te hosten. Ook moet hij je informeren over het gebruik dat hij maakt van je persoonsgegevens.

De ISPA (*Internet Service Providers Association*), een Belgische vereniging van internettoegangsverschaffers, stelde een gedragscode op die alle leden moeten nakomen. De internetproviders kunnen zich vrij aansluiten bij de ISPA die, hoewel ze niet over het monopolie van goed gedrag beschikt, zonder twijfel de voornaamste referentie vormt in België. In feite is de overgrote meerderheid van de Belgische ISP's lid van de ISPA.

De gedragscode van de ISPA is weliswaar uitgedrukt in zeer algemene en weinig dwingende bewoordingen, maar bevat toch een aantal verplichtingen :

- algemene verplichtingen inzake rechtmatigheid en welgemeendheid (de ISP's moeten ervoor waken dat hun promotionele diensten en producten geen aanleiding geven tot verwarring) ;

- verplichting inzake eerlijkheid (in dat opzicht moeten de ISP's hun klanten informeren over het bestaan van die gedragscode en over de klachtenprocedure) ;
- verplichtingen betreffende de bescherming van persoonsgegevens (de code wijst erop dat het belangrijk is de wet tot bescherming van de persoonlijke levenssfeer na te leven : die wet wordt maar al te vaak over het hoofd gezien) ;
- naleving van de reclamewetgeving (o.m. bedrieglijke reclame vermijden en zorgen voor een gezonde vergelijkende reclame) ;
- informatie over de prijzen (dubbelzinnigheid voorkomen) ;
- maatregelen in verband met de criminaliteit ;
- klachtenprocedure.

Volgens deze gedragscode kun je klacht indienen als een bij de ISPA aangesloten internetprovider één van de voorwaarden van deze code niet naleeft. Je kunt ofwel je beklag doen bij de internetprovider, lid van de ISPA, ofwel rechtstreeks klacht indienen bij het ISPA-comité. Als het ISPA-comité vaststelt dat de klacht gegrond is en het lid weigert in te gaan op de aanmaningen van het comité of als er herhaaldelijk inbreuk wordt gemaakt op de code, dan kan het lid uit de ISPA worden gesloten.

De lijst van de ISPA-leden evenals de gedragscode zijn te vinden op de site van de ISPA : <http://www.ispa.be>

10. Wat moet ik denken van het “gratis internet” ?

Er worden heel wat gratis internetaansluitingen aangeboden. Deze formule is beslist ideaal om het internet te ontdekken, maar is ze wel echt gratis ?

Ten eerste : al krijg je gratis toegang tot het internet, toch zal je de telefoonverbinding moeten betalen (in de veronderstelling uiteraard dat je een vaste telefoonlijn hebt) : momenteel is dat 1,00 EUR per uur tijdens de daluren en 2,50 EUR per uur tijdens de spitsuren ; hierbij moet je nog de prijs van de verbinding voegen, nl. 0,05 EUR. Bovendien moet je computer absoluut uitgerust zijn met een modem of moet je ten minste beschikken over een *Netbox* (minder duur dan een computer) die je kunt aansluiten op je TV, op voorwaarde dat daarop een scartingang aanwezig is.

Ook gaat het gratis websurfen vaak gepaard met de aankoop van een product of dienst (opening van een zichtrekening, aanschaf van een computer, enz.). Soms gaat de gebruiker ermee akkoord om reclame te ontvangen. Bij dergelijke aanbiedingen blijken de marketingtechnieken vaak agressiever en is er een groot risico voor inbreuken op het privé-leven. Weet dus dat zo'n gratis aanbieding secundaire effecten kan hebben.

Ten slotte ben je nooit zeker of een gratis aansluiting kwalitatief evenwaardig is aan een aansluiting tegen betaling. De verbinding kan traag tot stand komen of blokkeren (als de lijn bezet is). Daarenboven moet bij onlinecommercieel en/of technisch advies over de installatie of het gebruik (*helpdesk*) soms een rekening betaald worden.

Conclusie : een gratis aansluiting is ongetwijfeld de ideale oplossing voor gebruikers die hun eerste stappen willen doen op het internet of die slechts zelden surfen. Er zijn goede gratis aansluitingen, maar er zijn er ook die wel eens voor verrassingen kunnen zorgen. Je

moet dus zelf uitmaken of je bereid bent sommige verplichtingen na te komen in ruil voor een gratis internetaansluiting.

11. Wordt mijn privé-leven geëerbiedigd ?

Wanneer je een – al dan niet gratis – abonnement neemt bij een internetprovider, moet je een formulier invullen en enkele persoonsgegevens vermelden. Persoonsgegevens zijn inlichtingen over een natuurlijke persoon die deze persoon identificeren of het – rechtstreeks of onrechtstreeks (door toetsing aan andere gegevens) – mogelijk maken hem te identificeren.

Dat de ISP gegevens verzamelt is niet laakbaar en is zelfs onontbeerlijk om een goed gevolg te kunnen geven aan je verzoek. Door de hoeveelheid en de aard van de ingezamelde gegevens kun je echter de indruk krijgen dat dit niet in verhouding is met de aanvraag (nl. gewoon toegang bekomen tot het internet) : dat is onder meer het geval als men je inlichtingen vraagt over je geslacht, je beroep, je loon, je interessesfeer, je favoriete vrijetijdsbesteding, enz.

Je moet weten dat, op het stuk van de inzameling en meer algemeen de verwerking van persoonsgegevens, de wet tot bescherming van de persoonlijke levenssfeer je vaak protectie biedt (zie hierna nr. 72 en volgende). Die wet verschaft je onder meer het recht op volledige voorafgaande informatie, het recht op toegang tot gegevens over jezelf, het recht op verbetering of schrapping van al die gegevens of een deel ervan, met eventueel het recht om je te verzetten tegen onrechtmatige verwerking van je gegevens of tegen de verwerking van je gegevens voor directe-marketingdoeleinden.

12. Wat zijn mijn verplichtingen tegenover de internetprovider.

Over het algemeen kun je niet onderhandelen over het contract met je internetprovider. Het gaat om een toetredingscontract, dat normaal “te nemen of te laten” is. Bij betwisting is het echter zo dat de rechter het contract in jouw voordeel zal interpreteren.

Dat je de mogelijkheid niet gehad hebt om over het contract te onderhandelen met je internetprovider betekent uiteraard nog niet dat je de clausules van dat contract niet moet naleven (voor zover je de kans kreeg om er kennis van te nemen en ze te aanvaarden). Doorgaans bepaalt het contract in het bijzonder dat de klant :

- de vermelde technische eisen moet naleven ;
- de regels in gebruik op het netwerk moet naleven ;
- de van kracht zijnde wetten en verplichtingen moet naleven ;
- de prijs moet betalen.

Vaak voegt de provider bepaalde clausules met verplichtingen voor de gebruiker aan het contract toe (bijvoorbeeld, het verbod om links te creëren naar ongeoorloofde mp3-bestanden of het verbod om op zijn webstek onwettige of schadelijke informatie te hosten). Je bent verplicht die clausules na te komen aangezien het contract als wet geldt tussen jou en de provider.

Dat principe heeft wel een aantal beperkingen. Vooreerst zijn sommige clausules soms ronduit illegaal omdat ze in strijd zijn met een of andere dwingende wettelijke bepaling. Als dusdanig kunnen zij nietig worden verklaard. Bovendien gaan bepaalde clausules die de

aansprakelijkheid van de provider beperken of die hem ervan vrijstellen de door de rechtspraak gelegde grenzen te buiten kunnen zij dus door de rechter worden bestraft. Ten slotte : de wet betreffende de handelspraktijken en de voorlichting en bescherming van de consument beschermt je tegen onrechtmatige bedingen, d.w.z. clauses die tot een duidelijke wanverhouding leiden tussen de rechten en plichten van de partijen. Onrechtmatige bedingen zijn verboden, vooral als ze de consument benadelen, en zijn dus nietig. In de praktijk moet je de clauses één per één uitpluizen om na te gaan of ze al dan niet onrechtmatig zijn.

13. Welke onrechtmatige bedingen zitten er soms in contracten van internet service providers ?

Zoals hierboven aangegeven, is een onrechtmatig beding een clause in een contract die een duidelijke wanverhouding veroorzaakt tussen de rechten en plichten van de partijen. In de praktijk komt het de rechter toe te beslissen over de onrechtmatige aard van een clause en zal hij ze desgevallend nietig verklaren.

Soms wordt de beoordelingsbevoegdheid van de rechter grotendeels beïnvloed door de wet. Artikel 32 van de wet van 14 juli 1991 betreffende de handelspraktijken en de voorlichting en bescherming van de consument bevat namelijk een lijst met clauses die als onrechtmatig en dus als verboden en nietig worden beschouwd. Hieronder vind je enkele onrechtmatige bedingen uit contracten van internettoegangverschaffers :

- “De ISP houdt zich het recht voor om op elk moment de prijs te veranderen”.

De wet bepaalt dat de verkoper de prijs niet naar eigen goeddunken mag veranderen ;

- “De abonnee mag de ontbinding van het contract niet aanvragen, ingeval de ISP zijn diensten niet levert om redenen van overmacht of om het even welke andere reden”.

Volgens de wet mag de verkoper je niet verbieden de vernietiging van het contract te vragen wanneer hij zijn plichten niet nakomt ;

- “De ISP behoudt zich het recht voor het contract zonder opzegging of vergoeding te ontbinden, ingeval er geen aansluiting op de dienst plaatsvindt gedurende een opeenvolgende periode gelijk aan of groter dan een maand, bij onderbreking van de exploitatie van de dienst, ...”.

Volgens de wet mag de ISP het contract niet eenzijdig naar eigen goeddunken verbreken of wijzigen, zonder je schadeloos te stellen, behoudens om redenen van overmacht ;

- “De ISP is niet aansprakelijk voor schade bij verlies van informaticagegevens opgeslagen op zijn eigen systeem of enige andere schade veroorzaakt door zijn diensten ...”.

Volgens de wet is de ISP op zijn minst aansprakelijk voor een met opzet begane fout of voor een ernstige fout van hemzelf of van zijn aangestelden ;

- “ De abonnee erkent uitdrukkelijk dat elke mededeling die per e-mail gericht is aan de ISP dezelfde waarde heeft als een geschreven document. Elk bericht dat

verstuurd wordt via het e-mailadres of een alias van de abonnee geldt als uitgaande van de abonnee, die zich ertoe verbindt alle mogelijke gevolgen daarvan te dragen”.

Volgens de wet mag de ISP het bewijsmateriaal dat de consument kan gebruiken niet beperken ;

- “Bij een geschil ziet de abonnee ervan af stappen te ondernemen tegen de ISP”.

Volgens de wet mag de ISP de consument niet verplichten af te zien van ieder verhaal tegen hem.

Deel 2. Op het internet communiceren



HOOFDSTUK I. INFORMATIE NASLAAN

Afdeling 1. Weg die de informatie volgt op het internet

14. Welke weg volgt de informatie die op het internet verstuurd wordt ?

Het internet wordt vaak bestempeld als "het net der netten". Die beschrijving strookt vrij goed met de waarheid. Het internet steunt namelijk op een technische architectuur bestaande uit computers, software, routers... Al die machines zijn met elkaar verbonden dankzij een wereldwijd netwerk van communicatielijnen. Om met elkaar te kunnen communiceren, maken de computers van dit reusachtig netwerk gebruik van een communicatiestandaard : het TCP/IP-protocol. Dat protocol is de kern van het internet, vermits het een soort "universele taal" is om via de computer te communiceren.

Als een machine met een andere in verbinding wil komen, verstuurt zij de informatie door ze onder te verdelen in pakketten (IP-pakketten). Elk pakket volgt zijn weg doorheen het internet door gebruik te maken van de minst belaste informaticaverbindingen, zodanig dat de transmissietijd optimaal wordt gebruikt. Bij aankomst worden de pakketten opnieuw samengevoegd. Met technische hulpmiddelen kan worden nagegaan welke weg gegevens afleggen om hun bestemming te bereiken. In tegenstelling met wat men denkt, volgen de data niet noodzakelijk de kortste weg. In feite volgen ze de minst drukke wegen. Ook al zijn er twee Belgische actoren betrokken bij de uitwisseling van gegevens, toch kan het gebeuren dat die gegevens langs Italië, Frankrijk, Noorwegen, de Verenigde Staten, enz. transiteren.

Concreet werkt dit protocol volgens het vraag/antwoordmodel. Je navigator vraagt een internetpagina op (*vraag*) en de ondervraagde server antwoordt op deze vraag (*antwoord*).

Je voert een domeinnaam in je navigator in (bijvoorbeeld : <http://www.droit.fundp.ac.be>). Dit adres wordt in cijfers omgezet en wordt *IP-adres* genoemd (bijvoorbeeld 138.48.9.6). Door op de ENTER-toets te drukken, wordt je verzoek naar je internetprovider gestuurd, die het op zijn beurt naar het internet stuurt.

Binnen dit netwerk is er bij elk belangrijk "kruispunt" een computer, "router" genoemd, die, op basis van het IP-adres, je verzoek in een bepaalde richting stuurt. Wanneer je verzoek bij de ontvangstcomputer, "server" genoemd, aangekomen is, stuurt die terug wat je gevraagd hebt. Ook het antwoord wordt via het web naar je computer of je elektronische brievenbus gestuurd.

15. Wat is het "cache(geheugen)" op je harde schijf ?

Voor het internet is het *cache* de ruimte op de harde schijf en in het vluchtig geheugen (RAM) van je computer, waar je navigator kopieën opslaat van de webpagina's die onlangs werden geraadpleegd. Je navigator gebruikt het cache als een kortetermijngeheugen.

Het **voordeel** van het cache is dat je computer die je verzoek herkent de informatie (het beeld op de website die je onlangs hebt bezocht) niet zal downloaden van het netwerk, maar het opgeslagen beeld vanuit je cachebestand zal laden, wat het navigeren aanzienlijk versnelt.

Het **nadeel** is dat de inhoud van sommige webpagina's geregeld wordt bijgewerkt. Als een pagina in je cachegeheugen werd opgeslagen, zal ze dus verschijnen zoals ze werd opgeslagen bij je recentste raadpleging, zonder de eventuele updates. Om de jongste

versie van de pagina te krijgen, moet je de navigator vragen de pagina te updaten. Een ander nadeel is dat een ervaren gebruiker het cachegeheugen kan openen en de pagina's die door de vorige surfer via dezelfde computer bezocht werden, kan bekijken.

Indien je het wenst, kun je het cache leegmaken, d.w.z. alle bestanden die erin zitten verwijderen als zij te veel ruimte op je harde schijf beginnen in te nemen, of als zij niet meer actueel zijn en niet langer met de bestanden van de webserver overeenstemmen. Je kunt ook de grootte van het cache wijzigen. Je kunt het cache kleiner maken als je ruimte op je harde schijf nodig hebt of het groter maken als je over voldoende ruimte beschikt. Met een ruimer cachegeheugen kun je vlugger een groter aantal recente pagina's raadplegen. Toch is een zeer omvangrijk cachegeheugen niet noodzakelijk een voordeel. In dat geval zou het wel eens kunnen dat je computer meer tijd nodig heeft om te gaan zoeken in de bestanden die in het cache zitten dan om een opzoeking te doen op het internet.

Je moet weten dat op een ander niveau de internetproviders ook een cachegeheugen gebruiken. Dit heeft dezelfde voor- en nadelen als het cache van je computer. Wanneer je je bij een internetprovider (ISP) abonneert, kun je hem vragen de webpagina's van zijn eigen *cache* niet te verschaffen. Dat kan eventueel de prijs van je abonnement verhogen.

Afdeling 2. Zoeken naar informatie op het internet

16. Wat is een URL ?

URL staat voor *Uniform Resource Locator*. URL's zijn de adressen van de verschillende elementen die toegankelijk zijn op het internet. Elk onderdeel dat zich op het internet bevindt, heeft namelijk zijn eigen adres, ook al gaat het enkel om een grafisch beeld van een webpagina. De adressen waar je meestal mee te maken hebt, zijn van een hoger niveau, bijvoorbeeld adressen waarmee je toegang kunt krijgen tot onthaalpagina's van websites.

De URL van de meeste websites bevat na het protocol (bijvoorbeeld : *http*, voor *Hypertext Transfer Protocol*), de letters *www*. Die drie letters geven aan dat de toegangsweg het *World Wide Web* is, namelijk de standaard die werd aangenomen op het internet om gemakkelijk toegang te krijgen tot alle mogelijkheden van het web.

Om gemakkelijker te kunnen internetten, doe je er goed aan je nuttige internetadressen (URL) te archiveren in je browser, zodat je ze niet hoeft te hertypen telkens je tot die sites toegang wil hebben. De browsers van Microsoft en Netscape maken het je heel gemakkelijk en bewaren je adressen onder de naam *favorites* (Internet Explorer) en "bladwijzers" of *bookmarks* (Netscape Navigator). Zodra je adressen gearchiveerd zijn, volstaat het ze te selecteren in een lijst en erop te klikken.

17. Wat is een zoekmachine ?

Om wegwijs te worden op het internet gebruik je best een "zoekmachine" (zoekmotor).

Weet je waarheen je wil surfen en ken je het adres van de site, voer het dan rechtstreeks in de browser in. Ben je integendeel op zoek naar een welbepaalde site waarvan je het adres niet kent of stel je je een vraag over een specifiek onderwerp, dan moet je eerst het adres vinden van de site die aan jouw verwachtingen beantwoordt. Zoekmachines zijn zo opgevat dat ze adressen van sites kunnen vinden aan de hand van de inlichtingen die je invoert.

Een zoekmachine maakt gebruik van exploratiesoftware, een zogenaamde "robot", die de webpagina's constant afloopt en automatisch in een databank indexeert volgens de

trefwoorden die erin voorkomen. Als de opzoeking op de site van de zoekmotor gebeurt door een of meer trefwoorden in te voeren, dan geeft de site als resultaat een reeks hypertext-documenten. Voor elk geselecteerd document wordt een “pertinentiescore” opgemaakt, waaruit kan worden afgeleid hoe vaak opgezochte sleutelwoorden voorkomen in het document, hoe dicht ze bij elkaar staan, of ze voorkomen in de titel van het document, enz. Er zijn heel wat factoren die een rol spelen bij het opnemen van sites in een zoekmachine : vooral van belang is de aanwezigheid van sleutelwoorden in de URL, d.i. het adres van de site, in de titel en de eerste ondertitel of paragraaf van de site, alsook in de metatags.

Metatags zijn verborgen woorden die ingevoegd zijn in de HTML-codes van een site. De voornaamste zoekmachines gebruiken zo'n metatags om een index op te maken van de sites die zij inventariseren. Indien de eigenaar van een site over de verkoop van luxewagens wenst dat de zoekmotoren verwijzen naar zijn webpagina's en de metatags herkennen via de trefwoorden “verkoop luxewagens”, dan volstaat het hem die woorden in te voegen in zijn HTML-codes.

Er bestaan veel zoekmachines. Ze werken echter niet allemaal op dezelfde manier. Sommige proberen volledig te zijn, andere verwijzen enkel naar de beste sites. De bekendste zoekmachines zijn Google, AltaVista, Advalvas, Lycos, Infoseek, enz.

Als je maar één zoekmachine gebruikt, dan weet je niet zeker of je vraag zal worden beantwoord. Indien de zoekmachine de site in kwestie niet vermeldt, krijg je namelijk geen antwoord. Als je een metamotor gebruikt (bijvoorbeeld <http://www.copernic.com/>), dan is er weinig kans dat dit ongemak zich voordoet. Een metamotor gebruikt immers software die simultaan toegang verschaft tot verschillende zoekmotoren. Je krijgt dan sowieso minstens één antwoord op je vraag. Het enige wat je aan een metamotor kunt verwijten, is dat hij te veel antwoorden geeft... Alles hangt dus af van de sleutelwoorden die je invoert. Zoek dus gericht, op basis van nauwkeurige sleutelwoorden, zodanig dat je niet overstelpt wordt met antwoorden.

En ten slotte : naast de “allround”-zoekmachines, die zonder onderscheid alle sites van het web verkennen en indexeren en over het algemeen opgenomen zijn in “publieksportalen”, duiken steeds meer gespecialiseerde motoren op (voor het opzoeken van juridische gegevens, online krantenartikels, mp3-bestanden, beelden en foto's, videosequensen, enz.).

18. Hoe kan mijn site in een zoekmachine worden opgenomen ?

Er zijn twee oplossingen.

Je kunt zelf je site of webpagina aangeven : bij het online brengen van een website of van webpagina's doe je er best aan die site onder te brengen in de gewenste zoekmachines. Daartoe begeef je je gewoon op de site van de zoekmotor en klik je op de link die je hulp of informatie over die aangifte voorstelt. Daar wordt je dan begeleid.

Je kunt ook wachten tot dit automatisch gebeurt : “robotten” (d.w.z. programma's die *browsers*, *webbrowsers*, *crawlers* of *spiders* worden genoemd) lopen het web af, gaan van de ene pagina naar de andere (in feite van de ene link naar de andere), slaan geleidelijk de tekstinhoud van de aangetroffen pagina's op en stellen zo een “index” samen. AltaVista slaat bijvoorbeeld 350 miljoen pagina's op. De robot overloopt op geregelde tijdstippen de pagina's die hij al geïndexeerd heeft om zijn informatiebasis bij te werken.

19. Wat is een webgids ?

Webgidsen (ook webindexen of *subject directories* genoemd) zijn lijsten van sites gerangschikt in categorieën en subcategorieën. Om in de databank te worden opgenomen, moet de site vooraf worden geregistreerd door middel van een formulier waarop een titel, een korte beschrijving en sleutelwoorden m.b.t. het document worden vermeld. Het gaat dus niet om een automatische indexering door een “robot”, maar om een menselijke en “vrijwillige” registratie, aangevraagd door de houder van de site zelf en “manueel” verwerkt door de webgids. Tal van webgidsen stellen ook “robotten” voor, waarbij je via sleutelwoorden opzoekingen kunt doen op sites die in de webgids en/of in het hele web opgenomen zijn.

20. Wat is een hypertextlink ?

Het websurfen gebeurt via hypertextlinks. Die techniek helpt de gebruiker bij het zoeken naar de gewenste informatie via opeenvolgende verwijzingen en loodst hem dus doorheen het reusachtige doolhof van gegevens op het internet.

Hypertextlinks (ook “hyperlinks” of kortweg “links” genoemd) zijn meestal in het blauw onderstreepte woorden (of in ieder geval in een andere kleur dan die van de hoofdtekst). Soms worden ze voorgesteld door een (vast of bewegend) beeld : een logo, een drukknop, een *Java script*, enz. Klik je op een hypertextlink, dan krijg je een andere webpagina. Elke hypertextlink is verbonden met een andere pagina of met een multimediadocument dat zijn eigen URL-adres heeft. Klik je op die link die verbonden is met een adres, dan geef je een bevel aan de server die deze pagina bevat. Een hypertextlink is een interactieve aanduiding van de adresgegevens van een webpagina, beeld of welbepaald gedeelte van een digitaal document. Dankzij die aanduiding ontstaat er een directe verbinding met het document waarnaar de link verwijst als je op de tekst of het beeld klikt.

Een hyperlink bestaat dus uit een zichtbaar en een verborgen deel. Het zichtbaar deel is het door de ontwerper van de pagina gekozen opschrift ; het dient enkel als visuele informatie. Het verborgen deel is het URL-adres. Het opschrift kan echter ook het URL-adres zijn van de pagina waarnaar de link verwijst.

21. Welke soorten hypertextlinks bestaan er ?

- HREF-link : een link die voorkomt in een document en naar een ander document verwijst door weergave van een volledig nieuw scherm op de browser.

Er bestaat wel een bijkomend onderscheid tussen een “simpele hypertextlink” (of *surface linking*) en een “diepe hypertextlink” (of *deep linking*). De eerste legt een verbinding naar de onthaalpagina (*homepage*) van een website, terwijl de andere verwijst naar een secundaire pagina van een website, d.w.z. elke pagina die verschilt van de onthaalpagina.

- Invoeging per hyperlink (inlining) : dat soort hyperlink maakt het mogelijk een beeld (grafiek, logo, enz.) van een andere webpagina (die behoort tot de bezochte website of tot een andere site) in te voegen in een webpagina zonder de bezochte webpagina te verlaten.

Die techniek kan de indruk geven dat je een beeld van de bezochte webpagina bekijkt, terwijl dat beeld eigenlijk van een andere website afkomstig is. Het aldus in de webpagina ingevoegde beeld bevindt zich namelijk op de server van een andere website. Deze link geeft dan ook de mogelijkheid in een webstek beelden in te voegen

die zich op andere sites bevinden, zonder dat je ze hoeft te kopiëren, zodanig dat je minder ruimte gaat gebruiken op de harde schijf van de server die de site herbergt.

- Kadrering (of framing) : met deze techniek kun je een pagina of informatie afkomstig van een site (bronsite) in je eigen webpagina opnemen (doelsite), zonder dat je een nieuw venster hoeft te openen in de browser die naar de bronsite verwijst. Het adres van de doelsite komt dus in de plaats van dat van de bronsite, wat verkeerdelijk de indruk wekt dat de informatie op de doelsite staat (zie hieronder nr. 59).

Dat soort hypertextlink verandert het URL-adres van de pagina die de kadrering uitvoert niet, zelfs indien een pagina van een andere website wordt bezocht.

HOOFDSTUK II. INFORMATIE VERZAMELEN

22. Mag ik alles wat op het internet staat downloaden ?

Het internet is een vergaarbak die constant bevoorraad wordt met teksten, beelden (tekeningen, foto's, logo's, grafieken), muziek- of videobestanden, software, enz. Je kunt je zelfs trakteren op een volledige film op het internet als je genoeg geduld kunt opbrengen en je over een snelle verbinding beschikt, wat steeds meer het geval is met ADSL of met een kabelabonnement. Technisch is er geen enkel probleem om al die bestanden te kopiëren, te downloaden en te hergebruiken. Maar mag je, juridisch gezien, alles downloaden wat zich op het internet bevindt ? Zeker niet !

Het internet is geen gratis zelfbedieningszaak, waar je om het even wat kan gaan halen, waarmee je om het even wat kan gaan doen. Net als in de gewone samenleving moet je ook hier een aantal regels en rechten eerbiedigen. Met andere woorden : de vrijheid van de enen houdt op waar die van de anderen begint. Een van je belangrijkste verplichtingen als internaut is de eerbiediging van de auteursrechten op de informatie die je wil kopiëren, downloaden en/of hergebruiken. Dit speelt uiteraard in beide richtingen : aan de ene kant worden beperkingen opgelegd aan de websurfer als hij bepaalde gegevens wil downloaden of uitbaten, maar aan de andere kant wordt hij beschermd als hij zelf actief deelneemt, bijvoorbeeld door een originele tekst of een beeld te creëren of door een volledige website te ontwerpen die op zijn beurt beschermd wordt.

Vooraleer je iets onderneemt, moet je je dan ook een aantal vragen stellen : wat is beschermd door het auteursrecht, welke zijn de auteursrechten, mag ik een door het auteursrecht beschermd werk dan nooit reproduceren, hoe krijg ik de toestemming van de auteur, mag ik een foto of tekst scannen en op mijn site plaatsen, mag ik muziekbestanden (bijvoorbeeld mp3's) op mijn site plaatsen, mag ik zonder problemen een zogezegd "freeware" of "shareware" programma gebruiken, ...?

Omwille van de eenvormigheid worden die vragen behandeld in het deel "Mijn website ontwerpen" (zie hieronder nr. 42 e.v.).

HOOFDSTUK III. INFORMATIE UITWISSELEN

Afdeling 1. Elektronische post

23. Wat is elektronische post ?

Elektronische post (e-mail, e-post) kan worden gedefinieerd als elk tekst-, spraak-, geluids- of beeldbericht dat over een openbaar communicatienetwerk wordt verzonden en in het netwerk of in de eindapparatuur van de ontvanger kan worden opgeslagen tot het er door de ontvanger wordt opgehaald.

Concreet kun je met de elektronische rechtstreeks berichten sturen aan elke internetgebruiker die een e-mailadres heeft. Een verzonden bericht bestaat uit twee gedeelten : het opschrift en het eigenlijke bericht. Aan het bericht kan ook een bestand (*attachment*) worden gehecht. Dat kan zowel tekst als beelden of geluid bevatten.

Er zijn twee grote soorten e-maildiensten. De eerste dienst wordt verstrekt door de internet provider : deze kent een elektronisch adres toe en zorgt voor de verzending over het netwerk. De berichten worden in de computer van de afzender verwerkt door middel van berichtensoftware. De meest gebruikte programma's voor elektronische post zijn Microsoft Outlook, Eudora en Netscape Messenger. De tweede soort e-maildienst, de webpost, is toegankelijk vanaf navigatiesoftware waardoor berichten via een op het internet aangesloten computer kunnen worden verzonden en ontvangen, zonder toedoen van een internetprovider. Dat is bijvoorbeeld het geval voor de gratis berichtendiensten zoals *hotmail*, *caramail*, *wanadoo*, enz.

Het begrip elektronische post omvat ook het gebruik van de *chat*, het houden van videoconferenties of het verzenden van SMS-berichten (*Short Message Systems*) met een mobiele telefoon. Het kan ook gaan om berichten die op telefonische antwoordapparaten of op de *voice mail* van mobiele telefoons worden achtergelaten.

24. Wat zijn de zwakke punten van e-mail ?

Een van de grootste problemen met elektronische post is het behoud van de integriteit en de vertrouwelijkheid van de inhoud. Door de manier waarop e-post is ontworpen, is dit medium immers niet echt beveiligd. Bij het openlijk hoppen van de ene computer naar de andere kan verzonden post worden onderschept, ingekeken en zelfs gewijzigd door een kwaadwillige gebruiker. Deze kan bovendien een ontvangen bericht anoniem verder verspreiden via een adressenlijst of een discussieforum. Daaruit vloeien dan alle risico's van openbare mededelingen voort : smaad, schending van de persoonlijke levenssfeer en zo meer.

De wachtwoorden die met je *e-mail account* verbonden zijn, wekken een illusie van intimiteit, terwijl een e-mail in feite net zo weinig vertrouwelijkheid biedt als een postkaart. Het gevaar blijft wel *relatief*. Dat een onbekende jouw gewone mails leest, is immers niet erg. Want geef toe : de meeste van onze berichten zijn wellicht van bitter weinig belang voor eventuele spionnen. Nu kan het wel gebeuren dat geheimhouding essentieel is : bij onderhandelingen in het zakenleven, uitwisseling van boodschappen die strict privé moeten blijven, enz.

Voor dat probleem zijn er twee oplossingen, die kunnen samengaan : het anoniem houden en coderen van het bericht. Bij de eerste techniek heeft de verzender de mogelijkheid om onbekend te blijven.

De tweede techniek bestaat erin een bericht enkel leesbaar te maken voor “gemachtigde” personen, d.w.z. personen die een sleutel hebben om kennis te nemen van het bericht. Zo kan e-post, dankzij nieuwe coderingssystemen, thans worden beschouwd als een geschikt middel om uiterst vertrouwelijke informatie over te zenden. Maar al biedt codering een goede bescherming en al is het een veilig middel om de verzender te authenticeren, toch kunnen hierbij andere problemen opduiken : als je de (de)coderingssleutel van een bericht verloren hebt, is dat bericht niet leesbaar. Gebruik dat soort beveiliging dus enkel indien je vindt dat geheimhouding echt nodig is. Als je nooit de behoefte hebt gehad om iets heel belangrijks te verbergen, gebruik dan verder je e-mail zoals je steeds gedaan hebt.

Een ander probleem : hoe kun je weten wie een bericht heeft opgesteld ? Er bestaan namelijk tal van programmaatjes waarmee je mails kunt versturen en het echte adres van de afzender kunt verbergen of verdraaien. Stel dat een flauwe grappenmaker er zo eentje gebruikt en zich onrechtmatig jouw identiteit toe-eigent om liefdesverklaringen of dreigbrieven naar sommige van je kennissen of collega's te sturen. Dat zou je heel wat kopzorgen kunnen geven.

Gelukkig bestaan er tal van methodes om in al je berichten een soort van “elektronisch teken” in te voegen, dat je automatisch authenticereert als auteur of althans bevestigt dat je berichten wel degelijk vanaf jouw computer werden verstuurd. Daarnaast kun je steeds gebruik maken van de elektronische handtekening, zoals ingevoerd bij de wet (zie hieronder nr. 137 e.v.).

Er kunnen ook problemen opduiken in verband met de veiligheid. Via elektronische post kunnen immers computervirussen worden verspreid (zie hieronder nr. 108 e.v.). Virussen huizen meestal in uitvoerbare bijgevoegde bestanden, maar kunnen ook de kop opsteken bij andere toepassingen (bijvoorbeeld in tekstverwerkingsbestanden).

Een laatste probleem met elektronische post : hoe bewijs je het bestaan of de inhoud van een verstuurd bericht ? Die vraag rijst onder andere in het kader van de e-commerce (zie hieronder nr. 133). Het probleem kan grotendeels worden opgelost door gebruik te maken van een beveiligde handtekening.

25. Hoe weet ik zeker dat de geadresseerde mijn e-mailbericht heeft ontvangen ?

Als je een elektronisch bericht verstuurt, kunnen er zich verscheidene problemen voordoen.

Vooreerst zou het kunnen dat jouw berichten om technische redenen niet ter bestemming geraken. Het probleem kan onder andere te wijten zijn aan de server van je correspondent : misschien is die defect en daardoor niet toegankelijk. In dat geval krijg je het bericht in principe snel teruggestuurd.

Het probleem kan ook bij jou liggen : misschien heb je de elektronische adresgegevens van de bestemming verkeerd gespeld. In dat geval stuurt de server het bericht terug en meldt hij dat hij het niet kan afleveren (*User unknown* of *Host unknown*).

Ook al is er geen technisch probleem, soms vraag je je af of je correspondent het door jou verstuurd bericht wel degelijk heeft ontvangen. Wanneer je geen antwoord krijgt, is het mogelijk dat de server van je correspondent het bericht wel ontvangen heeft, maar dat je correspondent zijn post niet heeft geopend.

Om niet met deze onzekerheid verveeld te zitten, kun je in je software de functie “ontvangstbevestiging” activeren. Aangezien er echter geen derde is om de verzending te bevestigen en de mogelijkheden om te knoeien met de datum en het uur legio zijn, is de waarde van zo'n ontvangstbevestiging zeer betrekkelijk. Bovendien wordt de bestemming meestal ingelicht over de aanvraag om ontvangstbevestiging en moet hij aanvaarden dat ze hem wordt toegezonden. Het spreekt voor zich dat hij resoluut zal weigeren als het bericht hem niet bevalt.

Om die redenen liberaliseerde de overheid de elektronische aangetekende brief en behoudt De Post enkel een monopolie op verzendingen in papiervorm (zie hieronder nr. 143). Net als voor een traditionele aangetekende brief kan de afzender van een elektronisch ondertekend bericht een bewijs bekomen van de verzending, de datum en eventueel de ontvangst. Daartoe is wel een vertrouwensderde nodig, die in zekere zin dezelfde functie vervult als De Post. Hij bevestigt de verzending door middel van het elektronisch ontvangstbewijs dat bij het aanbieden wordt verstrekt ; hij bewaart de datum en het uur van de verzending ; hij kan ten slotte gebruik maken van de technische hulpmiddelen die de ontvangst bewijzen.

26. Wat is een hoax ?

Een *hoax* (of solidariteitsketting of kettingmail) is een loze of valse waarschuwing, een poets, een e-mail-grap. De hoax bestond al voor de opkomst van het internet, maar vond in de e-mail een gedroomde drager om zich voort te planten.

De meest voorkomende hoaxes verwijzen naar de aanwezigheid van een zogezegd uiterst gevaarlijk virus. Ze kunnen ook de vorm aannemen van kettingbrieven : een boodschap waarin je uitgenodigd wordt je solidair te tonen met een of andere zaak en “deze boodschap door te zenden naar je kennissen”.

Een hoax heeft vaak een stereotiepe structuur. De boodschap is niet persoonlijk aan jou gericht, maar wordt naar een aantal correspondenten gestuurd, of die de afzender nu kennen of niet. In de boodschap worden de grote kanonnen ingezet om je aandacht te trekken door je te intrigeren of te verontrusten (alarmberichten, nepscenario's, enz.). De meegedeelde informatie steunt op betrouwbare bronnen. Ten slotte wordt je aanbevolen, ja zelfs opgelegd de boodschap door te sturen aan je vrienden of aan al wie in jouw adresboekje staat.

Op zich is een hoax geen gevaar voor je computer ; de risico's van zo'n nepbericht liggen elders, maar zijn wel reëel. Immers : al wie meent belangrijke informatie te moeten doorsturen of geestig wil doen, zendt de boodschap door naar een tiental mensen, die op hun beurt hetzelfde doen. Resultaat : door de vermenigvuldiging van die berichten wordt het netwerk overbelast. De verbindingen komen trager tot stand, de overdracht van gegevens neemt meer tijd in beslag en wordt dus duurder.

Daarnaast zijn er nog andere even nadelige gevolgen, afhankelijk van het thema van de hoax : risico van verspreiding van echte virussen door dit soort berichten, aanzetting tot het wissen van gezonde bestanden onder het mom van virusvoorkoming, financiële zwendel via kettingbrieven, misbruik van handtekeningen door valse petitie's, zelfs smaad en aanslag op de eer wanneer de naam van een persoon of maatschappij door het slijk wordt gehaald.

Om dat soort praktijken te bekampen, geven wij je de raad dergelijke berichten vooral niet te verspreiden zonder de bron nagegaan te hebben. Om de waarde van een boodschap in te schatten en de diverse soorten van nepberichten te herkennen, kun je terecht op de site

<http://www.hoaxbuster.com> (beschikbaar in het Frans en het Engels). Ten slotte dit nog : stuur een beleefd berichtje naar je afzender en wijs hem op de nadelen van dergelijke praktijken.

Afdeling 2. “Chatten”

27. Wat is “chatten” ?

Met *chatten*, dat in het Nederlands kan worden vertaald als “babbelen”, wordt naar de *Internet Relay Chat* (IRC) verwezen.

Door dat systeem kun je via het toetsenbord van je computer, in *real time* en over het internet ogenblikkelijk en om het even waar ter wereld dialogeren met elke andere persoon die aan IRC doet. Je kunt dan over een gegeven thema met een aantal correspondenten zeer levendige gesprekken voeren in virtuele babbelkamers (*chat rooms*). Op de IRC is elke internaut herkenbaar door een woord van zijn keuze, een pseudoniem.

Technisch gezien is de IRC een immens spinnenweb dat uit talrijke servers bestaat. Sommige servers zijn met elkaar verbonden : ze vormen een zogenaamd IRC-netwerk. Alle personen die op dezelfde server aangesloten zijn, kunnen dus dialogeren met elkaar of met de personen die op een andere server aangesloten zijn.

28. Hoe kan ik “chatten” ?

Om te kunnen chatten, moet je aangesloten zijn op een IRC-server, een IRC-netwerk kiezen en een verbinding tot stand brengen met de IRC-server.

Ook moet je een geschikte software installeren. Via deze software krijg je een verbinding met een IRC-server. Zodra dat gebeurd is, hoef je enkel nog een kanaal (*channel*) te kiezen op die server, d.w.z. een ingebeelde kamer waarin de discussie zal plaatsvinden. Elk discussiekanaal is aan een specifiek thema gewijd. Iedereen die met dit kanaal verbonden is, ontvangt alle berichten die ernaartoe worden gestuurd en kan zelf ook deelnemen.

Om te kunnen meedoen, moet je weten dat het chatten een eigen taal heeft (zie onder andere het gebruik van de *smiley's*). Aangezien de discussie online gebeurt, moet er zo snel mogelijk getypt worden. Daarom werden er talrijke afkortingen gecreëerd.

Elk kanaal heeft zijn eigen werkwijze : als je op een kanaal gaat, kijk dan eerst even toe voor je zelf deelneemt.

29. Welke risico's houdt het chatten in ?

Aan IRC doen, is net hetzelfde als een bar binnenstappen en met de eerste de beste persoon beginnen te praten. Verwacht dan ook niet te veel van een chat ; zo geraak je niet teleurgesteld. Onbekenden kunnen zich in een loped gesprek inmengen en het danig in de war sturen. Een ander risico is dat een of andere webhuffer van de gelegenheid (relatieve naamloosheid, afstand) misbruik maakt om grof te doen tegen zijn correspondenten.

Om te voorkomen dat de dingen spaak lopen door die naamloosheid, werd een hiërarchie ingesteld op de kanalen. De oprichter van een kanaal, die het thema definieert, verwerft meteen ook het statuut van kanaalbeheerder. Hij kan beslissen om internauten die de overeenkomsten niet eerbiedigen tijdelijk of definitief van het kanaal te stoten.

Elke websurfer kan ook een *ignore list* gebruiken om privé-boodschappen die hem worden toegestuurd niet te laten verschijnen.

Ten slotte bestaan er vooral risico's voor minderjarigen. Zet hen ertoe aan jou hun netvrienden "voor te stellen", nooit strict persoonlijke informatie door te spelen en raad hen vooral af in levende lijve af te spreken met een vermeende webvriend.

Afdeling 3. Discussiefora

30. Wat is een discussieforum ?

Een forum is een virtuele plaats om besprekingen en debatten te voeren (*newsgroup*). Anders dan bij het chatten, waar een rechtstreekse dialoog tot stand komt, gebeurt de gedachtewisseling in een forum met een zekere vertraging : een verzonden bericht verschijnt niet ogenblikkelijk op het scherm.

Er bestaan momenteel duizenden discussiefora over vrijwel alle mogelijke thema's. Als jouw favoriet onderwerp nog niet werd aangesneden, kun je steeds zelf een discussieforum lanceren. Je hebt daarvoor wel vooraf de goedkeuring nodig van de server waarop het nieuws zal worden uitgewisseld.

31. Hoe krijg ik toegang tot een discussieforum ?

Discussiefora – eigenlijk virtuele thematische vergaderzalen – zijn gestructureerd volgens taal of organisatie. Discussiefora zijn ingedeeld in "hiërarchieën".

Elke hiërarchie bestaat uit thematische fora. Het is gebruikelijk dat voor een forum een naam gekozen wordt die bestaat uit woorden gescheiden door punten, zoals voor domeinnamen op het internet. Het eerste woord is gemeenschappelijk voor de hele hiërarchie (dat is trouwens de naam die meestal aan de hiërarchie wordt gegeven : de "be"-hiërarchie omvat alle fora waarvan de naam begint met "be"), het tweede woord verwijst naar het algemeen kader van de besprekingen in dit forum (sociaal, informatica, artistiek, ...), de volgende woorden bepalen min of meer nauwkeurig, volgens de volgorde waarin ze voorkomen, het specifieke thema van het forum.

Een forum met als naam bijvoorbeeld "be.rec.sport.petanque" zou deel uitmaken van de "be"- hiërarchie (en dus onderworpen zijn aan de algemene regels die voor deze hiërarchie gelden), zou behoren tot de **recreatieve** sfeer en zou handelen over een **sport**, meer bepaald **petanque**.

In elk van die fora worden dus gesprekken gehouden over een thema dat te herkennen is aan de titel en de beschrijving van het forum. Er kan een groot aantal afzonderlijke discussies worden gevoerd binnen een en hetzelfde forum, waarbij elke discussie zich van de andere onderscheidt door de titels van de geposte berichten alsmede door de technische referenties die voorkomen in de technische velden die daartoe in elk artikel gecreëerd zijn.

Aan een forum kun je deelnemen als passieve lezer en enkel de debatten volgen, of als actieve gebruiker en zelf ook artikels posten. Het zijn die artikels die de inhoud vormen van het forum en die, als ze deel uitmaken van een en hetzelfde gesprek, gebundeld worden in de vorm van een "draad" (*thread*).

Een artikel dat in een forum werd gepost, kan door om het even wie, op om het even welk ogenblik op de server worden gelezen, zolang de vervaldatum van het artikel niet

verstrekken is. Die “vervaldatum” wisselt volgens de servers die de artikels van het forum opslaan, maar in sommige systemen kun je artikels lezen die al ruim twee jaar werden gepost.

32. Welke risico's zitten er aan een discussieforum ?

Het voornaamste risico van discussiefora heeft te maken met de aard van het medium. Vergeet niet dat een discussieforum een open, publieke en in zekere zin onbeschermd ruimte is. Een onbeperkt aantal personen heeft toegang tot het discussieforum waaraan jij deelneemt. Gezien deze verscheidenheid betekent dit concreet dat discussiefora zowel de beste als de slechtste informatie kunnen bieden.

Of je nu een actief of een passief gebruiker bent, besef dat wat je in een discussieforum verklaart aanleiding kan geven tot strafrechtelijke procedures wegens smaad, racisme, xenofobie, revisionisme, enz. Verklaar je iets in een discussieforum, wees dan even behoedzaam als wanneer je iets verklaart in de geschreven of audiovisuele pers. Je doet er dus goed aan sommige van je uitslatingen te temperen. Aarzel ook niet om berichten aan de kaak te stellen die je onrechtmatig lijken, vooral als het om minderjarigen gaat of als die berichten aan hen geadresseerd zijn.

Sommige *newsgroups* zijn echter “gematigd”. Alle aan de discussiegroep gestuurde berichten worden eerst bekeken door een moderator, die als taak heeft de inhoud van de berichten en bestanden te controleren alvorens ze te verspreiden. Het is de bedoeling na te gaan of de ontvangen berichten betrekking hebben op het forum en in overeenstemming zijn met het eventuele handvest waaraan het forum onderworpen is. De moderator onderzoekt echter de juistheid van de ontvangen informatie niet. Of de *newsgroups* nu een moderator hebben of niet, er bestaat geen enkele waarborg over de kwaliteit van de verspreide gegevens.

Tot slot dit nog : discussiefora zijn een bijzonder aantrekkelijke en unieke informatiebron voor prospectoren. Via *newsgroups* geraak je immers makkelijk aan de e-mailadressen van de internauten die eraan deelnemen. Zo kan een zeer doelgericht commercieel profiel worden opgemaakt aan de hand van de thematische lijsten van deelnemers aan discussiefora. Het gevaar bestaat ook dat er aan “wilde” inzameling van persoonsgegevens wordt gedaan (zie hieronder nrs. 81 en 82), al is deze praktijk volkomen illegaal (zie hieronder nr. 74).

33. Wat is netiquette ?

De *netiquette* is de gedragscode die je geacht wordt te eerbiedigen als je het internet gebruikt, vooral bij het communiceren met andere gebruikers. Het gaat in feite om regels van goed fatsoen en van protocol die je moet in acht nemen als je geen herrie wil met je gesprekspartners.

Wanneer je de geldende regels overtreedt of wanneer men oordeelt dat je ongepaste woorden gebruikt, kun je een terechtwijzing (of *flame*) krijgen van een andere gebruiker. Onderwerpen die het meest vatbaar zijn om een ware *flame-oorlog* te ontketenen (een opeenvolging van berichten naar aanleiding van de wederkerige ergernis van diverse gebruikers) zijn o.a. : politiek, religie, seks en alles wat van ver of dichtbij met informatica te maken heeft (beheersystemen, programmeertalen, computers, en zo meer).

Deel 3. Mijn website ontwerpen



Om je bekend te maken of om een van je interesses met anderen te delen, kun je een gepersonaliseerde website ontwerpen. Daartoe bestaan allerhande programma's waarmee je gemakkelijk pagina's in HTML-formaat kunt creëren. Bovendien verschaffen de providers die (gratis of tegen betaling) toegang tot het internet verlenen doorgaans een deel van het geheugen (verschillende Mbytes) op hun server, waar je je webpagina kunt opslaan en beschikbaar stellen op het internet.

Bij het ontwerpen van je webstek staat het je in principe vrij zelf de presentatie en de inhoud te kiezen : geef je fantasie en creativiteit de vrije loop. Betekent dit dat je er om het even wat kunt in opnemen ? Zeker niet !

In de eerste plaats ben je verplicht andermans rechten te respecteren (auteursrecht, beeldrecht, merkenrecht, recht op eerbiediging van de persoonlijke levenssfeer, enz.) en de inhoud mag niet illegaal zijn of mag geen schade toebrengen (racistische of revisionistische uitlatingen, smaad, inbreuk op het beeldrecht, enz.). Wees ook voorzichtig met informatie die je verspreidt (je aansprakelijkheid zou op het spel kunnen staan !) en denk aan de eerbiediging van je persoonlijke levenssfeer en die van anderen bij het invoeren van persoonsgegevens.

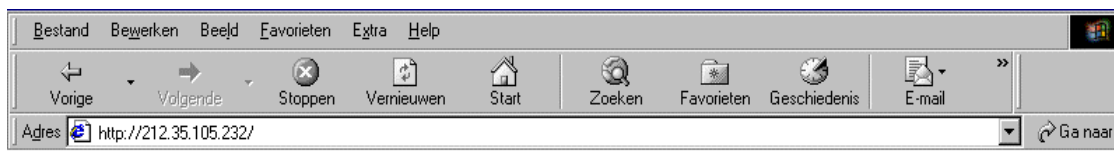
Omgekeerd is het mogelijk dat je echt een originele webpagina creëert. Als dusdanig is zij dan juridisch beschermd.

Maar voordat je al die aspecten bekijkt, moet je absoluut een plaats vinden om je pagina op te slaan en vooral een adres, zodanig dat internauten je webstek kunnen vinden op het internet. Dat alles heeft te maken met domeinnamen.

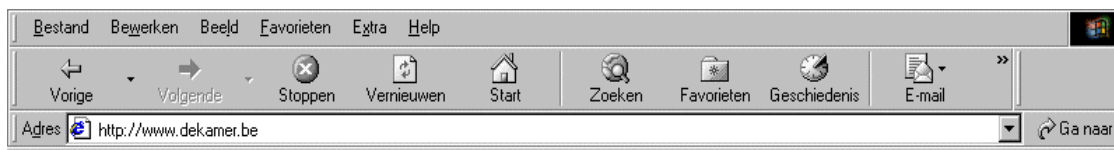
HOOFDSTUK I. EEN DOMEINNAAM RESERVEREN

34. Wat is een domeinnaam ?

Het internet kan pas degelijk functioneren als elk van de miljoenen onderling verbonden computers geïdentificeerd is door een IP-adres (*Internet Protocol*) : 4 getallen met elk maximum 3 cijfers tussen 0 en 255. Zo heeft de site van de Kamer als IP-adres 212.35.105.232., de Commissie voor de Bescherming van de Persoonlijke Levenssfeer 212.190.77.114. of de Federale Overheidsdienst Economie, KMO, Middenstand en Energie 193.191.210.45. Om toegang te krijgen tot de site van die instellingen moet je enkel dat IP-adres invullen in het daartoe bestemde vakje van je browser.



Het is wel zo dat computers geen moeite hebben om zo'n opeenvolging van cijfers te lezen en te begrijpen, maar voor een websurfer is het gebruik van zoveel numerieke gegevens niet meteen een makkie. Om de adressen gemakkelijker te kunnen onthouden en ze gebruiksvriendelijker te maken, kunnen die getallen (IP-adressen) omgezet worden in een voor de gebruiker bedrijselijke domeinnaam. Zo gaat het er trouwens meestal aan toe op het web, waar je geen 212.35.105.232. hoeft te typen, maar gewoon het voor de gebruiker transparante adres <http://www.dekamer.be>, dat dan automatisch wordt omgezet in het overeenstemmende IP-adres. Die omzetting gebeurt door een conversiesysteem, DNS genoemd (*Domain Name System*), dat geregeld wordt geüpdated.



Op die manier zou je een domeinnaam kunnen aanvragen voor je maatschappij (<http://www.jantjefriet.be> of [.com](http://www.janssens.be)) of voor jezelf (<http://www.janssens.be> of [.org](http://www.janssens.org)). Dat adres identificeert je heel precies, waardoor internetters moeiteloos naar je webpagina kunnen surfen.

35. Ben ik verplicht een domeinnaam te hebben ?

NEEN. Om je webpagina te kunnen opladen, moet je geen domeinnaam aanvragen. Het voordeel van een domeinnaam is wel dat je adres echt gepersonaliseerd is. Het nadeel is dat je ervoor moet betalen ! Voor de registratie van een domeinnaam rekent de door jou gekozen DNS-agent een jaarlijkse bijdrage aan. Meestal is de domeinregistratie niet de enige dienst die je krijgt van je DNS-agent. Vaak gaat de registratie gepaard met bijkomende diensten als daar zijn : *hosting* van je site, *e-mail* en *URL-forwarding*. De registratiekosten voor een domeinnaam vertegenwoordigen dan ook vaak slechts een fractie van de totale prijs van dat dienstenpakket.

Ook al heb je geen domeinnaam, toch kun je beschikken over een schijfruimte op de server van je *provider* (internetprovider). Die dienst is meestal gratis of inbegrepen in de prijs van je abonnement voor toegang tot het internet. In dat geval wordt je pagina opgeladen volgens de naam van de *directory* (map) die werd gemaakt om je webpagina op die server op te slaan. Het adres om die pagina op te laden, bestaat dus uit twee delen : enerzijds de domeinnaam van je *provider* en anderzijds de naam van je *directory* (bijvoorbeeld <http://users.provider.be/janssens>). Die oplossing kost je in principe niets, maar verschaft je geen echt gepersonaliseerd adres en beperkt dus je herkenbaarheid op het internet. Bovendien is zo'n adres helemaal niet gebruiksvriendelijk, omdat je het niet kunt hergebruiken als je van internetprovider verandert.

36. Waaruit bestaat een domeinnaam ?

Als je een domeinnaam wil hebben, moet je twee stappen doen om hem vast te leggen : de stam kiezen en de uitbreiding kiezen. Dat moet je heel zorgvuldig doen, want de herkenbaarheid van je site op het internet hangt ervan af. Over het algemeen is de *stam* de naam van de natuurlijke of rechtspersoon die de site beheert en stemt de *uitbreiding* overeen met de aard van de uitgeoefende bedrijvigheid of met de geografische zone waar deze bedrijvigheid wordt uitgeoefend. Handelsmaatschappijen kiezen meestal voor ".com", ".biz" of ".be", particulieren voor ".be", ".name" of ".info", instellingen of verenigingen zonder winstoogmerk voor ".org" of ".net" en internationale organisaties voor ".int", enz.

37. Welke uitbreidingen zijn mogelijk ?

Er bestaan momenteel twee soorten uitbreidingen op het internet.

De eerste omvat de zogenaamde "territoriale" uitbreidingen die, zoals de naam al zegt, verwijzen naar een geografische oorsprong. Ze bestaan uit twee letters die duiden op het land van oorsprong van de site. Ze komen heel veel voor en gaan van ".ac" voor Ascension Islands over ".be" voor België tot ".zw" voor Zimbabwe. Sommige instellingen die de toekenning van "nationale" domeinnamen beheren, bepalen regels voor de registratie van hun uitbreiding, maar andere zoals ".tv" (Tuvalu), ".md" (Moldavië), ".ac"

(Ascensioneilanden en “.vg” (Virgineilanden) stellen geen strenge eisen voor een registratie of eisen zelfs helemaal niets. Die uitbreidingen zijn dus niet echt meer territoriaal gebonden. Ze liggen dicht bij algemene uitbreidingen zoals “.com”, omdat om het even welke gebruiker ze kan aanvragen, ook al is hij niet woonachtig op het betreffende grondgebied.

Nu we het hier toch over territoriale uitbreidingen hebben : een nieuwe speciale uitbreiding wordt weldra boven de doopvont gehouden, met name “.eu”. De Raad van de Europese Unie en het Europees Parlement spraken onlangs af om die uitbreiding in te voeren, omdat ze dit als een prioriteit van het e-Europa-initiatief beschouwen. De uitbreiding “.eu” zal enkel mogen worden gebruikt door instellingen, ondernemingen en natuurlijke personen die op het grondgebied van de Europese Unie gevestigd zijn. Met die nieuwe uitbreiding is het vooral de bedoeling actoren te identificeren die onderworpen zijn aan een geharmoniseerd rechtsstelsel inzake elektronische handel en die de consument o.a. een hoge graad van bescherming bieden. In principe wordt “.eu” in 2003 beschikbaar.

De tweede soort uitbreiding verwijst naar de aard van de bedrijvigheid. Ze bestaat uit drie of meer letters die het activiteitsgebied van de gebruiker weergeven. Het gaat om algemene uitbreidingen van het type “.com” voor handelsvennootschappen, “.net” voor sites over de werking van het internet en “.org” voor organisaties en verenigingen zonder winstoogmerk evenals uitbreidingen bestemd voor specifieke instellingen : “.gov” voor regeringsinstellingen, “.int” voor internationale organisaties, “.mil” voor militaire activiteiten en “.edu” voor onderwijsinstellingen. Meer recent verschenen nog andere uitbreidingen zoals “.biz” voor ondernemingen, “.info” voor ondernemingen en particulieren, “.name” voor particulieren en “.coop” voor coöperatieve vennootschappen. Ook de uitbreidingen “.pro”, “.museum” en “.aero” werden goedgekeurd en zijn thans operationeel.

Het is niet verboden verscheidene domeinnamen met dezelfde stam maar met een verschillende uitbreiding te laten registreren. Naargelang van de gekozen uitbreiding moet je gewoon de autoriteit contacteren die verantwoordelijk is voor de toekenning van de soort domeinnaam die je gekozen hebt, de voorwaarden naleven die eventueel door die autoriteit worden opgelegd en de passende bijdrage betalen, zonder te vergeten eerst na te gaan of de domeinnaam al niet geregistreerd is.

38. Tot wie moet ik mij richten om een domeinnaam te laten registreren ?

De eenvoudigste oplossing is je internetprovider te contacteren, die tegen betaling het nodige zal doen om de gekozen domeinnaam te registreren met de uitbreiding “.be”, maar ook met andere uitbreidingen. In sommige gevallen kun je rechtstreeks terecht bij de instelling die instaat voor een welbepaalde uitbreiding (je vindt alle instellingen die verantwoordelijk zijn voor een specifieke uitbreiding op het volgende adres : <http://www.iana.org/domain-names.htm>). Voor de registratie van een domeinnaam in “.be” kun je niet meer rechtstreeks terecht bij de vzw DNS.BE. Nu moet je dat doen via een door die vzw erkend agent. Op de site <http://www.dns.be> vind je de lijst van de door DNS.BE erkende agenten, alsook de te volgen procedure voor de registratie van een domeinnaam in “.be”.

39. Moet ik aan voorwaarden voldoen om een domeinnaam te bekommen ?

Voor “.com”, “.org” en “.net” moeten geen specifieke criteria in acht worden genomen, voor zover de domeinnaam beschikbaar is. In België mocht tot december 2000 “.be” enkel worden gebruikt door handelsvennootschappen, openbare of privé-instellingen en verenigingen die een “reële en redelijke” wettelijke activiteit uitoefenen. Overigens moesten

die maatschappijen of organisaties in België gevestigd of vertegenwoordigd zijn. Na die datum herbekeek DNS.BE haar werkingsregels grondig, onder meer omdat gebleken was dat de strenge regels ter voorkoming van onrechtmatige registraties een deel van de Belgische siteontwerpers had doen grijpen naar algemene domeinnamen (bijvoorbeeld “.com”), waarvan de toekenning aan minder voorwaarden is onderworpen.

Voortaan mag de uitbreiding “.be” door iedereen worden gebruikt : zowel ondernemingen als Belgische of buitenlandse particulieren, die niet meer moeten voldoen aan specifieke voorwaarden om een domeinnaam te laten registreren. Behoudens andersluidende vermelding van DNS.BE is ook de registratie van algemene namen toegestaan. Zodra je domeinnaam geregistreerd is, krijg je een gebruiksvergunning voor één jaar. Vergeet niet je jaarlijkse bijdrage te betalen voor de vernieuwing van je vergunning, want anders loop je het risico dat je je domeinnaam niet meer mag gebruiken ! Voorts gelden voor de registratie algemene voorwaarden (beschikbaar op de site <http://www.dns.be>, die we je aanraden vooraf te lezen.

40. Kan ik om het even welke domeinnaam bekomen ?

NEEN ! Ook al denken de meeste mensen dat elke domeinnaam die nog niet werd gereserveerd vrij kan worden geregistreerd - het principe van “wie het eerst komt, het eerst maalt” - toch moet dit principe sterk worden genuanceerd. In de eerste plaats moet je namelijk het recht (de rechten) van derden op een domeinnaam (merk, handelsnaam, familienaam, enz.) eerbiedigen, vooral als jij geen enkel recht hebt op die domeinnaam. Verder zijn de rechters steeds meer geneigd om diegenen te straffen die massaal domeinnamen van bekende maatschappijen reserveren met als enig doel ze nadien peperduur verder te verkopen. De registratie van je domeinnaam zal zeker niet worden geweigerd, vermits de diverse maatschappijen die gemachtigd zijn domeinnamen te registreren *vooraf* niet nagaan of het recht dat andere personen zouden kunnen hebben op de naam die jij wil laten registreren wel degelijk wordt geëerbiedigd. Maar als een derde klacht indient en de rechter of een bemiddelaar de rechtmatige rechten van een derde (eiser) erkent, dan kun je worden verplicht die domeinnaam aan die derde af te staan.

Zo schijnt niets je dus te beletten “*jantjefriet.com*” te laten registreren indien die maatschappij het nog niet heeft gedaan. En toch kan het gebeuren dat de domeinnaam die je hebt gekozen vroeg of laat wordt betwist door de maatschappij Jantje Friet, waarvan je het merk of gewoon de handelsnaam hebt gebruikt. Iets gelijkaardigs is mogelijk als je de domeinnaam “*celinedion.be*” laat registreren, al draagt niemand van je familie die naam, ook jij niet. Als je aan *domain name grabbing*, *cybersquatting*, domeinkaping of wederrechtelijke inbezitneming van een domeinnaam hebt gedaan, kan de rechter je verplichten afstand te doen van de betwiste domeinnaam ten voordele van de houder van de rechten op die naam (de maatschappij Jantje Friet of Céline Dion) en je eventueel schadevergoeding doen betalen.

Om problemen te vermijden, raden wij je aan je domeinnaam te goeder trouw te kiezen, zonder de bedoeling schade te berokkenen, zonder winstoogmerk en om een geldige reden (je houdt van tuinbouw en je hebt de naam “bloemen.com” laten registreren om een site over Afrikaanse bloemen te creëren). In dat geval kan je domeinnaam in principe door niemand worden betwist. Kies ook geen domeinnaam waarin een bekende merknaam voorkomt, want zo'n merken zijn speciaal beschermd en je zal moeilijk kunnen bewijzen dat je een geldige reden hebt om die domeinnaam te gebruiken (een rechter zal wellicht moeilijk aanvaarden dat je “*dhl.com*” hebt gereserveerd onder het voorwendsel dat je de eerste letters van je drie honden, Dumbo, Happy en Lassie, hebt samengebracht en een site hebt gecreëerd over hondenrassen).

41. Waar kan ik terecht indien ik de reservatie van een domeinnaam door een derde betwist ?

Als je rechten kunt doen gelden op een domeinnaam die “ten onrechte” door een derde werd gereserveerd, dan kun je natuurlijk naar de bevoegde rechtbank stappen. Eventueel zal de rechter de derde veroordelen tot teruggave van de betwiste domeinnaam en tot betaling van schadevergoeding. Zo'n procedure kan echter lang aanslepen en duur uitvallen.

Om die nadelen te ondervangen, werkte DNS.BE een “alternatieve” procedure uit waardoor geschillen doeltreffend, snel (op enkele weken) en goedkoop (1.600,00 EUR om 1 tot 5 domeinnamen terug te krijgen) kunnen worden geregeld. Hierbij worden geschillen over een naam in “.be” voorgelegd aan het Belgisch Centrum voor Arbitrage en Mediatie (CEPINA: www.cepani.be). Dat centrum werkte een speciaal stelsel uit voor de beslechting van geschillen over domeinnamen (beschikbaar op het volgende adres: <http://www.tmab.be/ICTcongress/Index.htm>). Partijen die het wensen, kunnen hun geschil dus voorleggen aan een “derde beslisser”, die zich op de door het CEPINA gepubliceerde lijst bevindt. Ofwel verwerpt deze onafhankelijke derde het verzoek, ofwel schrapt hij de domeinnaam en draagt hij de registratie over aan de eiser. Via die alternatieve procedure kun je echter geen vergoeding krijgen voor eventueel berokkende schade. Je kunt wel steeds de zaak aanhangig maken bij een traditionele rechtbank, wiens beslissing het haalt op die van de derde beslisser.

Als een rechterlijke of scheidsrechterlijke procedure wordt ingesteld tegen het gebruik van een domeinnaam, dan plaatst DNS.BE die naam *on hold* tot er een uiteindelijke beslissing is gevallen over het geschil. DNS.BE houdt zich verder niet bezig met de procedure voor de regeling van het geschil.

HOOFDSTUK II. WAT KAN IK OP MIJN SITE PLAATSEN ZONDER DE RECHTEN VAN DERDEN TE SCHENDEN ?

Als je een webpagina creëert, dan moet je andermans rechten eerbiedigen en meer bepaald het recht dat een auteur kan hebben op een welbepaald werk (tekst, beeld, foto, muzieksequens of video, enz.) dat hij heeft gemaakt.

Voordat wij de concrete vragen aanpakken die je je zou kunnen stellen, lijkt het ons interessant even de *grondbeginselen van het auteursrecht* op een rijtje te zetten. Het auteursrecht wordt geregeld door de volgende wetgevingen : in de eerste plaats de wet van 30 juni 1994 betreffende het auteursrecht en de naburige rechten, maar ook de wet van 30 juni 1994 betreffende de rechtsbescherming van computerprogramma's, evenals de wet van 31 augustus 1998 betreffende de rechtsbescherming van databanken.

Op het internet wordt het auteursrecht niet altijd geëerbiedigd ! De mogelijkheden geboden door de nieuwe technologieën (de geduchte functie *knippen/plakken*, het feit dat je enkel op een knop moet drukken om een document van honderden bladzijden af te drukken, de mogelijkheid om snel werken te scannen, het gebruik van zoekmotoren waardoor heel snel een beeld of foto kan worden gevonden, enz.) zijn namelijk zo groot dat andermans werk thans nog gemakkelijker kan worden geëxploiteerd dan tot nu toe het geval was. Zo gebeuren er tegenwoordig zoveel manipulaties (reproductiewijziging, enz.) die in strijd zijn met de auteursrechten en komen er zo weinig reacties vanwege de auteurs die het slachtoffer zijn van die manipulaties dat je zou denken dat auteursrechten niet (meer) bestaan en je je ongestraft om het even wat kunt permitteren !

Dat is nochtans niet zo. Alles is niet toegestaan, zelfs niet op het internet. Een aantal beslissingen van de rechtspraak - slechts de eerste van een lange reeks - tonen aan dat het auteursrecht nog steeds geldt en dat je zware boeten kunt oplopen als je dat recht niet eerbiedigt.

Afdeling 1. Grondbeginselen van het auteursrecht

Het auteursrecht verschaft de auteurs exclusieve rechten voor het gebruik van hun werk. Daaruit volgt dat je doorgaans de voorafgaande toestemming moet hebben van de eigenaar van de rechten op het werk als je zijn werk wilt gebruiken (voor een reproductie zoals een fotokopie, een afdruk, om het te *knippen/plakken*, om het te wijzigen of aan het publiek mee te delen, wat het geval is als je het online op een website plaatst).

Op het internet wordt vaak op die manier tewerk gegaan. Een voorbeeld : de uitbater van het cybercafé van Besançon, die het werk "Le grand secret" van Dokter Gubler op het internet verspreidde, scande vooraf het boek (eerste reproductie) ; nadien plaatste hij het bestand op zijn webpagina en dus op een server (tweede reproductie en mededeling van het werk aan het publiek) ; vervolgens konden de personen die zijn site bezochten de tekst downloaden (andere reproductie) en hem eventueel afdrukken op papier (laatste reproductie). In dit geval kun je ook stellen dat er een mededeling aan het publiek is gebeurd, wat het exclusieve recht van de auteur is, enkel en alleen doordat het werk via de website voor het grote publiek toegankelijk werd gemaakt.

Om de regels over het auteursrecht na te leven, had de uitbater eerst de toestemming van de eigenaar van die rechten moeten bekomen. Dat gold ook voor de Franse studenten die de teksten van liederen van Jacques Brel en Michel Sardou digitaliseerden en online brachten en daarvoor werden veroordeeld. Voordat je een werk via het internet verspreidt, moet je dus eerst de toestemming hebben van de eigenaar van de rechten (die vaak ook

de schepper van het werk is, doch niet altijd, want hij kan zijn rechten hebben afgestaan, in het bijzonder aan een maatschappij voor het collectief beheer van auteursrechten).

42. Wat is beschermd door het auteursrecht ?

Elk werk dat oorspronkelijk is en in een bepaalde vorm is gegoten, is beschermd door het auteursrecht. Wat betekenen die begrippen : werk, oorspronkelijkheid en vorm ?

Het begrip *werk* wordt heel ruim opgevat en behelst onder meer :

- **teksten** van elke aard (romans, novellen, gedichten, wetenschappelijke of technische teksten, enz.), ongeacht de inhoud, lengte, bestemming (ontspanning, opvoeding, informatie, reclame, propaganda, enz.), vorm (met de hand geschreven, getypt, gedrukt of in elektronische versie) ;
- **fotografieën**, ongeacht de informatiedrager (papier of digitaal) en het onderwerp (persoon, landschap, actualiteit, tabel in het publiek domein, enz.) ;
- **beelden**, al dan niet virtueel, van welke aard ook (tekeningen, letterwoorden, iconen, logo's, landkaarten, enz.) ;
- **muzieksequensen, videosequensen of audiovisuele sequensen** in het algemeen, ongeacht het formaat of de informatiedrager ;
- **computerprogramma's** (spelletjessoftware).

Om beschermd te zijn, moet een werk *oorspronkelijk* zijn. Dit is een abstract criterium, dat in de praktijk moeilijk te definiëren is. Het betekent dat het werk de stempel moet dragen van de persoonlijkheid van de auteur. Wij zullen hier niet in details treden, maar de oorspronkelijke aard van een werk is een feitelijke aangelegenheid, die door de rechter soeverein wordt beoordeeld. Je kunt dus niet weten of een werk al dan niet als oorspronkelijk wordt beschouwd zolang de rechter zich niet heeft uitgesproken over die aard. Nu, de rechtspraak interpreteert dat begrip oorspronkelijkheid heel soepel. In de meeste gevallen zal een werk dus als oorspronkelijk worden beschouwd. Opgelet : oorspronkelijk betekent geenszins mooi ! Oorspronkelijkheid is een begrip dat niets te maken heeft met esthetica. Het is niet omdat je een werk lelijk of zelfs belachelijk vindt dat het niet als oorspronkelijk kan worden beschouwd.

Om beschermd te zijn, moet een werk ook gestalte hebben gekregen in een bijzondere *vorm* die door de zintuigen kan worden waargenomen. Die voorwaarde vormt geen probleem voor werken die online beschikbaar zijn, aangezien ze noodzakelijkerwijze vooraf in een vorm moeten worden gegoten om zichtbaar te kunnen zijn. Deze voorwaarde houdt a contrario in dat het auteursrecht geen bescherming biedt, noch aan ideeën (ook al zijn die *geniaal* of *oorspronkelijk*), noch aan methodes of stijlen, ook al zijn die oorspronkelijk (bij het creëren van een website kun je je dus laten inspireren door stijlen die door anderen worden gebruikt op voorwaarde dat je geen enkel oorspronkelijk formeel element kopieert).

43. Moet ik nog aan andere voorwaarden voldoen om door het auteursrecht te worden beschermd ?

NEEN, er worden geen andere voorwaarden opgelegd om auteursrechtbescherming te genieten. Het volstaat dat het werk oorspronkelijk is en een bepaalde vorm gekregen heeft.

Je moet dan ook geen formaliteiten vervullen, zoals een exemplaar van het werk indienen bij een bestuur of de *copyright*-vermelding © aanbrengen (wij raden je echter aan dit laatste toch te doen omwille van de bewijskracht). De bescherming begint te lopen vanaf het ogenblik dat het werk gecreëerd is.

Wil je daarentegen een onderscheidend teken laten beschermen door het merkenrecht (dat niet hetzelfde is als het auteursrecht), dan moet je het merk formeel deponeren.

44. Welke rechten heeft een auteur op zijn werk ?

Met andere woorden : welke rechten moet je bekomen als je andermans werk wilt gebruiken bij het ontwerpen van je website ?

In feite beschikt een auteur over twee soorten rechten :

- *vermogensrechten* (rechten die het een auteur mogelijk maken economisch voordeel te halen uit de exploitatie van zijn werk), die overdraagbaar zijn en waarvoor een vergunning kan worden verleend ;
- *morele rechten* (beschermen de integriteit van het werk, de relatie van het werk met de auteur en de reputatie van de auteur), die niet overdraagbaar zijn (hooguit kan er gedeeltelijk afstand van worden gedaan).

Vermogensrechten

In het kort omvatten de vermogensrechten :

- het *reproductierecht* in ruime zin :

het is een voorrecht waarbij een auteur kan verbieden of toestaan dat zijn werk wordt gereproduceerd en de voorwaarden van die reproductie kan vastleggen. Meer bepaald omvat het reproductierecht :

- het *reproductierecht* in enge zin : op grond van dat recht bepaalt de auteur de technische wijze van reproductie (fotografie, digitalisering met scanner), het soort informatiedrager (papier of digitaal), de plaats van de reproductie (op een website, op een cd-rom) en de voorwaarden voor de eerste commercialisering van de exemplaren. Dat recht omvat de al dan niet gedeeltelijke, tijdelijke of definitieve, directe of indirecte reproductie ;
- het *recht om de aanpassing en vertaling van het werk toe te staan* : dat recht slaat op de omzetting van het werk in een ander genre (een tekst interactief maken), het aanbrengen van allerlei wijzigingen (een tekst samenvatten, zoomen of de kleuren van een foto veranderen) en het vertalen in diverse talen ;
- het *verhuurrecht of uitleenrecht* : het recht voor een auteur om het origineel of een reproductie van zijn werk een zekere tijd ter beschikking te stellen van een derde (de houder van dat recht zou bijvoorbeeld de verhuur van een cd-rom gedurende een aantal maanden na het uitbrengen kunnen verbieden om genoeg tijd te maken voor de commercialisering van het werk) ;
- het *distributierecht* : dat recht verschaft een auteur de mogelijkheid te controleren op welke manier zijn werk wordt gecommmercialiseerd (dit recht leunt aan bij het reproductierecht in enge zin) ;

- het *opvoeringsrecht* of het recht om het werk aan het publiek mee te delen :

krachtens dat recht mag het werk aan het publiek worden meegedeeld en ook ter beschikking worden gesteld, zodanig dat elk lid van het publiek er individueel toegang kan toe krijgen op het door hem gekozen tijdstip en op de door hem gekozen plaats. Dat recht slaat op de *online*-overdracht van een werk (via het internet). Het gaat om de rechtstreekse communicatie aan het publiek, zonder dat hierbij een informatiedrager komt kijken.

Morele rechten

Naast de vermogensrechten geniet de auteur ook morele rechten, die de uitdrukking zijn van de band tussen de auteur en zijn werk.

De morele rechten omvatten :

- het *recht van openbaarmaking* : dat recht geeft de auteur de mogelijkheid te beslissen wanneer zijn werk voltooid is en aan het publiek kan worden voorgesteld. Zich een nog niet voltooid werk toe-eigenen (bijvoorbeeld een muziekstuk waarvan het scheppingsproces nog aan de gang is) en het op het internet plaatsen is dus een inbreuk op dat recht, want de auteur had zijn toestemming nog niet gegeven om het te verspreiden.
- het *vaderschapsrecht* : dit recht houdt in dat de auteur het vaderschap van een werk kan opeisen, d.w.z. dat hij kan beslissen dat zijn naam (of een pseudoniem) bij het exploiteren wordt vermeld of dat het werk anoniem wordt gepubliceerd. Het zich toe-eigenen van andermans werk is dus een schending van dat recht, net als het verspreiden ervan onder de naam van de auteur indien die het niet wenst.
- het *recht op integriteit* : met dit recht kan de auteur zich verzetten tegen elke wijziging van zijn werk (ingekorte of samengevatte tekst, anders in beeld gebrachte foto, met een filter of door trucage gewijzigde foto) evenals tegen alles wat zijn eer of reputatie aantast (naar aanleiding van een materiële wijziging van het werk of van een wijziging van de context of de wijze waarop het werk is voorgesteld).

45. Hoe lang is een werk beschermd ?

De bescherming door het auteursrecht is beperkt in de tijd. Als algemene regel geldt dat het werk beschermd is tot 70 jaar na de dood van de auteur. Dit betekent bijvoorbeeld dat de partituren van de concerto's van Mozart niet langer door het auteursrecht zijn beschermd. Je kunt ze dus reproduceren (bijvoorbeeld door fotokopieën te maken) zonder dat je daarvoor de toestemming nodig hebt van de erfgenamen van Mozart (maar eventueel moet je wel toestemming vragen aan de musici die de werken uitvoeren en aan de platenfirma's).

46. Wat is niet door het auteursrecht beschermd ?

De volgende werken zijn niet beschermd door het auteursrecht en mogen dus bijvoorbeeld worden gereproduceerd zonder toestemming van de auteur :

- een werk dat niet oorspronkelijk is ! Dit begrip is heel relatief en moet door de rechter worden beoordeeld. Wij raden je dus af vrij te beslissen of andermans werk oorspronkelijk is of niet ;

- een werk dat niet langer beschermd is, d.w.z. waarvan de auteur sedert meer dan 70 jaar overleden is (soms moet je wel het akkoord krijgen van andere eigenaars van rechten) ;
- een werk zoals bedoeld in artikel 8 van de wet op het auteursrecht. Dit artikel bepaalt dat er geen auteursrecht bestaat op sommige werken, ook al zijn die oorspronkelijk : redevoeringen uitgesproken in vergaderingen van vertegenwoordigende lichamen, in openbare zittingen van rechtscolleges of in politieke bijeenkomsten, alsook officiële akten van de overheid. (wet, decreet, ordonnantie, enz.).

Aangezien zo'n werken niet beschermd zijn door het auteursrecht, kunnen zij onder andere vrij worden gereproduceerd en onder het publiek verspreid.

Nogmaals : een idee, ook al is het origineel, wordt niet door het auteursrecht beschermd zolang het niet in een vorm werd gegoten en dus concreet gestalte heeft gekregen.

47. Mag ik een werk dat door het auteursrecht is beschermd nooit reproduceren ?

Er zijn gevallen waarin auteursrechtelijk werk beschermd werk geheel of gedeeltelijk mag worden gereproduceerd en waarvoor de toestemming van de auteur niet is vereist. De wet op het auteursrecht bevat namelijk enkele uitzonderingen. Zij zijn sowieso niet talrijk en bovendien onderworpen aan zo'n strenge voorwaarden dat het niet altijd gemakkelijk is zich daarop te beroepen in het kader van het creëren en het online plaatsen van een website. Hierop bestaat echter een belangrijke uitzondering in het kader van het ontwerpen van een website : het citaatrecht.

Krachtens het citaatrecht mag je een uittreksel van een werk reproduceren zonder dat je de toestemming van de auteur nodig hebt. Er moet wel gelijktijdig voldaan zijn aan een aantal voorwaarden :

- het citaat moet komen uit een werk dat op geoorloofde wijze werd gepubliceerd (je mag dus geen werk citeren zolang de auteur niet heeft beslist het openbaar te maken) ;
- het citaat moet kort zijn (dat is een feitelijke aangelegenheid die door de rechter moet worden beoordeeld) ;
- het citaat moet worden aangehaald met de bedoeling kritiek te leveren, een polemiek op gang te brengen, te onderrichten of moet uit wetenschappelijke werken komen (er mogen dus geen citaten worden gebruikt voor onspanningswebsites of louter commerciële websites) ;
- het citaat moet te goeder trouw worden gebruikt ;
- het citaat moet de bron en de naam van de auteur vermelden.

48. Van wie krijg ik toestemming ?

Uit wat voorafgaat, blijkt dat je de toestemming van de auteur van een werk nodig hebt en met hem dus een overeenkomst moet aangaan om dat werk te mogen exploiteren. Daartoe moet je je drie vragen stellen :

- Wie bezit de auteursrechten op het werk ?
- Is de auteur altijd de houder van de rechten ? Heeft hij die rechten niet overgedragen ?
- Heeft de auteur het beheer van zijn rechten niet toevertrouwd aan een maatschappij voor het beheer van auteursrechten ?

Principe

In principe is de houder van het auteursrecht de natuurlijke persoon die het werk heeft gecreëerd. Die persoon is de oorspronkelijke houder van de auteursrechten. Om de bewijslast te vergemakkelijken, wordt de persoon van wie de naam (of een willekeurig teken) op het werk vermeld staat, geacht de houder van de auteursrechten te zijn.

Indien het werk door meer dan een persoon werd gecreëerd, gaat het in principe om een samenwerking en behoort het auteursrecht toe aan alle scheppers van het werk. Een persoon mag slechts aanspraak maken op het medeauteurschap van het werk als hij effectief een creatieve bijdrage leverde tot de vormgeving van dat werk (dat geldt niet voor de persoon die enkel ideeën aanbracht of alleen technische gegevens invoerde). In dat geval moet je dus de toestemming vragen aan elk van de medeauteurs.

Overigens kunnen er voor een website of een database twee soorten auteurs zijn :

- de auteur of medeauteur van de website : immers, als dusdanig en ongeacht de inhoud, is een website vaak een door het auteursrecht beschermd werk doordat hij een originele samenstelling is van diverse elementen ;
- de auteur of auteurs, niet van de website maar van de onderdelen van de website (foto, logo, muzieksequens).

Overdracht van het auteursrecht

Mogelijk is de auteur van een werk geen houder meer van de (vermogens)rechten doordat hij ze heeft overgedragen of kan hij de rechten niet meer verlenen doordat hij een vergunning heeft gegeven aan een derde. Die persoon is dan de *afgeleide auteursrechthebbende*. Je moet de auteur dus vragen of hij nog steeds houder is van de rechten en, als dat niet zo is, wie de overdrager is van de rechten. Bovendien moet je eventueel de morele rechten van diezelfde auteur eerbiedigen, want die zijn niet overdraagbaar.

Vennootschappen voor het beheer van auteursrechten

Een auteur die niet zelf wil instaan voor het beheer van zijn rechten kan die taak toevertrouwen aan een vennootschap voor het beheer van auteursrechten (SABAM, SOFAM, SESAM, SCAM). Dit biedt het voordeel dat de gebruiker slechts te maken heeft met één gesprekspartner bij het onderhandelen over de rechten, wat interessant is als hij verscheidene werken wil exploiteren.

Afdeling 2. Concrete vragen die je je stelt !

49. Heb ik het recht om software voor de aanmaak van een webpagina te gebruiken ?

Om je webpagina te creëren, ga je waarschijnlijk gebruik maken van software die daarvoor ontworpen is. Om je website op de server van de internetprovider op te laden, ga je ook passende software gebruiken. Om je site te raadplegen, ga je navigatiesoftware gebruiken. Heb je het recht om gebruik te maken van al die software ? Zijn het geen bootlegs ?

Dat alles lijkt misschien evident, maar wij herinneren er toch aan dat ook software door het auteursrecht beschermd is. Stel dat je een programma koopt dat zich op een informatiedrager bevindt : dit betekent nog niet dat je houder bent van de intellectuele rechten op dat programma. In de praktijk komt het erop neer dat, als je gebruik maakt van een computerprogramma, je daarvoor de toestemming moet hebben van de eigenaar van het auteursrecht op dat programma. Doorgaans krijg je een licentie bij de aankoop van het programma op cd-rom of diskette.

50. Mag ik een foto scannen en in mijn webpagina invoegen ?

Om je website aantrekkelijker te maken, zal je waarschijnlijk geneigd zijn er één of meer gescande (gedigitaliseerde) foto's in te voegen. Mag ik een analoge foto scannen en in mijn website invoegen ? Hieromtrent is de knoop nog niet doorgehakt. Er zijn twee hypothesen :

1. Ofwel heb je zelf de foto genomen (van je vakantie, je gezin, je autoverzameling, enz.) en ben je dus zelf houder van het auteursrecht op die foto. In principe mag je ze dus vrij reproduceren en aan het publiek meedelen via je website, *voor zover* het gefotografeerde voorwerp niet zelf beschermd is door het auteursrecht (foto van een andere beschermde foto, van een schilderij, een beeldhouwwerk, een Kuifje-album). Is dat het geval, dan moet je toestemming vragen aan de auteur van het gefotografeerde voorwerp.

Maar opgelet : daar blijft het niet bij ! Als je een persoon fotografeert, moet je ook het recht op het beeld van die persoon eerbiedigen. Dit recht, dat niet rechtstreeks verbonden is met het auteursrecht, verschaft elke gefotografeerde persoon de mogelijkheid zich te verzetten tegen iedere reproductie van zijn beeld (onder meer via het internet) en tegen iedere mededeling aan het publiek. In dat geval moet je dus de toestemming vragen van de afgebeelde persoon. Weet echter dat hierop een aantal uitzonderingen bestaan voor het fotograferen van publieke figuren en privé-personen die zich in een menigte bevinden.

2. Ofwel scan (digitaliseer) je een foto uit een boek of tijdschrift met de bedoeling ze op je website te plaatsen. In dat geval is het best mogelijk dat de foto beschermd is door het auteursrecht, want het volstaat dat ze oorspronkelijk is, iets dat meestal door de rechter wordt erkend. Welnu, er wordt unaniem aangenomen dat het scannen (of op een andere manier digitaliseren) van een werk een reproductie is en onder het auteursrecht valt. Daaruit volgt dat je die foto doorgaans niet mag scannen en ze ook niet op je site mag plaatsen zonder het akkoord van de fotograaf (of een andere persoon aan wie de rechten zijn overgedragen). Buiten dat akkoord van de fotograaf moet je tevens de toestemming krijgen van de auteur van het gefotografeerde voorwerp of van de gefotografeerde persoon.

Opgelet ! Het is niet omdat je een foto of de negatieven ervan hebt aangekocht dat je ook houder bent van de auteursrechten. Je moet die rechten dus blijven eerbiedigen.

51. Mag ik een beeld (tekening) scannen en in mijn webpagina invoegen ?

Net zoals met foto's zal je misschien geneigd zijn enkele beelden (zoals humoristische tekeningen of gedeelten van tekenstrips) op je website te plaatsen om die aantrekkelijker te maken. Zoals voor foto's mag je een gescand beeld enkel in je site opnemen als je zelf de tekenaar van dat beeld bent en voor zover het geen herkenbaar portret van een persoon is.

In de andere gevallen is het beeld beschermd door het auteursrecht indien het oorspronkelijk is, wat vaak het geval is. Bijgevolg moet je vooraf de toestemming van de auteur vragen. Krachtens het beeldrecht moet je ook de toestemming krijgen van een getekende persoon. Soms is het beeld niet alleen beschermd door het auteursrecht maar ook door het merkenrecht.

Eens te meer blijkt dus dat je zelden zonder toestemming een beeld op je website mag exploiteren, tenzij je je creatieve scheppingskracht de vrije teugel laat.

52. Mag ik een tekst scannen en in mijn webpagina invoegen ?

Buiten foto's en beelden mag je ook tekst op je webpagina plaatsen. Je kunt bijvoorbeeld zelf zo'n tekst opstellen of een bestaande tekst scannen en hem in je site invoegen als beeldbestand of als tekstbestand nadat je een programma voor tekenherkenning hebt gebruikt. Kun je om het even welk type tekst in je site inbrengen ? Ook op deze vraag is het antwoord neen.

Op grond van bovenstaande principes weet je dat een tekst door het auteursrecht is beschermd als hij oorspronkelijk is. Het doet er niet toe hoe lang hij is (een slogan, enkele regels of verscheidene pagina's) of op welke informatiedrager hij aanvankelijk geplaatst werd (papier, diskette, CD-ROM, website, enz.).

Dat is geen probleem zolang je de auteur van de tekst bent, wat veronderstelt dat je de inhoud van de tekst zelf hebt uitgevonden. Het kopiëren van een bestaande tekst impliceert uiteraard niet dat je zelf de auteur van de tekst wordt.

Maar als de tekst beschermd is door het auteursrecht, mag hij niet op een site worden gereproduceerd zonder de toestemming van de auteur (behalve bij beroep op de uitzonderingen bepaald in het citaatrecht, zie hierboven nr. 47). Met toepassing van dat principe beschouwde de Franse rechtspraak dat het digitaliseren van het werk van Jacques Brel en van Michel Sardou, zonder toestemming van de auteurs van de rechten, namaak is. In België gaat de rechtspraak ervan uit dat de reproductie van persartikels op een internet-database de toestemming van de auteurs vereist.

53. Mag ik een werk (beeld, logo, icoon, foto, tekst, videosequens, muziekbestanden) van een andere site kopiëren of downloaden en op mijn site plaatsen ?

Hier gaat het niet meer om het digitaliseren van een werk vanaf een analoge informatiedrager (een papieren document), maar om het downloaden van een werk (beeld) dat zich op een site bevindt en dat de internetter op zijn eigen site plaatst en via het internet dus (her)verspreidt.

Met de bekende functie *knippen/plakken* (*copy/paste*), die in de meeste programma's zit, kun je in een mum van tijd een indrukwekkende reeks gegevens bijeenstellen die zich als tekstbestand, beeldbestand, foto's, enz. op andere websites bevinden. Nogmaals, deze technische functie, die het reproduceren heel makkelijk maakt, moet met mate worden aangewend en de auteursrechten moeten hoe dan ook geëerbiedigd worden.

Het kopiëren of downloaden van een werk komt namelijk neer op het reproduceren van dat werk en door het te (her)verspreiden via het internet wordt het aan het publiek meegedeeld. Welnu, een en ander valt onder het auteursrecht. Indien het werk beschermd is door het auteursrecht, wat doorgaans het geval is, moet je in principe dus vooraf de toestemming van de auteur bekomen.

54. Mag ik een beeld of foto van een analoge informatiedrager scannen of een beeld of foto van een digitale informatiedrager kopiëren en op mijn website plaatsen, zelfs als ik er vooraf wijzigingen in aanbreng ?

Op de markt bestaat er beeldverwerkings- of tekensoftware, waardoor een foto of een beeld zodanig kan worden gewijzigd (verandering van grootte, kleuren, vormen, contrast, oriëntatie, kadrering, enz.) dat het gewijzigde beeld geen enkele gelijkenis meer vertoont met het oorspronkelijke. Kun je het in dat geval stellen zonder de toestemming van de auteur van het oorspronkelijke werk (voor zover het beschermd is door het auteursrecht en dus oorspronkelijk is) ?

NEEN, het is niet omdat dit nieuwe beeld niet meer lijkt op het oorspronkelijke dat je je om het even wat mag permitteren. Om dat beeld te kunnen omvormen door middel van de geschikte software, heb je vooraf aan reproductie gedaan (hetzij door het werk te scannen, hetzij met *knippen/plakken*), waarvoor de toestemming van de auteur nodig is. Bovendien valt het herwerken van het beeld door middel van tekensoftware niet enkel onder het "aanpassingsrecht" maar ook onder het "recht op integriteit van het werk" en dat zijn exclusieve auteursrechten. Bijgevolg vergen zulke wijzigingen meestal wel de toestemming van de auteur.

Indien het omgevormde beeld helemaal niet meer lijkt op het oorspronkelijke, hoe kan de auteur dan een inbreuk op zijn rechten opsporen en zich op die rechten beroepen ? Een auteur heeft het inderdaad vaak moeilijk om na te gaan in hoever er inbreuk op zijn rechten is gemaakt. Wel bestaat er nu technische bescherming (bijvoorbeeld "tatoeëring" of "markering") die het mogelijk maakt een digitaal werk te identificeren, - ook al werd het grotendeels gewijzigd - en het gemakkelijk op het internet terug te vinden.

55. Mag ik muziekbestanden (bijvoorbeeld mp3's) op mijn site ter beschikking stellen van internetters ?

Wij zullen ons bij de behandeling van dit actueel probleem gemakshalve beperken tot muziekbestanden in mp3-formaat.

Wat is een mp3-formaat ?

De mp3-norm is een standaard voor de compressie van audiogegevens. Het mp3-formaat maakt het je mogelijk gewone geluidsbestanden 10 tot 13 maal te comprimeren met een uiterst miniem kwaliteitsverlies. Daardoor kun je de inhoud van 10 tot 13 "traditionele" cd's opslaan op één enkele cd van het mp3-formaat. Je snapt meteen wat voor mogelijkheden dit biedt op het internet : vroeger had je uren nodig om een lied van enkele minuten te downloaden, terwijl je de klus nu kunt klaren in een paar minuten als het om een mp3-

bestand gaat. Het internet puilt uit van geluidsbestanden in mp3-formaat (waarvan de meeste illegaal zijn), omdat ze van de ene internetter naar de andere circuleren of omdat sommige internetgebruikers de inhoud van hun “traditionele” cd's op hun computer opnemen, de bestanden comprimeren door middel van passende software en ze vervolgens verspreiden via het net.

Is zoiets toegelaten ?

Over het algemeen niet! Een muziekstuk is, zoals elke andere artistieke creatie, beschermd door het auteursrecht indien het oorspronkelijk is, wat vaak het geval is. Het is niet omdat je je op het internet begeeft dat die principes niet meer gelden, ook al is de omvang van de fraude op het net zo groot dat je de illusie krijgt dat het auteursrecht niet meer van toepassing is.

Indien het werk beschermd is door het auteursrecht, is het met name verboden de inhoud van een vinylplaat of audio-cd te digitaliseren en op je harde schijf of elke andere informatiedrager te kopiëren (behalve als je de kopie enkel in je familiekring beluistert). Bijgevolg is het ook verboden zulke bestanden te comprimeren met behulp van mp3-compressiesoftware en ze via je website ter beschikking te stellen van de internetters zonder toestemming van de eigenaar van de rechten op de aldus gecomprimeerde werken. Dergelijke daden zijn namelijk reproducties en mededelingen aan het publiek ; ze vallen onder het exclusieve recht van de auteur. Belgische en buitenlandse rechtbanken hebben die principes reeds toegepast en sommige personen tot verschillende maanden gevangenisstraf veroordeeld. Die personen werden schuldig bevonden voor namaak omdat ze een site hadden gecreëerd waar de bezoekers gratis illegale muziekstukken (in mp3-formaat) konden downloaden. Tal van maatschappijen (zoals *Napster*) kregen het ook aan de stok met het gerecht omdat ze software en een platform ontwikkelden waardoor websurfers (meestal illegale) mp3-bestanden vrij onder elkaar konden uitwisselen.

Mag ik dan nooit mp3-bestanden op mijn site plaatsen ?

Natuurlijk mag je dat. Het gebruik van de mp3-norm is als dusdanig niet verboden. Het probleem ligt hem bij de gevolgen die het gebruik van mp3-bestanden kunnen hebben op het auteursrecht. Er bestaan gevallen waarin het plaatsen van een mp3-bestand op een website niet strafbaar is :

- hetzij omdat het werk niet oorspronkelijk en bijgevolg niet beschermd is door het auteursrecht (zo'n geval komt wel zelden voor) ;
- hetzij omdat je zelf het werk hebt gecomponeerd, geïnterpreteerd en opgenomen. In dat geval ben je in principe de auteur van het werk en kun je het naar goeddunken verspreiden en reproduceren ;
- hetzij omdat het werk niet meer beschermd is door het auteursrecht doordat de auteur al meer dan 70 jaar overleden is. Maar opgelet hier : al moet je geen toestemming vragen aan de componist van het muziekstuk of lied, toch heb je soms het akkoord nodig van de muzikanten (de artiesten die het werk uitvoeren) en de platenmaatschappijen. Ook dan moet je nog voorzichtig zijn, want er bestaan tal van arrangementen van werken die nog beschermd zijn door het auteursrecht, ook al zijn de werken zelf het niet meer ;
- hetzij omdat de mp3-bestanden het auteursrecht eerbiedigen.

56. Mag ik hyperlinks aanbrengeen die verwijzen naar sites met mp3-bestanden ?

Hierop kan niet eenduidig geantwoord worden. Er bestaat geen algemene regel. Sommige rechtbanken beslisten dat het leggen van een link naar illegaal materiaal (bootleg-mp3's) helemaal niet in strijd is met de wet, zolang de gebruiker dat materiaal maar niet op zijn eigen site plaatst. Andere rechtbanken waren minder inschikkelijk. Gelet op de onzekerheid raden wij je aan voorzichtig te zijn en op je site geen hyperlinks te leggen naar sites die - waarschijnlijk illegale - mp3's bevatten.

57. Mag ik een werk zonder *copyright*-vermelding vrij kopiëren ?

Neen, niet noodzakelijk. Het voorkomen of het ontbreken van een *copyright* impliceert niet dat het werk beschermd of niet beschermd is door het auteursrecht. In wat voorafgaat hebben wij namelijk gezegd dat een werk automatisch beschermd is door het auteursrecht als het gecreëerd werd, oorspronkelijk is en een vorm heeft gekregen. Het is dus niet zo dat je een werk vrij mag kopiëren als er geen *copyright* op vermeld is. Als het werk beschermd is, ben je verplicht de toestemming van de auteur te vragen.

Ter wille van de bewijskracht raden wij je echter aan de vermelding *copyright Janssens – 2000* aan te brengen indien je een - waarschijnlijk door het auteursrecht beschermd - werk van jou (tekst, foto, enz.) in je site wilt invoegen. Volgens artikel 6 van de wet op het auteursrecht wordt iemand verondersteld houder te zijn van het auteursrecht als zijn naam of een of ander teken als dusdanig op het werk is vermeld.

58. En wat met de werken met de vermelding “zonder auteursrechten” (copyright free) of de zogenaamde “freewares” of “sharewares” ?

Op het internet vind je vaak databanken die werken voorstellen (foto's, beelden of software) waarvan gezegd wordt dat zij “zonder auteursrechten” zijn en vrij kunnen worden gereproduceerd. Voor software heeft men het ook over *freewares* (software die helemaal gratis is) of *sharewares* (software die vrij wordt verdeeld om door de gebruiker te worden geëvalueerd). Na een proefperiode moet de gebruiker een vergunning aanvragen ; zoniet mag hij de software niet verder gebruiken). Die problematiek rijst ook voor de zogenoemde “vrije” software.

Impliceren zo'n vermeldingen noodzakelijkerwijze dat die foto's, beelden of software niet door het auteursrecht beschermd zijn ? In principe is het antwoord neen. Indien het werk oorspronkelijk is en de duur van de rechten niet verstreken is, dan is het auteursrechtelijk beschermd en het feit dat de houders van de rechten verklaren dat het werk “vrij van rechten” (*copyright free*) is, doet eigenlijk niets ter zake. Je kunt dan wel beschouwen dat die houders een gratis gebruiksvergunning geven.

In zo'n hypothese moet je op twee zaken letten :

- enerzijds betekent een gebruiksvergunning niet dat je om het even wat kunt doen : doorgaans wordt in de databanken aangegeven welk gebruik effectief toegestaan is (uitgesloten is bijvoorbeeld het gebruik voor commerciële doeleinden) ;
- anderzijds is het mogelijk dat de vermeende houder van de rechten geen houder is van die rechten. In dat geval kan de auteur in kwestie zich bekend maken en zich verzetten tegen het gebruik van zijn werk. De goede trouw van de gebruiker kan niet ingebracht worden tegen de houder van de auteursrechten (goede trouw sluit namaak niet uit !).

59. Als ik met hyperlinks verwijs naar een andere website, moet ik dan de toestemming vragen van de eigenaar van die site ?

Als je een eigen website creëert, leg je waarschijnlijk een of meer links naar een andere site (of naar een specifieke pagina van een andere site) (zie hierboven nr. 20). Moet je in dat geval de toestemming vragen van de eigenaar van de site waarmee je een hypertextverbinding legt ?

Blijkbaar niet. Over het algemeen vormt dat soort handeling geen probleem op het vlak van het auteursrecht. Al wordt er over dat probleem nog onder juristen geredetwist, toch bestaat de neiging om te stellen dat elke persoon die verantwoordelijk is voor een website geacht wordt de andere operatoren van het netwerk stilzwijgend te hebben toegestaan een hypertextlink te leggen, voor zover die link eenvoudig is en hij verwijst naar de onthaalpagina (en niet naar een of andere onderpagina van die website. Wat je echter niet mag doen, is hyperlinks leggen naar sites met een illegale of schadelijke inhoud (revisionistische of pornografische sites bijvoorbeeld).

Gebruik je andere hyperlinktechnieken, die niet als “eenvoudig” beschouwd worden, hoed je dan voor eventuele juridische implicaties. Bijvoorbeeld : een hyperlink met titels (beschermde door het auteursrecht !) van persartikels met stelselmatige verwijzing naar de site die deze artikels publiceert. Zo'n praktijk kan worden beschouwd als oneerlijke concurrentie (*parasitisme*) en/of schending van het auteursrecht. Ook het gebruik van een “diepe link” kan voor problemen zorgen. Dat soort hyperlink verwijst naar een onderpagina van de site en veroorzaakt dus een “kortsluiting” van de onthaalpagina. Volgens sommige siteverantwoordelijken is dat een nadelige praktijk, onder meer als de onthaalpagina de enige is die reclame (webvertenties, *banners*) bevat en ze wegens de diepe link onzichtbaar blijft voor heel wat websurfers. Wees ook voorzichtig als je gebruik maakt van de *framingtechniek* (kaders, vensters) gecombineerd met hyperlinks. Zie dat je het publiek niet op een dwaalspoor brengt omtrent de echte houder van de site. Stel dat je in een venster (*frame*) een hyperlink legt naar een prachtig gedicht op een andere site. Bij het aanklikken van die link zou het kunnen dat de pagina waarop dat gedicht staat op een zodanige manier verschijnt dat de internetgebruiker niet merkt dat hij zich op een andere site bevindt en verkeerdelijk meent dat het gedicht van jou is. Vermijd zulke praktijken of zorg ervoor dat je de toestemming hebt van de persoon die verantwoordelijk is voor de in een zoekmachine opgenomen site.

60. Kan ik mij verzetten tegen het leggen van een hyperlink naar mijn site ?

Zoals we stelden in het antwoord op de vorige vraag, gaat men ervan uit dat de persoon die verantwoordelijk is voor een website de andere operatoren van het netwerk stilzwijgend toestond een hypertextlink te leggen naar zijn site.

Dat principe moet wel sterk genuanceerd worden. Je kunt je steeds verzetten tegen een hyperlink naar je site indien die jou schade kan toebrengen. Zo zou een pornografische of revisionistische website of een geringschattende of beledigende webtekst via een hyperlink kunnen verwijzen naar jouw site. Afhankelijk van de context kan een hyperlink ook worden beschouwd als bedrieglijke reclame (verboden door de wet) of vergelijkende reclame (zonder naleving van alle voorwaarden van de wet). Ook een hyperlink die overmatig voordeel haalt uit jouw werk wordt als schadelijk beschouwd : je ontwerpt een site met oorspronkelijke foto's over alpinisme en een andere gebruiker creëert een lege site die met een hyperlink stelselmatig naar de foto's op jouw site verwijst, dit alles in een waas van geheimzinnigheid.

Om schadelijke gevolgen bij gebruik van hyperlinks te voorkomen, nemen sommige sites in hun algemene voorwaarden de volgende clause op : “Elke gebruiker verbindt zich ertoe de toestemming te vragen aan de persoon die verantwoordelijk is voor deze website alvorens een hyperlink van welke aard ook te leggen naar deze site” of “Het is verboden zonder voorafgaande toestemming rechtstreekse links te leggen op deze pagina, op bestanden of toepassingen van deze site”.

61. Welke sancties worden er getroffen als ik het auteursrecht niet eerbiedig ?

Op het niet-eerbiedigen van bovenstaande principes staan strafrechtelijke sancties (gevangenisstraf of boete) en/of burgerrechtelijke straffen (betaling van schadevergoeding bijvoorbeeld).

Namaak houdt niet in dat men schade wil toebrengen, noch dat men andermans recht op het werk kent. Je ontloopt dus geen veroordeling door schuil te gaan achter het feit dat je te goeder trouw onwetend waart.

Bovendien kan de rechter bevelen dat het vonnis ten laste van de overtreder wordt bekendgemaakt in de pers of een ander medium (bijvoorbeeld op de *homepage* van een website). Nagemaakte voorwerpen kunnen in beslag worden genomen.

Die sancties kunnen theoretisch lijken omdat fraude op het internet een kolossale omvang heeft aangenomen en het risico om te worden gesnapt miniem is. Wees echter op je hoede ! Er worden steeds meer technische middelen gebruikt om beschermde werken te identificeren en fraude op het internet op te sporen met geautomatiseerde zoekmachines. Bovendien stellen beroepsorganisaties of vennootschappen voor collectief beheer van auteursrechten alles in het werk om de rechten van hun leden te doen eerbiedigen. Ten slotte werden al tal van personen door onder meer Belgische en Franse rechtbanken veroordeeld wegens namaak omdat zij op hun site werken hadden geplaatst die door het auteursrecht beschermd zijn. Een goed verstaander heeft maar een half woord nodig...

62. Is mijn site beschermd door het auteursrecht of door een ander recht ?

We hebben het er al over gehad : als je een website creëert, dan moet je andermans rechten en meer bepaald de auteursrechten eerbiedigen. Omgekeerd kun je bescherming wensen voor je eigen website en de inhoud ervan. Je bent bijvoorbeeld amateur-fotograaf en je wilt internetters de mogelijkheid bieden je foto's te raadplegen, maar vermijden dat iemand je hele verzameling kopieert en daarmee een gelijkaardige site creëert. Wat voor foto's geldt, geldt ook voor gedichten, muziekstukken, wetenschappelijke publicaties en dergelijke meer. Je kunt aan je site ook een heel aparte structuur hebben gegeven en daarvan het geestelijk vaderschap willen behouden.

Daar het hier om een complexe aangelegenheid gaat, treden wij niet in details. Je moet wel weten dat de inhoud van je site (teksten, beelden, foto's, enz.) door het auteursrecht kan worden beschermd voor zover je de auteur bent van de inhoud. Bovendien kan de site zelf (dat wil zeggen voorstelling, lay-out, typografie, tekeningen, structuur) ook door het auteursrecht worden beschermd, zoals we hierna zullen zien. De enige voorwaarde is dat de site en de inhoud ervan oorspronkelijk zijn (zie hierboven nr. 40), wat meestal wel het geval is. Bijgevolg kun je je ertegen verzetten dat een derde die inhoudsonderdelen reproduceert.

Voorts wordt door een Europese richtlijn van 11 maart 1996, omgezet in Belgisch recht bij de wet van 31 augustus 1998 (Belgisch Staatsblad van 14 november 1998, p. 36914), een

dubbele bescherming ingesteld voor databanken, enerzijds via het auteursrecht en anderzijds via een specifiek recht, recht *sui generis* genaamd.

Het auteursrecht beschermt oorspronkelijke databanken (een website kan namelijk worden beschouwd als een databank of kan een databank bevatten). Oorspronkelijke databanken zijn databanken die, door de keuze of de schikking van de bestanddelen, een eigen intellectuele schepping van de auteur vertegenwoordigen. De bescherming geldt niet voor de inhoud van de databank (die desgevallend beschermd blijft door een specifiek auteursrecht of door een ander recht zoals het merkenrecht), maar wel voor de structuur van die databank. De houder van het recht is de ontwerper van de databank (kan een natuurlijke of rechtspersoon zijn). De duur van het recht stemt overeen met de duur van het traditioneel auteursrecht, nl. 70 jaar na de dood van de auteur.

Databanken (vooral niet oorspronkelijke) genieten ook bescherming door het recht *sui generis* dat van toepassing is op alle databanken, waarvan het verkrijgen, het verifiëren of het voorstellen van de inhoud een aanzienlijke kwantitatieve of kwalitatieve investering vergde. De houder van het recht is de ontwerper van de databank, d.i. de natuurlijke of rechtspersoon die het initiatief en het investeringsrisico nam. Op grond van dit recht mag hij de overname en/of het hergebruik van de gehele databank of van een groot deel ervan verbieden (of tegen betaling toestaan). Dat recht loopt gedurende 15 jaar vanaf het ontwerpen van de databank. Elke wezenlijke verandering van de databank verschaft een bijkomende beschermingsperiode van 15 jaar.

Deel 4. Zich beschermen tegen “aanvallen” op het internet



HOOFDSTUK I. INBREUKEN OP HET PRIVÉ-LEVEN

Afdeling 1. Indringingstechnieken

63. In hoever wordt mijn privé-leven bedreigd als ik op het internet surf ?

Op het internet gaan is voor velen onder ons dagelijkse kost geworden : we verzenden e-mails, bezoeken websites, chatten *in real time* in babbelkamers, enz.

Telkens je op het internet gaat, heb je de indruk dat alles vrij en anoniem verloopt, maar is dat wel echt zo ? Bij het websurfen onthul je informatie over jezelf en laat je een aantal sporen na. Meestal speelt de *browser* die je gebruikt automatisch een hele reeks gegevens door aan de site die je bezoekt :

- het TCP/IP-adres, d.i. een enig nummer dat op het web aan je microcomputer wordt toegekend ;
- het merk en de versie van je browser en van je exploitatiesysteem ;
- de taal die je gebruikt ;
- de laatst geraadpleegde webpagina (als je een link hebt gevolgd naar de huidige bladzijde) ;
- de permanente cookies (zie hieronder nr. 64) die reeds door de bezochte site zijn opgezonden.

Al die informatie wordt automatisch toegankelijk gesteld voor de webserver, die op die manier rekening kan houden met de kenmerken van de door de internetter gebruikte configuratie. Als de server het browsertype kent en weet welke versie er werd gebruikt, dan zal hij sommige incompatibele toepassingen niet lanceren.

Inzake bescherming van de persoonlijke levenssfeer komt het probleem voort van het samengaan van die variabelen met andere gegevens over jou die de server elders kon vergaren (bijvoorbeeld via zijn internetprovider), dit alles zonder dat je erover ingelicht werd en ertegen kon reageren. Als je bijvoorbeeld een onlineformulier met persoonlijke gegevens invult, kan er moeiteloos een verband gelegd worden tussen het TCP/IP-adres van je computer en die informatie, zodanig dat jouw traject op de site kan worden gevolgd en er van jou een nauwkeurig profiel kan worden opgemaakt.

Aan de hand van diverse technieken kunnen aldus ongemerkt persoonlijke gegevens over jou worden ingewonnen en kunnen jouw internetgewoonten worden geobserveerd. Elk van die technieken afzonderlijk kan slechts een beperkte hoeveelheid informatie vergaren. Ze zijn dus betrekkelijk weinig “indringend”, maar kunnen toch overrompelend werken als ze worden gebruikt in combinatie met andere methodes. Ze worden dan machtige observatiemiddelen die thans voor marketingdoeleinden worden aangewend, maar eventueel kunnen worden gebruikt met het oog op discriminatie of wijziging van doorgegeven informatie.

De meest verspreide van die technieken is het gebruik van cookies die je bewegingen op het internet registreren (zie hieronder nr. 64 e.v.). Sommige technieken, zoals *spyware* (spionagesoftware), zijn nog indringender en kunnen zelfs achter persoonsgegevens komen die op je harde schijf staan (zie hieronder nr. 69 e.v.).

Als je wilt weten hoe je spoor op het internet wordt gevolgd, bezoek dan even de site van de *Commission Nationale Informatique et des Libertés* :

<http://www.cnil.fr> (Frans equivalent van onze Commissie voor de Bescherming van de Persoonlijke Levenssfeer).

64. Wat is een cookie ?

Een *cookie* is een automatisch bestand in tekstformaat dat door een webserver naar je computer wordt gestuurd en er wordt opgeslagen als je een internetsite bezoekt. Door middel van een cookie kan een webserver op je computer gegevens bewaren die hij nodig heeft wanneer je met die computer een bezoek brengt aan diezelfde internetsite.

In de praktijk stuurt de server een of meer cookies naar jouw navigatieprogramma. Je navigator ontvangt een cookie en registreert dit in een bepaald bestand op je computer. Voortaan zal je navigator dit cookie systematisch meedelen wanneer je dezelfde server raadpleegt als die welke het eerste cookie gestuurd heeft. Het is echter mogelijk dat een *cookie* gedeeld wordt met verscheidene servers van eenzelfde domein.

Er zijn twee soorten cookies : sessiecookies (tijdelijke cookies) en permanente cookies (blijvende cookies).

Sessiecookies hebben geen vervaldatum, worden niet op je harde schijf opgeslagen en worden automatisch verwijderd bij het verlaten van de bezochte website. Ze worden over het algemeen gecreëerd om technische redenen (als er geen sessiecookies zouden worden gemaakt, dan zouden je aanvragen, bij elk sitebezoek en elke overgang naar een andere pagina via hyperlinks, afzonderlijk worden behandeld alsof verscheidene gebruikers zich toegang wilden verschaffen tot een welbepaalde pagina van de site). Ze dienen niet om een blijvende band te leggen tussen jouw computer en de bezochte site.

Permanente cookies daarentegen bevatten een door de server vastgestelde vervaldatum, waardoor die server tot het verstrijken van die datum toegang heeft tot de daarin vervatte informatie.

De levensduur van een cookie hangt af van de wil van de bronserver : enkele minuten, de tijd van de verbinding of enkele jaren (maximum 35 jaar).

65. Waartoe dient een cookie ?

Cookies doen je opzoeken vlotter verlopen.

Cookies kunnen worden gebruikt voor diverse doeleinden.

Soms moet de server weten wie de bezoeker is. Zo bieden de meeste onlineverkoopsites hun klanten de mogelijkheid een soort van virtuele boodschappenmand aan te leggen vóór het doorgeven van de bestelling. De internaut surft op de site en kiest geleidelijk de artikels die hij wenst te bestellen. Die artikels worden opgeborgen in de mand ; de stand van de mand wordt bijgehouden door middel van mechanismen die met cookies werken. Als het om een meertalige site gaat, dan kan het interessant zijn te onthouden dat een persoon Nederlandstalig is om de pagina's bij een eventueel bezoek onmiddellijk in het Nederlands te laten verschijnen. Daartoe plaatst de server een cookie met die informatie op de harde schijf van de betrokken persoon ; bij een volgende bezoek leest de server eerst het cookie en leidt daaruit het taalgebruik af. Wanneer tijdens de transactie de

verbinding verbroken wordt, zal het cookie de verkoper in staat stellen jouw spoor terug te vinden dankzij het cookie dat vroeger op je computer opgeslagen werd.

Een cookie maakt het ook mogelijk je gewoonten in kaart te brengen en je gerichte informatie toe te sturen. Aan de hand van cookies kan een server je traject tijdens een sessie nagaan en dus je profiel bepalen. Daartoe volstaat het dat de server een cookie plaatst op elke pagina die je bezoekt of bij elke actie die je onderneemt en al die cookies nadien samenvoegt om je traject te analyseren. Vervolgens kan hij je moeiteloos op jouw profiel afgestemde pagina's voorstellen.

Het nadeel van deze techniek is dat zij de deuren wagenwijd opengooit voor indiscretie. Immers : op die manier kunnen sommige sitebeheerders of reclamebedrijven buiten je weten om informatie vergaren over jou. Bij een bezoek aan een website wordt bijvoorbeeld informatie over de bezochte pagina's, de taalvoorkeur, de aard van de opzoeken met een zoekmachine, op het cookie opgeslagen en bij elk bezoek teruggestuurd naar de sitebeheerder.

Zo kunnen de op het cookie aanwezige gegevens worden gebruikt om een steeds nauwkeuriger profiel op te maken van je gewoonten en voorkeuren, zodanig dat de sitebeheerder je producten kan voorstellen die met je smaak overeenstemmen. Een cookie kan dus een interessant middel worden voor directe-marketingmaatschappijen die op die manier een nauwkeurig beeld krijgen van je interessesfeer en je consumptiegewoonten opslaan in databanken.

66. Moet ik op mijn hoede zijn voor cookies ?

In principe verschaffen cookies geen informatie die je niet voordien op een of andere manier hebt doorspeeld. Bijgevolg maken cookies het als dusdanig niet mogelijk jouw naam of e-mailadres te kennen.

Doch, ook al word je niet altijd op een duidelijke manier geïdentificeerd, je bent tenminste identificeerbaar. Weet dat alle cookies die op je computer staan en waar je geen aandacht aan schenkt in verband kunnen worden gebracht met nauwkeuriger informatie (nominatieve gegevens) die je ooit eens hebt verstrekt, bijvoorbeeld bij het invullen van een formulier. Hetzelfde geldt voor alle informatie over de software die je gebruikt, bankinformatie of andere informatie die je spontaan hebt gegeven. Een dergelijke toetsing van informatie maakt het mogelijk - volledig buiten je weten - echte gedragsdatabanken op te maken !

Je moet ten slotte weten dat elk cookie een spoor nalaat op je harde schijf en aangeeft welk traject je op het internet hebt gevolgd. Houd je dus een sessie op een andere computer dan de jouwe, neem dan je voorzorgen als je niet wil dat de volgende gebruiker alles te weten komt over dat bezoek.

67. Hoe kan ik mij beschermen tegen cookies ?

Afhankelijk van je ergernis over die intrusie in je privé-leven, beschik je over verschillende mogelijkheden om daar een rem op te plaatsen of om dit een halt toe te roepen. Geen enkele oplossing is echter ideaal.

Je kunt eerst de alarmfunctie van je computer activeren. De belangrijkste navigatieprogramma's (Netscape Navigator en Microsoft Explorer) melden de komst van cookies "in real time". Op dat moment kun je het registreren van het cookie aannemen of weigeren. Goed idee natuurlijk, want zo kun je de cookies aanvaarden die voor jou nuttig

zijn en zien welke sites je proberen te bespieden. Maar helaas : in de praktijk zal je merken dat zo'n oplossing heel omslachtig is. Het aantal sites die cookies opsturen is reusachtig groot. Je webbezoek zal dus constant worden verstoord door cookies-alarmberichten van je browser. Dat is nu eenmaal de prijs die je moet betalen voor een doeltreffende controle ...

Bovendien is de bescherming niet standaard geactiveerd en mag de technische kennis die vereist is voor de activering niet worden onderschat. Om te worden ingelicht over de verzending van een cookie, moet je je browser parametriseren.

Sommige browsersversies bieden de mogelijkheid automatisch cookies te weigeren. Je kunt je browser zodanig instellen dat hij systematisch de indringing van cookies weigert. Die radicale oplossing heeft helaas niet enkel gelukkige gevolgen. De websites waarheen je gewoonlijk surft, zullen je niet meer herkennen. Je moet dan je gebruikersgegevens telkens opnieuw invoeren. Ander belangrijk detail : in sommige gevallen kun je geen online aankopen meer doen. Bovendien versperren sommige sites je de toegang als je hun cookies niet aanvaardt. Die oplossing is doeltreffender voor de bescherming van je intimiteit, maar verstoort enigszins je surfactiviteit en beperkt je actieradius.

Cookies kun je ook vernietigen. Je kunt de plaats vinden waar cookies op je harde schijf opgeslagen zijn. Eens je de ongewenste cookies gevonden hebt, volstaat het ze te verwijderen. Doe dat echter niet regelmatig, want als je terugkeert naar sites die je de week daarvoor met cookies opzadelden, zullen die je opnieuw bestanden toesturen. Een vicieuze cirkel, waarbij je ook het risico loopt nuttige cookies te verwijderen : namelijk cookies met persoonsgebonden informatie voor toegang tot sites die je regelmatig bezoekt. Als je je naar die sites begeeft, dan zal de browser je opnieuw vragen een aantal gegevens in te voeren : gebruikersnaam, wachtwoord... De handmatige methode biedt dus soelaas, maar enkel voor mensen die geen gebruik maken van netdiensten (mail, shopping, verkoop bij opbod, enz.)

Er bestaan ook andere mogelijkheden. Je kunt programma's gebruiken die cookies vernietigen (*cookie busters*) en gratis vanop het web gedownload kunnen worden. Een andere oplossing is het gebruik van een *proxyserver* (<http://www.inetprivacy.com/>) : dit is een firewallserver die als bemiddelaar tussen de surfer en het netwerk optreedt, de HTTP-verzoeken in zijn naam uitvoert en hem de resultaten meedeelt. In dat geval ben je dus niet geïdentificeerd door je correspondent. Het installeren van een proxyserver vereist een minimum aan technische kennis en alleen de demoversie is gratis.

68. Hoe kan ik mij juridisch beschermen ?

De Belgische wet regelt het gebruik van je persoonsgegevens (zie hieronder nr. 72 e.v.). Persoonsgegevens zijn inlichtingen over een geïdentificeerde of identificeerbare natuurlijke persoon. Het cookie, indien dit je kan identificeren (ook door verschillende bestanden aan elkaar te toetsen, enz.), kan als een persoonsgegeven worden beschouwd.

In dit geval moet een aantal regels worden nageleefd :

- De auteur van de site moet je inlichten voordat hij een cookie op je harde schijf opslaat.
- De auteur van de site moet zijn identiteit bekendmaken (niet alleen zijn URL-adres of e-mailadres, maar ook zijn andere adresgegevens).
- De auteur van de site moet aangeven waarvoor het cookie gebruikt zal worden.

- De auteur van de site moet het bestaan van het toegangsrecht signaleren.
- De auteur van de site moet het toegangsrecht toestaan.
- De auteur van de site moet een recht op verzet verlenen.

69. Wat is spionagesoftware ?

Spionagesoftware (ook spionsoftware of *spyware* genoemd) is een klein informaticaprogramma dat meestal in de hoofdsoftware geïntegreerd is of erbij geleverd wordt. Doorgaans zit spyware in de code van een programma dat je argeloos van het internet hebt gedownload. In de meeste gevallen bestaat die spionagesoftware uit deeltjes parasietcodes (routines) die deel uitmaken van de hoofdcode van het programma. In eenzelfde programma kunnen er verschillende parasietroutines zitten, met elk een welbepaalde functie.

Zo'n routines zijn heel moeilijk opspoorbaar. Hoe dan ook, spyware heeft een internetverbinding nodig om gegevens over te zenden. Daarom gaat spionagesoftware vaak samen met software die op het internet kan worden gedownload (programma's voor het binnenhalen van mp3-bestanden, films, vertaalsystemen, browsers, enz.). Over het algemeen zijn gratisware (*freeware*) en evaluatiesoftware (*shareware*) de voornaamste dragers van spionsoftware.

Spyware wordt op een computer geïnstalleerd zoals een ander programma, meestal zonder dat je het beseft of zonder dat je geïnformeerd wordt over het doel ervan, en verzamelt informatie over je surfgedrag en je machine.

Bij de verklikkers kun je ook de *web bugs* onderbrengen. Een web bug (ook *1-pixel gif* genoemd) is een onzichtbaar en onopspoorbaar beeld bestaande uit één enkele pixel ingevoegd in elektronische pagina's of in een e-mail in HTML-formaat. Web bugs worden echter niet blijvend geïnstalleerd op de computers van de betrokken gebruikers. Ze worden meestal gebruikt om de bezoekfrequentie te meten.

70. Waartoe dient spionagesoftware ?

Net als cookies zijn web bugs ware elektronische klikspanen, maar met veel ruimere functies : van bij het opstarten van je computer kunnen ze alle ingezamelde gegevens, zoals jouw surfgewoonten en de adressen van alle bezochte sites, doorsturen naar de servers van een centrale instelling.

Bovendien vormt spyware een grote bedreiging voor de veiligheid van het besmette informaticasysteem. Met spyware kan men de juiste configuratie van je computer en de inhoud van je harde schijf achterhalen ; met een reeks routines kan men gecodeerde wachtwoorden te weten komen en bestanden kraken.

De voornaamste bedoeling van spionagesoftware is het doorspelen van die gegevens naar degene die hem ontworpen heeft, al dan niet onder het mom van een of andere dienstverlening ; meestal wordt hij gebruikt voor publicitaire en commerciële doeleinden. Sommige bedrijven hechten veel belang aan dergelijke gegevens, omdat de waarde van hun bestanden en databanken bepaald wordt door een zo nauwkeurig mogelijke profilering van de gerepertorieerde internetgebruikers.

Los van de problematiek van de bescherming van de persoonlijke levenssfeer dient er nog te worden opgemerkt dat spyware een aantal onderdelen van je computer opeist als hij in

de achtergrond actief is (schijfgeheugen, vluchtig geheugen en bandbreedte voor de overdracht van gegevens).

71. Hoe kan ik mij beschermen tegen spionagesoftware ?

Je tegen *spyware* beschermen is geen sinecure. In de praktijk kun je als internaut verscheidene maatregelen nemen om je te beveiligen tegen de ongewenste effecten van spionagesoftware.

Vooreerst moet je letten op wat je op je computer plaatst. Wees vooral op je hoede met software die her en der gratis aangeboden wordt. Een van de hoofdkenmerken van spyware is dat hij vaak ergens geïnstalleerd is zonder dat de gebruiker het weet. Dialoogvensters geven je zelden de mogelijkheid dit te weigeren. Krijg je de keuze om een programma op gepersonaliseerde wijze te installeren, desactiveer dan de bijkomende modules die niet absoluut noodzakelijk zijn voor de werking van die software. Ga oordeelkundig tewerk bij het uitvoeren van de nodige commando's (voor ervaren gebruikers is dat geen probleem).

Tweede elementaire voorzorgsmaatregel : lees aandachtig de licentieovereenkomst. Hierin staat meestal voluit dat het programma dat je gaat installeren spionagefuncties bevat. Je kunt dan nog altijd kiezen voor een gelijkaardige software van de concurrent waarop geen spyware geïnstalleerd is.

Het gebruik van een antivirusprogramma en een *firewall* (vuurmuur, brandmuur, brandscherm) kan nuttig zijn. De doeltreffendheid van zulke software is wel heel relatief. Behoudens uitzonderingen kijkt een firewall niet naar wat je PC verlaat, maar naar wat er binnenkomt. Sommige brandmuren verwittigen de gebruikers van pogingen om hen te verbinden met andere servers. Een antivirusprogramma zal wellicht weinig uithalen, want spionagesoftware wordt niet beschouwd noch geregistreerd als een virus en glijpt vaak door de mazen van deze filters.

De meest doeltreffende manier om je te beschermen tegen spyware is het gebruik van programma's die hem identificeren en uitschakelen of die hem vernietigen. Zo verschaffen sommige sites een lijst van de gekende spyware en van de antispyspywareprogramma's die gratis beschikbaar zijn op het internet en efficiënt lijken te werken (zie <http://www.spychecker.com>). Geen enkele site kan echter beweren een volledige lijst te kunnen voorleggen van de bestaande spyware. Overigens kun je met sommige programma's software opsporen die spyware bevat, doch het gebruik van die programma's garandeert nog niet dat je computer daardoor op-en-top beveiligd is. Bovendien worden deze beschermtechnieken beter door ervaren gebruikers gehanteerd, want een verkeerd gebruik van de software of het ongelukkig wissen van bestanden kan de werking van je computer danig in de war sturen. Aarzel niet bij twijfel raad te vragen aan mensen met een informaticaknobbel.

Afdeling 2. Bescherming van de persoonlijke levenssfeer en verwerking van persoonsgegevens

72. Wat is verwerking van persoonsgegevens ?

De nieuwe informatica- en communicatietechnologieën bieden talrijke mogelijkheden en voordelen, maar houden ook gevaren in voor de persoonlijke levenssfeer en ieders vrijheden.

Vaak heeft de op het internet circulerende informatie betrekking op personen. Databanken of bestanden met persoonlijke informatie over jou worden aangemaakt, gebruikt, meegedeeld en verkocht. Je kan nog nauwelijks achterhalen wie wat van je afweet en wie er wat mee doet. Het individu heeft als het ware de beheersing over de hem betreffende informatie verloren. Om hieraan het hoofd te bieden, beschikt België, net als de overige landen van de Europese Unie, over een wetgeving betreffende de persoonlijke die de verwerking van persoonsgegevens reglementeert.

Onder *persoonsgegevens* verstaat men informatie die je identificeert of het mogelijk maakt je te identificeren. Je naam en adres (zelfs dat van de plaats waar je werkt), evenals je elektronisch adres worden beschouwd als persoonsgegevens.

Dit begrip heeft ook betrekking op een hoop informatie waarmee je onrechtstreeks (door toetsing) kan worden geïdentificeerd, namelijk door verwijzing naar een identificatienummer of één of meer specifieke elementen eigen aan je fysieke, psychische, economische, culturele of sociale identiteit. Het kan gaan om het inschrijvingsnummer van je voertuig, in een beroepengids vervatte gegevens, foto's, onzichtbare gegevens verzonden tijdens internet sessies (IP-adres), bibliografische gegevens, enz.

Om onder de wetgeving op de bescherming van persoonsgegevens te vallen, moet het gaan om *verwerking* van zulke gegevens. Dit begrip betreft alle handelingen of het geheel ervan toegepast op persoonsgegevens. Die handelingen kunnen zeer uiteenlopend zijn en omvatten het inwinnen van gegevens, het bewaren, gebruiken, wijzigen, verzenden ervan, enz. Telkens je bijvoorbeeld verzocht wordt een onlineformulier in te vullen, stemt dit overeen met verwerking van gegevens voor wie die inwint. Ook een hotel dat je de mogelijkheid biedt via het internet te reserveren, verwerkt gegevens, wanneer het je naam, de data van je verblijf en je kredietkaartnummer registreert.

De wet is van toepassing zodra persoonsgegevens volledig of gedeeltelijk door middel van geautomatiseerde procédés worden verwerkt (die procédés omvatten alle informatietechnologieën : informatica, telematica, communicatienetwerken). Bijvoorbeeld : een databank waarin de klanten van een onderneming geregistreerd zijn, een elektronische lijst van de verrichtingen op een bankrekening, een geïnformatiseerd personeelsbestand van een bedrijf, enz.

De wet is ook van toepassing wanneer de gegevens worden verwerkt zonder enig gebruik van geautomatiseerde procédés, ingeval de inlichtingen opgenomen zijn of bestemd zijn om te worden opgenomen in *bestanden* (d.w.z. een gestructureerd geheel waarin de gegevens toegankelijk zijn volgens specifieke criteria, zoals de alfabetische volgorde).

73. Hoe kan ik weten wie voor de verwerking van mijn gegevens verantwoordelijk is ?

Het is heel belangrijk dat je weet wie volgens de wet als "verantwoordelijk voor de verwerking" wordt beschouwd. Het is immers die persoon die belast is met bijna alle door de wet opgelegde verplichtingen ter bescherming van verwerkte gegevens. Hij wordt derhalve aansprakelijk gesteld in geval van moeilijkheden ; hij is je belangrijkste gesprekspartner.

Voor de wet is de verantwoordelijke voor de verwerking de persoon die, alleen of samen met anderen, de doelstellingen vastlegt (bijvoorbeeld het verzamelen van gegevens om marketingprofielen op te stellen) en de middelen aanduidt om persoonsgegevens te verwerken (onlineformulieren, cookies, enz.). Het gaat dus om de persoon die de beslissingsmacht heeft om gegevens te verwerken.

Wanneer iemand gegevens over jou inwint, is hij verplicht je de naam van de verwerkingsverantwoordelijke en de aard van de verwerking mee te delen. Je kunt je desnoods wenden tot de *Commissie voor de Bescherming van de Persoonlijke Levenssfeer*, waarvan de opdracht er met name in bestaat een openbaar register met die informatie bij te houden.

74. Over welke rechten beschik ik om mijn privacy te beschermen ?

Zodra je gegevens worden verwerkt, beschermt de wet op de persoonlijke levenssfeer je en kent ze je rechten toe :

1. Het recht op informatie

Over het algemeen verschaft de wet je "een recht om te weten", d.w.z. het recht om te worden ingelicht over het lot van de gegevens over jou. Zo mogen er geen bestanden zonder je medeweten worden aangelegd.

Elke verwerkingsverantwoordelijke dient bepaalde inlichtingen over de betrokken personen te verstrekken. Hij moet je inzonderheid zijn naam en adres, het doel waarvoor hij inlichtingen over jou inwint en de bestemmelingen van die gegevens meedelen. Hij moet je ook inlichten over je rechten (toegang, verbetering, verzet, enz.).

De verwerkingverantwoordelijke moet die informatieplicht nakomen, hetzij bij het inwinnen van de gegevens, ingeval hij de gegevens van jou persoonlijk heeft gekregen, hetzij ten laatste bij de eerste mededeling van die gegevens, ingeval hij ze onrechtstreeks heeft verkregen.

Bovendien moeten de gevraagde gegevens stroken met het doel van de inzameling. Vaak is het bijvoorbeeld niet nodig dat men je privé-telefoonnummer kent om de aangekondigde doelstellingen te verwezenlijken.

2. Het recht op nieuwsgierigheid

Je hebt het recht elke persoon verantwoordelijk voor gegevensverwerking aan te spreken om te weten of hij gegevens over jou bezit. De ondervraagde verantwoordelijke moet bevestigen of hij al dan niet zulke gegevens bezit. Zo ja, moet hij preciseren met welk doel hij die bewaart, over welke gegevenscategorieën het gaat en wie de bestemmelingen zijn.

3. Het recht op toegang

Je hebt het recht een duidelijke kopie van de verwerkte gegevens evenals van elke beschikbare informatie over de oorsprong van die gegevens te vragen.

Om je recht op toegang uit te oefenen, moet je een verzoek sturen naar de verwerkingsverantwoordelijke en daarbij een bewijs van je identiteit verstrekken. De verantwoordelijke moet, op straf van boete, ten laatste 45 dagen na ontvangst van het verzoek antwoorden.

4. Het recht op verbetering

De over jou ingewonnen gegevens moeten juist zijn. Desnoods moet de verwerkingsverantwoordelijke je redelijke middelen bieden om die gegevens te verbeteren, te wissen of te blokkeren.

5. Het recht op verzet

Behalve wanneer de verwerking nodig is om een overeenkomst te sluiten of uit te voeren of om een wettelijke verplichting na te leven, heb je het recht je tegen de verwerking van je gegevens te verzetten, maar daartoe moet je ernstige en gegronde redenen invoeren die verband houden met je bijzondere toestand.

Bovendien is het gebruik van persoonsgegevens voor marketingoperaties streng gereguleerd. De wet biedt je steeds de mogelijkheid je, zonder verantwoording en kosteloos, te verzetten tegen de geplande verwerking van persoonsgegevens voor directe marketing worden ingewonnen (zie hieronder nr. 83 e.v.).

6. Het recht op vergetelheid

De gegevens waarmee iemand kan worden geïdentificeerd mogen niet langer worden bewaard dan de tijd die nodig is om het aangekondigde doel te bereiken.

75. Welke mogelijkheden tot beroep heb ik als mijn rechten niet worden geëerbiedigd ?

Je kunt je gratis richten tot de *Commissie voor de Bescherming van de Persoonlijke Levenssfeer*, die de zaak zal onderzoeken. Inlichtingen over die instelling vind je op het volgende adres : <http://www.privacy.be>.

Je kunt in ieder geval je geschil voorleggen aan de hoven en rechtbanken.

76. Zijn mijn persoonsgegevens beschermd buiten de Europese Unie ?

Door het internationaal karakter van het web circuleren persoonsgegevens van particulieren vaak tussen verschillende landen, soms zelfs zonder dat de gebruiker weet waar ze terecht komen.

In principe mogen je persoonsgegevens slechts worden overgedragen naar landen waar je een gelijkaardige bescherming geniet als op het grondgebied van de Europese Unie.

Elke verwerkingsverantwoordelijke die *persoonsgegevens buiten de Europese Unie* wil uitvoeren, moet zich bijgevolg afvragen of het land van bestemming een degelijke bescherming biedt. Dezelfde waarborgen moeten worden geboden als op het Europese grondgebied. In het tegenovergestelde geval mag de overdracht slechts gebeuren middels strenge naleving van bepaalde voorwaarden. Dit is het geval indien de verwerkingsverantwoordelijke je onbetwiste instemming krijgt voor de overdracht of indien er waarborgen worden geboden door de opnemings van passende contractuele clausules tussen de uitvoerder en de invoerder van de gegevens.

Wanneer *gegevens vanuit een derde land in België worden verzameld*, zijn de bepalingen van de Belgische wet in welbepaalde gevallen van toepassing. Dit is met name het geval wanneer de verwerkingsverantwoordelijke de persoonsgegevens, met al dan niet geautomatiseerde middelen, op Belgisch grondgebied laat verwerken. In die veronderstelling kan de gebruiker die in België verblijft de door de Belgische wet geboden bescherming t.o.v. de verwerkingsverantwoordelijke genieten.

Afdeling 3. Cybercontrole op het werk

De informatica is langzaamaan in de bedrijfswereld binnengedrongen, wat niet zonder gevolgen is gebleven voor de betrekkingen tussen werknemers en werkgevers.

Wie nieuwe technologieën zegt, zegt ook nieuwe problemen inzake veiligheid in de ondernemingen, vermits informatie over het reilen en zeilen van een bedrijf tegenwoordig snel het enge werkkader overschrijdt. Bovendien moet de werkgever waken voor de goede uitvoering van de arbeidsovereenkomst.

Voor de werknemers ligt de moeilijkheid in het feit dat hun werkgever alle sporen kan vinden en bewaren die zij op het web achterlaten en dat hun persoonlijke levenssfeer zo in het gedrang kan komen.

Het is bijzonder moeilijk om een evenwicht te vinden tussen enerzijds de vereisten inzake rendabiliteit en veiligheid van de onderneming en anderzijds de mogelijkheid om op het werk tot individuele ontplooiing te komen.

77. Wat zijn de grote principes ?

Vandaag de dag wordt aanvaard dat de werknemer op zijn arbeidsplaats over een persoonlijke levenssfeer beschikt en als dusdanig een zekere bescherming geniet tegen inopportune controle, door de werkgever, van het gebruik dat hij maakt van de in het kader van zijn arbeidsovereenkomst de zijner beschikking gestelde communicatiemiddelen.

Dat neemt niet weg dat de huidige regelgeving waarbij de werkgever zowat elke controle wordt ontzegd op het gebruik van telefoon en computer niet adequaat is en niet met de werkelijkheid overeenstemt. De rechtspraak – die trouwens niet altijd eensgezind is over die kwesties – en de meeste rechtskundigen zijn er het thans over eens dat een zekere inmenging van de werknemer in het privé-leven van de werknemers wettelijk verantwoord is om het arbeidscontract correct te kunnen uitvoeren of om bepaalde belangen te beschermen die hoger worden geacht dan de eerbiediging van de persoonlijke levenssfeer van de werknemer.

Een collectieve arbeidsovereenkomst (cao nr. 81) bekrachtigde trouwens de mogelijkheid van een geleidelijke en voorwaardelijke cybercontrole op de werknemers. Die collectieve arbeidsovereenkomst geldt echter alleen voor de privé-sector.

Bij de controle van elektronisch meegedeelde gegevens moet de werkgever de principes van finaliteit, proportionaliteit en transparantie in acht nemen.

De werkgever heeft het recht controle uit te oefenen op voorwaarde dat dit gebeurt met het oog op één of meer wettelijk verantwoorde *doelstellingen*. Er zijn vier doelstellingen : 1° het voorkomen van onrechtmatige of lasterlijke feiten, 2° de bescherming van de commerciële belangen van de onderneming, 3° de veiligheid en goede werking van de informaticasystemen en ten slotte 4° de eerlijke naleving van de principes en regels voor het gebruik van de netwerktechnologieën die in het bedrijf geïnstalleerd zijn.

Krachtens het *evenredigheids*principe moet die controle in elk geval adequaat en relevant zijn en stroken met de beoogde doelstellingen. De onderneming mag niet meer doen dan wat nodig is om die doelstellingen te bereiken.

Het *transparantie*principe is essentieel omdat het de werkgever oplegt vooraf informatie te verschaffen over het gevoerde controlebeleid en de gehanteerde controleregeling. Op die

manier wil men komen tot meer preventie en duidelijkheid. De informatie moet zowel collectief als individueel zijn : collectief, via de representatieve organen die binnen de onderneming zijn opgericht, individueel, door het opnemen van die informatie in het arbeidsreglement, het arbeidscontract, enz.

Met inachtneming van de hierboven vermelde principes mag een procedure van individualisering van de gegevens slechts worden verwezenlijkt als er vooraf een onregelmatigheid werd vastgesteld. Die procedure bestaat erin dat de werkgever de algemene gegevens waarover hij beschikt, analyseert om de identiteit na te gaan van de auteur van de onregelmatigheid. In de praktijk komen eventuele onregelmatigheden aan het licht bij het naslaan van de in de onderneming elektronisch meegedeelde gegevens (bijvoorbeeld bij internetgebruik : duur van de verbinding, bedrijfsgewijs of per dienst uitgesplitst ; meest bezochte sites ; ...). De werkgever behoort dan de beschikbare informatie te analyseren, zoals hij zou doen met de gegevens van een telefoonrekening. Eventueel worden gerichte controles gehouden als er vermoedens zijn van misbruik van werkinstrumenten.

Die individualisering van de gegevens kan rechtstreeks gebeuren, zonder enige formaliteit, telkens als de controle wordt uitgevoerd op grond van de eerste drie van bovengenoemde doelstellingen.

In de andere gevallen gebeurt de individualisering van de gegevens onrechtstreeks. Vooraf komt de fase van de “alarmbel”, waarbij de werknemers op de hoogte worden gebracht van een onregelmatigheid en worden verwittigd dat er bij herhaling een individualisering van de gegevens kan gebeuren.

Uiteindelijk laat de cao de werkgever vrij bepalen onder welke voorwaarden zijn werknemers toegang krijgen tot de informaticatools van het bedrijf. Met andere woorden, de werkgever kan bijvoorbeeld bepaalde voorwaarden opleggen voor het gebruik van het internet, o.a. : verbod om zich op spellensites te begeven, verbod om deel te nemen aan onlinegesprekken, filtrering van sommige sites met specifieke of illegale inhoud.

78. Kan ik in de arbeidsovereenkomst afstand doen van mijn recht op privé-leven ?

Sommige werkgevers proberen hun personeel schriftelijke verbintenissen te doen ondertekenen waarbij ze volledig afstand doen van hun rechten.

Je moet weten dat het afstaan van je recht op privé-leven niet op algemene en abstracte wijze in de arbeidsovereenkomst mag worden opgenomen. Enkel een deel van dat recht zou kunnen worden afgestaan, bijvoorbeeld het recht om je te verzetten tegen inmenging in je privé-leven. Het afstaan van een fundamenteel recht is onderworpen aan een aantal voorwaarden, gelet op de onvervreembare en openbare aard van een dergelijk recht.

Het instemmen met zo'n inmenging moet op individuele, informatieve, vrije, voorafgaande, bijzondere en herroepbare wijze geschieden. Bovendien mag het afstaan van een recht niet raken aan de kern van het betreffende recht. Wij kunnen dus stellen dat zo de werknemer een deel van zijn recht op privé-leven afstaat in het arbeidscontract, die afstand meestal moet worden bevestigd bij elke nieuwe inmenging.

79. Mag mijn werkgever de inhoud van mijn e-mails controleren ?

Het gebruik van de e-mail van het werk om, binnen redelijke perken, persoonlijke berichten te versturen of te ontvangen is een algemeen en sociaal aanvaarde praktijk, die echter door de werkgever kan worden "gereguleerd".

In principe is een werkgever niet gemachtigd om kennis te nemen van de e-post die de werknemer verzendt en ontvangt door middel van een informaticamiddel dat hem ter beschikking wordt gesteld voor zijn werk. Elektronische post wordt namelijk beschermd door het briefgeheim.

Bijgevolg moet de inmenging van de werkgever in de persoonlijke levenssfeer van de werknemer tot een minimum beperkt blijven ; de werkgever mag enkel het gebruik van e-mail en niet de inhoud ervan controleren. Inbreuken op de door de werkgever ingestelde regels kunnen dus worden opgespoord aan de hand van e-maillijsten, zoals abnormaal hoge telefoonkosten kunnen worden gecontroleerd aan de hand van factuurgegevens. De werkgever mag de identiteit van de geadresseerde en de auteur van een verzonden bestand verifiëren, de grootte en de aard van dat bestand controleren en het volume van de uitgaande mail per werkpost nagaan. Als hij echter kennis neemt van de inhoud van je e-mails of als hij jouw telefoongesprekken afluistert of opneemt, dan oordeelt men dat hij zijn boekje te buiten gaat.

In sommige omstandigheden heeft je werkgever echter wel toegang tot de inhoud van je e-mails. Dat is onder meer zo wanneer je hem daartoe de toestemming hebt gegeven. Normaal moet de werkgever de toestemming hebben van alle deelnemers aan de communicatie, dus ook van de geadresseerde, hoewel er over dit principe nog een controverse bestaat.

80. Mag mijn werkgever mijn internetgebruik controleren ?

Als je een internetsite bezoekt, leg je een verbinding tussen de computer waarmee je de site bezoekt en een andere computer waarop de geraadpleegde informatie is opgeslagen. Tijdens die verbinding worden een aantal identificatiegegevens ingelezen, zoals bij een telefoongesprek : adres van de site, tijdstip en duur van het bezoek. Die gegevens worden ook automatisch geregistreerd op de server van het bedrijf of van de internetprovider. Een werkgever kan dus moeiteloos het internetgebruik van zijn personeel nagaan.

Bij een dergelijke controle mag de werkgever zich evenwel slechts in een beperkt aantal gevallen bemoeien met het privé-leven van zijn werknemers (zie hierboven nr. 77).

En ook als die controle toegestaan is, moet hij minimaal blijven. Hij moet in de eerste plaats betrekking hebben op een adressenlijst van sites die gedurende een bepaalde periode werden bezocht. De werkgever mag slechts maatregelen nemen indien hij sommige onregelmatigheden vaststelt (te lange bezoeksduur, raadpleging van onbetamelijke sites, enz.).

Bijgevolg mag de werkgever het internetgebruik van zijn personeelsleden controleren voor zover hij hen vooraf verwittigt en de vastgestelde doelstellingen naleeft.

Je moet ook weten dat inlichtingen over de bewegingen tussen de computer die je op het werk gebruikt en een internetsite persoonlijke gegevens zijn volgens de wet op de persoonlijke levenssfeer. Die wet moet dus worden nageleefd, wat onder meer inhoudt dat de werkgever zijn personeel ervan op de hoogte moet brengen dat hij de verbindingsgegevens bewaart.

HOOFDSTUK II. SPAMMING

81. Wat is spamming ?

In ruime zin betekent *spamming* de massale en herhaalde verzending van ongevraagde - meestal commerciële - berichten.

In enge zin betekent *spamming* het versturen van ongevraagde reclame per e-mail met het oog op een "wilde inzameling" (lees : met miskenning van de principes van de wetgeving over de bescherming van persoonsgegevens) van de adressen van de bestemmingen.

Nu is elektronische post wel een ideale reclamedrager : praktisch, goedkoop en doeltreffend ! E-post zit dan ook in de lift als middel om aan direct marketing te doen.

82. Hoe komen adverteerders aan mijn elektronisch adres ?

Reclamejongens kunnen jouw e-mailadres op verschillende manieren achterhalen :

- In de eerste plaats kun je zelf je adres hebben meegedeeld. Als je een website bezoekt om een product of dienst aan te kopen, als je je inschrijft op een mailinglijst of deelneemt aan een discussieforum, dan vraagt men je vaak een aantal persoonsgegevens in te voeren, zoals je naam, je geografisch adres... en je e-mailadres. Die gegevens worden dikwijls hergebruikt, hetzij door de persoon aan wie je ze verstrekte, hetzij door andere personen aan wie de eerste persoon ze doorgaf. Bovendien bepalen sommige providers van gratis e-mail dat je in ruil daarvoor aanvaardt reclame te ontvangen. Zo ook wordt een gratis internetaansluiting soms gekoppeld aan de bereidheid van de gebruiker om e-mailreclame te ontvangen.
- Daarnaast bestaan er allerhande methodes om clandestien je e-mailadres te pakken te krijgen, met of zonder jouw toestemming : gebruik van software waardoor op een maximum aantal mailinglijsten wordt ingeschreven teneinde de elektronische adressen van de leden te bekomen ; automatische inzameling van elektronische adressen op openbare ruimten van het internet (bijvoorbeeld jaarboeken of zoekmachines, jouw persoonlijke webpagina's...) ; beroep op diverse frauduleuze praktijken (bijvoorbeeld nepwedstrijden, aanbidding van gratis webruimten...).
- Ten slotte bestaat er een ware markt van elektronische adressenbestanden : sommige ondernemingen stellen beroepsmatig dergelijke bestanden ter beschikking (meestal worden ze verhuurd). Op het internet kun je tegen een zacht prijsje ook lijsten met duizenden adressen downloaden.

83. Kan spamming mij schade toebrengen ?

Spamming kan twee onaangename gevolgen hebben :

1. als er massaal boodschappen binnenkomen, kan dat jouw elektronische brievenbus (*inbox*) overbelasten en zo de toegang tot het netwerk bemoeilijken, en dan spreken we nog niet van de tijd die je verliest door al die reclameboodschappen te bekijken en te wissen ;
2. tenzij je een permanente internetverbinding hebt, zal je ook de verbindingskosten voor het downloaden moeten betalen en die kunnen hoog oplopen als het om een lang bericht gaat (dat bijvoorbeeld een groot attachment bevat).

Bovendien ontvang je misschien niet graag reclameberichten die agressief overkomen of haaks staan op je ethische opvattingen.

84. Hebben adverteerders het recht mij via e-mail ongewenste reclame toe te sturen ?

Neen ! Volgens de Belgische wet – en volgens de regelgeving die weldra toepasselijk zal zijn in alle lidstaten van de Europese Unie – *mag jou geen enkele reclame per e-mail worden toegezonden zonder je voorafgaande, vrije, specifieke en geïnformeerde toestemming.*

Overigens moeten bedrijven die aan direct marketing per e-mail doen, de wetgeving over de bescherming van persoonsgegevens volledig naleven (zie hieronder nr. 72 e.v.).

Ter herinnering, de wet kent je verscheidene rechten toe :

- *recht op informatie* : als je aan een onderneming persoonsgegevens meedeelt via een verzoek, bestelbon, inschrijvingsstrook, brief..., dan is zij ertoe gehouden je te melden waarvoor die informatie zal dienen (doel van de verwerking) en je de naam en het adres mee te delen van de persoon die verantwoordelijk is voor de verwerking ;
- *recht op toegang* : je kunt een onderneming steeds vragen welke gegevens zij over jou in haar bezit heeft ; zij moet je hierop binnen een redelijke termijn een antwoord geven ;
- *recht op verbetering* : je hebt het recht onjuiste gegevens over jou gratis te laten verbeteren.

85. Heb ik het recht om reclame via e-mail te weigeren ?

Ja ! De wet biedt je de mogelijkheid je toestemming om e-mailreclame te ontvangen op elk ogenblik in te trekken, zonder dat je daarvoor kosten hoeft te dragen of een reden moet opgeven.

Als een onderneming je reclame per e-mail toestuurt, moet zij :

- duidelijke en begrijpelijke informatie bezorgen over het recht om je te verzetten tegen het toesturen van reclame ;
- je een geschikt middel aanreiken om via de computer efficiënt gebruik te maken van dat recht.

86. Wat moet ik in de praktijk doen om gebruik te maken van mijn recht op verzet ?

Je hebt twee mogelijkheden :

- Als je geen e-mailreclame meer wenst te ontvangen van een welbepaalde onderneming, kun je haar vragen je e-mailadres te schrappen in haar bestanden.
- Als je geen enkele e-mailreclame meer wenst te ontvangen van om het even welke onderneming, kun je je inschrijven op de Robinson-e-maillijst van het Belgisch Direct Marketing Verbond (surf naar <http://www.bdma.be>, of rechtstreeks naar

pagina http://www.robinsonlist.be/mk/get/ROB_EMAIL). De doorgegeven data (voornaam, naam en e-mailadres) worden geregistreerd in het Robinsonbestand. In principe ontvang je dan geen e-mailreclame meer, althans niet van de talrijke ondernemingen die aangesloten zijn bij het BDMV.

Opgelet: de ondernemingen waarbij je klant bent en aan wie je de uitdrukkelijke toestemming hebt gegeven je e-mailreclame toe te sturen, mogen je reclameboodschappen blijven toezenden, ook al ben je ingeschreven op de Robinsonlijst. Wens je geen e-mailreclame meer te krijgen van die ondernemingen, wend je dan tot elk van hen met het verzoek je er in de toekomst geen meer op te sturen.

87. Geldt dit alles ook voor sms-berichten ?

Ja ! De bovenvermelde principes (zie hierboven nrs. 82 en 83) zijn ook toepasselijk op sms-berichten (*short message service*). In feite gebruikt de wet nooit de term “*e-mail*”, maar “elektronische post”, die een zeer ruime betekenis heeft en ontegensprekelijk ook sms-berichten omvat.

Weet dat het BDMV ook een Robinson-sms-lijst beheert, waarop je je kunt inschrijven om geen sms-reclame meer te ontvangen (surf naar <http://www.bdma.be> of rechtstreeks naar pagina http://www.robinsonlist.be/mk/get/ROB_EMAIL).

Die lijst is in alle opzichten vergelijkbaar met de e-maillijst (zie hierboven nr. 84).

88. Bestaan er technische middelen om je tegen spamming te beschermen ?

Ja hoor, er bestaan diverse filtreervoorzieningen om *spamming* te bekampen. De filters zijn zodanig ingesteld dat ongewenste berichten worden gesorteerd op basis van een aantal zoekcriteria, zoals de oorsprong (bv. IP-adres) en de inhoud van het bericht.

Voortaan verplicht de wet de verzender van een reclameboodschap ervoor te waken dat enerzijds het commercieel doel van de boodschap identificeerbaar is zodra de geadresseerde ze ontvangen heeft en dat anderzijds de natuurlijke of rechtspersoon voor wiens rekening reclame wordt gemaakt duidelijk identificeerbaar is.

Verder is het bij de verzending van e-mailreclame verboden enerzijds het elektronisch adres of de identiteit van een derde te gebruiken en anderzijds elke informatie waardoor de oorsprong en verzendingswijze van de e-mail kan worden nagegaan te vervalsen of te verbergen.

Door de invoering van die wettelijke vereisten zal de programmering van filters volgens het gekozen criterium worden vergemakkelijkt.

Filters geprogrammeerd volgens de oorsprong van de berichten blokkeren reclame afkomstig van geïdentificeerde IP-adressen. Filters die geprogrammeerd zijn volgens de inhoud van e-mails elimineren reclame die een specifiek woord of een specifieke combinatie van woorden bevat (bv. *sex* of *make money fast*). In dat geval loop je wel het risico dat gewenste berichten verloren gaan.

Welke keuze je ook gemaakt hebt, de filter kan op de server van je internetprovider of op je eigen computer worden geïnstalleerd.

Filtering bij je internetprovider is de handigste oplossing omdat de provider zelf de ongewenste reclame sorteert en elimineert. Bij zo'n systeem heb jij echter geen greep op

de sortering. Sommige selectiecriteria (bv. gelijkaardige berichten en groot aantal verzonden berichten) kunnen ook gewenste boodschappen tegenhouden. Bovendien controleert een volgens de inhoud ingesteld filtersysteem automatisch alle e-mails die jou worden toegezonden, wat problemen kan geven met de bescherming van de persoonlijke levenssfeer.

En omgekeerd, als er een filter op je computer staat, dan komt alle reclame onvermijdelijk in je inbox terecht. Op die manier kun je dus niet vermijden dat je met berichten wordt overstelpt en dat je aansluitingskosten daardoor hoog oplopen. Als je over filtersoftware beschikt, dan is die waarschijnlijk al geconfigureerd (de meeste e-mailprogramma's bieden filtermogelijkheden aan). In principe heb je wel de mogelijkheid om de filter te personaliseren door er selectiecriteria aan toe te voegen of uit te halen. Zo is het risico om gewenste reclame te verliezen dus minder groot, vermits je zelf de selectiewijze hebt ingesteld. Bovendien wordt je e-post niet door derden geopend.

HOOFDSTUK III. ILLEGALE EN NADELIGE SITES

89. Mag ik een illegale site op het web straffeloos raadplegen ?

Gewoon informatie raadplegen of bezitten is zelden een ongeoorloofde daad. De reden daarvoor is eenvoudig : wanneer er een probleem is met bepaalde informatie, verwijt men dit in het algemeen aan de auteur ervan en niet aan de persoon die de informatie raadpleegt.

Sommige gegevens liggen echter gevoelig of zijn ongeoorloofd. De wetgever oordeelde dan ook dat het goed was een deel van de aansprakelijkheid te doen dragen door de persoon die de informatie leest of bezit. Voorbeelden : staatsgeheimen en pedofilie. Enkel dit laatste punt wordt hier onder de loep genomen.

Na de smartelijke rechtszaken die in België veel beroering veroorzaakten, reikte de wet van 13 april 1995 nieuwe middelen aan om pedofilie te bestrijden :

- Enerzijds zijn personen die met kennis van zaken in het bezit zijn van foto's en andere visuele informatiedragers waarop seksuele posities of handelingen van pornografische aard worden voorgesteld en waarbij minderjarigen van minder dan 16 jaar betrokken zijn of getoond worden, volgens de wet strafbaar.
- Anderzijds kan, op grond van een nieuwe procedureregeling, een in België betrapte Belg of buitenlander, die op of buiten het grondgebied de hierboven vermelde overtreding pleegt, voor de Belgische strafrechtbanken worden gedaagd, zelfs al is er geen aangifte vanwege een buitenlandse overheid.

Toegepast op het internet opent de wet nieuwe perspectieven : iedere persoon die op het Belgische grondgebied woont en met kennis van zaken van het internet gedownload of in een forumdiscussie gekregen ongeoorloofde foto's *bezit*, kan er vervolgd worden, zelfs indien de foto's op een server in het buitenland bewaard worden, bijvoorbeeld op één van de op het internet aangeboden virtuele servers.

Op dezelfde wijze kan een buitenlander die deze foto's verspreidt, zelfs vanaf zich in het buitenland bevindende computers, in België worden vervolgd, voor zover hij in België wordt betrapt, bijvoorbeeld tijdens zijn vakantie in ons land.

In tal van landen bestaat een gelijksoortige wetgeving (Frankrijk, VS, Canada, enz.).

90. Wat moet ik doen als ik kinderpornografisch materiaal aantref op het internet ?

Uiteraard moet je vermijden informatie van pedofiele aard te raadplegen (een ministeriële richtlijn, die op 1 september 1999 in werking trad, omschrijft kinderpornografie als "voorwerpen of beelddragers van welke aard ook die houdingen of seksuele handelingen met pornografisch karakter vertonen waarbij minderjarigen worden voorgesteld of betrokken zijn").

Indien je enkele bestanden ongewild downloadde, hoef je niet in paniek te raken : meestal volstaat het ze te doen verdwijnen en de site waarop zij gevonden werden niet meer te raadplegen.

Je kunt ook verder gaan en die site aangeven. Daartoe heb je verscheidene mogelijkheden :

1. Je kunt een bericht sturen, telefoneren of je begeven naar om het even welk politiecommissariaat.
2. Je kunt ook elektronisch tewerkgaan, overeenkomstig de procedure die werd uitgewerkt in het kader van het akkoord tussen de vereniging van internetproviders (ISPA), de Federale Overheidsdienst Justitie en de Federale Overheidsdienst Informatie- en Communicatietechnologie :
 - Iedereen mag gegevens die hij illegaal vindt, aangeven bij zijn internetprovider of bij het contactpunt van de gerechtelijke politie (e-mail : contact@gpj.be). Indien de aangifte bij de provider werd gedaan, stuurt deze ze door naar het contactpunt.
 - Het contactpunt voert een sortering uit. Indien *duidelijk* blijkt dat de informatie *niet* illegaal is, wordt het dossier geseponneerd. In de andere gevallen wordt het dossier doorgezonden naar het Parket. Terzelfder tijd wordt de ISPA gewaarschuwd en de leden ervan verbinden zich ertoe de toegang tot de site te blokkeren met alle middelen waarover ze redelijkerwijs beschikken.
 - Bijkomende informatie kan verkregen worden op de site van de ISPA (<http://www.ispa.be>) of op de site van de gerechtelijke politie (<http://www.gpj.be>).
3. Ten slotte kun je je richten tot *Child Focus*, hetzij telefonisch (op nummer 110), hetzij via de website van de vereniging (www.childfocus-net-alert.be) :
 - www.childfocus-net-alert.be bewaart je anonimiteit als je dat wenst. De server is zodanig geconfigureerd dat men aan de hand van loggegevens onmogelijk de identiteit kan nagaan van personen die informatie verschaffen of die de site bezoeken, omdat zo'n gegevens niet worden bewaard.
 - Bovendien is de webserver op zo'n manier geconfigureerd dat er op de computer van een bezoeker geen cookie wordt geplaatst na zijn bezoek aan de site (zie hierboven nr. 64).
 - Ten slotte is je bezoek beveiligd : de webserver ontvangt de informatie zoals jij die hebt ingevoerd ; als je geen persoonlijke gegevens hebt meegedeeld, registreert hij geen inlichtingen over jou.

91. Hoe kunnen minderjarigen worden beschermd tegen ongewenste informatie ?

Het wereldwijde web bevat informatie die je ongeschikt acht voor minderjarigen die toegang hebben tot het internet in een bibliotheek, op school of thuis. Zo zijn er sites met gewelddadige, pornografische, haatdragende of racistische inslag, sites van bepaalde sekten of sites die aan drugshandel doen. Als opvoeder, als verantwoordelijke voor jongeren of als ouder wens je die minderjarigen te beschermen tegen zulke ongewenste of schadelijke pagina's. Dat kan via de op de markt beschikbare evaluatie- en filtersystemen.

Een filtersysteem bestaat uit een of meer softwareprogramma's die internetgebruikers de toegang tot sommige bestanden ontzeggen. Zo'n systeem werkt volgens twee principes : evaluatie en filtratie.

De evaluatiesoftware rangschikt de websites naar de inhoud op grond van waardeoordelen.

De filtersoftware onderzoekt de bron waartoe de gebruiker toegang wil hebben. Indien die bron niet beantwoordt aan de toegestane toegangscriteria, dan meldt de software de gebruiker dat de toegang hem wordt geweigerd en toont de browser de inhoud van deze site niet.

92. Welke filtersystemen zijn thans beschikbaar ?

Autonome filterprogramma's combineren twee principes om de inhoud van bestanden te evalueren : de opstelling van lijsten van aanvaardbare of onaanvaardbare sites en een selectie volgens trefwoorden.

In de lijsten wordt uitdrukkelijk vermeld welke sites geoorloofd zijn (witte lijsten) en verboden zijn (zwarte lijsten). Die lijsten worden meestal door de softwareverkopers op grond van eigen criteria opgesteld.

Voorts ontwikkelde het W3-consortium een open standaard, PICS genaamd (*Platform for Internet Content Selection*). Het gaat om een protocol voor de uitwisseling van evaluatiegegevens. Het is de bedoeling de internetters een middel te verschaffen om de inhoud te selecteren volgens hun eigen ethische criteria.

In de praktijk kun je een evaluatiesysteem kiezen dat met jouw waarden overeenstemt. De meest verspreide systemen zijn momenteel RSACi, SafeSurf en Netshepherd.

93. Zijn filtersystemen efficiënt ?

De waarde en de doeltreffendheid van op lijsten gebaseerde systemen hangen af van de keuze van de verkopers. In dat opzicht is er weinig of geen speelruimte. Bovendien zijn zulke lijsten snel verouderd omdat er steeds maar nieuwe sites verschijnen. De selectie op grond van trefwoorden heeft ook beperkingen, want ze houdt geen rekening met de context en blokkeert vaak sites zonder geldige reden.

Het PICS-systeem laat de ouders meer keuze, doch er bestaan tot nog toe weinig evaluatiesystemen. Bovendien - en vooral - moeten er door het succes van dit initiatief heel wat websites worden geëvalueerd. Het aantal geëvalueerde websites is momenteel nog klein.

94. Wat moet ik doen als ik op het web een illegale of nadelige site aantref ?

Hoe moet je reageren als je je bedreigd of benadeeld voelt door een illegale site (met gewelddadige, revisionistische, pedofiele, racistische, ... informatie) of door een voor jou lasterlijke site of door een site die een aanslag vormt op je eer, je reputatie, je privé-leven, ... ?

Vooreerst moet je je wenden tot je internetprovider of tot de *host* van de betreffende site (of van de discussiegroep) om zijn aandacht te vestigen op de schadelijke informatie en hem, afhankelijk van het geval, vragen de toegang tot die informatie te blokkeren of de informatie te laten verdwijnen. Bewaar liefst een spoor van je verzoek.

Komt er geen reactie, dan kun je een klacht indienen bij het dichtstbijzijnde politierechtspraak. Je klacht wordt dan voorgelegd aan de bevoegde gerechtelijke overheid, die een onderzoek kan openen en desnoods een rechtsvordering kan instellen bij een strafrechtelijke instantie.

Als je meent persoonlijk materiële schade te hebben geleden (bv. verlies van klanten ten gevolge van de verspreiding van lasterlijke of beledigende informatie over jou) of morele schade (bv. aanslag op je eer of op de intimiteit van je privé-leven), dan kun je steeds schadevergoeding eisen. Wij raden je dan ook aan je klacht in te dienen met burgerlijke partijstelling.

Buiten elke rechtsvordering kun je tevens vergoeding eisen voor geleden schade door een vordering inzake burgerlijke aansprakelijkheid in te stellen bij een burgerlijke rechtbank.

Als je wenst dat er zo spoedig mogelijk een einde wordt gemaakt aan de verspreiding van informatie die je beschouwt als een aanslag op je rechten, dan kun je gebruik maken van het snelrecht, waarbij je binnen een termijn van 24 uur tot enkele dagen een bevredigende oplossing kunt bekomen. Als je in 't gelijk gesteld wordt, kan de rechter bijvoorbeeld de toegang tot de kwetieuze site laten blokkeren of hem onmiddellijk doen verwijderen.

95. Wie kan ik voor het gerecht dagen om schadeloosstelling te krijgen ?

Volgens de wet is er voor sommige intermediaire activiteiten op het internet geen aansprakelijkheid. Zo zijn personen die louter informatie verzenden en die toegang tot het internet verschaffen vrijwel volledig vrijgesteld van aansprakelijkheid voor de inhoud van de gegevens. Een netwerkoperator of internetprovider die je aansprakelijk acht voor geleden schade daag je dus liever niet voor de rechter.

Je hebt meer kans om je gelijk te halen als je de hoster van een kwetieuze site vervolgt (op voorwaarde dat je hem kent). Volgens de wet is de aansprakelijkheid in geval van *hosting* echter beperkt. Zo kan een *hoster* niet aansprakelijk worden gesteld voor illegale informatie als hij er geen weet van had of als hij ze snel verwijderde of ontoegankelijk maakte zodra hij ervan op de hoogte was.

Je hebt er hoe dan ook alle belang bij de aansprakelijkheid van de auteur van de betwiste informatie aan de kaak te stellen, voor zover je hem natuurlijk kunt identificeren.

HOOFDSTUK IV. CYBERCRIMINALITEIT

Afdeling 1. Informaticavervalsing

96. Wat is informaticavervalsing ?

Volgens de wet wordt “valsheid in informatica” gepleegd door iemand die via een informaticasysteem opgeslagen, verwerkte of overgedragen gegevens wijzigt of wist, of op enige andere technologische wijze de mogelijke aanwending van gegevens in een informaticasysteem verandert, waardoor de juridische draagwijdte van dergelijke gegevens verandert.

Met andere woorden : valsheid in informatica is het via datamanipulatie vervalsen van juridisch relevante gegevens. Je kunt bijvoorbeeld elektronische gegevens vervalsen door ze (geheel of gedeeltelijk) te wijzigen of te wissen tijdens het invoeren, het terughalen of het opslaan in de computer.

Als je zonder toestemming binnendringt in een informaticasysteem om gegevens te vervalsen, dan maak je je misschien ook schuldig aan *hacking* (zie hieronder nr. 104 e.v.) en zelfs aan informaticabedrog indien de operatie je een vermogensvoordeel oplevert (zie hieronder nr. 100 e.v.). Bij zo'n “ideale samenloop van overtredingen” wordt enkel de grootste strafmaat toegepast.

97. Voorbeelden van informaticavervalsing

Valsheid in informatica is onder meer : namaak of vervalsing van kredietkaarten ; valsheid inzake digitale contracten (wanneer juridisch relevante gegevens niet meer op papier worden gedrukt, noch met de hand worden ondertekend) ; invoering van een vals kredietkaartnummer bij het tegen betaling intekenen op een internetsite ; inschrijving van fictieve schuldvorderingen of wijziging van loongegevens door een bediende in de boekhoudsoftware van een bedrijf ; kunstmatige opdrijving, door een bediende, van het aantal overuren in de software voor het beheer van de arbeidstijd ; vervalsing van een elektronische handtekening of bewust gebruik van vervalste gegevens.

98. Is informaticavervalsing strafbaar ?

Wie valsheid in informatica pleegt, krijgt een gevangenisstraf van zes maanden tot vijf jaar en een geldboete of een van beide straffen. Ook poging tot informaticavervalsing wordt bestraft. Bij herhaling wordt de strafmaat verdubbeld.

99. Kan ik informaticavervalsing plegen zonder dat ik mij daarvan bewust ben ?

Neen ! Om strafbaar te zijn, moet valsheid in informatica worden gepleegd met kennis van zaken en met bedrieglijk opzet of met het oogmerk te schaden.

Samengevat kan er enkel sprake zijn van inbreuk als alle bestanddelen aanwezig zijn, met name :

- Er moeten gegevens ingevoerd, gewijzigd of gewist zijn in een informaticasysteem of de mogelijke aanwending van die gegevens moet veanderd zijn.

- Door de manipulatie moet de juridische draagwijdte van de vervalste gegevens veranderen.
- Het misdrijf moet gepleegd zijn met bedrieglijk opzet of met het oogmerk te schaden.

Afdeling 2. Informaticabedrog

100. Wat is informaticabedrog ?

Volgens de wet wordt "informaticabedrog" gepleegd door iemand die, met het oogmerk voor zichzelf of voor een ander een bedrieglijk vermogensvoordeel te verwerven, via een informaticasysteem opgeslagen, verwerkt of overgedragen gegevens in een informaticasysteem invoert, wijzigt, wist of op enige andere technologische wijze de mogelijke aanwending van gegevens in een informaticasysteem verandert.

Met andere woorden : informaticabedrog is bedrieglijke gegevensmanipulatie om zich te verrijken.

101. Voorbeelden van informaticabedrog

Informaticabedrog is bijvoorbeeld het gebruik van een gestolen kredietkaart om geld te halen uit een bankautomaat, de onwettige overschrijding van het krediet verbonden aan je eigen kredietkaart, de invoering van commando's om na bepaalde verrichtingen andere onrechtmatige financiële voordelen te bekomen of de uitvoering van illegale manipulaties van klantenrekeningen door een bankbediende.

102. Is informaticabedrog strafbaar ?

Wie informaticabedrog pleegt, krijgt een gevangenisstraf van zes maanden tot vijf jaar en een geldboete of een van beide straffen. Ook poging tot bedrog wordt bestraft. Bij herhaling wordt de strafmaat verdubbeld.

103. Kan ik informaticabedrog plegen zonder dat ik mij daarvan bewust ben ?

Neen ! Om strafbaar te zijn, moet er bedrieglijk opzet zijn. Anders dan bij oplichting is er hier geen sprake van manipulatie om het vertrouwen van een persoon rechtstreeks te beschamen. Het is nodig en voldoende dat er aangetoond is dat het in de bedoeling lag zichzelf of iemand anders een illegaal vermogensvoordeel te verschaffen.

Afdeling 3. Hacking

104. Wat is hacking ?

Volgens de wet krijgt iemand die zich toegang verschaft tot een informaticasysteem of zich daarin handhaaft, terwijl hij weet dat hij daartoe niet gerechtigd is, een gevangenisstraf van drie maanden tot een jaar of een geldboete of een van beide straffen. Voorts krijgt iemand die, met bedrieglijk opzet of met het oogmerk te schaden, zijn bevoegdheid voor toegang tot een informaticasysteem overschrijdt, een gevangenisstraf van zes maanden tot twee jaar en een geldboete of een van beide strafmaten.

Iemand die poogt één van die misdrijven te plegen, krijgt dezelfde straffen als die welke gelden voor het misdrijf zelf. Bij herhaling wordt de strafmaat verdubbeld.

De wet onderscheidt dus twee mogelijkheden : enerzijds, ongeoorloofde toegang tot het informaticasysteem van een derde of er zich handhaven (externe *hacking*), anderzijds, overschrijding van bevoegdheid voor toegang tot dit systeem (interne *hacking*).

In het eerste geval volstaat het dat de overtreder zich volledig bewust is van de daad die hij stelt en de voltrekking ervan wil, of althans aanvaardt. Anders gezegd : externe *hacking* onderstelt geenszins dat de ongeoorloofde toegang tot het systeem of het er zich handhaven gepaard gaat met bedrieglijk opzet of met het oogmerk te schaden (zie hierboven nr. 103). Indien het misdrijf wordt gepleegd met een dergelijk opzet of doel, dan wordt de straf enkel verzwaaard (zie hieronder nr. 106). Er is sprake van het zich handhaven in het informaticasysteem zodra de indringer er zich gedurende een bepaalde tijd in verplaatst, ook al verschaft hij zich niet onrechtmatig toegang tot het systeem. De inbreuk is dus wel zeer ruim opgevat !

In het tweede geval moet de dader, die beschikt over de rechten voor toegang tot een systeem maar die bevoegdheid overschrijdt, handelen met een bedrieglijk opzet (d.w.z. om op onrechtmatige wijze enige winst of enig voordeel te bekomen) of om schade te berokkenen. Met andere woorden, interne *hacking* – door een bediende, arbeider, ambtenaar of zelfstandige consultant, vanuit een onderneming, instelling, bestuur of organisatie – is enkel strafbaar als de schuldige (bv. een al te nieuwsgierige bediende die vertrouwelijke dossiers inkijkt waarvan hij geacht wordt geen kennis te nemen) een speciale bedoeling heeft, zoals het zich onrechtmatig verrijken of kwaadwilligheid. Misbruik van bevoegdheid voor toegang tot een systeem kan diverse vormen aannemen : ofwel beschikt iemand over een beperkte toegangsbevoegdheid en verschaft hij zich toegang tot delen van het systeem waartoe hij geen toegang heeft, ofwel beschikt hij over een beperkte toegangsbevoegdheid en voert hij niet-toegestane manipulaties uit (bv. wijzigen of wissen van gegevens die hij alleen mag lezen).

105. Is ongeoorloofde toegang tot gegevens voor de lol, als uitdaging of om de veiligheid van een systeem te testen strafbaar ?

Je mag in geen geval zonder toestemming binnendringen in het informaticasysteem van een derde, noch uit nieuwsgierigheid, noch voor de grap of als uitdaging, noch om te kijken of het systeem bestand is tegen indringingen of aanvallen van buitenuit.

Ludieke binnendringing door jeugdige informaticafreaks of experimentele of ongeïnteresseerde binnendringing door “witte ruiters” is evenzeer strafbaar als ongeoorloofde binnendringing in een systeem in het kader van bedrijfsspionage voor winstgevende of militaire doeleinden.

Zo bepaalt de wet reeds straffen voor ongeoorloofde toegang tot een systeem of voor handhaving in een systeem, zonder dat zij enige andere voorwaarden stelt, zoals het “kraken” van een veiligheidssysteem, de bedoeling om zich gegevens toe te eigenen of de wil om sabotage te plegen (vernietiging van gegevens...).

Om aan vervolging te ontsnappen, kan een *hacker* echter aanvoeren dat hij te goeder trouw handelde en dat hij niet wist dat de toegang verboden was of dat hij dat verbod niet naast zich wou neerleggen. Het spreekt echter voor zich dat zijn goede trouw weinig geloofwaardig zal overkomen en als uitvlucht weinig aarde aan de dijk zal brengen indien hij een toegangscode kraakte of een ontradende waarschuwingsboodschap negeerde.

106. Zijn er omstandigheden die de strafmaat kunnen verzwaren ?

De wet bepaalt een aantal verzwarende omstandigheden en grotere straffen als iemand zich zonder toestemming - van binnenuit of van buitenuit - toegang verschaft tot een informaticasysteem en :

- op enige manier de door een informaticasysteem opgeslagen, verwerkte of overgedragen gegevens overneemt. Dat geldt bijvoorbeeld voor het ontvreemden van bedrijfsgeheimen in het kader van bedrijfsspionage ;
- enig gebruik maakt van een informaticasysteem dat een derde toebehoort of het informaticasysteem gebruikt om zich toegang te verschaffen tot het informaticasysteem van een derde. Hier gaat het bijvoorbeeld om het gebruik van de capaciteit van het systeem waarbij de mogelijkheden van andere gebruikers tijdelijk worden beperkt of om het gebruik van het systeem als springplank naar een ander systeem ;
- enige schade, zelfs onopzettelijk, veroorzaakt aan het informaticasysteem of aan de door middel van dat systeem opgeslagen, verwerkte of overgedragen gegevens of aan het informaticasysteem van een derde of aan de door middel van dat systeem opgeslagen, verwerkte of overgedragen gegevens.

Strafbaar is ook iemand die opdracht geeft of aanzet tot *hacking* en iemand die via *hacking* bekomen data heelt, onthult of er enig gebruik van maakt.

107. Kan ook ik het slachtoffer zijn van hacking ? Hoe kan ik mij daartegen beschermen ?

En of je door *hacking* kunt worden getroffen ! Sommige websurfers hebben er een handje van weg om op het internet aangesloten informaticasystemen te kraken, soms voor de lol, soms als uitdaging of soms gewoon met de bedoeling te schaden of de boel in 't honderd te doen lopen. Het zou naïef zijn te denken dat je bestand bent tegen dergelijke praktijken omdat je jezelf niets te verwijten hebt of omdat je systeem niets buitengewoons bevat.

Om jezelf te beschermen, installeer je best een *firewall* (brandmuur) : een software of hardware die een veiligheidsmuur opwerpt tussen jouw systeem en de rest van het web om ongewenste binnendringers op afstand te houden.

Besef wel dat een brandmuur je niet altijd zal zeggen dat men in je systeem binnengedrongen is. Daarom kan een veiligheidssysteem pas optimaal werken als je er ook een voorziening aan toevoegt om binnendringers op te sporen (een zogenaamd *Intrusion Detection System* of IDS, een soort inbraakalarm).

Afdeling 4. Verzending/ontvangst van virussen

108. Wat is een computervirus ?

Een virus is een programma dat de werking van informaticasystemen verstoort, of erger nog, dat de daarin opgeslagen gegevens wijzigt, verminkt, ja zelfs vernietigt.

Het virus is in staat zich te vermenigvuldigen en zodanig geconcipieerd dat het andere programma's kan opsporen en aantasten door er zichzelf in te kopiëren. Het virus wordt actief op het ogenblik dat het besmette programma wordt uitgevoerd. Zodra het

geactiveerd is, begint het virus uitwerking te krijgen : dat kan gewoon hinderlijk of storend zijn, maar ook rampzalig en zelfs ronduit catastrofaal.

Ergerlijk doch meestal ongevaarlijk zijn virussen die de volgorde van sommige letters van het toetsenbord omkeren of die de harde schijf bevelen op een vast tijdstip een welbepaalde boodschap te laten verschijnen.

Heel wat schadelijker zijn virussen met een vernietigingspotentieel, die bijvoorbeeld gegevens in je documenten overhoophalen of - erger nog - je harddisk herformatteren.

Andere virussen vernietigen niet echt je gegevens, maar vormen toch een grote bedreiging. Doordat ze bijvoorbeeld plaats innemen op je harde schijf en in je werkgeheugen, gaat je computer veel trager werken.

Ten slotte kunnen virussen een ware ravage aanrichten op economisch of menselijk vlak. Denk maar aan de mogelijke verlamming van een ziekenhuisnet of aan de verstoring van het informaticasysteem van een luchthaven door cyberterroristen.

Virussen hebben een ontzaglijk voortplantingsvermogen en hoe langer het spelletje duurt, hoe trager je computer gaat werken en/of hoe groter de schade is.

109. Welke levensloop heeft een computervirus ?

Computervirussen hebben, net als biologische virussen, een levenscyclus die loopt van de schepping tot de uitroeiing :

Schepping : de tijd die de programmeur besteedt aan de ontwikkeling van een al dan niet vernietigend virus.

Totstandkoming : de tijd die nodig is om het virus te kopiëren naar een strategische plaats om het zo vlug mogelijk te verspreiden. Het virus infecteert over het algemeen een zeer populair programma en wordt overgebracht door middel van *attachments* (aansluitingen, bijlagen) gelinkt met elektronische post, via het internet of binnen een bedrijf, school, enz.

Reproductie : door hun aard proberen virussen zich te vermenigvuldigen. Een correct samengesteld virus vermenigvuldigt zich een groot aantal keren voordat het actief wordt. Dat is de beste manier om te blijven bestaan.

Activering : sommige virussen worden pas actief als aan een aantal voorwaarden voldaan is. Zij worden actief op sommige datums of hebben een ingebouwd aftelsysteem. Andere virussen hebben geen specifieke activeringsprocedure nodig en kunnen schade aan je systeem toebrengen door beetje bij beetje je hele capaciteit in te palmen.

Ontdekking : de ontdekking van een virus is het ogenblik waarop iemand de aanwezigheid ervan vaststelt en erin slaagt het te isoleren. Zodra dit gebeurd is, wordt het nieuwe virus over het algemeen doorgezonden naar de NCSA (*National Computer Security Association*) in Washington DC, waar documentatie over het virus wordt verzameld en nadien verdeeld onder de ontwerpers van antivirusprogramma's.

Assimilatie : zodra de ontdekking gebeurd is, wijzigen de software-ontwikkelaars hun programma's om de aanwezigheid van het virus te kunnen vaststellen. Die fase duurt een dag tot zes maanden.

Uitroeiing : als er genoeg ontwikkelaars van antivirusprogramma's een virus kunnen bestrijden en genoeg personen zich het passende antivirusprogramma aanschaffen, kan een virus worden uitgeroeid of kan althans de bedreiging ervan worden gereduceerd.

110. Hoe krijg ik een virus ?

Virussen vermenigvuldigen zich op de code van andere programma's. Zij zijn dus ongevaarlijk tot je het besmette programma lanceert. Met andere woorden, een besmet programma van een website downloaden of een diskette in je computer steken is meestal ongevaarlijk, *zolang je geen software lanceert of geen bestand opent !*

Zodra een besmette toepassing of een besmet bestand gelanceerd is, kan het virus zich verspreiden over andere toepassingen en bestanden. Op die manier kunnen programma's of bestanden die je met vrienden of collega's deelt via een diskette, het internet of een lokaal netwerk eveneens besmet worden en kun je het virus dus overbrengen op andere computers.

Je kunt onmogelijk door een virus besmet worden als je alleen maar een e-mail in tekstformaat leest. Een tekstformaat kan geen virus bevatten. Daarentegen is het best mogelijk dat je een virus overdraagt via een document dat bij een elektronische boodschap is gevoegd (*attachment*). Macrovirussen, momenteel de meest verspreide vorm, worden hoofdzakelijk overgebracht binnen Wordbestanden die met e-mails worden meegestuurd. In HTML-formaat overgezonden e-mails zijn wel potentiële doelwitten voor virussen.

Sedert kort maken sommige versies van software voor elektronische post, zoals Outlook Express en Netscape Messenger, de uitvoering van "scripts" mogelijk, gewoon door het lezen van e-mails. Het lezen van een e-mail via zo'n kleine software volstaat dus al om je computer te besmetten. Dat zal je niet overkomen als je bijvoorbeeld gebruik maakt van Eudora als software.

111. Hoe kan ik weten of mijn computer besmet is ?

Vaak worden virussen te laat ontdekt, als hun activiteit al catastrofale gevolgen heeft : verschijning van niet-relevante boodschappen, uitzending van onverwachte geluiden of muziek, maar ook blokkering van de computer, formattering van de harde schijf, ...

Nochtans kunnen een heleboel aanwijzingen argwaan wekken : beschikbaar systeemgeheugen dat kleiner is dan het zou moeten zijn, verandering van de volumenaam van een schijf, plotselinge verdwijning van programma's of bestanden, verschijning van onbekende programma's of bestanden, of abnormaal gedrag van sommige programma's of bestanden.

Je kunt ook een beroep doen op *HouseCall* (<http://news.secuser.com/index.htm>), een gratis dienst van de uitgeverij Trend die de eventueel op je schijven aanwezige virussen onmiddellijk opspoort en uitroeit.

112. Hoe kan ik mij tegen virussen wapenen ?

Het beste wat je kunt doen, is op je computer een antivirusprogramma installeren, ook al biedt dat geen optimale bescherming. De meeste van die programma's volgen een procedure waarbij de inhoud van de schijf wordt ontsmet vooraleer de software wordt geïnstalleerd, doch het antivirusprogramma wordt best geïnstalleerd vóór de besmetting, want dan kunnen alle functies van het programma optimaal werken (controle van de

overbrenging van bestanden of van de toegang tot gevoelige bestanden, inoculatie van bestanden om elke verdachte verandering van grootte op te sporen, enz.).

Dagelijks ontstaan er echter nieuwe virussen. Je moet er dan ook voor waken dat je antivirusprogramma geregeld wordt geactualiseerd : de meeste producenten updaten het programma minstens een keer per maand, maar niet altijd kosteloos ...

Gelet op deze onzekerheid moet een aantal fundamentele regels in acht worden genomen : voorkomen is beter dan genezen.

- Download geen programma's van twijfelachtige oorsprong, die je worden voorgesteld op verdachte sites of naar aanleiding van louche *chats*.
- Hoed je voor sommige bestanden die worden meegestuurd met berichten : vernietig liever een verdachte mail (van een onbekende afzender, enz.) dan je computer te besmetten.
- Gebruik geen diskettes van verdachte oorsprong (of die gecirculeerd hebben in kwetsbare openbare plaatsen zoals lokalen van scholen of universiteiten). Als je je naar zo'n drukbezochte computerzalen begeeft, bescherm dan je diskettes tegen het schrijven (verschuif het grendeltje in de rechter benedenhoek van je diskette zodanig dat je er doorheen kunt kijken).
- Maak geregeld back-ups van belangrijke bestanden op je harde schijf nadat je bent nagegaan of er geen virussen in voorkomen : dat kan tijdrovend lijken, maar in geval van besmetting (of zelfs gewoon bij het crashen van je harde schijf) zal je beloond worden voor je moeite ...
- Blijf op de hoogte van het opduiken van nieuwe virussen. Sommige tijdschriften bieden je die service gratis aan door het afkondigen van "besmettingsgevaar" als een virus zich sterk aan het verspreiden is. Dat doet onder meer het magazine *Secuser News* : <http://news.secuser.com/index.htm>.

113. Is het verzenden van virussen strafbaar ?

De wet beteugelt inderdaad het ontwerpen, ter beschikking stellen, verspreiden of commercialiseren van virussen of programma's die zulke virussen kunnen aanmaken.

Wie zo'n overtreding begaat, krijgt een gevangenisstraf van zes maanden tot drie jaar en een geldboete of een van beide straffen.

Bij herhaling wordt de strafmaat verdubbeld.

114. Mag ik voor de lol of als grap een "sympathiek" virus versturen ?

Veel internauten zenden voor de fun programmaatjes naar elkaar, waarbij automatisch - en ongewild - animaties, tekst, beelden, klank of clips verschijnen op de computer van de geadresseerde. Ook dat is een soort virus, dat vaak onschuldig is, maar soms de werking van een informaticasysteem danig in de war kan sturen. Wees dus op je hoede vóór je zulke bestanden opent of doorstuurt, al zijn ze nog zo sympathiek.

In principe kun je alleen worden vervolgd en eventueel gestraft als je een virus opstuurt met bedrieglijk opzet of om schade te berokkenen. Je hoort dus te weten of de verzonden

boodschap schade kan toebrengen (d.w.z. de goede werking van het informaticasysteem van het “slachtoffer” totaal of gedeeltelijk verhinderen).

115. Kan ik worden gestraft als ik buiten mijn weten een virus verspreid dat mijn adressenbestand besmette ?

Neen ! Om strafbaar te zijn, moet je je ervan bewust zijn dat het verzonden virus in staat is gegevens te beschadigen of het gebruik van een informaticasysteem te belemmeren, en moet je willen of althans aanvaarden dat dit alles gebeurt.

Je bent dus niet strafbaar als je zonder het te weten een ontvangen virus verspreidt, met alle nare gevolgen vandien : besmetting van adressenbestanden, opduiken van nieuwe bestanden... en ongewenste verzending van e-mails naar talrijke niet zelf uitgekozen correspondenten...

116. Wat moet ik denken van e-mails die mij waarschuwen dat er een gevaarlijk virus in omloop is ?

Meestal worden zulke doemberichten verzonden door flauwe grappenmakers en vervolgens doorgestuurd door andere gebruikers die vaak te goeder trouw handelen. Nu, je bent nooit voorzichtig genoeg en je gaat best te rade bij een bevoegde persoon.

Verscheidene sites bevatten een regelmatig geüpdate lijst van de diverse nepberichten (*hoaxes*) die op het wereldwijde web circuleren (zie hierboven nr. 26).

Afdeling 5. Andere vragen die je je stelt

117. Mag het gerecht of de politie bij mij binnenvallen en mijn informaticamaterieel in beslag nemen ?

Als je verdacht wordt van piraterij, ongeoorloofde toegang tot informaticasystemen, namaak (reproductie van door het auteursrecht beschermde werken) of andere misdrijven (bezit van pedofiele beelden, mededelingen met racistische of revisionistische inslag...), dan kunnen de gerechtelijke en politieautoriteiten zich inderdaad bij jou vertonen en beslag leggen op je harde schijf, je diskettes of zelfs je hele informaticamaterieel, voor zover zij een huiszoekingsbevel hebben.

118. Mogen zij gegevens van mijn harddisk of mobiele informatiedragers kopiëren ?

Ja. Wanneer inbeslagname van informaticamaterieel of -dragers niet wenselijk is, mogen de kwetsieuze gegevens gewoon gekopieerd worden, in principe op informatiedragers van de overheid.

In dringende gevallen of om technische redenen (als het gegevensvolume de opslagcapaciteit van de door de overheid meegebrachte informatiedragers overschrijdt) kunnen de data op je eigen dragers worden gekopieerd. Ook de software gebruikt voor de aanmaak van de gegevens alsook de sleutels om ze te ontcijferen, mogen worden gekopieerd.

119. Mogen zij mij beletten toegang te hebben tot sommige gegevens of die gegevens wissen ?

Ja! De Procureur des Konings mag de toegang beletten tot gegevens die werden gekopieerd (onder meer door codering, d.w.z. door ze met een cryptosysteem om te zetten in een reeks alfanumerieke lettertekens die voor de gewone sterveling onbegrijpelijk zijn.

Hiermee wil men beletten dat je nog greep hebt op de “in beslag genomen” gegevens en vermijden dat het origineel van de gegevens gewijzigd wordt en zo zijn bewijskracht voor het gerecht verliest.

Het blokkeren van de toegang kan ook als alternatief dienen voor het kopiëren van de gegevens als dat laatste (om technische redenen of wegens de omvang van de gegevens) onmogelijk blijkt.

In principe mogen gegevens niet zomaar worden vernietigd als er nog geen uitspraak gedaan is. Bij wijze van uitzondering staat de wet de vernietiging toe van sommige soorten gegevens, met name die welke duidelijk strijdig zijn met de openbare orde of de goede zeden : pedofiele beelden, bijzonder schadelijke virussen ...

120. Mogen zij mij verplichten informatie te verschaffen over de manier waarop ik toegang kreeg tot beveiligde gegevens ?

De met een onderzoek belaste autoriteiten mogen de medewerking eisen van personen die beschikken over sleutels voor toegang tot het informaticasysteem en tot de erin opgeslagen data. Zij mogen alle personen die kennis kunnen hebben van jouw informaticasysteem gelasten informatie te verstrekken over de werking van het systeem en over de manier om toegang te krijgen tot het systeem of tot de gegevens. Zo mogen zij hun medewerking vragen om beveiligingen te kraken of gecodeerde gegevens te ontcijferen.

Voorts mag de onderzoeksrechter elke geschikte persoon gelasten zelf het informaticasysteem in werking te stellen of de door het systeem opgeslagen, verwerkte of overgedragen relevante gegevens, naargelang van het geval, op te zoeken, beschikbaar te stellen, te kopiëren, niet beschikbaar te stellen of te verwijderen.

Als je echter in staat van beschuldiging wordt gesteld, ben je er niet toe gehouden aan dat bevel gevolg te geven ; je verwanten trouwens ook niet. Dit is een fundamenteel principe : iedere persoon die van een overtreding wordt beschuldigd, heeft het recht om te zwijgen en om geen informatie mee te delen waardoor hij zou kunnen worden beticht.

Zo kan de medewerking worden gevraagd van de voor het systeem verantwoordelijke persoon of van andere gebruikers, maar ook van de netwerkbeheerder, de ontwerper of de verstrekker van de decodingssoftware, vertrouwensderden (bijvoorbeeld een verstrekker van certificatediensten), zelfs van deskundigen inzake informaticaveiligheid die het cryptosysteem voor de beveiliging van de kwetsbare gegevens beheersen.

Wie weigert om mee te werken of opzoekingen in een informaticasysteem belemmert, krijgt een gevangenisstraf van zes maanden tot een jaar en een geldboete of een van beide straffen.

121. Worden mijn oproep- en identificatiegegevens bij gebruik van het internet geregistreerd en bewaard door sommige netwerk- en dienstenoperatoren ?

Ja ! De wet verplicht de telefoon- of mobilfoonoperatoren, de internetproviders, de providers van e-mail, *chat*diensten, discussiefora, enz. je oproep- en identificatiegegevens te registreren en te bewaren tijdens een periode van ten minste twaalf maanden.

Die bewaarplicht (*ex ante*, vooraf) is permanent en niet gebonden aan een lopende onderzoeksprocedure (informatie of onderzoek).

De wet geeft geen definitie van het begrip “gegevens”, noch van de soorten gegevens waarvoor de bewaarplicht geldt ; ze zegt ook niet welke providers aan die bewaarplicht onderworpen zijn. Waarschijnlijk omvatten de oproep- en identificatiegegevens het uur en de duur van de verbindingen, de herkomst van de oproepen, het IP-adres van je computer, ...

Die (ruime en onduidelijke) plicht werd ingevoerd om de opsporing en vervolging van strafrechtelijke inbreuken te vergemakkelijken. Verwacht wordt dat de lijst van de betrokken gegevens bij koninklijk besluit zal worden vastgelegd. Dit is wel vatbaar voor kritiek omdat de grondwet bepaalt dat beperkingen van de persoonlijke levenssfeer door een wet moeten worden toegestaan.

Deel 5. Een overeenkomst sluiten op het web



HOOFDSTUK I. INFORMATIE

Krachtens de wet is de verkoper ertoe gehouden op zijn website een aantal inlichtingen te vermelden over zijn activiteit, over de bepalingen van de overeenkomst, over de aangeboden producten en diensten, over jouw bestelling, enz.

122. Met wie heb ik te maken ? Welke inlichtingen over de verkoper en zijn activiteiten moet ik kunnen vinden ?

Om een zekere transparantie te waarborgen in de contractuele betrekkingen die op netwerken ontstaan, moet de verkoper alle bezoekers een minimum aan informatie over zijn activiteit verstrekken, nl. :

- zijn naam en firmanaam ;
- het geografisch adres waar hij gevestigd is ;
- zijn personalia, met inbegrip van zijn e-mailadres, waardoor je snel, rechtstreeks en efficiënt met hem kunt communiceren ;
- eventueel het handelsregister waarin hij ingeschreven is en zijn inschrijvingsnummer ;
- eventueel zijn BTW-nummer ;
- de gedragscodes waaraan hij eventueel onderworpen is, alsook informatie over de manier waarop die codes elektronisch kunnen worden geraadpleegd (zie hieronder nr. 179 e.v.) ;
- ingeval de activiteit van de verkoper onderworpen is aan een vergunningsregeling, de adresgegevens van het bevoegde toezichtsorgaan ;
- en ten slotte, voor verkopers die een gereguleerd beroep uitoefenen (bv. vrije beroepen) :
 - de beroepsvereniging of bedrijfsorganisatie waarbij de verkoper aangesloten is,
 - de beroepstitel en de staat waarin die titel werd toegekend,
 - een verwijzing naar de toepasselijke beroepsregeling en naar de middelen om daartoe toegang te krijgen.

Die informatie moet hoe dan ook beschikbaar zijn, of het nu gaat om een site voor e-handel, een informatiesite, een zoekmachine, een internetprovider, een e-mailprovider, een discussieforum, enz.

Die informatie moet gemakkelijk, rechtstreeks en altijd toegankelijk zijn, bijvoorbeeld door te klikken op een hyperlink die zich onderaan op elke webpagina bevindt en naar een specifieke pagina verwijst.

123. Hoe kan ik op netwerken het verschil zien tussen reclame en andere informatie ?

Je bent waarschijnlijk op het internet ooit al eens in de val gelokt door een handige adverteerder, die je aandacht probeerde te trekken en je ertoe aanzette om te gaan klikken op ongewone en aantrekkelijke boodschappen die in werkelijkheid reclamepagina's verbergen. Onder het mom van objectieve informatie (bv. dieet-, schoonheids- of medisch advies) worden sommige sites in feite gefinancierd door een of andere adverteerder die erop uit is je warm te maken voor zijn producten of diensten.

Zulke praktijken zijn verboden door de wet, die stelt dat elke reclame, banner, *pop up*-boodschap, e-mail, verkoopinformatie, ... bij de verzending onmiddellijk wordt geïdentificeerd.

Dit betekent dat de commerciële bedoeling van dat soort berichten duidelijk naar voren moet komen, onder meer door de vermelding "reclame".

Zo mag er bij de presentatie van de site geen enkele verwarring mogelijk zijn tussen informatie en promotie. Bovendien moet de adverteerder voor wiens rekening reclame wordt gemaakt duidelijk identificeerbaar zijn.

124. Wat met promotieaanbiedingen, wedstrijden en promotiespelen op de netwerken ?

Promotieaanbiedingen op het internet moeten steeds duidelijk als dusdanig identificeerbaar zijn. Promotieaanbiedingen zijn aankondigingen van prijsverminderingen of gezamenlijke aanbiedingen, d.w.z. aanbiedingen die bij de aankoop van een product of dienst recht geven op een kortingbon, een geschenk, een gratis product of dienst, enz.

De voorwaarden om in aanmerking te komen voor die aanbiedingen moeten gemakkelijk kunnen worden gevonden (bv. door op een hyperlink te klikken) en opgesteld zijn in duidelijke en ondubbelzinnige bewoordingen. Bovendien moet de verkoper, bij prijsvermindering, de oude of gewone prijs in de nabijheid van de verminderde prijs aanduiden.

Ook wedstrijden en andere promotiespelen die op netwerken door adverteerders worden georganiseerd, moeten duidelijk identificeerbaar zijn. Voorts moet je gemakkelijk toegang kunnen krijgen tot de deelnemingsvoorwaarden. Deze moeten duidelijk en ondubbelzinnig zijn.

125. Over welke informatie moet ik beschikken voor ik een bestelling plaats ?

Als je op het internet een overeenkomst sluit, zijn er twee problemen : enerzijds heb je geen rechtstreeks en concreet contact met het aangeboden product, anderzijds moet je een geautomatiseerd proces volgen voor het sluiten van het contract. Om vergissingen en misverstanden te vermijden, moet de verstrekker je dus een zeker aantal gegevens meedelen vooraleer je bij hem een bestelling plaatst, wanneer je een overeenkomst aangaat voor je eigen behoeften (en niet voor je beroep).

Hij moet je eerst informeren over de producten of diensten die hij levert, alsook over de voorwaarden van de overeenkomst, d.w.z. :

- gegevens over zijn identiteit en beroepsactiviteit (zie hierboven nr. 122) ;

- essentiële kenmerken van het product of de dienst ;
- prijs van het product of de dienst, met aanduiding of de belasting en leveringskosten inbegrepen zijn ;
- eventuele leveringskosten ;
- wijze van betaling (zie hieronder nr. 156 e.v.), levering of uitvoering van de overeenkomst ;
- het al of niet bestaan van een verzakingsrecht (zie hieronder nr. 144 e.v.) ;
- wijze van terugneming of teruggave van het product, met inbegrip van de eventueel daarmee gepaard gaande kosten ;
- kosten voor het gebruik van de techniek voor communicatie op afstand, wanneer die niet overeenstemmen met het basistarief (m.a.w. indien het bezoek aan de site duurder uitvalt dan het tarief van de basisaansluiting, bv. voor een site die niet gratis toegankelijk is) ;
- geldigheidsduur van het aanbod of de prijs ;
- in geval van duurzame of periodieke dienstverlening of productlevering, minimumduur van de overeenkomst (bv. abonnement op een tijdschrift).

Hij moet je ook informatie geven om wegwijs te worden op zijn site, nl. :

- talen waarin het contract kan worden gesloten ;
- de diverse technische formaliteiten voor het sluiten van de overeenkomst (zie hieronder nr. 129) ;
- wijze waarop eventueel verkeerd ingevoerde gegevens kunnen worden gecorrigeerd voordat de bestelling wordt doorgegeven (zie hieronder nr. 130) ;
- eventuele archivering van de gesloten overeenkomst en, in voorkomend geval, voorwaarden voor toegang tot dit archief na plaatsing van de bestelling (zie hieronder nr. 128).

Die informatie moet duidelijk, begrijpelijk en ondubbelzinnig zijn.

Indien je beroepshalve een overeenkomst sluit, hoeft de verkoper je al die inlichtingen niet te verstrekken.

126. Moeten de algemene voorwaarden mij worden meegedeeld vóór het sluiten van de overeenkomst ?

Neen, maar als ze je niet werden meegedeeld vóór het sluiten van de overeenkomst, dan kunnen ze ook niet tegen jou worden ingebracht.

Met andere woorden, de verlener mag niet verwijzen naar algemene voorwaarden die je niet hebt kunnen raadplegen en aanvaarden vóór het sluiten van de overeenkomst. Hij mag zich bijvoorbeeld tegen jou niet beroepen op contractuele bepalingen die niet op zijn website voorkwamen en die hij je niet door enig ander middel meedeelde vóór het sluiten van de overeenkomst. Een rechter zou zelfs kunnen oordelen dat de algemene

voorwaarden niet zijn meegedeeld als ze niet zichtbaar genoeg zijn op de website. Dat zou het geval kunnen zijn als ze weggemoffeld zijn in een uithoek van de site, waar ze enkel na grondig speurwerk of bij gelukkig toeval te vinden zijn.

Op tal van sites die onlinediensten aanbieden, worden de algemene voorwaarden wel getoond. Je hebt er toegang toe via een hyperlink die zich op elke pagina van de site of naast het samenvattend overzicht van je bestelling bevindt. Soms kom je bij het uitvoeren van de commando's sowieso terecht op de pagina met de algemene voorwaarden en moet je klikken op een "Ik aanvaard"-icoon om je bestelling nader te bepalen.

Je moet wel weten dat je door dat klikken akkoord gaat met die voorwaarden en dat de verkoper ze dus tegen jou kan inbrengen. We raden je dan ook stellig aan de algemene voorwaarden van de verkoper aandachtig te lezen voordat je de overeenkomst sluit. Je doet er goed aan daarvan een kopie te bewaren door ze te printen of op te slaan op je harde schijf of op een diskette. Trouwens, volgens de wet moet een verkoper die je zijn algemene voorwaarden meedeelt je toestaan ze te bewaren en te kopiëren.

127. Welke informatie moet ik krijgen na mijn bestelling ?

Nadat je een bestelling hebt geplaatst op een website, is het van belang te weten of de verkoper ze wel geregistreerd heeft. Daarom is de verkoper ertoe gehouden je zonder onverantwoorde vertraging de ontvangst te melden van je bestelling en je tevens een samenvattend overzicht van je bestelling te bezorgen. Dat overzicht kan de vorm aannemen van een webpagina, die verschijnt nadat je je bestelling hebt doorgegeven, of van een e-mail, die je zo spoedig mogelijk wordt toegezonden.

Bovendien moet de verkoper je een document bezorgen waarin alle gegevens over de overeenkomst worden bevestigd :

- identiteit en geografisch adres van de verkoper ;
- prijs van het product of de dienst ;
- eventuele leveringskosten ;
- wijze van betaling (zie hieronder nr. 156 e.v.), levering of uitvoering van de overeenkomst
- geldigheidsduur van het aanbod of de prijs,
- bij duurzame of periodieke productlevering of dienstverlening, minimumduur van de overeenkomst ;
- geografisch adres waar je een klacht kunt indienen ;
- inlichtingen over bestaande klantenservice en commerciële waarborgen (zie hieronder nr. 178) ;
- bij een overeenkomst van onbepaalde duur of van meer dan 1 jaar, de voorwaarden waaronder je de overeenkomst kunt opzeggen ;
- het al of niet bestaan van een verzakingsrecht (zie hieronder nr. 144) en de wijze waarop en de voorwaarden waaronder dat recht kan worden uitgeoefend.

In dat opzicht moet een van de volgende twee clausules in vetgedrukte letters en in een kader los van de tekst op de eerste bladzijde van het document of in ieder geval op een goed zichtbare wijze worden vermeld :

- indien je een verzakingsrecht hebt : “De consument heeft het recht aan de verkoper mee te delen dat hij van de aankoop afziet, zonder een boete te betalen en zonder een reden op te geven, gedurende ... werkdagen (ten minste 7 dagen) vanaf de dag die volgt op de levering van het product of op het sluiten van de dienstverleningsovereenkomst”.
- indien je geen verzakingsrecht hebt : “De consument beschikt niet over het recht om van een aankoop af te zien”.

Als je een product hebt gekocht, moet je deze informatie ten laatste bij de levering ontvangen.

Als je een dienstverleningsovereenkomst hebt gesloten, moet je deze informatie normaal vóór de uitvoering van de overeenkomst ontvangen.

Als de uitvoering van de overeenkomst echter met jouw akkoord is aangevat vóór het einde van de verzakingstermijn (minimum 7 dagen), dan moeten die inlichtingen je bereiken tijdens de uitvoering van de overeenkomst. Wil je bijvoorbeeld een online downloadbare software aankopen, dan moeten die inlichtingen je worden verstrekt vóór of ten laatste tijdens het downloaden.

Die inlichtingen zijn belangrijk, want aan de hand daarvan kun je een aantal zaken nagaan : de juistheid van je bestelling, de draagwijdte van je rechten, de praktische regeling voor de uitvoering van de overeenkomst, maar tevens alle stappen die moeten worden gedaan als er een probleem rijst (verzaking aan de overeenkomst, klacht, klantenservice, waarborgen, enz.)

Bewaar dus zorgvuldig het document met die informatie, want het kan een kostbaar bewijsmiddel zijn in geval van betwisting (zie hieronder nr. 133). De verkoper moet je die gegevens op een duurzame informatiedrager bezorgen, zodat je ze kunt bewaren en nadien raadplegen. Dit kan een papieren versie, een cd-rom of een diskette zijn, die met de post of samen met je pakket opgestuurd wordt, of ook een e-mail of een fax.

Indien je beroepshalve een overeenkomst sluit, hoeft de verlener je al die inlichtingen niet te verstrekken.

128. Kan ik het verloop van mijn bestelling volgen na het sluiten van de overeenkomst ?

Als de verlener je toegang geeft tot een gearchiveerde copie van je bestelling, moet hij je dit duidelijk meedelen vóór je bestelt.

Zo laten sommige verleneren je op hun site nagaan hoe ver het staat met je bestelling, welke bestellingen je bij hen reeds hebt geplaatst, welke persoonsgegevens over jou bij hen werden geregistreerd, enz. Soms kun je zelfs een reeds geregistreerde bestelling wijzigen of annuleren, voor zover ze nog niet werd uitgevoerd. Als zoiets mogelijk is, laat de verkoper je het weten op zijn site of in het ontvangstbewijs van de bestelling.

HOOFDSTUK II. HET SLUITEN VAN EEN OVEREENKOMST OP HET INTERNET

129. Hoe kan ik iets bestellen op een website ?

Om je in volle vertrouwen op zijn site te laten surfen, moet de verkoper je het verloop van een bestelling stap voor stap uitleggen (zie hierboven nr. 125). Indien je beroepshalve een overeenkomst sluit, mag de verkoper van die verplichting afzien.

Over het algemeen verloopt de bestelling als volgt (de hieronder beschreven methode is slechts één van de vele voorbeelden van het mogelijke verloop van een onlinebestelling).

Om te beginnen kun je het gewenste product of de gewenste dienst misschien vinden in de onlinecatalogus van de verkoper waarin per rubriek alle te koop gestelde producten en diensten opgenomen zijn. Het grasduinen in die catalogus wordt soms vergemakkelijkt door het gebruik van een zoekmotor. Naarmate je opzoeking vordert, kun je één of meer artikels selecteren en in je "aankoopmand" stoppen.

Eens je keuze gemaakt is, kun je beslissen om de overeenkomst te sluiten door een specifiek icoontje aan te klikken. Dan volg je een parcours dat, als het goed opgevat is, nauwkeurig in stappen is ingedeeld : telkens je akkoord bent, klik je een passende icoon aan en ga je over naar de volgende stap. Je kunt op elk ogenblik het verloop onderbreken en terugkeren naar de vorige stap zonder een overeenkomst te sluiten.

Aldus vul je stap voor stap het bestelformulier in, voer je je persoonsgegevens in, kies je de betalings- en leveringswijze, enz. Onderweg heb je toegang tot een massa informatie over de algemene verkoopsvoorwaarden, de tarieven en leveringstermijnen, eventuele taksen, de bescherming van je persoonsgegevens, enz.

Veel sites tonen een samenvattend overzicht zodra alle gegevens van de overeenkomst ingebracht zijn. Ga zeker nog een laatste maal na of de gegevens juist zijn vooraleer de bestelling definitief te valideren door de passende icoon aan te klikken. De bestelling is slechts geregistreerd als al die stappen gedaan zijn. Soms komt een webpagina tevoorschijn om de registratie van je bestelling te bevestigen (zie hierboven nr. 127).

Talrijke verkopers verstrekken je informatie op hun site om je vertrouwd te maken met het onlinekopen. Soms loodst de startpagina je doorheen de site met een simulatie van een bestelling. Vaak vind je heel wat informatie over de werking van de site, oplossingen voor problemen, verkoopsvoorwaarden, surftrucjes, enz. in een helprubriek op de startpagina of onderaan elke bladzijde.

130. Hoe kan ik weten of ik geen fouten heb gemaakt in mijn bestelling ?

Iedereen kan zich vergissen : een verkeerd artikel kiezen of verschillende keren hetzelfde artikel kiezen, een fout maken bij het invullen van het kredietkaartnummer, het leveringsadres, enz.

Om te vermijden dat de doorgegeven bestelling fouten bevat, verplicht de wet de verkoper de verkeerd ingebrachte gegevens op te sporen en te verbeteren. Opgelet : indien je beroepshalve een overeenkomst sluit, mag de verkoper van die verplichting afzien.

Sommige sites gebruiken software die evidente fouten bij het registreren van de bestelling automatisch opspoort : ongewoon grote hoeveelheden, gegevens onverenigbaar met de bepaling van een veld, invoer van tegenstrijdige gegevens, onjuist kredietkaartnummer,

geen naam of leveringsadres, ... Een foutbericht verschijnt dan en vraagt je de nodige verbeteringen aan te brengen.

Bovendien kan de verkoper de risico's gemakkelijk beperken door bij het hele verloop van het bestelproces, vanaf het selecteren van een artikel tot het valideren van de bestelling, knoppen te plaatsen om de verschillende onderdelen van de bestelling te corrigeren, te veranderen, te annuleren of te schrappen. Zo kun je steeds je bestelling wijzigen indien je een vergissing vaststelt of gewoon van mening verandert.

Zoals we hierboven (nr. 129) gezien hebben, wordt de verkoop vaak afgesloten met een bevestigingspagina waarop je de juistheid van de ingebrachte gegevens kunt nagaan alvorens alles te valideren.

Indien je, ondanks al deze voorzorgen, bij de uitvoering van de overeenkomst vaststelt dat je je bij de bestelling vergist hebt, beschik je vaak nog over een verzakingsrecht (zie hieronder nr. 144 e.v.).

131. Vanaf wanneer ben ik contractueel verbonden ?

Het antwoord op die vraag verschilt volgens het recht dat op de overeenkomst van toepassing is (zie hieronder nr. 194 e.v.), naargelang je bestelling wordt beschouwd als een aanvaarding van het door de verkoper gedane aanbod of als een aan de verkoper gedane aanbod. We onderzoeken hier slechts enkele mogelijkheden.

Indien het Belgische recht van toepassing is, dan houdt je bestelling in dat je akkoord gaat met het aanbod dat de (in België gevestigde) verkoper je op zijn e-commercesite (of per e-mail) gedaan heeft. De overeenkomst is dus gesloten op het ogenblik waarop je bestelling bij de verkoper aankomt. In het Franse recht wordt de overeenkomst gesloten op het ogenblik dat je je bestelling valideert. In de praktijk komt dit op hetzelfde neer, daar er slechts enkele seconden verlopen tussen deze twee ogenblikken.

Volgens het Duitse en Engelse recht is je bestelling daarentegen een aanbod tot het sluiten van een overeenkomst, dat je aan de verkoper stuurt en hij vooralsnog kan weigeren of aanvaarden. De overeenkomst is dus slechts gesloten op het ogenblik dat de verkoper je meedeelt dat hij je aanbod aanvaardt. Meestal blijkt zijn aanvaarding uit de uitvoering van de overeenkomst. Let wel : in principe bindt je aanbod je en mag je het niet meer intrekken. Niettemin kun je nog je verzakingsrecht uitoefenen als je nadien van mening verandert (zie hieronder nrs. 144 e.v.).

Hou dus rekening met het rechtsstelsel dat op de overeenkomst van toepassing is.

132. Hoe ben ik zeker dat de verkoper mijn bestelling gekregen heeft ?

Wanneer je op een website een bestelling geplaatst hebt, is het belangrijk te weten of de verkoper je bestelling geregistreerd heeft. Vergeet niet dat de verkoper verplicht is je onverwijld een ontvangstbericht te sturen met een samenvattend overzicht van je bestelling (zie hierboven nr. 127). Dit bericht kan de vorm aannemen van een webpagina die verschijnt na afloop van een bestelproces of een elektronische mail die je zo snel mogelijk wordt toegestuurd.

Opgelet : indien je beroepshalve een overeenkomst sluit, mag de verkoper van die verplichting afzien.

HOOFDSTUK III. BEWIJS EN ELEKTRONISCHE HANDTEKENING

Je hebt een overeenkomst gesloten op het internet en je hebt erop gelet dat de voorgescreven procedure werd gevolgd. Toch wil je weten of je door die bestelling op dezelfde wijze als bij een traditionele schriftelijke bestelling bent gebonden en meer bepaald of je dat gemakkelijk kunt bewijzen.

In principe wel. Twee recente wetten (van 20 oktober 2000 en van 9 juli 2001) erkennen de juridische waarde van de elektronische handtekening. Je moet wel weten dat die juridische erkenning niet geldt voor alle technieken van elektronische handtekening en aan strenge voorwaarden is onderworpen. Wij zullen dit aan de hand van enkele voorbeelden verduidelijken.

Wat gebeurt er als er tussen jou (consument) en de verkoper een geschil ontstaat over het bestaan of de inhoud van de overeenkomst? Hier moeten we een onderscheid maken naargelang de betwisting uitgaat van jezelf of van de verkoper.

133. Hoe kan ik bewijzen dat ik iets op het internet heb besteld ?

Indien je als consument wilt bewijzen dat je een bestelling hebt geplaatst bij een verkoper-handelaar (de zaken liggen anders als het over een verkoper-particulier gaat), dan beschik je over de vrijheid van bewijs. Met andere woorden : je mag op alle mogelijke manieren aantonen dat je een bestelling hebt geplaatst. Hoe? Onder andere met een elektronische kopie van je bestelbon en van de bevestiging van je bestelling die je van de verkoper hebt gekregen (bv. per e-mail). Toch komt het de rechter toe de waarde te beoordelen van het document dat je hem voorlegt in geval van geschil. Het is dus opletten geblazen! Gebruik, voor belangrijke bestellingen, liefst een beveiligd handtekeningsysteem.

Twee tips dus :

- Bewaar steeds een gedrukte of elektronische kopie van je bestelbon en van de bevestiging van de verkoper !
- Gebruik voor belangrijke bestellingen liefst een elektronische-handtekeningsysteem dat beantwoordt aan alle wetsvereisten, zodanig dat je handtekening kan worden gelijkgesteld met een geschreven handtekening (zoals hieronder uitgelegd).

134. Hoe kan de verkoper bewijzen dat ik iets via het internet heb besteld ?

Voor alle duidelijkheid : de verkoper zal het moeilijker hebben dan jij om het bestaan van de overeenkomst te bewijzen (tenzij je de verkoper hebt betaald ! In dat geval zal hij minder moeite hebben om het bewijs te leveren).

Er moet een onderscheid worden gemaakt naargelang het totale bedrag van je bestelling lager is dan (of gelijk aan) of hoger is dan 375,00 EUR.

In het eerste geval valt de verkoper onder het stelsel van de bewijsvrijheid. Hij kan zich dus beroepen op de bestelbon die je hebt ingevuld, ook al gaat het om een elektronische en niet ondertekende versie. Een rechter kan evenwel oordelen dat een bestelbon geen bewijskracht heeft doordat hij niet met de nodige veiligheid is opgemaakt.

In het tweede geval zou de verkoper normaal in het bezit moeten zijn van een ondertekend document. Tegenwoordig verstaat men onder een ondertekend document niet alleen een met de hand ondertekend papieren document, maar ook een document dat door middel

van een mechanisme voor elektronische handtekening werd ondertekend, voor zover die elektronische handtekening aan de wetsvereisten beantwoordt. Indien de verkoper niet beschikt over een van die ontertekeningstechnieken, valt er te vrezen dat hij moeilijk het bewijs zal kunnen leveren van de bestelling en van het sluiten van de overeenkomst (alsook van de inhoud van de overeenkomst).

We herinneren er ook aan dat een onlineverkoper zonder onverantwoorde vertraging en op elektronische wijze de ontvangst moet melden van de bestelling, ongeacht het bedrag van de bestelling. Bij betwisting moet hij ook het bewijs leveren dat hij effectief de ontvangst van de bestelling heeft gemeld.

135. Wordt een gewone e-mail als bewijs erkend ?

Een e-mail kan hooguit als een vermoeden en/of een begin van schriftelijk bewijs worden beschouwd. Wat eigen is aan beide middelen, is dat ze noodzakelijkerwijs moeten worden aangevuld met andere bewijsmiddelen om de rechter te overtuigen van de bewijskracht. In het juridisch jargon spreekt men dan ook van “onvolkomen” bewijsmiddelen. Als je je dus alleen maar kunt beroepen op een gewone e-mail (niet aangevuld door andere aanwijzingen of getuigenissen), dan ziet het er sterk naar uit dat die e-mail alleen de rechter niet zal overtuigen van de realiteit of de inhoud van de overeenkomst, althans wanneer er hierover betwisting bestaat. Dat komt door de relatieve onzekerheid rond het opmaken en verzenden van een gewone e-mail en door de vele vervalsingsmogelijkheden.

Indien de e-mail niet elektronisch ondertekend is, wordt hij volgens de wet doorgaans niet beschouwd als een met de hand ondertekend document, tenzij de rechtspraak hierover eerlang een ander standpunt inneemt. Wanneer de wet dus als bewijs een met de hand ondertekend document eist (inzonderheid tegenover een particulier voor een rechtshandeling die 375,00 EUR overschrijdt), dan kunnen wij redelijkerwijs stellen dat een gewone e-mail niet aan die voorwaarde voldoet.

Die stelling moet echter worden genuanceerd. De bepalingen over het bewijs zijn namelijk niet van openbare aard. Vóór het elektronisch sluiten van een overeenkomst kunnen de ontvankelijkheid en de bewijskracht van de elektronische documenten dus in een contract worden vastgelegd. Zo zouden de partijen kunnen overeenkomen dat een e-mail of telefax en een met de hand ondertekend document gelijkwaardig zijn. Een dergelijke overeenkomst wordt over het algemeen als geldig aanvaard en voorkomt dat de partijen achteraf al te gemakkelijk de bewijskracht van die elektronische documenten kunnen betwisten.

Dat soort clause wordt vaak gebruikt (bv. in de betrekkingen tussen banken en klanten). Wil je dus de juridische waarde van een e-mail of fax aanvechten, kijk dan eerst na of je bij het aanknopen van de relatie met de verkoper geen overeenkomst ondertekend hebt waarin zo'n bepaling voorkomt !

136. Is een elektronisch ondertekend document een afdoend bewijsmiddel ?

Een van de voordelen van de elektronische handtekening is dat de verkoper de zekerheid heeft dat het ondertekende document evengoed als bewijs kan dienen als een papieren document met een klassieke (handgeschreven) ondertekening. Laten we even preciseren wanneer een elektronische handtekening automatisch met een handgeschreven handtekening wordt gelijkgeschakeld.

Om automatisch geassimileerd te worden met een handgeschreven handtekening, om in aanmerking te komen voor het juridisch stelsel dat reeds voor de handgeschreven ondertekening bestaat en om aldus een voldoende rechtskundige bescherming te genieten, moet een elektronische handtekening aan al de volgende voorwaarden voldoen :

- de elektronische handtekening moet geavanceerd zijn in de zin van de wet van 9 juli 2001 betreffende de elektronische handtekening ;
- de geavanceerde elektronische handtekening moet gebaseerd zijn op een gekwalificeerd certificaat : dit is een certificaat met een bij de wet bepaalde minimuminhoud (bijlage I van de wet van 9 juli 2001) en afgegeven door een certificatie dienstverlener die voldoet aan een aantal strenge bij de wet bepaalde voorwaarden (bijlage II van dezelfde wet) ;
- de elektronische handtekening moet worden geplaatst door middel van een veilig middel voor het aanmaken van een elektronische handtekening : een middel voor het aanmaken van een handtekening wordt slechts als veilig beschouwd indien het voldoet aan de eisen van bijlage III van de wet van 9 juli 2001.

Om het belang van al die voorwaarden en de rol van elke acteur te begrijpen, moet je goed weten wat een geavanceerde elektronische handtekening is en hoe een digitale handtekening werkt, welke rol een certificatie dienstverlener speelt, wat een (gekwalificeerd) digitaal certificaat is, wat een veilig middel voor het aanmaken van een elektronische handtekening is en hoe dit alles concreet in zijn werk gaat.

137. Wat is een geavanceerde elektronische handtekening ?

De wet definieert de “*geavanceerde elektronische handtekening*” als “*elektronische gegevens vastgehecht of logisch geassocieerd met andere elektronische gegevens, die worden gebruikt als middel voor authenticatie en aan de volgende eisen voldoen :*

- a) *de handtekening is op unieke wijze aan de ondertekenaar verbonden ;*
- b) *zij maakt het mogelijk de ondertekenaar te identificeren ;*
- c) *zij wordt aangemaakt met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden ;*
- d) *zij is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke latere wijziging van de gegevens kan worden opgespoord”.*

Die definitie is in algemene bewoordingen opgesteld om een technische neutraliteit te waarborgen en een of andere op de markt bestaande technologie niet te bevoordelen. In de praktijk is het echter niet altijd eenvoudig om uit te maken of de diverse technische mechanismen voor de aanmaak van een elektronische handtekening, zoals de biometrische handtekening, de geheime code die samengaat met het gebruik van een kaart en met de digitale (of numerieke) handtekening wel voldoen aan alle voorwaarden van de definitie. Nu, alle commentatoren zijn het erover eens dat de digitale handtekening die gebaseerd is op de asymmetrische cryptografie en gebruikt wordt in een infrastructuur met een openbare sleutel (zoals aangeboden door Isabel, Globalsign of Belgacom E-Trust bijvoorbeeld) aan het begrip geavanceerde elektronische handtekening beantwoordt. Aangezien deze technologie momenteel doordringt op de markt en door de regering gekozen werd voor haar *e-Governmentprojecten* (inzonderheid het project i.v.m. de

elektronische identiteitskaart), is het misschien interessant om uit te leggen hoe dit handtekeningsysteem functioneert.

De zogenaamde digitale of numerieke handtekening steunt op de technologie van de “openbare sleutel” of asymmetrische cryptografie. Als de identificatie met een openbare sleutel gebeurt, beschik je over twee aanvullende wiskundige sleutels : een privé-sleutel, die geheim moet blijven en een openbare sleutel, die vrij mag worden doorgegeven. Beide sleutels worden gegenereerd aan de hand van een wiskundige functie, die ervoor zorgt dat de privé-sleutel gedurende een zekere tijd en met normale middelen niet kan worden afgeleid uit de bijbehorende openbare sleutel. De openbare sleutel moet dus een onomkeerbare functie zijn van de privé-sleutel. Met je privé-sleutel kun je een bericht “ondertekenen”. De ontsleuteling gebeurt volgens het principe van de complementariteit van het sleutelpaar : een bericht dat versleuteld werd met een privé-sleutel kan enkel worden ontsleuteld met de bijbehorende openbare sleutel. De identiteit van de ondertekenaar wordt bevestigd door een certificaat, dat wordt uitgegeven door een certificatedienstverlener (CDV) en bekrachtigt dat de openbare sleutel wel degelijk de ondertekenaar toebehoort.

In het volgende voorbeeld zie je hoe een digitale handtekening functioneert.

Alice wil een elektronisch ondertekende boodschap naar Johan mailen. Nadat ze haar bericht heeft getypt, maakt Alice daarvan een *message digest* (= samenvatting) door middel van een wiskundige bewerking. Die digest is het resultaat van een functie die *hashing* (= inkerving) wordt genoemd en onomkeerbaar is. Met deze functie kun je op een beknopte wijze een keten van gegevens genereren die het bericht voorstelt. Deze voorstelling maakt het mogelijk elke in het bericht aangebrachte wijziging op te sporen. De ontvanger hoeft dus enkel de hashfunctie op het ontvangen bericht toe te passen en de zo verkregen digest te vergelijken met die van de afzender. Elk verschil tussen de digests betekent dat het bericht tijdens het versturen werd gewijzigd.

Deze digest wordt vervolgens gecodeerd (onleesbaar en ontoegankelijk gemaakt) met behulp van de privé-sleutel van Alice. Deze gecodeerde digest vormt de digitale handtekening. Alice stuurt dan haar (niet gecodeerd) bericht samen met de digitale handtekening naar Johan.

Wanneer Johan het bericht en de digitale handtekening ontvangt, ontcijfert hij deze laatste door middel van een wiskundige bewerking waarin de complementaire openbare sleutel van Alice is opgenomen. Als hij erin slaagt de handtekening te ontcijferen, is het voor Johan duidelijk dat deze werd aangemaakt met de complementaire privé-sleutel van Alice : op dat ogenblik weet hij met zekerheid dat zij de auteur is van het bericht mits een derde partij (een certificerende autoriteit of certificatedienstverlener) bevestigt dat die openbare sleutel wel degelijk aan Alice toebehoort (zie hieronder nr. 142). Dankzij de hashfunctie en een vergelijking van beide “vingerafdrukken”, kan de integriteit van het bericht van Alice gecontroleerd worden.

In werkelijkheid worden al die operaties heel snel door je software voor het aanmaken van een elektronische handtekening uitgevoerd.

Ten slotte dit nog : om gebruik te kunnen maken van de openbare-sleutelcryptografie moeten de publieke sleutels worden bekendgemaakt en dient een controlesysteem te worden ingesteld zodanig dat constant kan worden nagegaan of die sleutels wel degelijk overeenstemmen met de personen die beweren dat ze hun toebehoren. Die bekendmakings- en certificatieopdracht wordt momenteel uitgevoerd door een derde certicator (“certificatedienstverlener”, ook “certificerende autoriteit” of CA genoemd).

138. Wat is een certificatedienstverlener ?

De certificatedienstverlener (hieronder CDV genoemd) is een onafhankelijke instelling die bevoegd is om, enerzijds de *identiteit na te gaan* van de houders van de openbare sleutel en *certificaten af te geven*, d.w.z. elektronische attesten die een verband leggen tussen een persoon en zijn openbare sleutel, en anderzijds, om te zorgen voor een zo ruim mogelijke *bekendmaking* van de aldus afgegeven certificaten.

De CDV moet ook het register met de openbare-sleutelcertificaten bijwerken en desgevallend certificaten intrekken. Deze derde partij bij de elektronische communicatie speelt een cruciale rol voor de betrouwbaarheid van de digitale handtekening, de identificatie van de betrokkenen om te komen tot een vaste handelwijze in open netwerken.

Zoals we hebben gesteld, heeft een CDV als voornaamste opdracht een formele verbinding tot stand te brengen tussen een persoon en zijn openbare sleutel via het afgeven van een certificaat. Dit certificaat bevat verschillende inlichtingen over de identiteit van de certificaathouder (degene die wil tekenen en zich als dusdanig wil identificeren) en zijn openbare sleutel. Het certificaat wordt ondertekend door de CDV met behulp van zijn eigen privé-sleutel en is op die manier beschermd tegen vervalsing.

In het volgende voorbeeld wordt getoond hoe certificaten kunnen worden gebruikt. Alice stuurt Johan een bericht samen met haar digitale handtekening, aangemaakt door middel van haar privé-sleutel. Na ontvangst van deze documenten (nl. twee met elkaar verbonden informaticabestanden : het bericht en de digitale handtekening), kijkt Johan eerst het certificaat na (dat hij van Alice gekregen heeft of dat hij uit een elektronische map met certificaten heeft gehaald) met behulp van de openbare sleutel van de CDV. Als de echtheid bevestigd blijkt, is hij zeker van de integriteit van de informatie die in het certificaat voorkomt, d.w.z. de identiteit van Alice en haar openbare sleutel. Hij kan vervolgens de openbare sleutel van Alice gebruiken om de handtekening in het door haar verstuurd bericht te verifiëren. Johan weet dan zeker dat het bericht van Alice komt.

De CDV kan andere functies vervullen die samengaan met de certificatie : de archivering van informatie over de certificaten (vooral i.v.m. het leveren van bewijzen ; eventueel het genereren van het sleutelpaar zonder evenwel een kopie van de privé-sleutel te bewaren ; het bijhouden van een elektronisch certificatenregister dat toegankelijk is voor het publiek ; de datum- en tijdaanduiding bij digitaal ondertekende berichten ; de archivering van elektronische documenten, enz.

In België zijn momenteel verscheidene certificatedienstverleners actief, waaronder Globalsign (<http://www.globalsign.net>), Belgacom E-Trust (<http://www.e-trust.be>) en Isabel (<http://www.isabel.be>).

139. Wat is een gekwalificeerd digitaal certificaat ?

Zoals we hierboven reeds hebben vermeld, is een certificaat niets anders dan een elektronisch attest dat een band legt tussen een natuurlijke of rechtspersoon en zijn openbare sleutel en dat de identiteit van die persoon bevestigt. Door het afgeven van het certificaat "certificeert" de certificatedienstverlener die band en verklaart hij openlijk dat de daarin opgenomen inlichtingen juist zijn.

We wezen er ook op dat de gebruiker onder andere een *gekwalificeerd* certificaat moet bezitten opdat zijn elektronische handtekening automatisch zou worden gelijkgeschakeld met een handgeschreven handtekening. Een certificaat wordt beschouwd als

gekwalficeerd certificaat als het voldoet aan de eisen van bijlage I – d.w.z. als het een minimumaantal gegevens bevat – en als het afgegeven wordt door een CDV die voldoet aan de eisen van bijlage II – d.w.z. als het in veilige omstandigheden afgegeven is (bijlage II bevat de voorwaarden inzake veiligheid, betrouwbaarheid, informatie, bewijskracht alsook de financiële voorwaarden).

Als een operator oordeelt dat hij voldoet aan die voorwaarden (waarvan sommige in zeer algemene bewoordingen opgesteld zijn), dan kan hij gekwalficeerde certificaten afgeven. De naleving van die voorwaarden wordt echter niet *a priori* nagegaan door het Bestuur of enige andere zelfstandige autoriteit. De wet verplicht die operator hoogstens een voorafgaande aangifte te doen bij het Bestuur. Die verplichte aangifte is er onder meer op gericht het Bestuur in staat te stellen zijn door de wet verleende controlebevoegdheid *a posteriori* uit te oefenen.

Momenteel geven in België enkel Belgacom E-Trust et GlobalSign “*gekwalficeerde*” certificaten af (die informatie is beschikbaar op de site van de Federale Overheidsdienst Economie, KMO, Middenstand en Energie : http://mineco.fgov.be/information_society/index_fr.htm).

140. Wat is een veilig middel voor het aanmaken van een elektronische handtekening ?

De laatste voorwaarde opdat een elektronische handtekening wordt gelijkgesteld met een handgeschreven handtekening is, zoals we hierboven hebben gesteld, het gebruik van een *veilig* middel voor de aanmaak van een handtekening.

Het begrip "middel voor het aanmaken van een handtekening" wordt door de wet gedefinieerd als geconfigureerde software of hardware om de gegevens voor het aanmaken van een handtekening te implementeren (d.w.z. de privé-sleutel). Meer concreet is dat bijvoorbeeld software waarmee je de gegevens voor het aanmaken en verifiëren van de handtekening kunt genereren (privé-sleutel/openbare sleutel), software waarmee je een elektronische handtekening kunt aanmaken en/of verifiëren, de chipkaart waarop de gegevens voor het aanmaken van de handtekening opgeslagen zijn, de lezer van de chipkaart, enz.

De middelen voor het aanmaken van een handtekening worden slechts als *veilig* beschouwd indien ze voldoen aan de eisen van bijlage III van de wet. Ze zijn opgesteld in zeer algemene bewoordingen : de middelen moeten ervoor zorgen dat de enigheid en het behoud van de vertrouwelijkheid van de voor de aanmaak van een elektronische handtekening gebruikte gegevens wordt gegarandeerd ; de middelen moeten ervoor zorgen dat het onmogelijk is de voor de aanmaak van een elektronische handtekening gebruikte gegevens af te leiden uit de voor het verifiëren van de handtekening gebruikte gegevens (door iedereen gekend) ; de middelen moeten ervoor zorgen dat het onmogelijk is een handtekening te vervalsen ; de middelen moeten ervoor zorgen dat de “ondertekenaar” de voor de aanmaak van de handtekening gebruikte gegevens technisch kan beschermen (bv. met een wachtwoord of biometrische controle) ten einde elke onrechtmatige toegang tot die gegevens te voorkomen. Ten slotte mogen die middelen de te ondertekenen gegevens niet wijzigen noch beletten dat die gegevens vóór het ondertekeningsproces aan de “ondertekenaar” worden voorgelegd. Het is namelijk absoluut noodzakelijk dat de ondertekenaar de inhoud kan bekijken en controleren, eventuele wijzigingen kan opsporen en zodoende akkoord kan gaan met wat hij ondertekent.

In de praktijk is het voor de vervaardiger van dergelijke middelen echter niet makkelijk uit te maken aan welke technische eisen ze moeten voldoen om als *veilig* te kunnen worden bestempeld. Volgens de wet zal de Europese Commissie de referentienummers van reeds algemeen aanvaarde normen voor de middelen voor het aanmaken van een elektronische handtekening echter toekennen en in het Publicatieblad van de Europese Gemeenschappen publiceren. Wanneer een product voor elektronische handtekeningen overeenstemt met die normen, wordt het *verondersteld te voldoen* aan de eisen van bijlage III. De wet voegt eraan toe dat “de overeenstemming met de veilige middelen voor het aanmaken van een elektronische handtekening met de eisen van bijlage III van deze wet, wordt bevestigd door de bevoegde instellingen, aangewezen door het Bestuur en waarvan de lijst wordt meegedeeld aan de Europese Commissie”. Paragraaf 3 bepaalt dat de voorwaarden waaraan die instellingen moeten voldoen door een koninklijk besluit zullen worden vastgelegd. Bovendien wordt een overeenstemming die is vastgesteld door een instelling aangewezen door een andere lidstaat van de Europese Economische Ruimte ook in België erkend.

Volgens een algemeen aanvaarde interpretatie van artikel 3, § 4 van de Richtlijn over de elektronische handtekening moet die overeenstemming niet *a priori*, d.w.z. vóór het op de markt brengen van de middelen, worden aangetoond. Fabrikanten kunnen dus door hen “veilig” verklaarde middelen voor het aanmaken van een handtekening op de markt brengen. Dit betekent dat er, in geval van geschil over een door zulke middelen ondertekende overeenkomst, een betwisting kan ontstaan over het al dan niet veilige karakter van het voor de ondertekening gebruikte middel en bijgevolg over de bewijskracht van de handtekening. Als dat zo is, dan dient de rechter die overeenstemming te bepalen.

141. Hoe kan ik een digitaal certificaat bekomen ?

Welke verrichtingen moet je in de praktijk uitvoeren om een digitaal certificaat te bekomen en je elektronische documenten te ondertekenen door middel van een digitale handtekening ?

Als je aan digitale ondertekening wilt gaan doen, moet je je eerst persoonlijk aanbieden bij een CDV (of bij een instelling aan wie de CDV de registratie uitbesteedt) om een certificaat te bekomen (doorgaans tegen betaling).

Vóór het afgeven van het certificaat doet de CDV het volgende :

- hij produceert een sleutelpaar (een privésleutel en een openbare sleutel) aan de hand van een geschikte software en registreert de privé-sleutel bijvoorbeeld op een met een wachtwoord beveiligde chipkaart, ten behoeve van de aanvrager (dit is de veiligste opslagmethode) ;
- hij controleert de identiteit van de aanvrager door middel van bewijskrachtige documenten (identiteitskaart, paspoort, enz.) alsook eventuele andere gegevens die op het certificaat moeten komen (beroep, hoedanigheid van afgevaardigd bestuurder van een maatschappij, enz.) ;
- hij genereert het certificaat, dat minstens de identiteit en de openbare sleutel van de houder bevat ;
- hij tekent het certificaat door middel van zijn privé-sleutel, enerzijds om zich als dusdanig te identificeren en anderzijds om de integriteit van de inhoud van het certificaat te garanderen ;

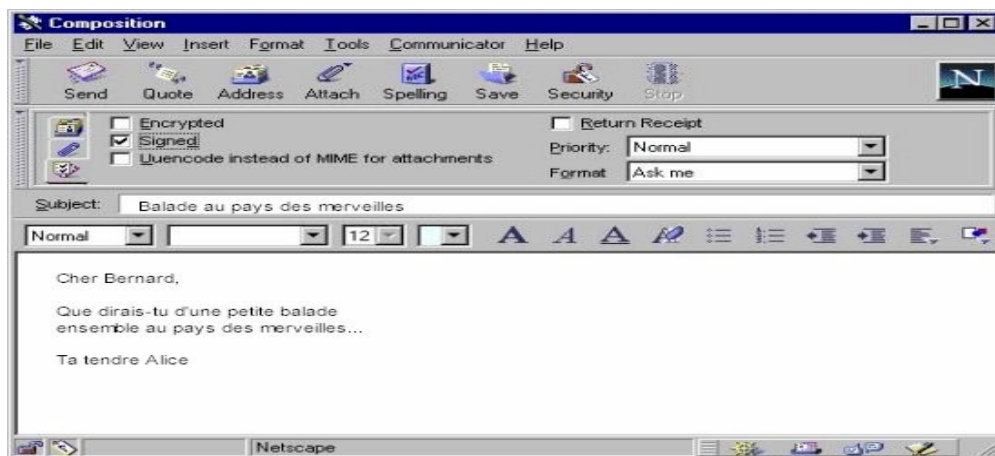
- hij slaat het certificaat op in een elektronisch register dat permanent online beschikbaar is voor elke geïnteresseerde persoon ;
- hij verschaft de aanvrager een exemplaar van het digitaal certificaat.

Vervolgens moet software worden geïnstalleerd met een module voor de aanmaak van digitale handtekeningen ; recente *browsers* zijn daarmee uitgerust. Ook Windows 2000 bevat een module voor de aanmaak van digitale handtekeningen. Sommige maatschappijen ontwikkelden hun eigen software (bijvoorbeeld Isabel). *Nu is het wel zo dat niet alle softwareprogramma's een gelijkaardige bescherming en veiligheid bieden. We raden je dus ten stelligste aan te rade te gaan bij een deskundige.*

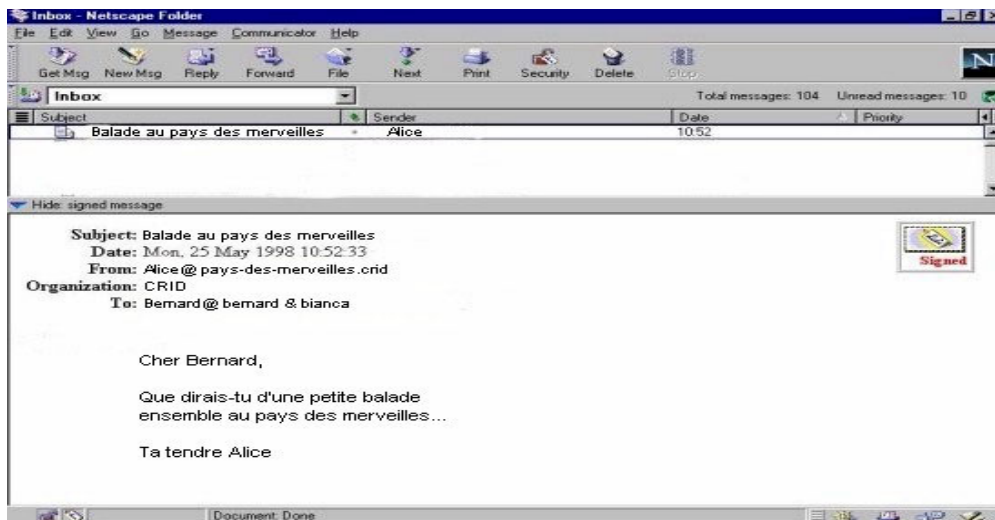
142. Hoe werkt een digitale handtekening in de praktijk ?

Zodra je een digitaal certificaat hebt bekomen, rest er je enkel nog het opgestelde document te ondertekenen of de handtekening van het ontvangen document na te gaan. In de praktijk verricht de software automatisch alle operaties die we hierboven theoretisch hebben uiteengezet. De ingewikkeldheid van het mechanisme wordt verborgen door de software-interface.

Nemen we opnieuw het voorbeeld van Marleen die een bericht naar Johan stuurt. Ze moet enkel het bericht opstellen, de optie “ondertekenen” aanvinken en het bericht versturen (“send”).



Als Johan het bericht ontvangt, moet hij alleen maar nagaan of het “icoon van de handtekening” zich in de rechter bovenhoek van het scherm bevindt, hetgeen erop wijst dat het document werd ondertekend en dat de procedure voor het verifiëren van de handtekening correct verliep.



Om de handtekening te kunnen verifiëren, moet de software beschikken over het certificaat van Marleen. Ofwel moet het worden gedownload vanaf het elektronisch register van de CDV, ofwel was het certificaat reeds opgeslagen in de software, in welk geval er moet worden nagegaan of het niet verstreken of ingetrokken is.

Dit is geen alleenstaand voorbeeld. Tal van andere softwareprogramma's bieden gelijkaardige functies aan, maar wel met een verschillende interface.

143. Wordt de elektronische aangetekende brief in het Belgisch recht erkend ?

Als je van plan bent een elektronische overeenkomst te sluiten, moet je niet enkel oog hebben voor de identificatie van de partijen en het behoud van de integriteit van de inhoud van het bericht. Je moet de juridische verrichting in een brede elektronische context plaatsen. Het komt er dus ook op aan een bewijs te bewaren van je bericht alsook van de datum en eventueel de ontvangst van het bericht.

Dat kan echter maar als de wetgever, naast de elektronische handtekening, ook het bestaan erkent van de elektronische aangetekende brief en hem dezelfde waarde toekent als een papieren ter post aangetekende brief. Heel wat wet- en regelgevingen bepalen namelijk dat sommige formaliteiten moeten worden vervuld via een aangetekende brief, eventueel met ontvangstbewijs (onder meer in het kader van een gerechtelijke of administratieve procedure).

Maar ook al ligt dat gebruik niet wettelijk vast, toch doe je er vaak goed aan voor belangrijke handelingen een aangetekende brief te gebruiken, zodanig dat je een bewijs hebt van het bestaan en de datum van een bericht of van enige andere kennisgeving.

In België is het gebruik van een *elektronische* aangetekende brief juridisch toegestaan. Bovendien mag je tegenwoordig een beroep doen op andere operatoren dan De Post voor de verzending van elektronische aangetekende brieven.

HOOFDSTUK IV. VERZAKINGSRECHT

144. Wat is het verzakingsrecht ?

Koop je iets op afstand, dan is het best mogelijk dat je na een tijdje om een of andere reden je aankoop betreurt: ofwel handelde je in een opwelling, ofwel lijken de aankoopvoorwaarden je alles wel beschouwd niet interessant, ofwel beantwoordt het geleverde product gewoon niet aan je verwachtingen...

Behoudens bijzondere gevallen, geeft de wet je het recht aan de overeenkomst te verzaken binnen een termijn van ten minste 7 werkdagen. Dit recht kan discretionair worden uitgeoefend: als je aan de overeenkomst verzaakt, moet je daarvoor geen reden opgeven.

145. Voor welke soort aankopen beschik ik over een verzakingsrecht ?

Behalve in de hierna uiteengezette situaties, mag je verzaken aan elke op afstand gesloten overeenkomst voor de levering van een product of dienst, op voorwaarde dat je niet beroepshalve handelt.

Toch bestaan er gevallen waar je niet over een verzakingsrecht beschikt:

- indien je de uitvoering van de dienst vraagt vooraleer de verzakingstermijn afgelopen is (bijvoorbeeld wanneer je toegang wil tot een databank en onmiddellijk de gevraagde informatie wenst te raadplegen, zonder het einde van de verzakingstermijn af te wachten);
- indien je producten bestelt die volgens jouw wensen vervaardigd zijn of die voor jou werden gepersonaliseerd (bijvoorbeeld een op bestelling vervaardigd kledingstuk, een product met je naam erop, op maat gemaakte inbouwmeubelen voor je keuken, ...);
- indien de gekochte producten niet kunnen worden teruggestuurd of snel kunnen bederven of verouderen (bijvoorbeeld aan bederf onderhevig voedsel, verse producten, enz.);
- indien je kranten, tijdschriften of magazines koopt;
- indien je online weddingschappen aangaat of loterijbriefjes koopt;
- indien je een muziek- of video-opname of informaticabestanden ontzegt (bv. dvd, cd, cd-rom, videocassette, ...). Als je daarentegen niet aan het veiligheidssysteem raakt, dan kun je aan de overeenkomst verzaken en het product ongeschonden teruggeven. Die uitzondering geldt eveneens voor online downloadbare opnames en bestanden die beschermd zijn met toegangssleutels of veiligheidssystemen.

Ten slotte, indien je overeenkomst financiële diensten betreft (bank, verzekeringen, financiële investeringen, beursoperaties, pensioenfondsen), beschik je tot nu toe niet over een verzakingsrecht. Een Europese richtlijn betreffende de verkoop op afstand van financiële diensten aan consumenten werd onlangs gepubliceerd en zal eerlang in het Belgische recht worden omgezet. Die richtlijn voorziet onder andere in een verzakingsrecht voor bepaalde financiële diensten, volgens bijzondere regels.

146. Hoe kan ik weten of ik over een verzakingsrecht beschik ?

De verkoper is verplicht je in te lichten over het bestaan of niet-bestaan van een verzakingsrecht. Hij moet je die informatie geven voordat de overeenkomst wordt gesloten (ze moet bv. op de site van de verkoper staan) (zie hierboven nr. 125).

Bovendien moet die informatie worden herhaald na het sluiten van de overeenkomst, bij de bevestiging van bepaalde gegevens (bv. in een e-mail of op de factuur die bij het geleverde product is gevoegd) (zie hierboven nr. 127).

147. Wat kan ik doen als ik niet werd ingelicht over mijn verzakingsrecht ?

De wet voorziet in sancties wanneer de verkoper zijn verplichting om informatie te verschaffen over het verzakingsrecht niet nakomt.

Indien de verkoper je, vóór het sluiten van de overeenkomst, niet meldde dat je over *geen verzakingsrecht* beschikt (zie hierboven nr.125), bedraagt de verzakingstermijn 3 maanden in plaats van 7 dagen (zie hieronder nr. 148).

Indien de *verzakingsclausule*, na het sluiten van de overeenkomst, niet is opgenomen in het document dat een aantal inlichtingen bevestigt (zie hieronder nr. 127), stelt de wet de overeenkomst gelijk aan een gedwongen verkoop. Met andere woorden, alles verloopt alsof het product of de dienst werd geleverd zonder dat je het vooraf hebt gevraagd : je bent er niet toe gehouden het product te betalen of terug te geven.

148. Binnen welke termijn mag ik aan een overeenkomst verzaken ?

In principe beschik je over een verzakingstermijn van minimum **7 werkdagen**. Dat betekent dat je de verkoper vóór het verstrijken van die termijn moet verwittigen dat je de bedoeling hebt de overeenkomst op te zeggen (zie hieronder nr. 152).

De verkoper mag die termijn verlengen indien hij dit wenst, maar hij mag hem niet verkorten.

Het begin van de termijn verschilt naargelang de overeenkomst de levering van een product of van een dienst betreft :

- voor producten begint de termijn te lopen de dag na de leveringsdag. A fortiori, mag je aan de overeenkomst verzaken nog voor het product geleverd is (bv. wanneer de verkoper te lang draait om de overeenkomst uit te voeren en je aan de overeenkomst wil verzaken om een bestelling te plaatsen bij een andere verkoper) ;
- voor producten met opeenvolgende leveringen begint de termijn te lopen de dag na de eerste levering ;
- voor diensten begint de termijn :
 - de dag na het sluiten van de overeenkomst,
 - of
 - de dag nadat de verkoper je een aantal gegevens bevestigde, na het sluiten van de overeenkomst (zie hierboven nr. 127) (je sluit bijvoorbeeld een dienstverleningsovereenkomst die slechts over 4 maanden zal worden uitgevoerd.

Een maand na het sluiten van de overeenkomst bevestigt de verkoper de door de wet vereiste gegevens. De verzakingstermijn begint bijgevolg te lopen de dag nadat hij de gegevens bevestigde en niet de dag na het sluiten van de overeenkomst). In dit geval mag de termijn geenszins langer zijn dan drie maanden vanaf de dag van het sluiten van de overeenkomst.

De verzakingstermijn mag echter met **drie maanden** worden verlengd vanaf de dag na de levering van het product of na het sluiten van de dienstverleningsovereenkomst :

- wanneer de verkoper je vóór het sluiten van de overeenkomst niet meedeelde dat je niet over een verzakingsrecht beschikt (zie hierboven nrs. 125, 146 en 147) ;
- wanneer de verkoper, na het sluiten van de overeenkomst, zijn verplichting om de door de wet vereiste inlichtingen te bevestigen niet nakwam (zie hierboven nr. 127).

In dit laatste geval, wanneer de ontbrekende inlichtingen je nadien worden verstrekt binnen die termijn van drie maanden, begint de gewone termijn van 7 dagen opnieuw te lopen. Bijgevolg mag je aan de overeenkomst slechts verzaken binnen **7 werkdagen**, vanaf de dag nadat je de ontbrekende inlichtingen kreeg.

Je moet de verkoper meedelen dat je afziet van de overeenkomst vooraleer de termijn verlopen is.

149. Mag ik aan de overeenkomst verzaken indien ik de prijs reeds betaalde ?

Ja. Je moet weten dat geen betaling noch voorschot mag worden *geëist* vóór de verzakingstermijn verlopen is (zie hieronder nr. 155).

Niettemin mag je het product of de dienst onmiddellijk betalen indien je dat wenst. In dat geval moet de verkoper je de gestorte bedragen kosteloos terugbetalen als je je verzakingsrecht doet gelden. Die terugbetaling moet ten laatste binnen 30 dagen na je verzaking gebeuren (zie hieronder nr. 175 e.v.).

150. Moet ik een vergoeding betalen om aan de overeenkomst te kunnen verzaken ?

Neen. Het verzakingsrecht is **gratis** : het wordt uitgeoefend zonder enige vergoeding of straf.

De enige kosten die je moet dragen, zijn de kosten voor terugzending van het product aan de verkoper (d.w.z. de portokosten).

In twee gevallen moet je zelfs geen terugzendingskosten betalen :

- indien het geleverde product of de verleende dienst niet beantwoordt aan de beschrijving van het aanbod (zie hieronder nr. 172) ;
- indien de verkoper zijn verplichting van informatie vóór of na het sluiten van de overeenkomst niet nakwam (zie hierboven nrs. 125 en 127).

151. Mag ik aan de aankoop van een product of dienst verzaken wanneer ik een lening aanging om de betaling te financieren ? Wat gebeurt er met mijn kredietovereenkomst bij verzaking ?

Ja, je mag aan een op afstand gesloten overeenkomst verzaken, zelfs indien je een lening aanging om de betaling van de prijs van het product of de dienst volledig of gedeeltelijk te financieren.

In dat geval mag je ook, zonder kosten of vergoeding, van de kredietovereenkomst afzien indien deze :

- rechtstreeks met de product- of dienstverlener werd gesloten ;
of
- werd gesloten met een derde, indien er tussen die derde en de verkoper een akkoord bestaat om voor de financiering van de geleverde producten of diensten te zorgen.

In dit geval gebeurt de verzaking aan de kredietovereenkomst binnen de termijnen en volgens regels bepaald voor de overeenkomsten op afstand, zoals in bovenstaande punten uitgelegd.

152. Hoe moet ik de verkoper laten weten dat ik aan de overeenkomst verzaak ?

De wet bevat geen procedure om de verzaking aan de overeenkomst mee te delen.

Je kunt dus om het even welk middel gebruiken om de verkoper mee te delen dat je aan de overeenkomst verzaakt (gewone brief, fax of e-mail).

Daar de verzaking binnen de door de wet voorgeschreven termijnen moet gebeuren, doe je er niettemin goed aan een verzendingsbewijs te bewaren, voor het geval de verkoper te kwader trouw is (en beweert geen brief of e-mail te hebben gekregen of die na het verstrijken van de termijn te hebben gekregen).

Stuur dus liefst een aangetekende brief om je verzaking aan de overeenkomst mee te delen. Weet dat de certificatedienstverleners tegenwoordig diensten voor elektronische aangetekende brieven aanbieden (zie hierboven nr.143).

153. Welke zijn mijn verplichtingen als ik aan de overeenkomst verzaak ?

Wanneer je beslist aan de overeenkomst te verzaken, moet je dit gewoon meedelen aan de verkoper (zie hierboven nr. 152) en hem het geleverde product terugsturen (de verkoper kan je ook producten leveren ter uitvoering van een dienstverleningsovereenkomst).

De kosten voor terugzending van het product zijn voor jouw rekening, tenzij :

- het geleverde product of de verleende dienst niet overeenstemt met de beschrijving van het aanbod ;
- de verkoper zijn informatieplicht niet nakwam voor of na het sluiten van de overeenkomst (zie hierboven nrs.125 en 127).

154. Welke verplichtingen heeft de verkoper wanneer ik aan de overeenkomst verzaak ?

Indien je je verzakingsrecht uitoefent, moet de verkoper je een reeds betaalde prijs of voorschot terugbetalen. Die terugbetaling moet worden uitgevoerd binnen 30 dagen na de verzaking (zie hieronder nr. 175 e.v.). Van die terugbetaling mogen geen kosten worden afgehouden.

HOOFDSTUK V. BETALING

155. Ben ik verplicht te betalen vóór de levering ?

Neen ! Geen betaling noch voorschot mag worden *geëist* vóór de verzakingstermijn van 7 dagen verlopen is (zie hierboven nr. 144 e.v.).

Dat betekent dat de verkoper je in principe niet mag verplichten te betalen voor het verstrijken van de termijn ! Hij moet je de keuze laten tussen een voorafbetaling (bv. online met kredietkaart) en een achterafbetaling (d.w.z. na het verlopen van de verzakingstermijn, bv. met een bankoverschrijving binnen 15 dagen na de levering). Hij mag in geen geval de levering onderbreken zolang je niet betaald hebt.

Als je over een verzakingsrecht beschikt, ben je vrij om het product of de dienst onmiddellijk of niet onmiddellijk te betalen. Betaal je onmiddellijk, dan bewaar je het recht om aan de overeenkomst te verzaken binnen de wettelijk vastgestelde termijn en worden je alle gestorte bedragen terugbetaald (zie hierboven nr. 149).

Beschik je daarentegen niet over een verzakingsrecht voor het product dat of de dienst die je aankoopt (zie hierboven nr. 145), dan mag de verkoper eisen dat je onmiddellijk betaalt vóór het uitvoeren van de overeenkomst. Dat is bijvoorbeeld het geval bij de aankoop van aan bederf onderhevige producten, een magazine of tijdschrift ...

Welnu, in de praktijk geven sommige verkopers je die keuze niet en dringen ze je een vervroegde betaling op, zonder dewelke het technisch onmogelijk is bij hen te bestellen ! (bv. de bestelprocedure is zo geprogrammeerd dat enkel per kredietkaart voorafbetaalde bestellingen worden geregistreerd, ofwel voert de verkoper de bestelling pas uit als hij je cheque heeft gekregen of als het bedrag is overgeschreven). Zij hebben daartoe het recht niet.

Die met de wet strijdige houding is te verklaren door het feit dat sommige verkopers vrezen dat hun klanten niet zullen betalen. Zelf ben je misschien weinig geneigd om vooraf te betalen aan een onbekende verkoper waarvan je niet weet of hij wel degelijk de bestelling zal uitvoeren (zie hieronder nrs. 162 en 169).

Laat je echter niet overmeesteren door paranoïde gevoelens : niet elke verkoper is een potentiële oplichter die klaar staat om je lieve centen op te strijken en met de noorderzon te verdwijnen. De grote meerderheid van de verkopers die hun diensten op de netwerken aanbieden, zijn ernstig en betrouwbaar en weten dat zij alleen door zo'n ingesteldheid hun zaak kunnen uitbreiden.

De meeste e-commercesites bevatten duidelijke informatie over de betalings- en terugbetalingsformaliteiten. Bovendien volgen tal van verkopers een gedragscode met eerlijke regels inzake betaling en terugbetaling (zie hieronder nr. 179 e.v.). Vaak wordt hun een kwaliteitslabel toegekend, eventueel onder toezicht van een labelinginstantie, als ze zo'n code in acht nemen (zie hieronder nr. 182 e.v.). Zo krijgen de verkopers die het beveiligd betalingssysteem Banxafe gebruiken (zie hieronder nrs. 159 en 163) een label van Banxafe. Bij niet-eerbiediging van sommige betalings- en terugbetalingsregels wordt hun het recht ontnomen om het Banxafe-systeem verder te gebruiken.

Buiten die privé-initiatieven zal een koninklijk besluit worden uitgevaardigd met betrouwbaarheidscriteria die de verkopers moeten volgen om een betaling te mogen eisen vóór het verstrijken van de verzakingstermijn van 7 dagen. Het is de bedoeling criteria vast te leggen waarbij wordt gegarandeerd dat de klant zijn geld terugkrijgt als de bestelling niet

wordt uitgevoerd. Hierbij zou een gedragscode of kwaliteitslabel wettelijk worden vastgelegd om de privé-initiatieven op dat gebied kracht bij te zetten. Tot nog toe bestaat zo'n koninklijk besluit echter nog niet.

156. Welke betaalmiddelen kan ik op de netwerken gebruiken ?

De onlinebetaalmiddelen zijn legio en verschillen van de ene verkoper tot de andere. Kijk dus goed uit je doppen vóór je iets aankoopt en ga na of je wel over de nodige software en hardware beschikt om elektronisch te betalen. Ter herinnering : de verkoper is verplicht je vóór en na het sluiten van de overeenkomst in te lichten over de geboden betaalmogelijkheden (zie hierboven nrs. 125 en 127).

In de hierna volgende vragen (nrs. 157 tot 167) vind je meer informatie over de diverse middelen om je aankopen op het internet te vereffenen, met de voor- en nadelen, alsook over de uitrusting die je daarvoor eventueel nodig hebt.

157. Kan ik met een kredietkaart betalen ?

Natuurlijk, dat is het meest praktische en meest verspreide onlinebetaalmiddel. Als je de bestelbon invult, moet je de verkoper het nummer en de vervaldatum van je kredietkaart meedelen. Bij ontvangst van je bestelling neemt de verkoper contact op met de uitgever van je kredietkaart, die de betaling toestaat nadat hij heeft nagegaan of de meegedeelde inlichtingen juist zijn.

Dit betaalmiddel is eenvoudig (het vereist geen speciale informatica-uitrusting), het werkt snel en het wordt aanvaard voor de meeste internationale verrichtingen (je kunt er in heel veel munten mee betalen).

Heel wat mensen aarzelen nog om met hun kredietkaart online te betalen, omdat het systeem een aantal risico's inhoudt (zie hieronder nr. 158). De uitgevers van kredietkaarten hebben echter doeltreffende technische methodes uitgewerkt om onlinebetalingen te beveiligen (zie hieronder nr. 159). *Ze raden trouwens uit één mond betalingen met kredietkaarten op niet-beveiligde e-commercesites af !* Juridisch ben je wel 100% beschermd bij bedrieglijk gebruik van je kredietkaart (zie hieronder nr. 160).

158. Welke risico's zitten er aan het gebruik van een kredietkaart op de netwerken ?

Misschien aarzel je om je kredietkaart online te gebruiken als je denkt aan de hele heisa over hackers en andere informaticaboeven. Maar zo erg is het nu ook weer niet ! Tegenwoordig bestaan er namelijk technieken en afweermiddelen die een hoge graad van veiligheid waarborgen voor onlinebetalingen. Toegegeven : inzake veiligheid op de netwerken bestaat er geen nulrisico.

Het eerste probleem met kredietkaartbetalingen is dat het nummer en de vervaldatum van je kaart volstaan om op jouw kosten aankopen te doen. Om te betalen met een kredietkaart hoef je je namelijk niet te identificeren als houder van die kaart noch een geheime code in te voeren. Die gegevens mogen dus niet in handen van derden vallen. Let er dus op dat de overdracht van die gegevens beveiligd is door technische middelen (zie hieronder nr. 159).

Overigens bewaren sommige verkopers die informatie in gegevensbanken, in het bijzonder als je op hun site als klant geregistreerd wordt. Zo'n systeem maakt het je wel gemakkelijk, want je hoeft niet telkens opnieuw al je persoonsgegevens in te voeren bij elke bestelling.

Maar het gevaar bestaat dat een of andere kraker erin slaagt binnen te dringen in de database van de verkoper en die gegevens bemachtigt (zie hieronder nr. 104 e.v.). Die database moet dus worden beveiligd. Ga op de site van de verkoper na hoe lang je bankgegevens bewaard worden en of zijn database beveiligd is tegen indringers. Om zo'n problemen te vermijden, bewaren sommige verkopers die gegevens nooit langer dan de tijd die nodig is om de betaling te registreren.

Ten slotte kan ook de verkoper zelf bedrog plegen : dankzij je bankgegevens zou hij een hoger bedrag dan dat van je aankopen van je rekening kunnen halen of verscheidene betalingen te zijnen gunste verrichten. Dat risico is echter inherent aan het gebruik van om het even welke kredietkaart, zelfs buiten de netwerken (het bestaat trouwens ook als je je bankgegevens per telefoon of per fax doorgeeft). Bovendien is elke in Europa gevestigde verkoper voortaan verplicht op zijn site een aantal gegevens over zijn identiteit en beroepsactiviteit te vermelden en kan hij niet zo gemakkelijk meer het hazenpad kiezen (zie hierboven nr. 122). Ten slotte volgen tal van verkopers gedragscodes of laten zij hun site labelen om hun klanten een waarborg te bieden van hun ernst en betrouwbaarheid (zie hieronder nr. 179 e.v.).

Heeft de verkoper geen veiligheidssysteem ingebouwd of identificeert hij zich niet op correcte wijze, dan raden wij je ten stelligste af online te betalen met je kredietkaart. Als je je aankopen met je kredietkaart wilt betalen, doe je er dus goed aan eerst te informeren naar de veiligheidsmaatregelen die de verkoper heeft genomen ; zo vermijd je dat je kaart met bedrieglijk opzet wordt gebruikt.

159. Met welke technische middelen worden kredietkaartbetalingen op de netwerken beveiligd ?

Er bestaan diverse systemen om onlinebetalingen met kredietkaart te beveiligen. Als je je aankopen met je kredietkaart wil betalen, informeer dan eerst naar de veiligheidsmaatregelen die de verkoper heeft genomen ; zo vermijd je dat je kaart met bedrieglijk opzet wordt gebruikt. Heeft de verkoper op zijn site geen veiligheidssysteem ingebouwd, dan raden wij je af online te betalen met je kredietkaart. Een verkoper die geen technische maatregelen neemt om je betalingen te beveiligen, komt immers niet ernstig en betrouwbaar over.

Er bestaan twee grote standaarden voor de beveiliging van betalingen op netwerken : SSL en SET. In België worden die technieken onder meer aangewend voor een nieuw beveiligd betaalsysteem, Banxafe genoemd, dat we hieronder kort voorstellen.

SSL (Secure Sockets Layer)

Dit is een protocol dat zorgt voor de betrouwbaarheid en integriteit van online overgedragen gegevens door het coderen van die gegevens (via een digitale handtekening). Dit efficiënt systeem wordt gebruikt door de grote meerderheid van de ernstige en betrouwbare providers. Op hun site vind je daarover duidelijke informatie.

Je hoeft zelf niets te doen om de overdracht van je bankgegevens te beschermen, want het beveiligingssysteem maakt al deel uit van de huidige navigatiesystemen Netscape en Internet Explorer. Alles gebeurt automatisch. Als er een gesloten hangslot verschijnt in de rechter benedenhoek van je navigatievenster en het URL-adres met de letters "https" begint, weet je dat je gegevens veilig overgedragen zijn.

Dankzij die standaard circuleren je bankgegevens - kaartnummer en vervaldatum - in gecodeerde vorm op de netwerken. Op die manier zijn ze enkel toegankelijk voor de

provider. Als die gegevens tijdens de overdracht door een derde worden onderschept, dan kan hij ze niet ontcijferen. Dat systeem garandeert de vertrouwelijkheid bij de overdracht van bankgegevens op netwerken, maar lost het probleem van de bewaring van je bankgegevens door de provider niet op.

SET (Secure Electronic Transaction)

Deze standaard werd specifiek ontworpen om onlinekaartbetalingen te beveiligen. Hij is veiliger dan de SSL omdat de provider geen toegang heeft tot jouw bankgegevens. Die gegevens worden namelijk rechtstreeks in gecodeerde vorm naar de uitgever van jouw kredietkaart gestuurd. Alleen hij kan ze ontcijferen, zodat hij de geldigheid van de verrichting kan nagaan. Zo voorkom je dat jouw bankgegevens, die de provider in een database heeft opgeslagen, gekraakt worden (of met oneerlijke bedoelingen worden gebruikt door de provider zelf). Ten slotte wordt je persoonlijke levenssfeer gerespecteerd, aangezien de uitgever van de kaart geen toegang heeft tot de details van je bestelling.

Met de SET-standaard worden zowel jij als de verkoper op de netwerken geïdentificeerd dankzij een certificaat. Zo kan niemand anders dan jij met jouw kredietkaart betalen.

Een concrete toepassing in België : Banxafe

Banksys ontwikkelde een veilig betaalsysteem in samenwerking met BCC (*Bank Card Company*, nl. Visa en MasterCard) en een aantal Belgische banken (Bacob, BBL, Dexia, Fortis en KBC). Dankzij dat systeem, Banxafe genaamd, kun je 100% veilig online betalen met je kredietkaart. Het systeem wordt ook gebruikt met een chipkaartlezer voor internetbetalingen door middel van een debetkaart van Bancontact/Mister Cash (zie hieronder nr. 163).

Het is heel gebruiksvriendelijk en je moet er geen software op je computer voor installeren. Dit betaalsysteem wordt aangeboden op de Belgische sites die aangesloten zijn bij Banxafe (en waarvan de lijst te vinden is op de site www.banxafe.be). Je kunt het ook gebruiken op buitenlandse sites die werken met de SSL- en SET-standaarden (de logo's "SET" of "MasterCard SET" moeten op de site verschijnen op het moment van de betaling) of met de 3D Secure-standaard.

Als je voor een beveiligde betaling via Banxafe kiest, klik je in feite op een hyperlink naar de site van Banksys. Je voert dan je bankgegevens (kaartnummer, vervaldatum en soort kaart) niet meer in op de site van de verkoper, maar op de beveiligde server van Banksys. Zo krijgen noch de verkoper noch een eventuele *hacker* toegang tot je gegevens. Vervolgens bevestigt Banksys aan de verkoper dat je betaling geldig werd geregistreerd. Wil je meer weten over die nieuwe betaalmethode, surf dan naar www.banxafe.be en www.mybanxafe.be.

160. Moet ik de gevolgen dragen van het feit dat iemand met mijn kredietkaart bedrog pleegt op de netwerken ?

Neen !

De meeste mensen menen dat zij de financiële gevolgen moeten dragen van een bedrieglijk gebruik van hun kredietkaart. Dat is niet waar ! In zo'n geval ben je beschermd door de wet : niet jij, maar de uitgever van de kredietkaart draagt de gevolgen van een dergelijk bedrog.

De wet bepaalt namelijk dat je niet aansprakelijk bent - met andere woorden dat je geen schade moet dragen - als je kredietkaart buiten jouw weten op afstand wordt gebruikt (d.w.z. als ze niet door jou persoonlijk wordt aangeboden : op netwerken, per telefoon, per fax, ...) en zonder elektronische identificatie (d.w.z. zonder aanwending van een systeem voor het aanmaken van een elektronische handtekening of enig ander veiligheidssysteem). Enkel het gebruik van een vertrouwelijke code, zonder ander procédé voor elektronische identificatie (zonder digitale handtekening) volstaat niet om je aansprakelijk te stellen.

Met andere woorden : als iemand met bedrieglijk opzet het nummer en de vervaldatum van je kredietkaart gebruikt voor onlineaankopen, moet je daarvan de financiële gevolgen niet dragen. Tenzij je met bedrieglijk opzet handelt (bv. je geeft je kredietkaart aan iemand en meldt nadien aan de uitgever dat je ze verloren bent of dat ze gestolen is ; of je meldt aan de uitgever dat je ze verloren bent of dat ze gestolen is en je gebruikt ze nadien zelf).

Bijgevolg mag je de annulatie aanvragen van een betaling die werd uitgevoerd ten gevolge van bedrieglijke praktijken (zie hieronder nr. 161). De uitgever is verplicht je al het geld dat op die manier van je rekening werd gehaald zo spoedig mogelijk terug te betalen.

Hiermee wou de wetgever de uitgevers van kredietkaarten verplichten systemen uit te werken die een veilig gebruik van kredietkaarten op netwerken garanderen. Dat blijkt te werken, want inzake bescherming van overgedragen bankgegevens werd de jongste jaren flink wat technische vooruitgang geboekt onder impuls van de uitgevers van kredietkaarten (zie hierboven nr. 159).

161. Wat moet ik doen als iemand mijn kredietkaart met bedrieglijk opzet gebruikt ?

Werd je kredietkaart gestolen of ben je ze verloren, verwittig dan onmiddellijk de uitgever van je kaart. Je kunt daarvoor 24 uur op 24 terecht op een speciaal nummer (het Card Stop-nummer van BCC voor Visa en MasterCard is bijvoorbeeld : 070 344.344).

Merk je op het uittreksel van je bankkaartverrichtingen vergissingen, onregelmatigheden of operaties die zonder jouw toestemming werden verricht, verwittig dan onmiddellijk je kredietkaartuitgever. Bij hem kun je ook terecht op een speciaal nummer waar je elk frauduleus gebruik van je kaart kunt melden (bij BCC bv. kan dat telefonisch op het nummer 02 205.87.87 of per fax op het nummer 02 205.81.08). Na een snel onderzoek betaalt hij je de onrechtmatig geïnde bedragen zo spoedig mogelijk terug.

162. Wat moet ik doen als ik vooraf betaalde met mijn kredietkaart en de verkoper de overeenkomst niet nakomt ?

Als je vooraf betaalde met je kredietkaart en de verkoper draait om je bestelling uit te voeren, hoef je niet te panikeren ! Neem eerst contact op met hem om uitleg te vragen (zie hieronder nr. 169).

Antwoordt hij niet of is hij duidelijk niet bereid je geld terug te geven, dan kun je ook contact opnemen met de uitgever van je kredietkaart. Misschien geeft hij je de mogelijkheid om bij hem een betwistingprocedure in te leiden bij niet-nakoming van de overeenkomst waarvoor geld van je rekening werd gehaald. Je moet wel weten dat de wet de uitgever niet verplicht dergelijke dienst aan te bieden. Je kredietkaartuitgever is namelijk slechts een betalingstussenpersoon, die zich niet met je verrichtingen mag bemoeien als de levering niet of met vertraging wordt uitgevoerd en zeker niet als de levering niet beantwoordt aan wat werd overeengekomen. Informeer dus bij hem over de oplossingen die hij aanreikt.

Vaak hebben de uitgevers van kredietkaarten een betwistingsprocedure uitgewerkt. Als dat het geval is, verstrek dan zorgvuldig alle details over de verrichting die je betwist. Heel nuttig is bijvoorbeeld een kopie van het uittreksel van je bankkaartbetalingen, dat de uitgever je regelmatig verstrekt (vaak eenmaal per maand) en waarop je de betwiste verrichting aanduidt. Verschaf ook alle bewijsmiddelen waarover je beschikt (briefwisseling met de verkoper bijvoorbeeld). Belangrijk is ook het ontvangstbewijs van de bestelling dat de verkoper verplicht is je te sturen (zie hierboven 127). Bij ontvangst van je betwisting neemt de uitgever van je kredietkaart zelf contact op met de verkoper om hem uitleg te vragen.

163. Mag ik met mijn debetkaart van Bancontact / Mister Cash betalen ?

Op sommige sites kun je betalen met je debetkaart (Bancontact/MisterCash) dankzij het door Banksys ontwikkelde Banxafe-systeem (zie hieronder nr. 159).

Om op het internet met een debetkaart te kunnen betalen, moet je beschikken over een kaartlezer (een behuizing met scherm en toetsenbord waarin je je chipkaart kunt steken) die met je computer verbonden is. Zo'n lezer (C-ZAM/PC) kun je aankopen bij je bank (tegen 19 euro) of in sommige winkels (waarvan de lijst te vinden is op de webstek www.banxafe.be, tegen ongeveer 50 euro in een meer gesofistikeerde versie). Op je computer moet je ook een software installeren : de "elektronische portefeuille" (of *banxafe wallet*, die op de installatie-cd-rom staat die samen met de kaartlezer geleverd wordt).

Het systeem werkt zoals een gewone winkel : zodra je je artikelen gekozen hebt, opteer je voor Bancontact en de verkoper stuurt je elektronisch alle informatie die nodig is voor de betaling (product, prijs, ...). Om jezelf te identificeren, voer je een eerste maal de geheime code van je kaart in via het toetsenbord van de lezer. Het bedrag van je aankopen verschijnt dan op de kaartlezer en dan moet je enkel nog het bedrag valideren door een tweede maal je geheime code in te voeren. Je geheime code transiteert in geen geval op de netwerken ! Hij verlaat zelfs de lezer niet.

Dankzij de kaartlezer kun je ook je Protonkaart online heropladen. Betalingen met Proton daarentegen zijn niet mogelijk op het internet.

Wil je meer weten over die betaalmethode, surf dan naar www.banxafe.be en www.mybanxafe.be.

164. Kan ik rechtstreeks op de site betalen met een elektronische overschrijving ?

Sommige verkopers geven je de mogelijkheid om je aankopen rechtstreeks op hun site te vereffenen met een elektronische overschrijving. Dat systeem verschilt van een betaling met een klassieke overschrijving (op papier, via *selfbanking*, *phonebanking* of *homebanking*), doordat de betaling maar enkele minuten in beslag neemt in plaats van verschillende dagen.

Om dat betaalsysteem te kunnen gebruiken, moet je computer uitgerust zijn met een *homebankingsysteem*, dat je bank je kan leveren. Met om het even welke *homebankingsoftware* kun je thuis overschrijvingen maken, op dezelfde manier als met de *selfbankingtoestellen*. Je kunt echter niet met alle softwareprogramma's *rechtstreeks* een elektronische overschrijving maken *op een website*. Daartoe moet je bank je die dienst verschaffen.

Zo biedt ING thans die mogelijkheid via een dienst die Home'Pay wordt genoemd (www.bbl.be/homebank/fr en www.bblshoppingmall.be).

Bovendien kun je die betaalwijze slechts gebruiken bij verkopers die een overeenkomst hebben aangegaan met jouw bank om een verbinding te maken tussen hun site voor elektronische handel en het *homebanking*platform van je bank.

Concreet : als de site die je bezoekt je de mogelijkheid biedt om je aankopen op die manier te betalen en je over de nodige uitrusting beschikt, ga je als volgt tewerk. Wens je met een elektronische overschrijving te betalen op de site, klik dan op de link die rechtstreeks verwijst naar het *homebanking*platform van je bankinstelling, waar je een kant-en-klare overschrijving op naam van de verkoper kunt vinden. Dan moet je alleen nog die overschrijving valideren door middel van een vertrouwelijke code. Je bank meldt aan de verkoper dat je betaling wordt uitgevoerd.

Dat systeem is zowel eenvoudig als veilig, vermits je rechtstreeks in verbinding staat met je bank, op een beveiligd *homebanking*platform, zonder dat je bankgegevens op netwerken circuleren. Momenteel wordt dat systeem echter enkel tussen banken en verkopers van ons land gebruikt en kun je er geen internationale betalingen mee doen.

165. Kan ik met een bankoverschrijving betalen ?

Soms kun je ook je aankopen betalen met een gewone overschrijving (op papier), met de klassieke *selfbanking*, *phonebanking* of *homebanking* (niet te verwarren met de elektronische overschrijving die je rechtstreeks op de site van de verkoper kunt verrichten : zie hierboven nr. 164). Vergeet niet het referentienummer van de bestelling duidelijk te vermelden.

Sommige sites bieden je de mogelijkheid met een overschrijving te betalen na ontvangst van je bestelling, wat heel handig is. Uit vrees voor wanbetalingen aanvaarden veel sites overschrijvingen enkel bij voorafbetalingen. In dat geval wordt je bestelling pas uitgevoerd na ontvangst en registratie van je betaling, wat de leveringstermijn kan verlengen. Bovendien is die formule niet voordelig voor grensoverschrijdende aankopen, gezien de hoge bankkosten die gepaard gaan met internationale overschrijvingen.

166. Kan ik met een cheque betalen ?

Bij sommige verkopers mag je je aankopen betalen met een bankcheque, die je door *De Post* wordt toegestuurd. Indien je voor die betaalwijze kiest, dan worden de praktische inlichtingen over de betaling (gegevens die op de cheque moeten voorkomen, verzendingsadres van de cheque, voorwaarden voor de aanvaarding, ...) je na de bestelling meegedeeld, via een webpagina en/of een e-mail waarbij de registratie van je bestelling wordt bevestigd.

Zo'n formule kan handig zijn als je online wilt betalen. Ze is echter beperkt tot ons land, aangezien handelaars doorgaans geen eurocheques aanvaarden (sinds 1 januari 2002 worden eurocheques immers niet meer gewaarborgd). Als de verkoper voorstelt vooraf met een cheque te betalen, dan wordt de leveringstermijn bovendien verlengd, aangezien de verkoper zal wachten op de betaling vooraleer de bestelling op te sturen.

167. Kan ik bij de levering betalen ?

Sommige verkopers geven je de mogelijkheid het product bij de levering te betalen. Zo kun je rechtstreeks betalen aan de persoon die het product thuis bezorgt (contant, per cheque

of eventueel met maaltijdcheques of met je kredietkaart). Soms moet je de bestelling zelf in ontvangst gaan nemen op een of ander afhaalpunt (benzinestation, supermarkt, ...), waar je je aankopen aan de kassa kunt betalen. Die formule wordt veel gebruikt in de voedingssector (onlinesupermarkt, traiteur die aan huis levert, pizzabezorger, enz).

Betalen bij de levering kan handig zijn als je geen ander betaalmiddel hebt of als je ertegenop ziet je kredietkaart op netwerken te gebruiken, ondanks de technische en juridische beveiligingen die er nu bestaan (zie hieronder nr. 159 e.v.).

Het systeem is evenwel lang niet veralgemeend op de netwerken en kan - om duidelijke praktische redenen - niet worden gebruikt voor internationale aankopen. Bovendien worden je daarvoor vaak bijkomende kosten aangerekend. Ook moet je aanwezig zijn op het ogenblik van de levering of moet je je verplaatsen om de bestelling te gaan afhalen.

HOOFDSTUK VI. LEVERING VAN HET PRODUCT OF DIENSTVERLENING

168. Wanneer moet de verkoper de overeenkomst uitvoeren ?

De verkoper is ertoe gehouden je bestelling uit te voeren binnen een termijn van maximum 30 dagen, vanaf de dag na de dag van het plaatsen van de bestelling.

Je kan met hem ook een andere termijn bedingen, desnoods van meer dan 30 dagen.

169. Wat moet ik doen wanneer de verkoper draait om mijn bestelling uit te voeren ?

Wanneer de verkoper de bestelling niet direct uitvoert en je niets van hem hoort, hoef je niet te panikeren ! Je neemt best contact met hem op voor uitleg. Mogelijk is het bestelde product tijdelijk niet voorradig. Ofwel is het product bij de verzending zoekgeraakt ; daarvoor is de verkoper dan volledig verantwoordelijk (zie hieronder nr. 171).

Indien de verkoper na de wettelijke termijn van 30 dagen (of de met jou afgesproken termijn) je bestelling nog niet uitgevoerd heeft, is de overeenkomst van rechtswege ontbonden. Dat betekent dat je niet langer door de overeenkomst gebonden bent indien de uitvoeringstermijn voorbij is (tenzij de verkoper zijn verbintenis niet heeft kunnen uitvoeren wegens overmacht). Bij ontbinding van de overeenkomst kunnen je geen kosten of vergoeding worden aangerekend. Indien je bovendien reeds een voorschot of de hele prijs betaalde, moet de verkoper je die bedragen binnen 30 dagen volledig terugbetalen (zie hieronder nr. 175 e.v.). Ten slotte kun je hem eventueel schadevergoeding vragen indien de niet-uitvoering je schade berokkende.

Zo je het wenst, kun je echter met de verkoper de verlenging van de termijn overeenkomen.

Je bent ook niet verplicht het verstrijken van de termijn van 30 dagen af te wachten om een einde te maken aan de overeenkomst : je kunt eveneens je verzakingsrecht uitoefenen, nog vóór de levering van het product of binnen 7 werkdagen na het sluiten van de dienstverleningsovereenkomst (zie hieronder nr. 144 e.v. en inzonderheid nr. 148).

170. Wordt de overeenkomst online of offline gesloten ?

Indien de bestelling betrekking heeft op een product of een immateriële dienst (software, video of film op verzoek, raadpleging van een informatiedienst...), dan wordt de overeenkomst eveneens onmiddellijk uitgevoerd via het downloaden op netwerken.

Indien de bestelling een materieel goed betreft (boek, kledingstuk, elektrisch huishoudapparaat...) of een dienst die bestaat in de levering van een product (abonnement op een papieren tijdschrift...), dan wordt ze uitgevoerd met traditionele vervoermiddelen (pak of postcolli verzonden met het vliegtuig, de trein, het schip, langs de weg, ...).

Een overeenkomst kan dus ofwel via een netwerk worden gesloten en uitgevoerd, ofwel via een netwerk worden gesloten, maar buiten een netwerk worden uitgevoerd.

171. Moet ik betalen als het product zoek raakt of bij de levering beschadigd is ?

Neen. Het sturen van producten of van stukken die diensten vertegenwoordigen gebeurt steeds op risico van de verkoper.

Bijgevolg kan van jou geen betaling geëist worden indien het product niet aankomt. Indien je reeds de volledige prijs of een voorschot betaald hebt, moeten die bedragen worden terugbetaald (zie hieronder nr. 175).

Indien het product in slechte staat toekomt, moet de verkoper daarvan de gevolgen dragen. In de praktijk mag je het product houden en aan de verkoper een prijsvermindering vragen. Je mag het product ook terugsturen naar de verkoper, die je een nieuw product in perfecte staat moet leveren.

172. Wat moet ik doen indien het geleverde product niet beantwoordt aan de beschrijving op de site ?

Je mag de overeenkomst opzeggen binnen 7 werkdagen vanaf de dag na de leveringsdag en het niet-conforme product naar de verkoper terugsturen (zie hieronder nr. 144 e.v.). In dat geval zijn de verzendkosten ten laste van de verkoper (zie hieronder nr. 150).

173. Op welke informatie heb ik recht bij de levering ?

De verkoper moet je na het sluiten van de overeenkomst informatie geven en in elk geval ten laatste op het ogenblik van de levering van de producten (zie hierboven nr. 127).

Het betreft de volgende gegevens :

- identiteit en geografisch adres van de verkoper ;
- prijs van het product of de dienst ;
- eventuele leveringskosten ;
- wijze van betaling, levering of uitvoering van de overeenkomst ;
- geldigheidsduur van het aanbod of de prijs ;
- bij duurzame of periodieke productlevering of dienstverlening, minimumduur van de overeenkomst ;
- geografisch adres waar je een klacht kunt indienen ;
- inlichtingen over de bestaande klantenservice en commerciële waarborgen ;
- bij een overeenkomst van onbepaalde duur of van meer dan 1 jaar, de voorwaarden waaronder je de overeenkomst kunt opzeggen ;
- het al of niet bestaan van een verzakingsrecht (zie hierboven nr. 144) en de wijze waarop en de voorwaarden waaronder dit recht kan worden uitgeoefend.

In dat opzicht moet een van de volgende twee clausules in vetgedrukte letters en in een kader los van de tekst op de eerste bladzijde van het document of in ieder geval op een goed zichtbare wijze worden vermeld :

- (indien je een verzakingsrecht hebt) : "De consument heeft het recht aan de verkoper mee te delen dat hij van de aankoop afziet, zonder een boete te betalen en zonder een reden op te geven, gedurende ... werkdagen (ten minste 7 dagen) vanaf de dag die volgt op de levering van het product of op het sluiten van de dienstverleningsovereenkomst" ;

- (indien je geen verzakingsrecht hebt) : "De consument beschikt niet over het recht om van een aankoop af te zien".

Indien de verkoper je die informatie vroeger al meedeelde (bijvoorbeeld per e-mail), moet ze je bij de levering niet meer worden verstrekt.

174. Welke gevolgen heeft de levering ?

Bij de levering start de termijn waarbinnen je aan de overeenkomst mag verzaken. Vanaf de dag na de leveringsdag beschik je immers over 7 werkdagen om aan de verkoper mee te delen dat je de overeenkomst opzegt (zie hierboven nr. 148).

HOOFDSTUK VII. TERUGBETALING EN KLANTENSERVICE

175. In welke gevallen mag ik terugbetaling van mijn aankopen eisen ?

Er zijn twee gevallen waarin je de verkoper terugbetaling mag vragen :

- als je gebruik maakt van je verzakingsrecht (zie hierboven nrs. 149, 150 en 154) ;
- als de overeenkomst niet uitgevoerd werd (zie hierboven nr. 169).

Je hebt dan het recht terugbetaling te vragen van de reeds gestorte bedragen, of het nu gaat om het volledige bedrag of om een voorschot. De verkoper mag je geen kosten en andere vergoedingen aanrekenen.

176. Welke formaliteiten moet ik vervullen om terugbetaald te worden ?

Je moet contact opnemen met de verkoper en hem melden dat je de hem gestorte bedragen wilt terugbetaald krijgen. Herinner hem aan alle gegevens over je bestelling en ook aan de reeds gestorte bedragen. Bewaar een betalingsbewijs dat je hem kunt voorleggen in geval van betwisting.

Voor een terugbetalingsaanvraag is geen specifieke vorm vereist. Ze kan worden ingediend per telefoon, per fax, per e-mail of met een gewone brief. We raden je echter aan een bij *De Post* aangetekende brief of een elektronische aangetekende brief te gebruiken ; dan heb je een bewijs van je aanvraag.

Heb je met een kredietkaart betaald, neem dan contact op met de uitgever van je kaart : misschien kun je bij hem een betwistingprocedure inleiden wegens niet-nakoming van de overeenkomst waarvoor geld van je rekening werd gehaald (zie hierboven nr. 162).

177. Als ik aan de overeenkomst verzaak, binnen welke termijn moet de verkoper me dan terugbetalen ?

Als je aan de overeenkomst verzaakt, moet de terugbetaling binnen 30 dagen na de verzaking plaatsvinden.

Wordt de overeenkomst niet uitgevoerd binnen 30 dagen na verzending van je bestelling, dan wordt ze van rechtswege ontbonden en moet de terugbetaling plaatsvinden binnen 30 dagen na de ontbinding. Dit betekent dat er meer dan 60 dagen kunnen voorbijgaan tussen jouw (niet-uitgevoerde) bestelling en de terugbetaling.

178. Geldt er voor de producten en diensten die ik op het internet koop een waarborg of klantenservice ?

Ja, net als voor je aankopen in een gewone winkel kunnen je onlineaankopen worden gedekt door een waarborg en eventueel ook door klantenservice.

De verkoper is dan ook verplicht je inlichtingen te verstrekken over bestaande commerciële waarborgen en klantenservice. Die informatie moet je na het sluiten van de overeenkomst worden verstrekt (zie hierboven nr. 127).

HOOFDSTUK VIII. GEDRAGSCODES EN LABELING

179. Wat is een gedragscode ?

Probleemstelling : enerzijds moesten de diverse internetactoren lijdzaam toezien hoe een aantal duidelijk ongeoorloofde cyberpraktijken straffeloos bleven, anderzijds wilden ze hieromtrent vertrouwen inboezemen bij de consumenten. Al gauw kwamen ze dus tot het besef dat ze de potentialiteiten van het internet als nieuw sociaal-economisch medium moesten benutten om een “privé-regulering” uit te werken.

Globaal gezien bieden gedragscodes houvast aan de actoren van een bepaalde gemeenschap of sector doordat ze duidelijke “spelregels” vastleggen. Meer concreet is een gedragscode een door een instelling uitgewerkt geheel van regels die, ofschoon ze niet helemaal dwingend zijn, tot doel hebben het gedrag te begeleiden en te richten.

Geconfronteerd met een grensoverschrijdend, ondoorzichtig, veelvormig en ambivalent fenomeen als het internet, verbinden bedrijven, verenigingen en instellingen zich via gedragscodes ertoe de handelspraktijken bij te sturen of te reglementeren voor hun eigen bestwil en voor die van hun gemeenschap. Zulke gedragscodes bestaan voor diverse activiteitengebieden (reclame, direct marketing, enz.) en beogen diverse doelen (bescherming van de consumenten, van de minderjarigen, van de persoonlijke levenssfeer, enz.). Gedragscodes zijn belangrijk, want ze vaardigen een reeks zelfregulerende maatregelen uit, die de bestaande wetgeving aanvullen om te garanderen dat de bedoelde bedrijven zich loyaal en eerlijk gedragen.

Als een website een gedragscode volgt, wil hij dat over het algemeen kenbaar maken. Vaak geeft een site dit op zijn homepage aan door een icoontje, een label of een hypertextlink die naar deze gedragscode verwijzen. De site kan deze gedragscode ook opnemen in zijn algemene voorwaarden.

180. Kan ik vertrouwen hebben in een gedragscode ?

In het digitale landschap worden gedragscodes gekenmerkt door een grote verscheidenheid, zowel wat de auteurs betreft als inzake inhoud en doelpubliek. Een webstek met een gedragscode is niet noodzakelijk meer betrouwbaar dan een andere.

Doorgaans is een gedragscode niet louter de uiting van een “ethische” bewustwording van de actoren van een gemeenschap. Een gedragscode is namelijk ook een onbetwistbaar commercieel argument, een soort kijkraam op een beroep, sector of groepering.

Blijf dus waakzaam, want de kwaliteit van de gedragscodes is zeer veranderlijk... Wil je een idee hebben over de betrouwbaarheid van sommige gedragscodes, surf dan bijvoorbeeld naar *e-confidence forum*, een initiatief van de Europese Unie, op het adres <http://econfidence.jrc.it>.

181. Kan ik mij beroepen op een gedragscode ?

De juridische draagwijdte van een gedragscode valt niet makkelijk te bepalen. Heel wat gedragscodes, ethische codes en deontologische codes bevatten immers enkel aansporingen of aanbevelingen. *A priori* hebben zij dus niet dezelfde legitimiteit en rechtskracht als wetten en reglementeringen die van de overheid uitgaan.

Sommige gedragscodes voorzien in de mogelijkheid voor een derde (een gebruiker of iemand anders) om een klacht in te dienen bij de betrokken vereniging wanneer één van

haar leden zich niet houdt aan de gedragscode. Gewoonlijk wordt er dan een procedure gestart en kunnen er sancties worden genomen. Dit is een eerste soort mogelijk verhaal.

Een consument kan zich ook beroepen op de bepalingen van een gedragscode wanneer hij gerechtelijke stappen onderneemt, ongeacht de acties die door de vereniging kunnen worden genomen. Daartoe moet de professional met wie je een overeenkomst sluit, in een van de documenten die hij je bezorgt, er echter uitdrukkelijk op wijzen dat de gedragscode moet worden nageleefd. De code wordt dan een onderdeel van de overeenkomst, waarop de gebruiker kan terugvallen (bijvoorbeeld wanneer de verkoper op zijn site met een hyperlink verwijst naar die gedragscode).

Maar als er in de contractuele documenten helemaal niet verwezen wordt naar een gedragscode, dan is het niet zeker of de code enige dwingende waarde heeft en je er een beroep kan op doen om je rechtsvordering kracht bij te zetten.

182. Wat is labeling ?

Labeling is een techniek die erin bestaat een label - of etiket - aan te brengen op een website, om erop te wijzen dat die site zich aan een aantal criteria houdt. Het labelen van websites heeft tot doel het vertrouwen van de consumenten te vergroten door hun meer doorzichtigheid en waarborgen te bieden over de eerbiediging van welbepaalde normen en criteria.

Concreet zal je bij het bezoeken van een website misschien merken dat er een label is aangebracht, hetzij door de site zelf, hetzij door een derde maatschappij. Als je het label aanklikt, verschijnen er op je scherm regels over de werking van de site en kun je zien welke verbintenissen de site aangaan.

Een label heeft slechts zin indien het meer inhoudt dan alleen maar de eerbiediging van de wetgeving. Een label wijst dus niet enkel op de naleving van de wetgeving maar verschaft eveneens een toegevoegde waarde aan de reglementaire voorschriften die eenieder moet volgen. In dat opzicht kan een label dan ook synoniem zijn van “kwaliteitsstempel”.

183. Kan ik een op een website aangebracht label vertrouwen ?

Opgelet ! Een label is geen voldoende waarborg voor de kwaliteit en betrouwbaarheid van een site. Koop dus niets “blindelings” aan, enkel afgaande op de aanwezigheid van een label.

Diverse factoren moeten je duidelijkheid verschaffen over de betrouwbaarheid van een gelabelde site.

In de eerste plaats moet je de reflex hebben om het label (of de hyperlink die op de site wordt geboden) aan te klikken, zodat je kunt nagaan wat het precies inhoudt. Logischerwijze brengt de hyperlink je naar een pagina waar je alle nuttige informatie over het label aantreft.

Belangrijk is dat je weet wie aan de oorsprong van het label ligt en welke controles er bijgevolg worden uitgevoerd. Het labelen kan immers intern of extern gebeuren, naargelang een of meer derde instellingen betrokken worden bij de controle op de naleving van welbepaalde criteria. Externe labeling biedt meer waarborgen, hetzij omdat er een toevallige controle *a posteriori* wordt uitgevoerd over de naleving van die welbepaalde criteria, hetzij omdat het label wordt toegekend op basis van een controle *a priori* van de website.

In die geest nam de consumentenvereniging Test-Aankoop het initiatief om op grond van een gedragscode een labelingsysteem uit te werken, nl. de *Web Trader*. Dat labelingsysteem heeft tot doel de elektronische handel te promoten door de betrouwbaarheid en de ernst van de websites die het logo voeren te certificeren. De consument die dergelijke sites bezoekt, weet dan zeker dat die sites de *Web-Tradercode* naleven (zie http://www.budget-net.com/webtradersite/webtrader_home_be.html). Een vergelijkbaar labelinginitiatief werd opgezet door het netwerk van Kamers voor Handel en Nijverheid van België (zie <http://www.chamber-trust.be/fr/label-qui.html>).

HOOFDSTUK IX. WISSELMECHANISMEN VOOR DE REGELING VAN ONLINEGESCHILLEN

184. Wat is een wisselmechanisme voor de regeling van onlinegeschillen (ADR) ?

Het internet is een communicatieforum waarbinnen onvermijdelijk conflicten ontstaan. Die conflicten kunnen heel verscheiden zijn. Naast geschillen in het kader van een contractuele verbintenis duiken er nu ook nieuwe vormen van onlineconflicten op. Aangezien er op de netwerken geen grenzen bestaan, kunnen de bij een geschil betrokken partijen ver van elkaar wonen. Door die internationale dimensie worden de geschillen nog ingewikkelder.

Om hieraan het hoofd te bieden, zetten sommige actoren geschillenregelingsmechanismen op die zich onderscheiden van de gewone rechtswegen (hoven en rechtbanken).

Die wisselmechanismen voor de regeling van geschillen of ADR (*Alternative Dispute Resolution*) steunen op bemiddeling, verzoening, arbitrage of op een gemengde procedure. Hierbij kun je je wenden tot een persoon die een oplossing zal trachten te vinden voor het conflict of, althans, de partijen zal helpen een oplossing te vinden.

Sedert kort kun je bij sommige instellingen terecht om een geschil rechtstreeks via het internet te laten regelen. Uiteraard stellen een aantal sites voor ontvangen klachten intern te regelen en geven ze je de mogelijkheid je grieven voor te leggen aan een “hotline”. Zij verbinden zich ertoe het geschil met jou te regelen. Voor het oplossen van onlineconflicten ben je echter beter af op sites die laten bemiddelen door een derde instelling. Zo'n oplossing biedt meer waarborgen, omdat een neutrale derde bemiddelt bij de regeling van het geschil tussen de partijen.

Wend je je tot een derde om je geschil op te lossen, dan kunnen er zich verscheidene gevallen voordoen. Kies je voor een bemiddelings- of verzoeningsmechanisme, dan leg je het geschil voor aan een neutrale derde, die zal pogen communicatie tot stand te brengen tussen jou en de maatschappij of de persoon waarmee je een geschil hebt om zo tot een akkoord te komen. Heb je het eerder voor arbitrage, dan leg je het geschil voor aan een neutrale derde, de *scheidsrechter*, die zal beslissen welke oplossing moet worden aangenomen. In tegenstelling tot de verzoening en de bemiddeling moeten de conflicterende partijen zich onderwerpen aan de beslissing van de scheidsrechter.

185. Wanneer en hoe kan ik een beroep doen op dat soort mechanisme ?

Geschillenregelingsprocedures bieden een geschikte en efficiënte oplossing voor kleine geschillen. Ze vormen een alternatief bij de regeling van geschillen over kleine bedragen waarvoor een klassieke rechtsvordering te duur zou uitvallen.

Als je voor een dergelijke procedure kiest, ga dan gewoon naar een site die dat soort diensten aanbiedt en vul een onlineformulier in (zie bijvoorbeeld <http://www.ecodir.org>).

Om een beroep te kunnen doen op een wisselmechanisme voor de regeling van geschillen, moet je het akkoord hebben van de persoon waarmee je een geschil hebt. Ofwel verklaarde deze laatste op zijn site of in een brief dat hij akkoord gaat met een bemiddeling of arbitrage en dan is hij verplicht zich daaraan te onderwerpen als jij het vraagt. Ofwel ging hij vooraf geen enkele verbintenis aan, maar aanvaardt hij de bemiddelings- en arbitrageprocedure.

Er zijn wel gevallen waarin je geen beroep kunt doen op bemiddeling of arbitrage. Zo moet je voor zaken die onder de openbare orde vallen steeds naar een rechter stappen.

186. Wat zijn de voordelen van ADR ?

Vrijheid : als het geschil grensoverschrijdend is, kun je via ADR de klassieke problemen inzake rechtsbevoegdheid en toepasselijke wet omzeilen (zie hieronder nr. 190 e.v.). De partijen mogen vrij het aantal scheidsrechters, de mogelijkheid van verhaal, enz. bepalen.

Soepelheid : deze oplossing is soepeler dan de traditionele rechtspraak. Je kunt op elk ogenblik tot een vergelijk komen met je “tegenstander” en de procedure stopzetten. Hier zijn de partijen veel meer betrokken bij het samen zoeken naar een oplossing voor het geschil. Bovendien kan de bemiddelaar, verzoener of scheidsrechter voor zijn beslissing niet alleen steunen op wettelijke bepalingen maar ook op zijn rechtsgevoel en op gedragscodes.

Gemakkelijkheid : geleidelijk aan wordt het mogelijk een geschil volledig op het internet te behandelen. Om een klacht in te dienen, vul je online een formulier in en hoef je niet meer naar een rechtbank te stappen. In principe moet je niet aan een advocaat vragen om zich met je dossier bezig te houden. Het kan echter wel nuttig zijn je te laten adviseren door een advocaat.

Snelheid : over het algemeen verloopt de procedure heel snel en krijg je spoedig uitsluitel over de afloop van het conflict. Soms volstaat het een derde te doen bemiddelen om het probleem op te lossen.

Prijs : de kosten liggen lager dan bij een rechtsvordering. De tendens bestaat erin de kosten van de procedure te laten betalen door de handelsmaatschappij en de procedure te beschouwen als een dienst aan de consument. In dat geval is de procedure dus gratis of goedkoop voor de consument.

Eigenheid : een groot voordeel van ADR is dat je zelf een derde kunt kiezen. Als je naar de rechtbank stapt, wordt de rechter je immers toegewezen en heb je geen enkele waarborg dat hij vertrouwd is met de nieuwe technologieën. Hier mogen de partijen een specialist in het vakgebied kiezen.

187. Kan ik een elektronisch bemiddelings- of arbitragemechanisme vertrouwen ?

Wij raden je aan, vooraleer je een dergelijke procedure aanvaardt, na te gaan of aan de volgende voorwaarden is voldaan : onafhankelijkheid van de derde (scheidsrechter, bemiddelaar of verzoener), transparantie van de procedure, mogelijkheid om je te laten adviseren door een advocaat, veiligheid en prijs. Ga in geval van twijfel om raad bij een advocaat.

Kies je voor dergelijke mechanismen om een geschil te regelen, dan mag je daardoor niet worden benadeeld en mag je (als consument) niet minder bescherming genieten dan als je naar een hof of rechtbank stapt.

188. Mag men mij dit soort mechanisme opleggen bij het sluiten van een overeenkomst ?

Vóór het ontstaan van een geschil kun je er niet rechtsgeldig mee instemmen om een beroep te doen op een arbitrageprocedure. Indien je dat wel doet, dan wordt zulke clause

als nietig beschouwd. Zodra er een geschil ontstaat, kun je op rechtsgeldige wijze een arbitrageovereenkomst sluiten die je (net als je “tegenstander”) verplicht een beroep te doen op de arbitrage- of bemiddelingsprocedure.

Het probleem rijst niet op dezelfde manier voor de bemiddeling of de verzoening, waarvoor wel een clause kan worden bepaald vóór het ontstaan van het conflict. Die geschillenregelingsprocedures zijn namelijk minder dwingend.

189. Welke waarde heeft een ADR-beslissing ?

Je kunt nog steeds naar de rechtbank stappen als het conflict niet kon worden opgelost via de bemiddelings- of verzoeningsprocedure.

Daarentegen kun je in principe niet meer terecht bij hoven en rechtbanken als je een arbitrageprocedure hebt ingesteld. In zekere zin is arbitrage de meest volledige vorm van buitengerechtelijke geschillenregeling ; een scheidsrechterlijke beslissing staat vrijwel gelijk met een beslissing van een hof of rechtbank en moet derhalve worden nagekomen.

Deel 6. Regeling van grensoverschrijdende geschillen op het internet



Het internet bevordert de betrekkingen tussen mensen over de grenzen heen. Die grensoverschrijdende dimensie kan een probleem vormen als er zich een geschil voordoet. Wanneer je een rechtsvordering wilt instellen tegen een particulier of een vennootschap die in een ander land gevestigd is, dan moet je namelijk eerst uitmaken welke rechtbank bevoegd is voor het geschil en vervolgens nagaan welke wet toepasselijk is.

Om je hierbij te helpen, zetten we even een aantal regels van het internationaal privaatrecht op een rijtje. In principe beschikt elk land over zijn eigen regels om de bevoegde rechtsinstanties en de toepasselijke wetten te bepalen. Op Europees vlak werden die regels echter in grote mate geüniformeerd via internationale juridische akten. Wil je met vrijwel volledige zekerheid te weten komen welke rechter bevoegd is om je geschil te behandelen, raadpleeg dan een recente Europese verordening, de zogenoemde “Verordening van Brussel”. De moeilijkheden beginnen echter wanneer je probeert uit te vissen welk recht in jouw specifiek geval van toepassing is, omdat je dan een heleboel juridische bronnen moet doornemen. Gemakkelijkheidshalve worden inzake overeenkomsten enkel die regels in aanmerking genomen die van toepassing zijn als je een contract sluit in de hoedanigheid van “consument”, d.w.z. voor niet-professioneel gebruik. Personen die beroepshalve een overeenkomst aangaan, vallen onder een ander stelsel.

En tot slot dit nog : een gerechtelijke beslissing die in België wordt genomen, moet ook nog kunnen worden uitgevoerd in het land waar de andere partij is gevestigd. Het volstaat dus niet dat een beslissing in een bepaalde staat wordt genomen opdat zij uitvoerbaar zou zijn in een andere staat. Doch binnen de Europese Unie worden de gerechtelijke beslissingen, krachtens de Verordening van Brussel, vrijwel automatisch erkend en uitgevoerd. Daarentegen verloopt de uitvoering van een in België geveld vonnis soms moeizamer buiten de Europese Unie.

HOOFDSTUK I. BEVOEGDE RECHTBANK BIJ GRENSOVERSCHRIJDENDE GESCHILLEN

190. Mag ik een buitenlandse persoon of vennootschap in België dagvaarden ?

In principe is de bevoegde rechtbank in Europa doorgaans die van de Staat waar de verweerder (de persoon tegen wie de rechtsvordering wordt ingesteld) zijn woonplaats heeft. Dat is de algemene regel die wordt gehanteerd in de Verordening van Brussel.

Diezelfde Verordening voorziet echter ook in bijzondere strafbepalingen in het kader van overeenkomsten aangegaan door een consument.

Op *contractueel vlak* heb je als consument de keuze tussen twee mogelijkheden : ofwel stap je naar een Belgische rechtbank, ofwel stap je naar een rechtbank van de Staat waar de andere partij gevestigd is. Daartoe moet de medecontractant zijn beroeps- of handelsactiviteit echter uitoefenen in of richten op het land waar jij woonachtig bent. Concreet : indien de overeenkomst wordt gesloten op een interactieve website, die toegankelijk is vanuit jouw land van verblijf, dan kun je van die optie gebruik maken. Dankzij die beschermingsregel kun je desnoods een vordering instellen bij een Belgische rechtbank.

Het volstaat echter niet dat je informatie krijgt over een product of dienst via een “passieve” site (waarop je geen overeenkomst kunt sluiten) die toegankelijk is in het land waar je verblijft. In dat geval geldt voor jou hetzelfde stelsel als voor de handelaars : een partij kan voor de rechtbank worden gedaagd in het land waar de verbintenis die aan de eis ten

grondslag ligt, werd of moet worden uitgevoerd. Meer concreet maakt de Verordening in dat opzicht een onderscheid tussen verkoop van goederen en verstrekking van diensten. Zo is de plaats van uitvoering van de verbintenis die aan de eis ten grondslag ligt :

- voor de verkoop van goederen, de plaats in een lidstaat waar de goederen volgens de overeenkomst geleverd werden of geleverd hadden moeten worden ;
- voor de verstrekking van diensten, de plaats in een lidstaat waar de diensten volgens de overeenkomst verstrekt werden of verstrekt hadden moeten worden.

Op *strafrechtelijk* vlak heb je ook een keuze. Zo kun je naar de rechtbank stappen in het land waar zich het schadebrengende feit heeft voorgedaan of in het land waar de schade is gebeurd. Daaruit kunnen wij bijvoorbeeld afleiden dat je, in geval van smaad op het web, de uitbrenger van de informatie die je schade berokkende hetzij voor een rechtbank kunt dagen in het land waar de informatie werd uitgebracht (een rechtbank van een andere staat), hetzij voor de rechtbank van het land waarin de schadeberokkende informatie werd ontvangen (een Belgische rechtbank).

191. Kan ik voor een buitenlandse rechtbank worden gedaagd ?

De Verordening van Brussel beschermt de consument op dat vlak. Tegen jou kan enkel een vordering worden ingesteld bij rechtbanken van de staat waar je woonachtig bent. Daartoe moet ook de medecontractant zijn beroeps- of handelsactiviteit uitoefenen in of richten op het land waar je woonachtig bent (zie hierboven nr. 190). Als consument kun je dus enkel gedagvaard worden voor Belgische rechtbanken.

Doch als de andere overeenkomstsluitende partij niet door de Verordening van Brussel is gebonden, verlies je dat voorrecht.

192. Mag men in een overeenkomst bepalen dat een buitenlandse rechtbank bevoegd is bij eventuele conflicten ?

Algemeen geldt dat geen enkele overeenkomst je als consument mag beroven van de beschermingsregels ingesteld door de Verordening van Brussel. Koop je bijvoorbeeld een product op een buitenlandse site, dan kun je met eventuele problemen steeds terecht bij een Belgische rechtbank, ook al bepalen de algemene voorwaarden van de site dat de rechtbanken van de plaats waar de onlineverkoper gevestigd is uitsluitend bevoegd zijn.

HOOFDSTUK II. TOEPASSELIJK RECHT BIJ GRENSOVERSCHRIJDENDE GESCHILLEN

193. Wat zijn de grote principes ?

Het valt niet makkelijk om te bepalen welk recht toepasselijk is op een grensoverschrijdend geschil. Aangezien het om een ingewikkelde materie gaat, kunnen wij je enkel aanraden het advies in te winnen van een specialist. Het is echter niet overbodig hiervan even de grote principes uiteen te zetten.

De wet inzake de elektronische handel stelt dat de rechter ertoe gehouden is het recht van oorsprong van de verkoper toe te passen, d.w.z. het recht van het land waar hij gevestigd is. Voorbeeld : bij een conflict tussen een Franse hoster en een Belgisch bedrijf dat ontevreden is over de geleverde diensten is bijgevolg het recht van oorsprong van de provider van toepassing, dus het Franse recht.

Van die regel wordt in sommige gevallen echter afgeweken, met name wanneer de partijen gekozen hebben welk recht toepasselijk is op hun overeenkomst of voor contractuele verbintenissen in overeenkomsten tussen consumenten. Ter herinnering : aangezien hier enkel consumentenovereenkomsten aan bod komen, schenken we geen aandacht aan de regels van de wet inzake de elektronische handel en bekijken we enkel de regels van het Verdrag van Rome.

Voordat we nagaan wat het Verdrag van Rome zoal als oplossingen voorstelt, willen we wijzen op twee zaken die van grote invloed kunnen zijn bij de bepaling van het toepasselijk recht : enerzijds de regels ter bescherming van de consument (die in zijn voordeel spelen op voorwaarde dat hij een aantal voorwaarden in acht neemt), anderzijds de vrijheid van de partijen om het op hun overeenkomst toepasselijke recht te kiezen).

194. Bevat het Verdrag van Rome beschermingsregels voor de consumenten ?

Ja, maar de door het Verdrag bepaalde regels ter bescherming van de consument gelden slechts in een beperkt aantal gevallen. We zullen het hier enkel hebben over de meest algemene hypothese, nl. een residuele categorie die de meeste consumptieovereenkomsten omvat. In die hypothese moet de consument, vóór het sluiten van de overeenkomst, in het land waar hij zijn gewone verblijfplaats heeft, een bijzondere aanbieding of een reclameaanbieding hebben gekregen en in dat land de nodige stappen hebben gedaan om de overeenkomst te sluiten.

Door te eisen dat er een aanbieding is gebeurd of dat er reclame werd gevoerd in het land van de consument wil het verdrag van Rome een onderscheid maken tussen “actieve” en “passieve” consumenten en de beschermingsmaatregelen beperken tot zogenaamde “passieve” consumenten. Een dergelijk onderscheid geeft echter aanleiding tot heel wat moeilijkheden bij het sluiten van overeenkomsten op het internet.

In sommige gevallen zijn er geen grote problemen. Waarschijnlijk zal de consument blijk geven van een zekere passiviteit als hij een geïndividualiseerde aanbieding of gepersonaliseerde reclame ontvangt. We weten immers dat door het verzamelen van persoonsgegevens over internauten en het centraliseren van die gegevens in databases een consumptieprofiel kan worden opgemaakt waardoor personalisatie van de reclame mogelijk is (zie hierboven nr. 63 e.v.).

In andere gevallen liggen de zaken een heel stuk moeilijker. Tijdens het surfen kun je namelijk op een site stoten waarop een database of producten worden aangeboden en kun je de persoon die verantwoordelijk is voor de site mededelen dat je wenst in te gaan op de aangeboden dienst zonder dat je ooit wordt benaderd door de handelaar. Je kunt bij het surfen ook aangetrokken worden door een webvertentie. De interactiviteit die eigen is aan het internet - en onder meer tot uiting komt in de verscheidenheid van de gebruikte reclametechnieken - maakt het verschil tussen actieve en passieve consumenten nog groter. Elke websurfer blijkt namelijk een ambivalent gedragspatroon te hebben. Een consument die zich op het web begeeft is "actief", vermits hij het initiatief neemt om zich aan te sluiten, doch hij wordt tijdens het surfen ook op diverse manieren aangesproken zonder dat hij daarop vat heeft of daarvan de invloed onderkent.

In afwachting dat de tekst van het Verdrag van Rome wordt gewijzigd, blijven de rechters sowieso met een groot interpretatieprobleem zitten.

195. Kan ik "onderhandelen" over het recht dat toepasselijk is op de overeenkomst ?

Volgens de regels van het internationaal privaatrecht staat het de partijen vrij het op hun overeenkomst toepasselijke recht te kiezen. In principe kun je dus onderhandelen.

Doch heel vaak wordt het toepasselijke recht vermeld in de algemene voorwaarden die op de site te vinden zijn en kan hierover niet worden onderhandeld. Als je dus iets aankoopt op een buitenlandse site, dan is het toepasselijke recht waarschijnlijk datgene dat de verkoper wenst toegepast te zien, nl. dat van zijn eigen land.

De vermelding van het toepasselijke recht in de algemene voorwaarden biedt wel een zekere transparantie. Maar daarmee los je de problemen nog niet op die kunnen optreden als het toepasselijke recht dat is van een derde land en jou niet dezelfde bescherming waarborgt als het Belgische recht. Het zou bijvoorbeeld wel eens kunnen dat het verzakingsrecht niet is opgenomen in sommige buitenlandse wetgevingen, althans in wetgevingen van buiten de Europese Unie (zie hierboven nr. 144 e.v.).

Laten we eerst even veronderstellen dat de hierboven vermelde beschermingsregels van toepassing zijn. Er is bepaald dat de vrijheid van de partijen om het toepasselijke recht aan te wijzen er niet toe mag leiden dat de consument "*de bescherming verliest welke hij geniet op grond van het recht van het land waar hij zijn gewone verblijfplaats heeft*". Hiermee wordt onder meer verwezen naar de wet van 14 juli 1991 betreffende de handelspraktijken en de bescherming en de voorlichting van de consument. Het is de bedoeling de consument dezelfde bescherming te bieden als in het land waar hij verblijft. Met die beschermingsmaatregelen wil de consumentenwet voorkomen dat de verkopers zich via een buitenlandse wet geheel of gedeeltelijk onttrekken aan de nationale consumentenbeschermingsregels. Ga je als consument een overeenkomst aan onder de voorwaarden van het Verdrag (zie hierboven nr. 194), dan heb je de zekerheid dat je minstens beschermd bent door de specifieke maatregelen van het Belgisch gebiedend recht.

Ingeval die beschermingsmaatregelen echter niet kunnen worden toegepast (bijvoorbeeld omdat aan de hierboven vermelde voorwaarden niet is voldaan), dan valt de overeenkomst onder het door de partijen gekozen recht ; de rechter bij wie de zaak aanhangig wordt gemaakt kan evenwel steeds het nationaal gebiedend recht toepassen.

196. Welk recht is toepasselijk als de partijen geen keuze maken ?

Als de partijen geen keuze maken, dan valt de overeenkomst onder *het recht van het land waar de consument zijn gewone verblijfplaats heeft*, indien die overeenkomst tot stand is gekomen in de hierboven vermelde omstandigheden, d.w.z. inzonderheid wanneer het sluiten van de overeenkomst is voorafgegaan door een speciale aanbieding of een reclameaanbieding en wanneer de consument in dat land het nodige gedaan heeft met het oog op het sluiten van de overeenkomst.

Indien de beschermingsmaatregelen niet toepasselijk zijn, bepaalt het Verdrag van Rome dat de overeenkomst onder het recht valt van het land waarmee de consument het nauwst is verbonden. In dat verband wordt verondersteld dat de overeenkomst het nauwst verbonden is met het land waar de partij die de kenmerkende prestatie moet verrichten haar gewone verblijfplaats of hoofdbestuur heeft. Stel dat je een boek aankoopt op een Nederlandse website en je om de ene of andere reden gerechtelijke stappen moet ondernemen tegen de verkoper. Het Nederlandse recht is dan toepasselijk, omdat de kenmerkende prestatie in casu de levering van het boek is en de persoon die deze verplichting moet nakomen (de verkoper) zijn hoofdbestuur in Nederland heeft. Maar zelfs in dat geval kan de behandelende rechter de gebiedende bepalingen van zijn nationaal recht toepassen.

197. Welk recht is toepasselijk in geval van misdrijf ?

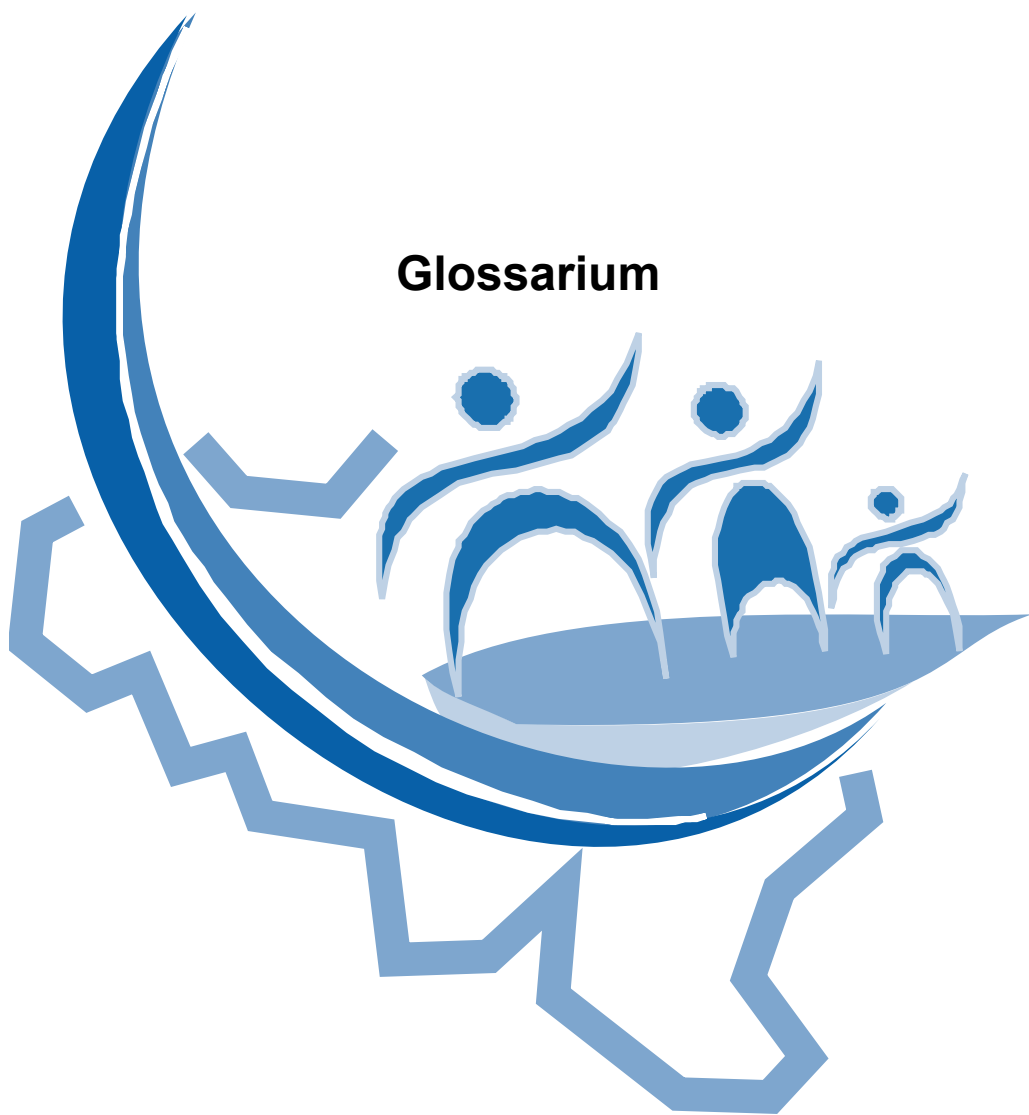
In behoorlijk wat gevallen kan een vordering inzake aansprakelijkheid uit onrechtmatige daad worden overwogen : bijvoorbeeld om sancties te nemen tegen onrechtmatige reclame, smaad of uitlatingen die aansporen tot rassenhaat, enz.

Hierover werd op internationaal niveau nog niets overeengekomen. Intussen kunnen we ons wel baseren op de wetgeving over de elektronische handel om te weten welk recht toepasselijk is op een internetmisdrijf. Ter herinnering : die wetgeving steunt op het principe van het “land van oorsprong”, op grond waarvan elke onlinedienstverlener onderworpen is aan het recht van het land waar hij gevestigd is. Telkens een verkoper een cybermisdaad begaat, is dat recht toepasselijk.

Nu kan het evenwel gebeuren dat je aansprakelijkheidsvordering niet is ingesteld tegen een verkoper, maar tegen een gewone particulier die zich bijvoorbeeld schuldig maakt aan smaad op een discussieforum. Om uit te maken welk recht toepasselijk is op dergelijke eis tot schadevergoeding, moet je uitgaan van het internationaal privaatrecht. Daartoe moet je eerst kijken welke nationale rechtsinstanties bevoegd zijn voor een dergelijke vordering, aangezien elke rechtbank enkel gebonden is door de regels m.b.t. de aanduiding van het toepasselijk nationaal recht die bindend zijn in haar land !

Naargelang van de staten zal het toepasselijk recht dus op een verschillende manier worden benaderd. In de meeste Europese landen wordt gesteund op het recht van het land waarin het misdrijf werd begaan. Het valt evenwel niet mee om op het internet de plaats te bepalen waar het misdrijf werd begaan. De rechtspraak hanteert dan ook diverse oplossingen : soms steunen de rechters op het recht van het land waar de overtreding heeft plaatsgevonden, dan weer baseren zij zich op het recht van het land waar de schade werd geleden.

Glossarium



GLOSSARIUM

A

ADR

Alternative Dispute Resolution. Proces waarbij (online) conflicten worden opgelost door andere middelen dan hoven en rechtbanken, inzonderheid via bemiddeling, verzoening of arbitrage.

ADSL

Asymmetric Digital Subscriber Line. Datatransmissie-techniek die een snelle verbinding mogelijk maakt. ADSL maakt gebruik van een traditionele telefoonlijn (twee koperdraden), maar op hogere frequenties via een modem van de nieuwe generatie, waardoor je voortdurend op het internet aangesloten kunt blijven en kunt surfen zonder dat je telefoonlijn bezet is. De overdrachtssnelheid is aanzienlijk groter dan met een traditionele modem : zowat 10 keer sneller voor het downloaden van gegevens en 2 maal sneller voor het verzenden van gegevens.

applet

APPLication Light wEighT. Klein computerprogramma geschreven in de Java-programmeertaal. *Applets* zijn toepassingen die vaak in een webpagina worden opgenomen om ze aantrekkelijker of interactief te maken (bijvoorbeeld rolmenu's, knipperende of scrollende tekst, enz.). Ze kunnen slechts worden uitgevoerd als de webbrowser van de internetgebruiker met Java compatibel is. Als een webpagina applets bevat, duurt het downloaden meestal langer.

B

bandbreedte

Debiet van een transmissielijn ; komt overeen met de hoeveelheid gegevens die in een bepaalde tijdsperiode kunnen worden verstuurd. De bandbreedte wordt doorgaans uitgedrukt in bits per seconde (bps). Hoe groter de bandbreedte, hoe groter de hoeveelheid gegevens die per tijdseenheid kan worden overgebracht.

banner

Zie webverrentie

baud

Eenheid om de modulatiesnelheid te meten. Baud wordt vaak verward met bits per seconde (bps). Over het algemeen is een baud gelijk aan één bit per seconde, maar dit hangt af van de valentie van het signaal (d.w.z. het aantal verschillende waarden die het kan hebben). Bij huidige modems is een baud gelijk aan verscheidene bps.

Zie ook modem en bps.

bit

binary digit. Kleinste informatie-eenheid, die een waarde van 0 of 1 kan hebben. Met bits kunnen codes worden gevormd om lettertekens, getallen of om het even welke informatie

weer te geven. Zo zijn er 8 bits nodig om een letterteken te vormen. Die groepering van 8 bits wordt *byte* genoemd.

bit per seconde (bps, bit/s)

Eenheid om de overdrachtssnelheid in netwerken te meten. Zie ook “bandbreedte”.

bit/s

Zie bit per seconde

bps

Zie bit per seconde

brandmuur

Zie firewall

Browser (navigators)

Software waarmee de internetgebruiker informatie op het internet kan zoeken en raadplegen. De meest bekende zijn Netscape Navigator en Internet Explorer.

bug

Programmeerfout die een verkeerde werking van een programma veroorzaakt.

byte

Informatie-eenheid bestaande uit 8 bits die op 256 manieren kunnen worden gecombineerd (2^8). Elke bit kan 0 of 1 zijn. Voorbeeld van een byte : 01001010. Eén megabyte is gelijk aan één miljoen bytes.

C

certificatiedienstverlener (CDV)

De certificatiedienstverlener is een onafhankelijke instelling die bevoegd is om, enerzijds de *identiteit na te gaan* van de houders van de openbare sleutel en *certificaten af te geven*, d.w.z. elektronische attesten die een persoon en zijn openbare sleutel verbinden, en anderzijds, om te zorgen voor een zo ruim mogelijke *bekendmaking* van de aldus afgegeven certificaten. De CDV moet ook het register met de openbare-sleutelcertificaten bijwerken en desgevallend certificaten intrekken. Belgacom E-Trust, Globalsign en Isabel zijn certificatie-dienstverleners.

chat

Onlinegesprek in “real time” tussen verschillende internetgebruikers die ingetypte berichten uitwisselen.

client-server (gebruiker-server)

Systeem van verscheidene via een netwerk onderling verbonden computers waarbij een toepassingsprogramma, *client* genoemd, een beroep doet op verschillende middelen die zich op een andere computer van het netwerk, *server* genoemd, bevinden. Via vragen en antwoorden worden op die manier diensten geleverd tussen computers.

Codering

Zie encryptie

Commissie voor de Bescherming van de Persoonlijke Levenssfeer

Instelling die optreedt als contactpunt en adviesorgaan voor de bescherming van privé-leven en persoonsgegevens.

cookie

Klein computerbestand in tekstformaat dat bij het bezoek van een website door een webserver naar de computer van een internetgebruiker wordt gestuurd en er wordt opgeslagen. Cookies bevatten gegevens die bij elk bezoek aan dezelfde website worden hergebruikt om de computer of de gebruikersinstellingen te identificeren.

cybersquatting (domain name grabbing, domeinkaping)

Het laten registreren van de domeinnaam van een merk, handelsnaam of familienaam om de houder van dit merk of van die naam te beletten de domeinnaam te registreren of om hem die domeinnaam peperduur te verkopen.

D

digitaal certificaat

Elektronisch attest dat door een verstrekker van certificatiediensten wordt afgegeven en dat een natuurlijke of rechtspersoon aan zijn openbare sleutel bindt en zijn identiteit bewijst. De band wordt voor echt verklaard door de certificerende autoriteit die het certificaat ondertekent. Deze handtekening bewijst de authenticiteit van het certificaat en belet dat de erin voorkomende informatie wordt gewijzigd.

discussieforum (nieuwsgroep, newsgroup)

Interactieve discussieruimte waar gebruikers informatie, ideeën, tips en meningen over een bepaald onderwerp kunnen uitwisselen. Anders dan bij het *chatten* worden berichten niet in *realtime* maar met een zekere vertraging verspreid. Gebruikers kunnen alle door andere forumgebruikers geschreven berichten lezen en hun collectief of afzonderlijk antwoorden.

DNS

Domain Name System. Systeem waardoor een URL (zoals *www.site.com*) in een IP-adres (bijvoorbeeld 193.190.127.2) kan worden omgezet.

Zie ook “URL” en “IP-adres”.

domain name grabbing

Zie cybersquatting.

domeinkaping

Zie cybersquatting

domeinnaam

Gebruikersvriendelijker en gemakkelijker te onthouden koppeling aan het IP-adres, waarmee een computer of een groep computers kan worden geïdentificeerd op het

internet. De domeinnaam bestaat uit twee hoofdbestanddelen : de stam en de uitbreiding. De stam is meestal de naam van de organisatie en de uitbreiding verwijst naar de geografische oorsprong (.be, .fr, .uk, enz.) of het activiteitstype (.com, .org, .net, enz.). Bijvoorbeeld : de domeinnaam van de Kamer voor Volksvertegenwoordigers is "dekamer.be".

downloaden

Proces waarbij een bestand wordt opgevraagd uit een afgelegen computer en wordt binnengehaald en opgeslagen op een lokale computer.

E

elektronische aangetekende brief

De afzender van een elektronisch ondertekend bericht kan, net als voor een traditionele aangetekende brief, een bewijs bekomen van de verzending, de datum en eventueel de ontvangst, via een vertrouwensderde.

elektronische post

Zie e-mail.

e-mail (elektronische post)

Elk bericht in de vorm van tekst, stem, geluid of beeld dat via een openbaar communicatienetwerk wordt verzonden en in het netwerk of de eindapparatuur van de ontvanger kan worden opgeslagen tot hij het leest.

encryptie (codering)

Handeling ter bescherming van de vertrouwelijkheid van gegevens door middel van sleutels (wachtwoorden, geheime code...) die informatie coderen en in cijfers omvormen, zodat enkel degenen die over deze sleutels beschikken de aldus beveiligde informatie kunnen lezen.

F

FAQ (Frequently Asked Questions, veel gestelde vragen)

Lijst van antwoorden op de meest gestelde vragen door internetgebruikers over een website of de erin behandelde onderwerpen.

File Transfer Protocol

Zie FTP

filtering

Systeem dat uit één of meer softwareprogramma's bestaat en de toegang blokkeert tot sommige gegevens die internetgebruikers ongeschikt achten, in het bijzonder voor hun kinderen. Filters kunnen ook dienen om ongevraagde, via e-mail verstuurde reclame te weren.

firewall (brandmuur)

Hardware en software om elke ongeoorloofde toegang tot een computernetwerk te voorkomen.

flame

Berisping vanwege internetgebruikers tegen een persoon die onaanvaardbare berichten op een discussieforum post.

framing

Met deze techniek kun je een pagina of informatie afkomstig van een site (bronsite) in je eigen webpagina opnemen (doelsite), zonder dat je een nieuw venster hoeft te openen in de browser die naar de bronsite verwijst. Het adres van de doelsite komt dus in de plaats van dat van de bronsite, wat verkeerdelijk de indruk wekt dat de informatie op de doelsite staat.

Frequently Asked Questions

Zie FAQ

freeware

Gratis toegankelijke software. Niet te verwarren met *shareware*.

FTP (File Transfer Protocol)

Protocol voor de uitwisseling van bestanden op het internet.

G**gebruiker-server**

Zie client-server

GIF

Graphics Interchange Format (grafisch bestandsformaat). Bestandsformaat speciaal voor grafische bestanden van het *World Wide Web*.

H**hacking**

Het ongeoorloofd binnendringen of blijven in het computersysteem van een derde (externe hacking). *Hacking* is ook het overschrijden van zijn toegangsbevoegdheid tot dit systeem (interne *hacking*).

hardware

Informaticamaterieel. *Hardware* staat tegenover *software*, die betrekking heeft op de programma's.

hoster

Technische operator op het internet die ruimte ter beschikking stelt om een website onder te brengen en raadpleegbaar te maken.

helpdesk (hotline)

Telefonische bijstand (gratis of tegen betaling) verstrekt door een professional om tegemoet te komen aan de vragen van zijn klanten.

hoax

Vals bericht of nepbericht dat vaak via e-mail op het internet wordt verspreid.

homepage

Zie thuispagina

hotline

Zie helpdesk

HTML

HyperText Markup Language. Taal die gebruikt wordt om webpagina's (hypertekst-documenten) op het internet te ontwerpen en te beschrijven.

HTTP

HyperText Transfer Protocol (protocol voor de overdracht van hypertekstkoppelingen). Het protocol dat de basis vormt van de *World Wide Web*-technologie en de communicatie tussen computers op het internet beheert.

hypertekst

Voorstellingswijze van informatie op het internet waardoor afbeeldingen, geluid en tekst worden verbonden, zodanig dat de inhoud kan worden geraadpleegd ongeacht de localisatie en de drager van die informatie. Zie ook hypertekstlink.

hypertekstlink

Reactieve zone in een webdocument. Het kan een actief beeld zijn of een woord van de tekst dat zich qua kleur van de rest van het document onderscheidt. Bij het aanklikken van een hypertekstlink wordt de gebruiker doorverwezen naar het door de link aangegeven document, dat zich op dezelfde of een andere webpagina bevindt en tot dezelfde of een andere website behoort. Zie ook hypertekst.

ICANN

Internet Corporation for Assigned Names and Numbers. Vereniging die alle internetactoren en -gebruikers vertegenwoordigt en verantwoordelijk is voor het beheer en de coördinatie van de domeinnamen, de toekenning van IP-adressen, de parameters van het IP-protocol en de *root server*.

informaticabedrog (informaticafraude)

Bedrieglijke gegevensmanipulatie om zich te verrijken. Informaticabedrog is bijvoorbeeld het gebruik van een gestolen kredietkaart om geld te halen uit een bankautomaat, de onwettige overschrijding van het krediet verbonden aan je eigen kredietkaart, de invoering van commando's om na bepaalde verrichtingen andere onrechtmatige financiële voordelen te bekomen of de uitvoering van illegale manipulaties van klantenrekeningen door een bankbediende.

informaticafraude

Zie informaticabedrog

informaticavervalsing

Zie valsheid in informatica

interface

Schakel tussen twee operatoren (hardware, software, mens) waardoor ze informatie kunnen uitwisselen op grond van gemeenschappelijke, fysische en logische regels.

internationaal privaatrecht

Geheel van rechtsregels waarmee in geval van supranationaal geschil het bevoegde rechtcollege en de geldende wetgeving kunnen worden bepaald.

internet

Wereldwijd netwerk dat bestaat uit kleinere netwerken waardoor computers uit de hele wereld onderling kunnen communiceren via een gemeenschappelijk protocol (TCP/IP). De meest voorkomende diensten zijn het *world wide web*, de elektronische post, de discussieforums en de gegevensoverdracht.

internetprovider

Zie Internet Service Provider

internetter

Internetgebruiker.

Internet Service Provider (ISP, internetprovider)

Organisatie die particulieren en ondernemingen toegang biedt tot het internet.

intranet

Privé-netwerk binnen een organisatie. Intranetwerken maken veelvuldig gebruik van internetprotocollen om informatie aan te bieden. Ze zijn meestal beveiligd door *firewalls* (brandmuren).

IP

internetprotocol : op het internet gebruikt protocol voor de uitwisseling van in pakketten onderverdeelde gegevens.

IP-adres

Internet protocoladres dat wordt toegekend aan iedere op het internet aangesloten computer, waardoor hij op unieke wijze kan worden geïdentificeerd. Een IP-adres bestaat uit vier groepen getallen, gescheiden door punten, zoals 193.190.127.2.

ISDN

Integrated Services Digital Network. Volledig gedigitaliseerd netwerk voor een snelle en vlotte informatieoverdracht. Er bestaan twee soorten ISDN-lijnen : ISDN-2, uitgerust met twee communicatiekanalen van 64.000 bits per seconde en ISDN-30, uitgerust met dertig communicatiekanalen.

ISP

Internet Service Provider.

Zie internetprovider.

J

Java

Objectgerichte programmeertaal, door Sun Microsystems en IBM ontwikkeld, waarmee programmeurs autonome en interactieve internettoepassingen kunnen ontwerpen. Het Java-programma wordt in brontaal geschreven en dan door een compiler omgezet, waardoor een applet-programma ontstaat dat op een html-pagina kan worden gebruikt. Als de gebruiker een pagina met een Java-applet oplaadt via een browser die de Javataal herkent, wordt de appletcode naar zijn systeem overgedragen en door de browser uitgevoerd. Zie ook Applets.

JPEG

Joint Picture Expert Group. Op het internet veelgebruikt compressieformaat voor afbeeldingen. Zie ook GIF.

L

login

Gebruikersnaam of identificatienummer om zich op een server te identificeren. Een login gaat meestal gepaard met een wachtwoord.

M

metatag

Soort baken bovenaan elke html-pagina die een website door middel van trefwoorden beschrijft met het oog op een optimale referencering van de site door zoekmotoren.

modem

Acroniem voor **mod**ulator/**dem**odulator. Randapparaat van een computer waarmee deze in verbinding staat met een netwerk, meestal het internet, via de telefoonlijn of de kabeltelevisie. Een modem kan *intern* (ingebouwd in een computer) of *extern* zijn. Modems worden ingedeeld op basis van de overdrachtssnelheid van gegevens (uitgedrukt in *baud rate*) en van de gekozen telecommunicatietechnologie (ADSL, ISDN, enz.).

moderator

Persoon die verantwoordelijk is voor het beheer van een discussieforum of een mailinglijst. Hij filtert de door de leden verzonden berichten en verwijdt die welke niet relevant zijn of waarvan de inhoud niet strookt met de vastgestelde ethische of deontologische regels.

mp3

Mep-1 Layer 3. Formaat voor audiobestanden waarmee een luisterkwaliteit kan worden bereikt die gelijk is aan die van een audio-cd, met een compressieverhouding die tot 13 kan gaan.

multimedia

Elke informatie waarin tekst, grafieken, geluidsbestanden en/of videobeelden gecombineerd worden.

N

navigator

Zie browser

net

Gebruikelijke term om het internet aan te duiden.

netiquette

Geheel van regels met betrekking tot het fatsoen en de omgangsvormen op het internet.

newsgroup

Zie discussieforum

nieuwsgroep

Zie discussieforum

O

overeenkomst op afstand

Elke overeenkomst inzake producten of diensten gesloten tussen een verkoper en een consument in het kader van een door de verkoper georganiseerd systeem voor verkoop of dienstverlening op afstand waarbij uitsluitend gebruik gemaakt wordt van één of meer technieken voor communicatie op afstand tot en met de sluiting van de overeenkomst zelf (artikel 77 § 1, 1° wet betreffende de handelspraktijken en de voorlichting en bescherming van de consument).

P

pdf

Portable Document Format. Bestandsformaat dat door Adobe werd ontwikkeld om de omvang van bestanden (tot 10 keer) te verkleinen en waarmee gegevens op elk platform via Acrobat Reader kunnen verschijnen en worden afgedrukt.

persoonsgegevens

Elke informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Iemand is identificeerbaar als hij rechtstreeks of onrechtstreeks kan worden herkend - namelijk door verwijzing naar een identificatienummer of één of meer specifieke gegevens eigen aan zijn fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.

PIN

Personal Identification Number. Persoonlijke geheime code.

platform

Besturingssysteem van een computer.

plug-in

Bestanddeel of softwaremodule die de prestaties van een toepassing verbetert, over het algemeen om meerdere bestanden van een bepaald type te kunnen lezen of laden. Bij een webbrowser dienen *plug-ins* om bestanden met een rijke inhoud te laden, zoals audio- of videobestanden of animaties.

pop-up

Browsersvenster dat boven elk hoofdvenster wordt geopend. Talrijke sites nemen reclame op in dergelijke vensters.

portaal

Internetsite van waaruit de gebruiker zijn opzoeken start. Over het algemeen biedt een portaal diverse diensten aan, zoals het beheer van een e-mailadres, actuele informatie, webgidsen... Yahoo !, Belgacom en Advalvas behoren tot de meest bekende portaalsites.

protocol

Geheel van regels of normen voor gegevenscommunicatie op een netwerk, in het bijzonder het internet. Computers communiceren via protocollen die hun onderling gedrag bepalen om gegevensoverdracht mogelijk te maken. Op het internet is TCP/IP het referentieprotocol.

provider

Zie internetprovider.

R

Robinsonlijst

Lijst waarop iedereen zich kan inschrijven als hij geen reclame meer wil ontvangen van firma's waarbij hij geen klant is of waaraan hij geen informatie heeft gevraagd. Deze lijsten bestaan voor alle communicatiemiddelen, zowel het internet (elektronische post) als de mobiele telefoons (sms).

router

Apparaat dat netwerken met elkaar verbindt doordat het een signaal kan filteren en richten afhankelijk van het IP-adres.

S

script (scripttaal)

Geheel van opdrachten waarmee verschillende taken van een communicatieprogramma worden geautomatiseerd.

server

Computer of software binnen een netwerk, die sommige diensten kan verlenen aan de andere computers van het netwerk welke als klanten worden beschouwd.

SET

Secure Electronic Transactions. Beveiligingsprotocol voor elektronische betalingen, gebaseerd op encryptie en waarmee de partijen kunnen worden geauthentificeerd.

shareware

Zie software met vrijwillige bijdrage

SMTP

Simple Message Transfer Protocol. TCP/IP-communicatieprotocol dat gebruikt wordt voor het verzenden van elektronische post op het internet.

software met vrijwillige bijdrage (shareware)

Software die gratis kan worden getest maar waarvoor bij gebruik een vergoeding aan de auteur of ontwikkelaar moet worden betaald. Doorgaans worden dergelijke programma's ontwikkeld door kleine ondernemingen of programmeurs voor het oplossen van een specifiek informaticaprobleem of het uitwerken van een nieuwe toepassing. Tegen een bijdrage krijgt de gebruiker documentatie over de software, updates...

spionagesoftware (spyware)

Elektronische spion in de vorm van een klein programma dat in een software geïntegreerd is (bv. van het internet gedownloade *freeware* of *shareware*) en dat gegevens over een internetgebruiker, zijn surfgewoontes en de configuratie van zijn pc verzamelt. Bij elk internetbezoek wordt deze informatie naar een server gestuurd, vaak om de internetter doelgerichte reclame toe te sturen.

software

Computerprogramma. Zie ook hardware.

spamming

Massale en herhaalde verzending van ongevraagde - meestal commerciële - berichten.

spyware

Zie spionagesoftware.

SSL

Secure Socket Layer. Protocol voor beveiligde communicatie via het internet. Het maakt deel uit van browsersoftware (Netscape Navigator en Internet Explorer) en wordt gebruikt om de overdracht van vertrouwelijke gegevens in netwerken te beveiligen.

streaming

Techniek waardoor een bestand kan worden gelezen (beeld, audio- of videobestand) zonder te moeten wachten tot het bestand volledig gedownload is. Een *plug-in*, aan de webbrowser toegevoegd, deprimeert en leest de gegevens naarmate ze op de computer binnenkomen.

subject directory

Zie webgids

T

TCP/IP

Combinatie van de acroniemen *Transmission Control Protocol* (protocol voor transmissiecontrole) en *Internet Protocol* (internetprotocol). Beide communicatieprotocollen vormen de basis voor het functioneren van het internet en regelen de overdracht van gegevens in netwerken.

thuispagina (homepage)

Hoofdpagina van een website. Thuispagina's bevatten doorgaans links die naar andere pagina's van de eigen site of van externe sites verwijzen. Sommige grote websites kunnen meerdere homepages bevatten.

U

URL

Uniform Resource Locator. Adres van een server of van elk op het internet verkrijgbaar bestand. Het eerste gedeelte van een URL verwijst naar het protocol (http of ftp) en het tweede gedeelte is de domeinnaam of het IP-adres (www.lachambre.be of 212.35.105.232). Verder bevat de URL eventueel een of meer directories die toegang bieden tot het bestand op de server.

Bijvoorbeeld : http://www.dekamer.be/parlementaire_documenten.html.

V

valsheid in informatica (informaticavervalsing)

Informaticamanipulatie van gegevens om de juridische draagwijdte ervan opzettelijk te wijzigen. Elektronische gegevens kunnen bijvoorbeeld worden vervalst door ze (geheel of gedeeltelijk) te wijzigen of te wissen tijdens het invoeren, binnenhalen of opslaan in de computer. Valsheid in informatica is onder meer: namaak of vervalsing van kredietkaarten; valsheid inzake digitale contracten (wanneer juridisch relevante gegevens niet meer op papier worden gedrukt, noch met de hand worden ondertekend); invoering van een vals kredietkaartnummer bij het tegen betaling intekenen op een internetsite; inschrijving van fictieve schuldvorderingen of wijziging van loongegevens door een bediende in de boekhoudsoftware van een bedrijf; kunstmatige opdrijving, door een bediende, van het aantal overuren in de software voor het beheer van de arbeidstijd; vervalsing van een elektronische handtekening of bewust gebruik van vervalste gegevens.

veel gestelde vragen

zie FAQ

verwerking van persoonsgegevens

Elke bewerking of geheel van bewerkingen, al dan niet uitgevoerd met behulp van geautomatiseerde methoden en toegepast op persoonsgegevens. Het kan onder meer gaan om het verzamelen, vastleggen, organiseren, bewaren, aanpassen, wijzigen, extraheren, raadplegen, gebruiken, verspreiden enz. van gegevens.

Zie ook persoonsgegevens.

verzakingsrecht

Mogelijkheid die de consument geboden wordt om bij een overeenkomst op afstand van zijn aankoop af te zien, zonder betaling van een boete en zonder opgave van een reden.

virus

Programma dat de werking van informaticasystemen verstoort of de daarin opgeslagen gegevens wijzigt, vervalst, ja zelfs vernietigt. Het virus is in staat zich te vermenigvuldigen en zodanig geconcipeerd dat het andere programma's kan opsporen en aantasten door er zichzelf in te kopiëren. Het virus wordt actief op het ogenblik dat het besmette programma wordt uitgevoerd. Zodra het geactiveerd is, begint het virus te werken : dat kan gewoon hinderlijk of storend zijn, maar ook rampzalig en zelfs ronduit catastrofaal.

W

web

Verkorte naam voor *World Wide Web*. Zie aldaar.

webgids (webindex, subject directory)

Een webgids is een middel om informatie op het internet op te zoeken en te rangschikken. Het is meestal een lijst van sites, ingedeeld in categorieën en subcategorieën volgens het onderwerp (bijvoorbeeld informatica, wetenschappen, gezondheid, sport, vrijetijdsbesteding, cultuur, enz.).

webindex

Zie webgids

website

Geheel van webpagina's op eenzelfde server, die onderling verbonden zijn door hyperlinks.

webvertentie (banner)

(Vaak kleine) reclametekst op een deel van de webpagina.

World Wide Web (www, web)

Geheel van op het internet aangesloten computersystemen (webservers) die gemeenschappelijke normen (hypertekst-technieken) hanteren om multimedia-informatie aan te bieden (webpagina's).

www

Zie World Wide Web

W3C

Zie "W3-Consortium".

W3-Consortium (W3C)

World Wide Web Consortium (www.w3.org).

Organisatie die normen voor het internet uitwerkt en de uitwisseling van *World Wide Web*-producten bevordert.

Z

zoekmachine (zoekmotor)

Programma of dienst om informatie op het internet te lokaliseren. Elke zoekmotor gebruikt een browsersoftware die webpagina's afzoekt en deze in een databank indexeert. Bij een zoekopdracht van de internetgebruiker verschijnt een reeks hypertextdocumenten op de zoekmachine die met de aangegeven trefwoorden overeenkomen. De bekendste zoekmotoren zijn Google, Alta Vista, Lycos en Yahoo!

zoekmotor

Zie zoekmachine

Nuttige teksten en adressen



NUTTIGE TEKSTEN

Bescherming van de consument

- Wet van 14 juli 1991 betreffende de handelspraktijken en de voorlichting en bescherming van de consument, BS van 29 augustus 1991.

Bescherming van de persoonlijke levenssfeer

- Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, BS van 18 maart 1993.
- Koninklijk besluit ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, BS van 13 maart 2001.

Auteursrecht en merkenrecht

- Wet van 30 juni 1994 betreffende het auteursrecht en de naburige rechten, BS van 27 juli 1994, blz. 19297-19314.
- Wet van 30 juni 1994 houdende omzetting in Belgisch recht van de Europese richtlijn van 14 mei 1991 betreffende de rechtsbescherming van computerprogramma's, BS van 27 juli 1994, blz. 19315-19317.
- Wet van 31 augustus 1998 houdende omzetting in Belgisch recht van de Europese richtlijn van 11 maart 1996 betreffende de rechtsbescherming van databanken, BS van 14 november 1998, blz. 36914.
- Wet van 30 juni 1969 houdende goedkeuring van het Benelux Verdrag inzake de warenmerken, en van de bijlage, ondertekend te Brussel op 19 maart 1962, BS van 14 oktober 1969. Deze eenvormige Beneluxwet werd vaak gewijzigd. De jongste wijziging werd aangebracht door de wet van 3 juni 1999 houdende instemming met het Protocol houdende wijziging van de eenvormige Beneluxwet op de merken, gedaan te Brussel op 7 augustus 1996, BS van 26 oktober 1999.

Elektronische Handel

- Wet van 11 maart 2003 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, BS van 17 maart 2003.
- Wet van 20 oktober 2000 tot invoering van het gebruik van de elektronische handtekening in de gerechtelijke en de buitengerechtelijke procedure, BS van 22 december 2000.
- Wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatediensten, BS van 29 september 2001.
- Wet van 17 juli 2002 betreffende de transacties uitgevoerd met instrumenten voor de elektronische overmaking van geldmiddelen, BS van 17 augustus 2002.

Computercriminaliteit

- Wet van 13 april 1995 houdende bepalingen tot bestrijding van de mensenhandel en de kinderpornografie, BS van 25 april 1995, blz. 10823.
- Wet van 28 november 2000 inzake informaticacriminaliteit, BS van 3 februari 2001.

Internationaal privaatrecht

- Verordening (EG) nr. 44/2001 van de Raad van 22 december 2000 betreffende de rechterlijke bevoegdheid, de erkenning en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken, PB nr. L 12/1 van 16 januari 2001.
- Verdrag van Rome van 19 juni 1980 inzake het recht dat van toepassing is op verbintenissen uit overeenkomst, PB nr. L 266/1 van 9 oktober 1980.

NUTTIGE ADRESSEN

- Website van de **Federale Overheidsdienst Economie, KMO, Middenstand en Energie** :

<http://mineco.fgov.be>

- **Algemene Directie Controle en Bemiddeling** : om een klacht in te dienen :

World Trade Centre III

Simon Bolivarlaan 30

1000 Brussel

Tel : 32 (0) 2 208 36 11

Fax : 32 (0) 2 208 39 15

E-mail : Eco.Inspec@mineco.fgov.be

- Website van het **Observatorium van de Rechten op het Internet** :

<http://www.internet-observatory.be>

- **Strategisch Digitaal Forum** :

<http://www.eflanders.be>

- Agence **Wallonne des Télécommunications** :

<http://www.awt.be>

- **Federale staat, Gemeenschappen en Gewesten : institutionele portalen**

<http://www.belgium.be>

Federale staat

<http://www.cfwb.be>

Franstalige Gemeenschap

<http://www.vlaanderen.be>

Vlaamse Gemeenschap (Vlaams Gewest)

<http://www.dglive.be>

Duitstalige Gemeenschap

<http://www.wallonie.be/>

Waals Gewest

<http://www.bruxelles.irisnet.be>

Brussels Hoofdstedelijk Gewest

- **Contactpunt van de gerechtelijke politie** : om illegale informatie op het internet aan te geven

E-mail : contact@gpj.be

– **Child Focus :**

Tel. : 110

www.childfocus-net-alert.be

– Website van de **Commissie voor de Bescherming van de Persoonlijke Levenssfeer :**

<http://www.privacy.fgov.be>

– Website van het **Interdisciplinair Centrum voor Recht en Informatica**

<http://www.icri.be>

– Website van het “**Centre de Recherches Informatique et Droit**” :

<http://www.crid.be>

– ASBL “**Droit et Nouvelles Technologies**” :

<http://www.droit-technologie.org>



INDEX

A

ADR 130, 131, 132, 140
ADSL 16, 17, 18, 19, 20, 21,
 22, 33, 140, 147
algemene voorwaarden..... 22, 45, 59, 96,
 97, 127, 135, 137
Alternative Dispute ResolutionZie *ADR*
antivirusprogramma..... 67, 86, 87, 88
arbitrage..... 130, 131, 132, 140
attachment..... 34, 74, 87
auteursrecht..... 33, 42, 47, 48, 49,
 50, 51, 52, 53, 54, 55,
 56, 57, 58, 59, 60, 89, 156

B

<i>bandbreedte</i>	67, 140, 141
<i>banner</i>	95, 140, 152
<i>baud</i>	140, 147
<i>beeldrecht</i>	42, 54
<i>bemiddeling</i>	130, 131, 132, 140
<i>bestelling</i>	94, 95, 96, 97, 98, 99, 100, 101, 102, 110, 111, 115, 116, 118, 119, 120, 121, 122, 123, 126 Zie ook <i>betaling</i>
<i>archivering</i>	96, 105
<i>bewijs</i>	35, 36, 69, 101, 102, 109, 126, 143
<i>ontvangstbericht</i>	100
<i>ontvangstbevestiging</i>	35, 36
<i>ontvangstbewijs</i>	36
<i>stap voor stap</i>	99
<i>technische formaliteiten</i>	96

- uitvoering 71, 83, 87, 96, 97,
..... 98, 100, 110, 113, 123,
..... 124, 134, 135, 145, 156
- vergissing 95, 100, 119
- betaling* 18, 22, 23, 42, 44, 46, 59,
..... 60, 82, 96, 97, 107, 112,
..... 113, 115, 116, 117, 118,
..... 119, 120, 121, 124, 144, 151, 152
- bankoverschrijving..... 115
- bij de levering 121
- cheque..... 121
- debetkaart..... 118
- elektronische overschrijving 120
- kredietkaart..... 122
- terugbetaling..... 126
- voorafbetaling 115
- bevoegde rechtbank* 46, 134
- bit*..... 140, 141
- bps*..... 140, 141
- brandmuur* 67, 85, 141, 143
- browser*..... 29, 31, 32, 42, 62, 65,
.... 80, 144, 147, 148 Zie ook Navigator
- bug*..... 66, 141
- byte*..... 141

C

<i>cache(geheugen).....</i>	<i>28</i>
<i>certificatiedienstverlener.....</i>	<i>103, 104,</i>
<i>.....</i>	<i>105, 141</i>
<i>chatten.....</i>	<i>16, 37, 38, 62, 142</i>
<i>Child Focus.....</i>	<i>79, 159</i>
<i>citaatrecht.....</i>	<i>51, 54</i>

codering 35, 89, 90, 143
 commerciële waarborgen 97, 124, 126
 Commissie voor de Bescherming van de
 Persoonlijke Levenssfeer 42, 63,
 69, 70, 142, 159
communicatiekosten 16
**Contactpunt van de gerechtelijke
 politie** 158
 cookie 63, 64, 65, 79, 142
 cookies 62, 63, 64, 65, 66, 68
 copyright Zie auteursrecht
 cybercontrole 71
 cybersquatting 45, 142

D

database 52, 54, 117, 118, 137
 directe marketing 70
 directe-marketingdoeleinden 24
 discussieforum 34, 38, 39, 74, 94,
 138, 142, 144, 147, 148
 DNS 42, 43, 44, 45, 46, 142
 domain name grabbing 142
 Domain Name System Zie DNS
 domeinkaping 45, 142
 domeinnaam 28, 42, 43, 44, 45, 46,
 142, 143, 151

E

elektronische aangetekende brief 36,
 109, 126, 143
 elektronische handtekening 35, 82,
 101, 102, 103, 104, 105,
 106, 107, 109, 119, 151, 156
 certificaat 103, 104, 105, 107,
 108, 109, 118, 142
 definitie 91, 103
 veilig middel voor het aanmaken
 103, 106

werking 44, 67, 71, 78, 85, 88,
 90, 99, 128, 141, 152
 e-mail 2, 25, 34, 35, 36, 43, 66,
 73, 74, 75, 76, 79, 87, 90,
 95, 97, 98, 100, 101, 102,
 111, 113, 121, 125, 126, 143, 145
 Ethernet 19

F

FAQ 143, 144, 151
 filtering 76
 filtermogelijkheden 77
 filtersoftware 77, 80
 filtersystemen 79, 80
 firewall 67, 85, 141, 143
 flame 39, 144
 framing 32, 144
 freeware 33, 66, 144, 150
 FTP 16, 143, 144

G

gebruiksvergunning 45, 57
 gedragscode 22, 23, 39, 115,
 116, 127, 128, 129
 GIF 144
 gratis internet 23

H

hacker 84, 118
 hacking 82, 83, 84, 85, 144
 helpdesk 22, 23, 144, 145
 hoax 36, 145
 homebanking 120, 121
 homepage 31, 59, 127, 145, 151
 hosting 43, 81
 html 2, 129, 147, 151
 http 2, 3, 16, 17, 23, 28, 29, 30,
 36, 42, 43, 44, 45, 46, 63, 65,
 67, 70, 75, 76, 79, 87, 88, 105,

..... 106, 127, 129, 130, 151, 158, 159
hyperlink 31, 58, 59, 94, 95,
..... 97, 118, 128

I

ICANN 145
Illegale en nadelige sites 78
illegale of nadelige site 78, 79
informaticavervalsing 82, 146, 151
informatie 2, 5, 16, 17, 22, 23, 24,
..... 28, 29, 30, 31, 32, 33, 35, 36,
..... 38, 39, 42, 48, 62, 63, 64, 65,
..... 66, 68, 69, 71, 72, 73, 75, 76,
..... 78, 79, 80, 81, 90, 94, 95, 96,
..... 97, 98, 99, 105, 106, 110, 111,
..... 112, 115, 116, 117, 120, 124,
..... 125, 126, 128, 134, 135, 140,
..... 141, 142, 143, 144, 145, 146,
..... 148, 149, 150, 152, 153, 158
interface 16, 18, 108, 109, 146
internationaal privaatrecht 134, 137,
..... 138, 146
internet service provider 22
internetprovider 16, 18, 19, 21, 22,
..... 23, 24, 28, 29, 34, 43,
..... 44, 53, 62, 73, 76, 79,
..... 80, 81, 90, 94, 146, 147, 149
intranet 146
IP-adres 28, 42, 62, 68, 76,
..... 91, 142, 146, 149, 151
IRC 37
ISDN 16, 17, 18, 21, 22, 146, 147
ISP 22, 23, 24, 25, 26, 29, 146
ISPA 22, 23, 79

J

Java 31, 140, 147
JPEG 147

K

klacht 23, 45, 80, 81, 97,
..... 98, 124, 127, 131, 158
knippen/plakken 47, 55
kopiëren 32, 33, 54, 55, 56, 57,
..... 85, 86, 89, 90, 97, 152
kredietkaartbetaling 117, 118, 119
kredietkaartuitgever 119

L

labelen 117, 128
labeling 127, 128
labelinginitiatief 129
labelinginstantie 115
labelingsysteem 129
leveringskosten 96, 97, 124
licentie 53
login 147

M

*maatschappij voor het beheer van
auteursrechten Zie vennootschap voor
het beheer van auteursrechten*
metatag 147
metatags 30
minderjarigen 38, 39, 78, 79, 127
modem 16, 17, 18, 19, 20,
..... 21, 22, 23, 140, 147
moderator 39, 147
morele rechten 49, 50, 52
mp3 24, 30, 33, 55, 56, 57, 66, 147
multimedia 148, 152

N

namaak 54, 56, 57, 59, 82, 89, 151
navigator 28, 29, 63, 141, 148
nepbericht 36, 145
netiquette 39, 148
newsgroup 38, 142, 148
nieuwsgroep 142

O

onrechtmatige bedingen..... 25
onthaaltapagina..... 29, 31, 58
ontvangstbewijs..... 98, 109, 120
overdracht van gegevens. 18, 36, 67, 151
overeenkomst op afstand..... 148, 152

P

pdf..... 2, 148
pedofilie..... 79
persoonsgegevens..... 22, 23, 24, 39, 42,
..... 62, 65, 67, 68, 70, 74, 75,
... 98, 99, 116, 136, 142, 148, 151, 156
plug-in..... 149, 150
pop-up..... 149
portaal..... 149
processor..... 16
promotieaanbiedingen..... 21, 95
protocol..... 28, 29, 39, 80, 117,
..... 145, 146, 149, 151
proxyserver..... 65

R

RAM..... 16
RAM-geheugen..... 16
recht op integriteit..... 50
recht op verbetering..... 24, 69, 75
recht op verzet..... 66, 70, 75
recht sui generis..... 60
recht van openbaarmaking..... 50
reclame..... 23, 48, 58, 74, 75, 76,
... 77, 95, 127, 136, 138, 143, 149, 150
reproductie..... 47, 49, 53, 54, 55, 89
reproductierecht..... 49

S

script..... 31, 149
scripttaal..... 149
Secure Electronic Transactions .. Zie SET

Secure Socket Layer.....Zie SSL
server..... 28, 31, 35, 37, 38, 42, 43,
..... 47, 53, 62, 63, 64, 73, 76, 78, 79,
..... 118, 141, 144, 145, 147, 149,
..... 150, 151, 152
SET..... 117, 118, 150
shareware..... 33, 66, 144, 150
smaad..... 34, 36, 39, 42, 135, 138
SMS..... 34
SMTP..... 150
software..... 16, 22, 28, 30, 33, 35, 37,
..... 53, 55, 56, 57, 64, 66, 67, 74,
..... 80, 82, 85, 86, 87, 89, 98, 99,
..... 104, 106, 107, 108, 109, 116,
..... 118, 120, 123, 143, 144, 146,
..... 149, 150, 151
software met vrijwillige bijdrage..... 150
spamming..... 74, 76, 150
spionagesoftware..... 62, 66, 67, 150
spyware..... 62, 66, 67, 150
SSL..... 117, 118, 150

T

TCP/IP..... 28, 62, 146, 149, 150, 151
televisiekabel..... 17, 18, 19
thuispagina..... 145, 151
toegangsrecht..... 66
transfersnelheid..... 17, 21

U

URL..... 117

V

vaderschapsrecht..... 50
valsheid in informatica..... 82, 146, 151
vennootschappen voor het beheer van
auteursrechten..... 52
vergunning..... 45, 49, 52, 57
vermogensrechten..... 49, 50
verzakingsrecht..... 96, 97, 98, 100, 110,

..... 111, 112, 113, 114, 115,
 123, 124, 125, 126, 137, 152
virus 17, 36, 67, 85, 86, 87, 88, 89, 152

W

W3C..... Zie W3-Consortium
 W3-Consortium..... 152
webgids..... 31, 150, 152
webpagina 22, 28, 29, 30, 31, 32,
 42, 43, 47, 53, 54, 62, 74,

..... 94, 97, 99, 100, 121, 140,
 144, 145, 152, 153
wedstrijden en promotiespelen 95
werknemer 71, 72, 73
World Wide Web..... 29, 144, 145, 152

Z

zoekmachine 29, 30, 58, 64, 94, 153
zoekmotor 29, 30, 99, 153