april
2011

Gids voor internetgebruikers

economie
FOD Economie, K.M.O., Middenstand en Energie

.be

Gids voor internetgebruikers

economie
FOD Economie, K.M.O., Middenstand en Energie

Federale Overheidsdienst Economie, K.M.O., Middenstand en Energie
Vooruitgangstraat 50
B - 1210 BRUSSEL
Ondernemingsnr.: 0314.595.348
http://economie.fgov.be

tel. 02 277 51 11

Vanuit het buitenland:
tel. + 32 2 277 51 11

Verantwoordelijke uitgever: Regis Massant
Voorzitter a.i. van het Directiecomité
Vooruitgangstraat 50
B-1210 BRUSSEL

Wettelijk depot: D/2011/2295/19

S4-11-0079/0964-11

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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 maart 2011. Sedertdien kunnen de wetgeving of de tarieven wijzigingen hebben ondergaan. Deze gids is een vulgariserend werk. Voor bijkomende informatie kun je steeds terecht bij technische of juridische adviseurs.

Vertaling

Dit werk werd oorspronkelijk in het Frans opgesteld. De Nederlandse versie werd verzorgd door de vertaaldienst 'King Darling Communications'.

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://economie.fgov.be/information_society/consumers/consumers_internetguide/home_fr.htm

Nederlandse versie:

http://economie.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

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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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:

Alexandre Cruquenaire
Marie Demoulin
Didier Gobert
Christophe Lazaro
Benjamin Marthoz
Étienne Montero
Romain Robert
Aurélie Van der Perre
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

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Voorwoord

Deze gids wil, in zo duidelijk mogelijke taal, de sluier rond het internet oplichten en een antwoord bieden op heel wat vragen die u zich stelt, als potentiële surfer of als echte internetgebruiker.

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 internet-medium te komen.

Gelet op het stijgend aantal internetgebruikers en op de mogelijke risico's die met dit medium gepaard gaan, en met het oog op meer transparantie en voorlichting naar het publiek toe 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.

Het internet maakt ook het uitwisselen van informatie mogelijk. 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 veelbelovende toekomst tegemoet lijkt te gaan.

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

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

Veel leesgenot!

Regis MASSANT,

Voorzitter van het Directiecomité a.i.

© Nmedia - Fotolia.com

Inhoudstafel

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Inhoud

Nota van de uitgever ... **3**

Voorwoord ... **7**

Deel 1. Zich aansluiten op het internet ... **23**

Hoofdstuk I. Aansluiting op het internet ... **25**

1. Waar en hoe kan ik op het internet? ... 25
2. Welke hardware en software moet ik gebruiken? ... 26
3. Welke communicatietechnologie moet ik kiezen? ... 27
4. Hoe kan ik surfen via het telefoonnetwerk? ... 27
5. Hoe kan ik surfen via de televisiekabel? ... 30
6. Met welke draadloze technologieën kan ik surfen? ... 30
7. Hoe kan ik thuis Wi-Fi gebruiken? ... 32

Hoofdstuk II. Toegang tot het internet ... **34**

8. Waarmee moet je rekening houden bij het kiezen van een internet service provider (ISP)? ... 34
9. Zijn groepsaanbiedingen interessant? ... 35
10. Wordt mijn privéleven geëerbiedigd? ... 36
11. Wat zijn mijn verplichtingen tegenover de internetprovider? ... 37
12. Welke onrechtmatige bedingen zitten er soms in contracten van internet service providers? ... 38

Deel 2. Op het internet communiceren ... **41**

Hoofdstuk I. Informatie naslaan ... **43**

13. Welke weg volgt de informatie die op het internet verstuurd wordt? ... 43
14. Wat is het "cache(geheugen)" op je harde schijf? ... 44
15. Wat is een URL? ... 45
16. Wat is een zoekmachine? ... 45
17. Hoe kan mijn site in een zoekmachine worden opgenomen? ... 46
18. Wat is een webgids? ... 47
19. Wat is een hypertekstlink? ... 47
20. Welke soorten hypertekstlinks bestaan er? ... 48

Hoofdstuk II. Informatie downloaden 49

21. Mag ik alles wat op het internet staat downloaden? 49
22. Wat is peer-to-peer? 49
23. Wat zijn de meest uitgewisselde media? 50
24. Hoe kan de muziekindustrie de strijd aanbinden tegen het illegale gebruik van p2p? 51
25. Mag ik bestanden (muziek, films enz.) downloaden via een p2p-systeem? 51

Hoofdstuk III. Zich uitdrukken op internet 53

26. Wat is elektronische post? 53
27. Wat zijn de zwakke punten van e-mail? 53
28. Hoe weet ik zeker dat de geadresseerde mijn e-mailbericht heeft ontvangen? 55
29. Wat is een hoax? 56
30. Wat is "chatten"? 57
31. Hoe kan ik "chatten"? 57
32. Welke risico's houdt het chatten in? 58
33. Wat is Web 2.0? 58
34. Wat zijn de risico's die aan Web 2.0 zijn verbonden? 59
35. Wat is een discussieforum? 60
36. Hoe krijg ik toegang tot een discussieforum? 60
37. Welke risico's zitten er aan een discussieforum? 61
38. Wat is een blog? 62
39. Hoe kan ik deelnemen aan een blog? 63
40. Hoe maak je een blog aan? 63
41. Welke risico's zijn er verbonden aan het gebruik van een blog? 64
42. Is de blogger verantwoordelijk voor berichten die door derden zijn gepost? 64
43. Wat is netiquette? 65

Deel 3. Mijn internetruimte ontwerpen 67

Hoofdstuk I. Een domeinnaam reserveren 69

44. Wat is een domeinnaam? 69
45. Ben ik verplicht een domeinnaam te hebben? 70

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

46. Waaruit bestaat een domeinnaam? 71
47. Welke uitbreidingen zijn mogelijk? 71
48. Tot wie moet ik mij richten om een domeinnaam te laten registreren? 72
49. Moet ik aan voorwaarden voldoen om een domeinnaam te bekomen? 72
50. Kan ik om het even welke domeinnaam bekomen? 73
51. Waar kan ik terecht indien ik de reservatie van een domeinnaam door een derde betwist? 74

Hoofdstuk II. Mijn rechten en plichten 75

52. Welke basisregels moet ik respecteren? 75
53. Wat zijn mijn rechten en plichten met betrekking tot de eerbiediging van de privacy van derden? 76
54. Wat zijn mijn rechten en plichten met betrekking tot het recht op afbeelding van derden? 77
55. Wat zijn mijn rechten en plichten met betrekking tot het recht van de eer van derden? 78
56. Wat zijn mijn rechten en plichten met betrekking tot de eerbiediging van de intellectuele rechten van anderen? 78
57. Wat is beschermd door het auteursrecht? 79
58. Moet ik nog aan andere voorwaarden voldoen om door het auteursrecht te worden beschermd? 80
59. Welke rechten heeft een auteur op zijn werk? 81
60. Welke vermogensrechten heeft een auteur op zijn werk? 81
61. Welke morele rechten heeft een auteur op zijn werk? 82
62. Hoe lang is een werk beschermd? 83
63. Wat is niet door het auteursrecht beschermd? 83
64. Mag ik nooit een auteursrechtelijk beschermd werk reproduceren? 84
65. Tot wie moet ik mij richten indien ik toestemmingen voor het gebruik van een auteursrechtelijk beschermd werk wens te verkrijgen ? 85
66. Wat is een merk? Wat is zijn rol? 86
67. Wat zijn de voorwaarden om te kunnen genieten van de bescherming door een merk? 86
68. Wat is de draagwijdte van de bescherming door een merk? 87
69. Heb ik het recht om software voor de aanmaak van webinhoud te gebruiken? 88

70. Mag ik een foto scannen om in mijn persoonlijke ruimte te plaatsen? 89
71. Mag ik een beeld (tekening) scannen en op mijn persoonlijke ruimte plaatsen? 90
72. Mag ik een tekst scannen en op mijn persoonlijke ruimte plaatsen? 90
73. Mag ik een werk (beeld, logo, icoon, foto, tekst, videosequens, muziekbestanden) van een andere site of persoonlijke ruimte kopiëren of downloaden om het op mijn persoonlijke ruimte plaatsen? 91
74. Mag ik een beeld of foto vastgelegd op een analoge drager scannen of een beeld of foto vastgelegd op een digitale drager kopiëren en op mijn persoonlijke ruimte plaatsen, zelfs als ik er vooraf wijzigingen in aanbreng? 92
75. Mag ik muziekbestanden (bijvoorbeeld mp3's) op mijn persoonlijke ruimte ter beschikking stellen van internetgebruikers? 92
76. Mag ik hyperlinks die verwijzen naar sites met mp3-bestanden, op mijn persoonlijke ruimte plaatsen? 94
77. Mag ik beschermde werken (muziek, films, enz.) verspreiden via peer-to-peersystemen? 94
78. Mag ik een werk zonder copyright-vermelding vrij kopiëren? 95
79. En wat met de werken die worden verspreid met de vermelding "zonder auteursrechten" (copyright free), "open access", "vrije licentie", "freeware" of "shareware"? 96
80. Wanneer ik met een hyperlink verwijs naar een andere website, moet ik dan de toestemming vragen aan de eigenaar van die site? 97
81. Kan ik mij verzetten tegen het plaatsen van een hyperlink naar mijn site? 98
82. Welke zijn de sancties i.g.v. niet naleving van het auteursrecht ? 98
83. Mag ik het merk van een derde op mijn persoonlijke ruimte gebruiken? 99
84. Hoe kan ik mijn persoonlijke ruimte optimaliseren voor zoekmachines zonder de rechten van derden te schenden? 100
85. Is mijn persoonlijke ruimte beschermd door het auteursrecht of door een ander recht? 101

Deel 4. Zich beschermen tegen "aanvallen" op het internet 103

Hoofdstuk I. Inbreuken op het privéleven 105

86. In hoever wordt mijn privéleven bedreigd als ik op het internet surf? 105
87. Wat is een cookie? 106
88. Waartoe dient een cookie? 107
89. Moet ik op mijn hoede zijn voor cookies? 108

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

90. Hoe kan ik mij beschermen tegen cookies? 108
91. Hoe kan ik mij juridisch beschermen? 110
92. Wat is spionagesoftware? 110
93. Waartoe dient spionagesoftware? 111
94. Hoe kan ik mij beschermen tegen spionagesoftware? 111
95. Wat is verwerking van persoonsgegevens? 113
96. Hoe kan ik weten wie voor de verwerking van mijn gegevens verantwoordelijk is? 114
97. Wat zijn de algemene principes van de gegevensverwerking door de verantwoordelijke? 114
98. Over welke rechten beschik ik om mijn privacy te beschermen? 115
99. Welke mogelijkheden tot beroep heb ik als mijn rechten niet worden geëerbiedigd? 117
100. Zijn mijn persoonsgegevens beschermd buiten de Europese Unie? 118
101. Wat zijn de grote principes? 119
102. Kan ik in de arbeidsovereenkomst afstand doen van mijn recht op privé-leven? 121
103. Mag mijn werkgever de inhoud van mijn e-mails controleren? 121
104. Mag mijn werkgever mijn internetgebruik controleren? 122

Hoofdstuk II. De oplichters en ongewenste e-mail 124

105. Wat zijn de meeste verspreide vormen van ongewenste e-mail? 124
106. Hoe komen verzenders van ongevraagde e-mails aan mijn elektronisch adres? 126
107. Moet is spam vrezen? 126
108. Bestaan er technische middelen om je tegen spamming te beschermen? 127
109. Zijn er technische mogelijkheden om me te beschermen tegen oplichters? 128

Hoofdstuk III. Illegale en nadelige sites 129

110. Mag ik een illegale site op het web straffeloos raadplegen? 129
111. Wat moet ik doen als ik kinderpornografisch materiaal aantref op het internet? 129
112. Hoe kunnen minderjarigen worden beschermd tegen ongewenste informatie? 131

113. Welke filtersystemen zijn thans beschikbaar? 131
114. Zijn filtersystemen efficiënt? 132
115. Wat moet ik doen als ik op het web een illegale of voor mij nadelige site aantref? 132
116. Wie kan ik voor het gerecht dagen om schadeloosstelling te krijgen? 133

Hoofdstuk IV. Cybercriminaliteit 134

117. Wat is informaticavervalsing? 134
118. Voorbeelden van informaticavervalsing 134
119. Is informaticavervalsing strafbaar? 135
120. Kan ik informaticavervalsing plegen zonder dat ik mij daarvan bewust ben? 135
121. Wat is informaticabedrog? 136
122. Voorbeelden van informaticabedrog 136
123. Is informaticabedrog strafbaar? 136
124. Kan ik informaticabedrog plegen zonder dat ik mij daarvan bewust ben? 137
125. Wat is hacking? 137
126. Is ongeoorloofde toegang tot gegevens voor de lol, als uitdaging of om de veiligheid van een systeem te testen strafbaar? 138
127. Wat met hulpmiddelen en apparatuur om gemakkelijker te kunnen hacken? 139
128. Zijn er omstandigheden die de strafmaat kunnen verzwaren? 139
129. Kan ook ik het slachtoffer zijn van hacking? Hoe kan ik mij daartegen beschermen? 140
130. Wat is computersabotage? 141
131. Zijn er verzwarende omstandigheden? 141
132. Wat met sabotagehulpmiddelen? 142
133. Wat is een computervirus? 142
134. Welke levensloop heeft een computervirus? 143
135. Hoe krijg ik een virus? 144
136. Hoe kan ik weten of mijn computer besmet is? 144
137. Hoe kan ik mij tegen virussen wapenen? 145
138. Is het verzenden van virussen strafbaar? 145
139. Mag ik voor de lol of als grap een "sympathiek" virus versturen? 146

140. Kan ik worden gestraft als ik buiten mijn weten een virus verspreid dat mijn adressenbestand besmette? 146

141. Wat moet ik denken van e-mails die mij waarschuwen dat er een gevaarlijk virus in omloop is? 146

142. Mag het gerecht of de politie bij mij binnenvallen en mijn informaticamaterieel in beslag nemen? 147

143. Mogen zij gegevens van mijn harddisk of mobiele informatiedragers kopiëren ? 147

144. Mogen zij mij beletten toegang te hebben tot sommige gegevens of die gegevens wissen? 147

145. Kan een huiszoeking worden uitgebreid naar de elektronische gegevens buiten mijn eigen systeem? 148

146. Mogen zij mij verplichten informatie te verschaffen over de manier waarop ik toegang kreeg tot beveiligde gegevens? 149

147. Worden mijn oproep- en identificatiegegevens bij gebruik van het internet geregistreerd en bewaard door sommige netwerk- en dienstenoperatoren? 149

Deel 5. Een overeenkomstsluiten op het web 151

Hoofdstuk I. Reclame, wedstrijden en promotionele aanbiedingen op internet 153

148. Hoe kan ik op netwerken het verschil zien tussen reclame en andere informatie? 153

149. Wat met promotieaanbiedingen, wedstrijden en promotiespelen op de netwerken? 153

150. Hoe moet ik denken over aanbiedingen voor gratis goederen of diensten? 154

151. Hebben adverteerders het recht mij via e-mail ongewenste reclame toe te sturen? 156

152. Zijn er uitzonderingen op het principe van voorafgaande toestemming? 156

153. Heb ik het recht om reclame via e-mail te weigeren? 157

154. Wat moet ik in de praktijk doen om gebruik te maken van mijn recht op verzet? 158

155. Geldt dit alles ook voor sms-berichten en pop-ups? 158

Hoofdstuk II. De sleutel van het vertrouwen: goede informatie 159

156. Met wie heb ik te maken? Op welke informatie over de dienstverlener en zijn activiteiten heb ik recht? 159

157. Over welke informatie moet ik beschikken voor ik een bestelling plaats? ... 160
158. Moeten de algemene voorwaarden mij worden meegedeeld vóór het sluiten van de overeenkomst? ... 162
159. Welke informatie moet ik krijgen na mijn bestelling? ... 162
160. Kan ik het verloop van mijn bestelling volgen na het sluiten van de overeenkomst? ... 164

Hoofdstuk III. Het sluiten van een overeenkomst op het internet ... 165

161. Hoe kan ik iets bestellen op een website? ... 165
162. Hoe kan ik weten of ik geen fouten heb gemaakt in mijn bestelling? ... 166
163. Vanaf wanneer ben ik contractueel verbonden? ... 167
164. Hoe ben ik zeker dat de verkoper mijn bestelling gekregen heeft? ... 167

Hoofdstuk IV. Bewijs en elektronische handtekening ... 168

165. Hoe kan ik bewijzen dat ik iets op het internet heb besteld? ... 168
166. Hoe kan de onderneming bewijzen dat ik iets via het internet heb besteld? ... 169
167. Wordt een gewone e-mail als bewijs erkend? ... 169
168. Is een elektronisch ondertekend document een afdoend bewijsmiddel? ... 170
169. Wat is een geavanceerde elektronische handtekening? ... 171
170. Wat is een certificatiedienstverlener? ... 173
171. Wat is een gekwalificeerd digitaal certificaat? ... 174
172. Wat is een veilig middel voor het aanmaken van een elektronische handtekening? ... 175
173. Hoe kan ik een digitaal certificaat bekomen? ... 176
174. Hoe werkt een digitale handtekening in de praktijk? ... 177
175. Wordt de elektronische aangetekende brief in het Belgisch recht erkend? ... 177

Hoofdstuk V. Herroepingsrecht ... 179

176. Wat is het herroepingsrecht? ... 179
177. Voor welke soort aankopen beschik ik over een herroepingsrecht? ... 179
178. Hoe kan ik weten of ik over een herroepingsrecht beschik? ... 180
179. Wat kan ik doen als ik niet werd ingelicht over mijn herroepingsrecht? ... 181
180. Binnen welke termijn mag ik aan een overeenkomst verzaken? ... 181
181. Mag ik aan de overeenkomst verzaken indien ik de prijs reeds betaalde? ... 182

182. Moet ik een vergoeding betalen om aan de overeenkomst te kunnen verzaken? 183

183. Mag ik aan de aankoop van een goed of dienst verzaken wanneer ik een lening aanging om de betaling te financieren? Wat gebeurt er met mijn kredietovereenkomst bij herroeping? 183

184. Hoe moet ik de verkoper laten weten dat ik aan de overeenkomst verzaak? 184

185. Welke zijn mijn verplichtingen als ik de overeenkomst herroep? 184

186. Welke verplichtingen heeft de verkoper wanneer ik aan de overeenkomst verzaak? 184

Hoofdstuk VI. Betaling 185

187. Ben ik verplicht te betalen bij de levering? 185

188. Welke betaalmiddelen kan ik op de netwerken gebruiken? 185

189. Kan ik met een kredietkaart betalen? 185

190. Welke risico's zitten er aan het gebruik van een kredietkaart op de netwerken? 186

191. Met welke technische middelen worden kredietkaartbetalingen op de netwerken beveiligd? 187

192. Moet ik de gevolgen dragen van het feit dat iemand met mijn kredietkaart bedrog pleegt op de netwerken? 188

193. Wat moet ik doen als iemand mijn kredietkaart met bedrieglijk opzet gebruikt? 189

194. Wat moet ik doen als ik vooraf betaalde met mijn kredietkaart en de verkoper de overeenkomst niet nakomt? 189

195. Mag ik met mijn debetkaart van Bancontact / Mister Cash betalen? 190

196. Kan ik rechtstreeks op de site betalen met een elektronische overschrijving? 190

197. Hoe betaal ik met behulp van mijn telefoon? 191

198. Hoe doe ik online aankopen met een voorafbetaalde kaart? 191

199. Kan ik met een bankoverschrijving betalen? 192

200. Kan ik bij de levering betalen? 192

Hoofdstuk VII. Levering van het goed of dienstverlening 193

201. Wanneer moet de verkoper de overeenkomst uitvoeren? 193

202. Wat moet ik doen wanneer de verkoper draalt om mijn bestelling uit te voeren? 193

203. Wordt de overeenkomst online of offline gesloten? ... 194
204. Moet ik betalen als het product zoek raakt of tijdens het transport beschadigd raakt? ... 194
205. Wat moet ik doen indien het geleverde goed niet beantwoordt aan de beschrijving op de site? ... 194
206. Op welke informatie heb ik recht bij de levering? ... 195
207. Welke gevolgen heeft de levering? ... 196

Hoofdstuk VIII. Terugbetaling en Klantenservice ... 197

208. In welke gevallen mag ik terugbetaling van mijn aankopen eisen? ... 197
209. Welke formaliteiten moet ik vervullen om terugbetaald te worden? ... 197
210. Als ik aan de overeenkomst verzaak, binnen welke termijn moet de verkoper me dan terugbetalen? ... 198
211. Geldt er voor de goederen en diensten die ik op het internet koop een waarborg of klantenservice? ... 198

Hoofdstuk IX. Minderjarigen en e-commerce ... 200

212. Kan mijn kind zelf geldige aankopen doen op het internet? ... 200
213. Kan ik onlineaankopen van mijn kind annuleren? ... 201
214. Kan een onderneming eisen dat een overeenkomst die mijn kind heeft afgesloten nietig wordt verklaard omwille van zijn minderjarigheid? ... 201
215. Kan de onderneming bij annulering van een overeenkomst een schadevergoeding eisen van de ouders? ... 202
216. En als mijn kind heeft gelogen door zich uit te geven voor een volwassene? ... 202
217. Kan ik het herroepingsrecht van mijn kind inroepen om terug te komen op onlineaankopen? ... 203
218. Kan ik me verzetten tegen betalingen die mijn kind heeft gedaan met mijn kredietkaart? ... 203
219. Hoe kan ik de aankopen van mijn kind op het internet in goede banen leiden? ... 203
220. Ik heb op het web een goed gekocht dat door een minderjarige te koop werd aangeboden. Kunnen zijn ouders de overeenkomst annuleren? ... 204

Hoofdstuk X. Veilingen en handel tussen privépersonen ... 205

221. Kan je je kost verdienen door voorwerpen te verkopen op het internet? ... 205
222. Kan je alles verkopen en aankopen op het internet? ... 205

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

223. Welke regels zijn van toepassing op de veilingen en de handel tussen privépersonen op het internet? 206

224. Kan ik me tot de verantwoordelijke van de site wenden als de verkoop slecht afloopt? 206

Hoofdstuk VIII. Gedragscodes en labeling 208

225. Wat is een gedragscode? 208

226. Kan ik vertrouwen hebben in een gedragscode? 208

227. Kan ik mij beroepen op een gedragscode? 209

228. Wat is labeling? 209

229. Kan ik een op een website aangebracht label vertrouwen? 210

Deel 6. Regeling geschillenop internet 211

230. Wat te doen bij geschillen? 213

231. Wat te doen bij geschillen met een persoon of een bedrijf in het buitenland? 213

232. Wat is een wisselmechanisme voor de regeling van onlinegeschillen (ADR)? 214

233. Wanneer en hoe kan ik een beroep doen op dat soort mechanisme? 215

234. Wat zijn de voordelen van ADR? 216

235. Kan ik een elektronisch bemiddelings- of arbitragemechanisme vertrouwen? 216

236. Mag men mij dit soort mechanisme opleggen bij het sluiten van een overeenkomst? 217

237. Welke waarde heeft een ADR-beslissing? 218

Glossarium 219

Glossarium 221

Nuttige teksten en adressen 243

Nuttige teksten 245

Nuttige adressen 247

© olly - Fotolia.com

Deel 1.
Zich aansluiten op het internet

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Hoofdstuk I. Aansluiting op het internet

Het internet is een communicatiemiddel waardoor je trefzeker de meest diverse informatie kunt opzoeken en raadplegen. Je kunt hierdoor 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), snel bestanden overzenden (*FTP*), telefoneren (Voice over IP) of zelfs deelnemen aan videoconferenties via computernetwerken. Welke sleutels heb ik nodig om toegang te krijgen tot die mogelijkheden?

1. Waar en hoe kan ik op het internet?

Thuis, in de privésfeer, wordt het vaakst gebruik gemaakt van het internet.

Een groot aantal personen kan niettemin op hun werk op het internet als hun werkgever hen dergelijke toegang voorziet. Bepaalde universiteiten en scholen bieden aan hun studenten en leerlingen ook internettoegang aan om opzoekingen te doen en om hun taken te maken. In dit opzicht willen we aangeven dat deze gebruikers zich meestal aan een "IT-handvest" moeten houden dat werd opgesteld door de netwerkbeheerder en dat het toegelaten of het verboden gebruik van het internet en de door de instelling ter beschikking gestelde IT-infrastructuur beschrijft. Inbreuken op dit IT-beleid gaan over het algemeen vergezeld van sancties.

Sinds kort stellen bepaalde gemeentes "Openbare Computerruimtes" ter beschikking van hun inwoners. Het zijn voorzieningen die zijn bedoeld om de bevolking in te wijden in de informatica en het internetgebruik.

Naast deze mogelijkheden willen we ook de "cybercafés" aanhalen. Het zijn openbare en commerciële ruimtes waar computers met internetverbinding ter beschikking worden gesteld. Het gebruik van de computer moet worden betaald en de prijs is over het algemeen afhankelijk van de gebruiksduur.

Door de ontwikkeling van de "Wi-Fi-technologie" kun je met je laptop gratis of tegen betaling draadloos surfen in bepaalde restaurants, cafés, stations, luchthavens of andere openbare plaatsen.

Voor privégebruik van het internet moet de gebruiker een abonnement nemen bij een internetprovider. Er zijn verschillende internetproviders op de markt. Er wordt tussen de verschillende leveranciers voornamelijk geconcurreerd op het vlak van de prijs, de snelheid van de internetverbinding, de gebruikte technologie of de eventuele bijkomstige diensten.

Om te kunnen surfen, moet je over de nodige apparatuur beschikken (computer, modem enz.) en over een geschikte verbindingsmogelijkheid om de computer in verbinding te stellen met de internetprovider (distributiekabel, telefoonlijn, draadloze verbinding enz.).

2. Welke hardware en software moet ik gebruiken?

Doorgaans heb je een computer (pc of laptop) nodig om op het internet te kunnen surfen. Momenteel kun je je met alle op de markt beschikbare computers op het internet begeven. Surfen op het internet is wel een heel stuk aangenamer als je over een voldoende krachtig apparaat beschikt (on het bijzonder voor het downloaden van video's, software of muziek).

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. Alle types en merken van computers zijn dus geschikt om verbinding te maken.

Er zijn ook andere toestellen dan computers waarmee kan worden gesurft, zoals bepaalde draagbare telefoons, PDA's (*Personal Digital Assistant*) of nog andere mediaspelers die kunnen worden geconfigureerd om verbinding te maken met het internet en om te surfen, te downloaden of om e-mails te versturen. Deze terminals die soms op kleine zakcomputers lijken, kunnen een geïntegreerde modem bevatten of een systeem waarmee draadloos kan worden verbonden en beschikken over speciaal ontwikkelde software voor een vlotter en aan hun grootte aangepast gebruik van het internet.

Er is heel veel software beschikbaar om gebruik te maken van de internetfunctionaliteiten. Je kunt bijvoorbeeld je *e-mail beheren* door middel van specifieke software als o.a. Eudora, Thunderbird of Outlook. Om op *het web te surfen* kan je met een programma dat over het algemeen een "browser" wordt genoemd de inhoud van internetwebsites bekijken. De meest gebruikte programma's hiervoor zijn Internet Explorer en Mozilla Firefox. Om te *chatten* kun je met MSN Messenger of Yahoo! Messenger, in realtime (=live) gesprekken voeren of zelfs een videoconferentie (gesprek met geluid en beeld) starten. Er bestaat nog andere software die wordt gebruikt voor andere internetfunctionaliteiten, maar het is moeilijk om daarvan een complete lijst op te stellen.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Op internet kun je ook een heleboel programma's van uiteenlopende aard downloaden. Die programma's zijn vaak gratis. Soms zijn ze dat enkel tijdens een demoperiode en moet je daarna betalen om ze verder te kunnen gebruiken. Kijk uit en download enkel die programma's waarvan je de oorsprong kent. Het risico om een virus binnen te halen loert immers altijd om de hoek.

3. Welke communicatietechnologie moet ik kiezen?

Je kunt met verschillende communicatietechnologieën verbinding maken met het internet. Voor elke technologie is er een "modem" nodig. De modem is een technische interface tussen de gebruikte computer en de internetprovider. Hij zorgt ervoor dat er kan worden gecommuniceerd met de server van de internetprovider en dat er numerieke gegevens kunnen circuleren op de netwerken (via een kabel of draadloos).

Dit zijn de belangrijkste verbindingsmogelijkheden:

- het telefoonnetwerk;
- de televisiekabel;
- de draadloze technologieën

Wat de "modems" betreft, zijn er voor elk communicatiemiddel verschillende normen, technologieën en merken. Ze worden vaak door de internetproviders voorzien en kunnen bij hen worden gehuurd of gekocht. Het is natuurlijk eveneens mogelijk om ze aan te schaffen in een speciaalzaak.

4. Hoe kan ik surfen via het telefoonnetwerk?

Het telefoonnetwerk is het netwerk waarop de traditionele telefoonlijn is aangesloten. Op dit type netwerk kunnen ook elektronische gegevens circuleren en kan er dus worden gesurft.

Er bestaan verschillende technologieën om gegevens over te dragen op het telefoonnetwerk: de inbelverbinding, ISDN en xDSL en zijn varianten. We zullen de eerstgenoemde technologieën slechts kort behandelen, aangezien er tegenwoordig nog zelden van wordt gebruikgemaakt.

De inbelverbinding

Deze technologie maakt gebruik van de gewone telefoonlijn (het Public Switched Telephone Network of "PSTN") en maakt gegevensoverdracht mogelijk met een maximale theoretische snelheid van 56.000 bits per seconde, wat relatief traag is in vergelijking met de andere beschikbare technologieën (zoals ADSL).

Internetproviders bieden over het algemeen internettoegang via een inbelverbinding aan zonder abonnement, door middel van een eenmalige gratis inschrijving. Om gebruik te kunnen maken van dit type verbinding moet je over een vaste telefoonlijn beschikken. Er wordt ingebeld naar een speciaal nummer (tegen een hogere prijs dan een gesprek naar een vaste telefoon) en de verbinding wordt meestal per minuut aangerekend. Er is een specifieke modem en de installatiesoftware wordt over het algemeen verschaft door middel van een cd-rom of wordt online aangeboden.

De inbelverbinding legt beslag op de telefoonlijn, het gevolg daarvan is dat de gebruiker geen in- of uitgaande telefoongesprekken kan voeren als de internetverbinding actief is.

Het Integrated Services Digital Network (ISDN)

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

Een ISDN-verbinding is ook sneller dan een inbelverbinding (je kunt er viermaal vlugger mee surfen dan met een klassieke lijn) op het traditionele verwisselbare telefonische netwerk. Ze biedt dus meer gebruiksgemak tijdens het internetten, omdat deze oplossing overigens de mogelijkheid biedt tegelijk te surfen op het net en te telefoneren, aangezien er twee communicatiekanalen zijn. Doch, in wat volgt zal blijken dat ADSL interessanter kan lijken 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).

ADSL en de technologie afgeleid van xDSL

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 (tot 6 megabits per seconde ("Mbps") downloadsnelheid). ADSL biedt dus

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

breedbandsnelheid. Het gebruikt namelijk de twee koperdraden van de traditionele 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. Je moet dus steeds over een telefoonverbinding beschikken. Er zijn twee mogelijkheden in het geval van een ADSL-verbinding.

In bepaalde gevallen behoud je je traditionele telefoonabonnement bij je vertrouwde netwerkexploitant (bijvoorbeeld Belgacom) en verzoek je aan je internetpovider om een ADSL-verbinding, die de lijn van je exploitant zal gebruiken om je in verbinding te stellen met zijn internetinfrastructuur.

In andere gevallen kan de internetprovider je voorstellen om volledig onafhankelijk te worden van je vertrouwde netwerkexploitant, met wie je dan geen contractuele verbintenis meer zal hebben. Deze optie is echter niet voor alle gebruikers beschikbaar: het is afhankelijk van de configuratie van hun verbinding met het telefoonnetwerk. Als deze het toelaat, kan de internetprovider de totale controle nemen over de telefoonlijn en zo niet meer langs de exploitant passeren die daarvoor de lijn beheerde.

ADSL is eerder aangeraden voor relatief grote websurfers. Voor deze oplossing betaal je een forfaitair maandabonnement. Je telefoonrekening is dus niet meer gelinkt aan de duur van je internetverbinding (zoals bij een inbelverbinding het geval is). De internetprovider ontfermt zich over de technische installatie (te weten het bijstellen van de filter op je telefoonstekker en de levering van de geschikte modem, die kan worden gekocht of gehuurd). Naast de aankoop of de huur van de modem kunnen soms activatie- en/of installatiekosten in rekening worden gebracht.

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 gemiddelde internaut dat volume slechts zelden bereikt.

ADSL is een variant van de xDSL-technologie. Op deze technologie zijn ook de ADSL2+-verbindingen gebaseerd, die een hogere verbindingssnelheid bieden dan ADSL. Nog hogere verbindingssnelheden kunnen worden bereikt door middel van de VDSL- en VDSL2-verbindingen (ongeveer 17 Mbps voor VDSL). Deze twee worden nog niet aangeboden door alle internetproviders, maar de evolutie naar deze nieuwe verbindingssnelheden zou in de toekomst moeten blijken. We willen erop wijzen dat de beschikbaarheid van de verschillende xDSL-technologieën (in het bijzonder ADSL2+ en VDSL) om technische redenen niet voor alle gebruikers is gewaarborgd.

5. Hoe kan ik surfen via de televisiekabel?

Naast deze verbindingen die via het telefoonnetwerk verlopen, is het mogelijk om te surfen via de televisiekabel. De snelheden die worden bereikt met de kabelmodems liggen aanzienlijk hoger dan via het PSTN-netwerk.

Het voornaamste voordeel van deze technologie is dat het een wezenlijk gemak verschaft in het internetgebruik aangezien de meeste Belgische huizen een kabelaansluiting hebben. Ze biedt een snelle (tot 100 Mbps downloadsnelheid) en permanente verbinding zonder te interfereren met de televisiekabel en er is geen verbinding nodig met een telefoonlijn.

De kosten zijn vast en niet afhankelijk van telefooncommunicatiekosten. In het abonnement kan het maandelijkse verkeersvolume worden gelimiteerd en de internetprovider kan het volume dat deze limiet overstijgt, aanrekenen. Deze technologie is een interessant alternatief voor de hogesnelheidsaanbiedingen via xDSL-technologieën.

Om via de kabel te kunnen surfen, heb je net zoals bij een internetverbinding via de telefoonlijn een modem nodig.

6. Met welke draadloze technologieën kan ik surfen?

Sinds kort is het aantal draadloze internettechnologieën sterk toegenomen. Verschillende mogelijkheden worden al op de markt aangeboden, die elk gebruik maken van een andere technologie.

Wi-Fi

Wi-Fi (staat voor "Wireless Fidelity") is een draadloze communicatietechnologie waarmee tegen een hoge snelheid kan worden gecommuniceerd tussen computers en andere terminals die met elkaar zijn verbonden. Als je computer of PDA is uitgerust met een Wi-Fi-kaart kun je surfen met een verbindingssnelheid die in theorie meer dan 10 Mbps kan bedragen. Het bereik van Wi-Fi-golven is niettemin beperkt (in een vrije zone zonder obstakels in theorie tot maximum 300 meter). Dat zorgt ervoor dat er slechts verbinding kan worden gemaakt in het zendgebied van het Wi-Fi-signaal en dus van de antenne die het signaal uitzendt (ook *Hotspot*).

Verschillende internetproviders, openbare gelegenheden en andere commerciële entiteiten (hotels, café- of restaurantuitbaters, stations, luchthavens enz.) hebben Wi-Fi-

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

hotspots geïnstalleerd op drukbezochte plaatsen om hun klanten de mogelijkheid te bieden om te surfen. Deze Wi-Fi-toegang wordt ofwel gratis aangeboden ofwel tegen betaling.

De betaalverbinding is mogelijk door middel van voorafbetaalde kaarten of abonnementen die in het bijzonder bij de internetprovider kunnen worden gekocht die de Wi-Fi-hotspot met het internet verbindt (zoals Telenet of Belgacom, die beiden over een bepaald aantal hotspots beschikken). De gebruiker krijgt een gebruikersnaam en wachtwoord om te kunnen verbinden met de door de provider beheerde hotspots. Er bestaan verschillende websites die een lijst van hotspots in de wereld ter beschikking stellen en waarmee je de dichtstbijzijnde hotspot alsook de toegangsvoorwaarden voor de hotspot kan vinden (bijvoorbeeld: http://www.jiwire.com of http://www.trustive.com/hotspots/).

We willen tevens wijzen op het bestaan van "Wi-Fi-gemeenschappen" waarvan de leden hun internettoegang via hun Wi-Fi-verbinding delen. Een voorbeeld van een Wi-Fi-gemeenschap is de FON-gemeenschap (www.fon.com): de leden delen hun internetverbinding gratis met elkaar. Niet-leden kunnen toegang krijgen tot de hotspots van de leden door te betalen.

Wi-Fi-technologie wordt ook thuis aangewend om de computer met de draadloze modem te verbinden. Het gebruik ervan is in dat geval strikt persoonlijk en beoogt geen voorziening van een internettoegang aan derden. De gebruiker beschikt over zijn eigen Wi-Fi-hotspot die hij voor zijn eigen behoeften aanwendt, zonder deze te delen. We komen verder in de gids terug op het gebruik van Wi-Fi als standaard voor dergelijke doeleinden.

WiMAX

WiMAX is een draadloze communicatietechnologie via hertzgolven met hoge verbindingssnelheid. De verbindingssnelheid is hoger dan bij Wi-Fi, aangezien meerdere kilometers worden overbrugd. Het vermogen (tot meer dan 20 Mbps) zorgt voor een internettoegang zonder kabelverbinding, telefoonlijn, en zonder de nabijheid van een Wi-Fi-hotspot.

Aangezien de WiMAX-frequentieband zeer beperkt is, werden slechts twee licenties afgeleverd in België. Ze werden toegewezen aan ClearWire en Mac Telecom. Het netwerk is niet in heel het grondgebied toegankelijk maar wel in Brussel en andere grote steden zoals Leuven of Gent en de netwerkdekking wordt op korte termijn nog verder uitgebreid.

Om via WiMAX-technologie te kunnen surfen, moet je over een specifieke modem beschikken die de WiMAX-frequentie ontvangt. Je kunt je WiMAX-modem dus verbinden

met je computer via een kabel of ook door middel van Wi-Fi-technologie. De kosten van een abonnement bij ClearWire zijn vergelijkbaar met een ADSL-abonnement. Er moet in eerste instantie worden nagegaan indien je je in een zendgebied van het WiMAX-signaal bevindt.

Mobiel internet

Bepaalde gsm-operatoren stellen nu voor om hun mobiele netwerk te gebruiken om op een laptop of een andere terminal te surfen vanaf eender welke locatie. Dit is in het bijzonder mogelijk gemaakt dankzij de ontwikkeling van 3G-telefonie (mobiele communicatietechnologie van de derde generatie, die gebruik maakt van de UMTS-standaard) die hoge verbindingssnelheden aanbiedt, waarmee een comfortabele mobiele internettoegang mogelijk wordt.

De mobiele internetdiensten aangeboden door gsm-operatoren zijn veel duurder dan de hoger beschreven internettoegangsmogelijkheden en geven niet noodzakelijk een gelijkwaardige verbindingskwaliteit. De voornaamste troef van deze aanbiedingen is niettemin de grote mobiliteit die ze bieden aangezien de gebruiker zich overal kan begeven zonder bij zijn modem te moeten blijven (een specifieke modemkaart moet in de meeste gevallen rechtstreeks op de laptop worden aangesloten, wat voor een zeer mobiel gebruik zorgt).

7. Hoe kan ik thuis Wi-Fi gebruiken?

Thuisgebruik van Wi-Fi

Wi-Fi is een netwerktechnologie waarmee computers en andere terminals (zoals bepaalde mp3-spelers of draagbare telefoons) draadloos of zonder kabel kunnen communiceren via een bepaalde frequentie met hoge verbindingssnelheid.

Met Wi-Fi kan je een intern netwerk opzetten waarbij computers en randapparatuur (printers, modems enz.) binnen hetzelfde huis of binnen eenzelfde onderneming op een bepaalde radiofrequentie met elkaar worden verbonden.

Zo kan je draadloos surfen door je computer met een (geïntegreerde of externe) Wi-Fi-kaart uit te rusten en je modem met een router/Wi-Fi-toegangspunt te verbinden. De router kan over het algemeen worden gekocht of gehuurd bij internetproviders, maar is ook beschikbaar in de speciaalzaak.

De router doet dienst als antenne die in de nabije omgeving een Wi-Fi-signaal uitzendt met een bereik van enkele meters tot meer dan honderd meter, afhankelijk van de ob-

stakels en de omgeving. Dit signaal wordt opgevangen door de Wi-Fi-kaart. Deze kan al aanwezig zijn in de computer (vaak geïntegreerd). Indien dat niet het geval is, kan je er gemakkelijk een aansluiten op een USB-poort van de computer. Je kunt meerdere computers (of andere randapparatuur) verbinden met eenzelfde router, waardoor de internetverbinding kan worden gedeeld met alle computers binnen eenzelfde woning (je kan bijvoorbeeld de computers van het hele huis verbinden met de modem of met de printer via een Wi-Fi-router).

Zoals hierboven werd uitgelegd, wordt Wi-Fi eveneens aangewend om hotspots te installeren, waarmee je in openbare gelegenheden kan surfen. De werking is dezelfde, maar meestal moet je beschikken over een gebruikersnaam en een wachtwoord om met de router/het Wi-Fi-toegangspunt van de persoon die zijn internettoegang ter beschikking stelt, verbinding te kunnen maken.

Wi-Fi-beveiliging

Het probleem van de beveiliging van Wi-Fi-netwerken komt vaker naar voren. Bij draadloze netwerken is het voor derden inderdaad veel gemakkelijker om toegang te krijgen tot een systeem aangezien de door de router uitgestuurde golven zich niet beperken tot een welbepaalde zone. Bijgevolg is het voor hen veel gemakkelijker om er zich toegang tot te verschaffen als het systeem niet beveiligd is.

Het is dus van belang je computer en je Wi-Fi-systeem te beschermen tegen ongewenste indringers. In de handleidingen van de routers en bij de internetproviders kan je waardevolle aanwijzingen vinden om je netwerk te beveiligen. De codering van gegevens en de identificatie van computers die verbinding kunnen maken met het Wi-Fi-netwerk zijn enkele van de beveiligingsmethodes.

Je moet je bewust zijn van de noodzaak om je systeem te beveilige, want doe je dit niet, dan kunnen derden ongevraagd toegang krijgen tot je gegevens, en die zelfs wijzigen en/of vernietigen. Erger nog, het zou piraten de kans geven om de controle over je systeem volledig over te nemen, om zo vanaf je computer (vaak zeer zware) strafbare feiten te plegen, waardoor je op een gegeven moment wel eens bezoek van de federale politie zou kunnen krijgen!

We willen je er ook op wijzen dat verbinding kunnen maken met het onbeveiligde netwerk van een derde niet wil zeggen dat deze persoon je de toestemming geeft om zijn netwerk vrij te betreden, noch om gratis van zijn internetverbinding gebruik te maken. We herhalen dat de internetabonnementen tegen een vast tarief vaak beperkt zijn tot een bepaald maandelijks volume. Als je de verbinding van een derde gebruikt, kan zijn vaste volume immers snel worden verbruikt en dat kan hem duur komen te staan, aangezien elke gigabyte bovenop het maandelijkse volume hem over het algemeen ook zal worden aangerekend.

Hoofdstuk II. Toegang tot het internet

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

Om het internet thuis 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).

Ook als je gekozen hebt voor internettoegang via ADSL of de tv-kabel, verlopen de zaken nauwelijks anders. Voor de installatie heb je wel meestal de hulp van een technicus nodig.

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 internettoegangverschaffers, 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:

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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

9. Zijn groepsaanbiedingen interessant?

Bepaalde internetproviders hebben sinds enige tijd aanbiedingen waarbij verschillende communicatiediensten worden gebundeld. Het is gebruikelijk dat internettoegang wordt gekoppeld aan een telefonieaanbod en/of een televisieabonnement. Verschillende multimediadiensten kunnen dan langs één kanaal worden verzorgd (televisie, telefoon, internet).

De aangeboden packs op de markt bevatten internettoegang, telefoondiensten en/of een televisieabonnement. Elk van de drie elementen kan afzonderlijk bij de leverancier die het pack aanbiedt of bij andere leveranciers worden verkregen. Voor een pack opteren, is vaak goedkoper dan voor elke service afzonderlijk een abonnement te nemen.

De kabelexploitanten, die vanouds leveranciers zijn van televisiediensten, bieden nu hogesnelheidsinternetverbindingen via de kabel aan, alsook telefoondiensten (vaak op "Voice-over-IP-technologie" gebaseerd). Met deze oplossing kan je je losmaken van het telefoonnetwerk, en het internet-, telefoon- en televisieabonnement bij één enkele leverancier groeperen.

Belgacom, die oorspronkelijk een telefonieleverancier is, heeft een zenderaanbod ontwikkeld ("Belgacom TV") en biedt, naast de traditionele telefoonlijn en/of ADSL (of VDSL) een pack met een telefoon-, een internet- en een televisieabonnement aan door middel van de ADSL 2+- of VDSL-technologie. Je kunt je abonnementen dus ook groeperen bij deze ene leverancier en van een televisieabonnement bij een kabelexploitant afzien.

Bepaalde internetproviders die geen televisieabonnement aanbieden hebben een "dual play"-aanbod, d.w.z. een combinatie van een internettoegang en een vaste telefoonlijn, vaak tegen prijzen die veel interessanter zijn dan als op de twee diensten afzonderlijk of bij verschillende leveranciers wordt ingetekend.

De toename van de "packs" maakt de vergelijking complexer – in het bijzonder op het vlak van de tarieven -, maar voor iemand die al over een telefoonlijn, internet en een televisieabonnement beschikt, is het misschien wel voordelig om te kiezen voor een pack. Bepaalde packs bieden zelfs een gsm-abonnement bovenop de andere genoemde diensten. Onthoud niettemin dat de minimale contractduur voor elk abonnement van toepassing is en dat je dus bent gebonden aan dezelfde leverancier voor al je communicatiediensten gedurende deze periode.

10. Wordt mijn privéleven geëerbiedigd?

Wanneer je een abonnement neemt bij een internetprovider, moet je een formulier invullen en enkele persoonsgegevens vermelden.

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. Die wet verschaft je verscheidene rechten, onder meer het recht op volledige voorafgaande informatie, het recht op toegang tot gegevens over jezelf, het recht

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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.

De wet schrijft tevens voor dat de providers bepaalde gegevens moeten bewaren en dat ze deze aan de rechterlijke overheden moeten overmaken indien dat wordt gevraagd.

11. 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 marktpraktijken en consumentenbescherming beschermt je tegen onrechtmatige bedingen, d.w.z. clausules die tot een duidelijke wanverhouding leiden tussen de rechten en plichten van de partijen. Onrechtmatige bedingen zijn verbo-

den, vooral als ze de consument benadelen, en zijn dus nietig. In de praktijk moet je de clausules één per één uitpluizen om na te gaan of ze al dan niet onrechtmatig zijn.

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

Zoals hierboven aangegeven, is een onrechtmatig beding een clausule 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 clausule en zal hij ze desgevallend nietig verklaren.

Soms wordt de beoordelingsbevoegdheid van de rechter grotendeels beïnvloed door de wet. De wet betreffende de marktpraktijken bevat namelijk een lijst met clausules 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 onderneming de prijs niet naar eigen goeddunken mag veranderen;

  Bovendien voorziet de wet dat in geval van een tariefverhoging de abonnee het recht heeft om het contract zonder boete te ontbinden ten laatste op de laatste dag van de maand die volgt op de ontvangst van de eerste factuur nadat de veranderingen van kracht zijn geworden, behalve als de verhoging verbonden is aan de consumptieprijsindex;

- "De provider behoudt zich het recht voor om op elk moment de elementen van het contract te wijzigen zonder mogelijkheid om het contract te ontbinden".

  De wet voorziet dat abonnees ten minste een maand voorafgaand aan de wijzigingen individueel op de hoogte moeten worden gesteld van contractuele wijzigingen; bovendien voorziet de wet dat abonnees ten laatste op de laatste dag van de maand nadat de wijzigingen van kracht zijn geworden het contract kunnen ontbinden zonder boete als ze de wijzigingen niet aanvaarden;

- "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 onderneming 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 op-

eenvolgende 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.

- "De aangegeven prijs zal worden verhoogd met X euro als de abonnee niet betaalt via domiciliëring".

  De wet verbiedt clausules en voorwaarden die een verhoging van de aangekondigde prijs van een dienst tot doel stellen als de consument weigert te betalen via domiciliëring. De wet verbiedt echter niet om een korting op de aangekondigde prijs toe te kennen aan consumenten die via domiciliëring betalen.

- "Het contract zal automatisch worden verlengd op het einde van de contractuele periode zonder dat de consument de nieuwe contractuele termijn kan verbreken".

  De wet bepaalt dat in de dienstenovereenkomsten van bepaalde duur elk beding van stilzwijgende verlenging in het vet gedrukt en in een afzonderlijk kader moet staan op de achterzijde van de eerste pagina.

  Bovendien voorziet de wet dat de consument na stilzwijgende verlenging van het contract het contract op elk moment kan ontbinden met een maximale opzeggingstermijn van twee maanden.

Deel 2.
Op het internet communiceren

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Hoofdstuk I. Informatie naslaan

Afdeling 1. Weg die de informatie volgt op het internet

13. 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 infomatie 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.

14. 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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Afdeling 2. Zoeken naar informatie op het internet

15. 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 The Mozilla Foundation maken het je heel gemakkelijk en bewaren je adressen onder de naam *favorieten* of *favorites* (Internet Explorer) en "bladwijzers" of *bookmarks* (Mozilla Firefox). Zodra je adressen gearchiveerd zijn, volstaat het ze te selecteren in een lijst en erop te klikken.

16. 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. 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 hypertekst-documenten. Voor elk geselecteerd document wordt een "pertinentiescore" opgemaakt op basis van een algoritme dat ei-

gen is aan elke zoekmachine en met een hele reeks criteria zoals het aantal websites met een link naar de desbetreffende pagina, de relevantie van de links, hoe vaak opgezochte sleutelwoorden voorkomen in het document, hoe dicht ze bij elkaar staan, of ze voorkomen in de URL, de titel en de eerste ondertitel van het document, alsook in de metatags[1] enz.

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.).

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

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.

1 Metatags zijn verborgen worden die ingevoegd zijn in de HTML-code van een site.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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.

Er bestaat ook nog zogenaamde "gesponsorde" zoekmachine-optimalisatie waarvoor je een financiële bijdrage moet storten aan de zoekmachine. Je positionering zal voortreffelijk zijn maar je website zal tussen de andere commerciële links worden geplaatst, los van de gewone zoekresultaten, om de gebruikers van de dienst niet te misleiden.

18. 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. Zo is "dmoz" een algemene gids. Yahoo en Google leveren deze dienst ook, analoog aan hun zoekmachines.

19. Wat is een hypertekstlink?

Het websurfen gebeurt via hypertekstlinks. 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.

Hypertekstlinks (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 hypertekstlink, dan krijg je een andere webpagina. Elke hypertekstlink 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 hypertekstlink 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.

20. Welke soorten hypertekstlinks 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 hypertekstlink" (of *surface linking*) en een "diepe hypertekstlink" (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.

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

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Hoofdstuk II. Informatie downloaden

21. 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. 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".

Hoed je voor het bezit (en het uploaden of downloaden) van bestanden met pedofiel karakter dat in België strafrechtelijk strafbaar is!

22. Wat is peer-to-peer?

We staan even stil bij het revolutionaire "peer-to-peer"-systeem dat nauw verwant is aan het downloaden van bestanden op het internet.

"Peer-to-peer" ("gelijke naar gelijke" in het Nederlands) vaak afgekort als "p2p", ontstond in 1999 dankzij de Napster-gemeenschap en het verwijst naar een netwerk dat bestaat uit een aantal machines (computers) die op een gegeven ogenblik in wisselwerking staan met elkaar. De wisselwerking tussen computers is gebaseerd op het delen van gegevens die vaak de vorm hebben van muziekbestanden maar ook van bv. videostreaming. Telefonie over het internet (bv. Skype) is tevens mogelijk dankzij p2p. De netwerken hebben vaak de neiging om zich geografisch te organiseren om bestanden in dezelfde taal (films) te kunnen uitwisselen of volgens de artiesten die in zijn (muziek).

P2p verwijst tevens naar de manier waarop de gebruikers door middel van een protocol met elkaar communiceren. De term "p2p" betekent dat het delen van de gegevens plaatsheeft tussen de gebruikers en dat het niet binnen een "client-server"-relatie gebeurt. De gebruikers zijn tegelijkertijd servers en clients aangezien alle uitgewisselde bestanden worden opgeslagen op elk van hun harde schijven. De klassieke systemen zijn gedecentraliseerd. In een gecentraliseerde architectuur moeten alle bestanden die van één internaut naar een andere worden overgebracht echter over dezelfde server passeren. Als deze verdwijnt (bijvoorbeeld ten gevolge van een rechtsvordering) stort het hele netwerk in. Dit risico bestaat niet in een gedecentraliseerd systeem aangezien meerdere servers met elkaar zijn verbonden.

Bepaalde software (bv. Limewire, Shareaza, eMule, Morpheus) is noodzakelijk om toegang te krijgen tot een p2p-netwerk.

Concreet mikt p2p op een gemeenschap van gebruikers die op een netwerk de informatie plaatsen waarover ze beschikken. Daartegenover staat dat ze gemachtigd zijn om dankzij de uitwisselingssoftware bestanden te downloaden die door andere internauten online werden gezet.

23. Wat zijn de meest uitgewisselde media?

De meest uitgewisselde bestanden op p2p-netwerken zijn zonder twijfel muziekbestanden. Het meest verspreide formaat voor de compressie van muziekcomposities is mp3[2]. Hierna onderzoeken we in hoofdzaak het p2p-systeem vanuit deze invalshoek.

De uitwisseling is echter niet alleen beperkt tot muziekcomposities. Elk bestandstype kan op een p2p-netwerk worden gedeeld: films (waarvan het downloaden ook zeer populair is, bepaalde films worden – soms illegaal - gedownload voor ze in de bioscoop worden vertoond), documenten, foto's, software enz.

2 Het mp3-formaat wordt vaak gebruikt om audiogegevens te comprimeren. Technische informatie over het mp3-formaat vindt u in het volgende deel van deze gids: Mijn internetruimte ontwerpen"Mijn internetruimte ontwerpen".

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

24. Hoe kan de muziekindustrie de strijd aanbinden tegen het illegale gebruik van p2p?

P2p is een netwerk waarop internauten hun bestanden, vaak muziekbestanden, delen die zijn beschermd door de rechten van het intellectuele eigendom. Meestal worden de werken illegaal gekopieerd, d.w.z. dat ze vrij beschikbaar zijn voor de gebruikers van p2p-software zonder de toestemming van de auteurs.

Sinds hun ontstaan zijn p2p-netwerken blijvend in het nieuws geweest. Rechters hebben op verzoek van de muziekindustrie geprobeerd om orde te scheppen in de aansprakelijkheid van de verschillende betrokken personen, jammer genoeg zonder veel succes. Er zijn slechts enkele losstaande beslissingen genomen tegen de gebruikers daar immers de nieuwe technieken hun identificatie steeds complexer maken. De rechtsvorderingen die werden ingesteld tegen de uitgevers van software zijn vruchteloos gebleken. De hoven en rechtbanken waren over het algemeen van oordeel dat niet de softwaretoepassingen zelf illegaal zijn maar het doel waarvoor ze in sommige gevallen worden gebruikt. Bovendien zijn de uitgevers van software door de afwezigheid van een centrale server niet in staat om over de op het net circulerende gegevens te waken. Ten slotte is er nog een recente tendens dat de rechters van de internetproviders eisen dat ze filtermaatregelen toepassen. Er kan echter worden ingebracht dat het technisch moeilijk is om de toegestane inhoud van de niet-toegestane te onderscheiden. Bovendien belet er de gebruiker van p2p-software niets om van internetprovider te veranderen en zo te vermijden om in een conflict verwikkeld te raken.

We merken op dat bepaalde software-uitgevergemeenschappen zijn omgeschakeld naar de legale verkoop van muziek op het internet. De oplossingen hebben slechts weinig succes gehad, hetzij omdat de gemeenschappen failliet zijn gegaan, hetzij omdat de internauten een manier hebben gevonden om de legaal beschikbare bestanden illegaal te kopiëren.

Enkel en alleen de manier waarop p2p wordt gebruikt, kan worden betreurd want deze technologie, waarvan de onbaatzuchtige filosofie die is gebaseerd op delen, kan van aanzienlijk nut zijn voor de internauten.

25. Mag ik bestanden (muziek, films enz.) downloaden via een p2p-systeem?

In theorie niet!

Het downloaden van bestanden (muziek of andere) is een manier van kopiëren die wordt beschermd door het auteursrecht.

Het downloaden op zich is echter niet illegaal en blijkt toegestaan onder bepaalde voorwaarden. Zo kan je een bestand downloaden als de auteur toestemming geeft voor de reproductie van zijn werk (bv. voor reclamedoeleinden). Bovendien heeft de wetgeving over de auteursrechten de zogenaamde "privékopie" voorzien, die indien bepaalde voorwaarden zijn vervuld de auteur verbiedt om de reproductie van zijn werk te weigeren. In de eerste plaats moet het bestand op geoorloofde wijze zijn verspreid. Vervolgens moet het zijn gedownload in het kader van de familiale kring: d.w.z. een beperkte kring van personen die zijn verbonden door een familiale band of elke andere sociale band die daarmee vergelijkbaar is. Als de voorwaarden zijn vervuld, kun je een bestand via een p2p-systeem downloaden. Ten slotte, indien het werk niet origineel is of indien het niet langer is beschermd door de auteursrechten, is het downloaden ervan tevens toegestaan.

In alle andere gevallen is het downloaden ervan illegaal en word je mogelijk aansprakelijk gesteld.

Bovenop het downloaden rijst er een andere vraag die ook van belang is: de openbare uitwisseling van bestanden (bv. muziek- of geluidsbestanden) via een p2p-systeem.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Hoofdstuk III. Zich uitdrukken op internet

Afdeling 1. Elektronische post

26. Wat is elektronische post?

Elektronische post wordt 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. Deze wettelijke definitie dekt het begrip e-mail (of mail), het gebruik van de "chat", videoconferenties of het versturen van sms-berichten (*Short Message Systems*) vanaf een mobiele telefoon. Het kan ook om berichten gaan die op antwoordapparaten worden achtergelaten of op "voicemails" van mobiele telefoons. In de items die volgen zal het vooral over elektronische post gaan en dan zal daarnaar worden verwezen met de term "e-mail".

Je kunt met elektronische post 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 Thunderbird (openbronprogramma). 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.

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

Een van de grootste problemen met elektronische post is het behoud van de integriteit en de vertouwelijkheid 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.

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 eventueel 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 authentificeren, 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 authentificeert 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.

Er kunnen ook problemen opduiken in verband met de veiligheid. Via elektronische post kunnen immers computervirussen worden verspreid. 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. Het

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

probleem kan grotendeels worden opgelost door gebruik te maken van een beveiligde handtekening.

28. 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 bestemmeling 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 verstuurde 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 bestemmeling 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. Bovendien moet men weten, dat sommige systemen (bijvoorbeeld : © Hotmail) niet met ontvangstbevestigingen werken.

Om die redenen liberaliseerde de overheid de elektronische aangetekende brief en behoudt De Post enkel een monopolie op verzendingen in papiervorm. 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.

29. 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 hoaxen 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, financiele zwendel via kettingbrieven, misbruik van handtekeningen door valse petities, 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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Afdeling 2. "Chatten"

30. 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.

31. 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.

32. Welke risico's houdt het chatten in?

Aan IRC doen, is in zekere zin net hetzelfde als een openbare plek 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 webhufter van de gelegenheid (relatieve naamloosheid, afstand) misbruik maakt om grof te doen tegen zijn correspondenten.

Houd er tevens rekening mee dat de risico's vooral ten opzichte van minderjarigen bestaan. Spoor hen aan om jou hun vriendjes op het *net* "voor te stellen", om nooit heel persoonlijke gegevens door te geven en raad ze vooral af om een vermeende internetvriend persoonlijk te ontmoeten.

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.

Deze verschillende risico's kunnen nog worden beperkt als je de zogenaamde "gesloten" lijsten gebruikt – algemeen te vinden op het Web (bv. MSN) – waardoor je in een apart venster kunt *chatten* met de personen van uw keuze. Om dit te doen duid je de gesprekspartners aan die je aan je lijst wilt toevoegen. De gesprekken met deze internauten zijn altijd privé en worden niet gestoord door onbekende tussenkomsten. Natuurlijk beschermt het gebruik van privélijsten je niet tegen personen die je zelf hebt uitgenodigd.

Afdeling 3. Web 2.0 en sociale netwerken

33. Wat is Web 2.0?

Web 2.0 verwijst naar de tweede generatie van onlinediensten die de samenwerking en het delen van informatie tussen internauten willen vereenvoudigen. Bij zijn originele conceptie bevatte het Web – in deze context omgedoopt tot Web 1.0 – betrekkelijk statische pagina's, die online werden geplaatst en gewijzigd door enkele insiders (over het algemeen IT-professionals). De benadering van Web 2.0 op zijn beurt is gericht op de wisselwerking tussen de gebruikers en hun dynamische deelname aan de inhoud ervan.

De exacte betekenis van de term Web 2.0 staat op dit ogenblik ter discussie, vandaar de aarzelingen over de definitie van de toepassingen die onder dit begrip vallen. Niettemin

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

wordt overeengekomen om de virtuele sociale netwerken[3] (bv. Second Life, MySpace, Facebook, Netlog enz.), de sites waar inhoud kan worden gedeeld (Dailymotion, YouTube enz.), de wiki's[4] enz. eronder te rangschikken. De discussiefora en de blogs kunnen zonder twijfel worden beschouwd als virtuele sociale netwerken. Verder in de tekst komen we hierop terug.

Een van de voornaamste kenmerken van Web 2.0 is dat het elke gebruiker de mogelijkheid biedt om mee te werken aan de inhoud van een site. Met het oog hierop is het van belang dat de technische hulpmiddelen niet enkel voorbehouden zijn aan ervaren informatici. Ze moeten echter flexibel zijn en gemakkelijk in gebruik voor eenieder. Over het algemeen maakt Web 2.0 gebruik van de ontwikkelingstechnologie AJAX die verschillende technologieën groepeert (XML, HTML, CSS enz.).

34. Wat zijn de risico's die aan Web 2.0 zijn verbonden?

Het uitgangspunt van Web 2.0 is om de internaut een centrale plaats te geven binnen het uitwerken van inhoud: hij wordt als het ware webmaster. Als gebruiker van een Web 2.0-dienst loop je het gevaar om ofwel verboden gegevens online te plaatsen ofwel verboden gegevens te ontdekken. Bij de eerste veronderstelling ben je de auteur van illegale inhoud ((bv. lasterlijke, revisionistische, racistische enz. uitlatingen of inbreuken op auteursrechten) en loop je het gevaar je redactionele verantwoordelijkheid op het spel te zetten. Kijk uit als je gegevens op het net verspreid. Bij de tweede veronderstelling voel je je het slachtoffer van beweringen van een ander (bv. omdat ze je eer of privéleven niet respecteren) of je ontdekt gegevens die je schadelijk acht (bv. gewelddadig, racistische of zelfs pedofiele foto's of filmpjes). Er zijn manieren om dergelijke inhoud aan de kaak te stellen en als de inhoud je materiële of immateriële schade berokkent, om een schadevergoeding te krijgen.

Web 2.0 brengt ongetwijfeld bepaalde risico's met zich die zijn gekoppeld aan de bescherming van de persoonlijke levenssfeer. Om in te schrijven op een sociaal virtueel netwerk moet je als gebruiker over het algemeen je e-mailadres meedelen (bv. Facebook). Door je binnen een sociaal virtueel netwerk te bewegen loop je het gevaar om het slachtoffer

3 Een sociaal virtueel netwerk duidt ope en groep van entiteiten (individuen of organisaties) die virtueel met elkaar in contact staan, via internet, om een vriendengroep, een professionele samenwerking of een sociale structuur voor commerciële, affectieve of andere ontmoetingen op te zetten.

4 Een wiki is een inhoudbeheersysteem voor websites waarvan de pagina's vrij en gemakkelijk kunnen worden gewijzigd door elke bevoegde bezoeker. De wiki's zijn opgevat om kennis gemakkelijker te kunnen verdelen en om de redactie van documenten in samenwerking te vereenvoudigen.

te worden van *spamming* of van *phishing*. Deze laatste techniek wordt aangewend om door middel van een vals e-mailadres bepaalde van je vertrouwelijke gegevens te pakken te krijgen (bv. je ontvangt een e-mail die zogenaamd afkomstig is van je bankinstelling en je wordt gevraagd om je bankrekeningnummer mee te delen). Een gelijkaardig risico vloeit voort uit het feit dat je door je in te schrijven op een dergelijk netwerk het doelwit wordt van klantenwervers die je commerciële profiel gemakkelijk kunnen ontdekken. Deze praktijken doen verschillende vragen rijzen: welke rechten kan ik uitoefenen om mijn persoonlijke levenssfeer te beschermen? Wat zijn de mogelijke middelen als mijn rechten niet worden gerespecteerd?

Afdeling 4. Discussiefora

35. 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.

36. 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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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 verstreken 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.

37. 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 onbeschermde ruimte is. Het aantal personen dat toegang heeft tot het discussieforum waaraan jij deelneemt is nagenoeg onbeperkt. 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 uitlatingen 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 aanlokkelijke 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, al is deze praktijk volkomen illegaal.

Afdeling 5. Blogs

38. Wat is een blog?

Een blog is een gezellige en interactieve website die wordt onderhouden door een internaut (*blogger*) die er inhoud toevoegt onder de vorm van berichten die hij er geregeld post en waarop bezoekers kunnen reageren door commentaar te geven. Een blog wordt vaak vergeleken met een dagboek of logboek. De term blog komt trouwens van de samentrekking van de Engelse substantieven "web" (spinnenweb) en "log" (logboek). Er wordt een wisselwerking geschapen tussen de *blogger* die zijn site geregeld voorziet van nieuwe inhoud en de lezers die de mogelijkheid hebben om hun indrukken te delen.

Technisch gezien is de blog een instrument voor inhoudsbeheer (*Content Management System*) die zijn faam dankt aan het feit dat zijn systeem sterk is vereenvoudigd in vergelijking met de klassieke instrumenten. Talrijke opties die vaak complex en onbruikbaar waren voor de meeste internauten werden immers geëlimineerd.

Deze vereenvoudiging gaf de aanleiding tot standaardisatie van deze soort van miniwebsites die een reeks kenmerkende elementen bevatten. Eerst en vooral is de blog opgebouwd uit berichten van verschillende grootte, die door de blogger(s) worden geplaatst en die zijn gerangschikt van nieuw naar oud. Deze berichten of mededelingen vormen wat de ruggengraat van de blog kan worden genoemd. Het bijwerken van deze berichten wordt "blogging" genoemd. Onder elk bericht kunnen bepaalde vermeldingen worden gevonden onder de vorm van hyperlinks: permanente link (d.w.z. de URL van een artikel), de categorie waartoe het bericht hoort of het aantal commentaren die werden

gegeven. Andere elementen (zoals de toegang tot archieven, de lijst met behandelde thema's, links naar andere blogs, een zoekmachine of de mogelijkheid om zich in te schrijven op een RSS-feed[5]) zijn ook vaak aanwezig op een blog. Deze verschillende attributen worden op een dergelijke manier gerangschikt dat de blog over het algemeen kan worden opgesplitst in kolommen waarvan de centrale kolom is voorbehouden aan de berichten. De inhoud van deze berichten, die vaak uit tekst bestaat, wordt soms aangevuld met hyperlinks en multimedia-elementen (er wordt soms gesproken over een *fotoblog* of *filmblog*).

39. Hoe kan ik deelnemen aan een blog?

Je moet in de eerste plaats naar de hoofdpagina van de blog surfen. Aangezien de blog een website is, moet u de URL kennen, deze intikken in de browser en op de "enter"-toets drukken. Er bestaan zoals voor de klassieke webpagina's zoekmachines die uitsluitend zijn bestemd voor het opzoeken van blogs (bv. *blogsearch Google*). De traditionele zoekmachines nemen in iedere geval ook de adressen van de blogs op. Je krijgt dan gemakkelijk toegang tot deze kleine sites die uw favoriete onderwerpen behandelen.

Als je je vervolgens op een blog bevindt, kun je passief deelnemen en genoegen nemen met het lezen van de berichten en de commentaren waarvoor je interesse hebt. Als je dat wenst, kun je deelnemen door een eenvoudige opmerking toe te voegen of een grotere bijdrage te leveren. Om dit te doen, moet je een webformulier invullen.

40. Hoe maak je een blog aan?

Om je eigen blog aan te maken (voor persoonlijke, professionele, commerciële of andere doeleinden) hoef je geen expert te zijn en volstaan basistechnieken. Met dit systeem voor inhoudsbeheer kan elke internaut immers op dezelfde eenvoudige manier als bij een tekstverwerkingsprogramma tekst en foto's online plaatsen.

Met verschillende gratis en vrij toegankelijke oplossingen op het net (bv. *Wordpress, Blogger, Over-Blog, Skyblog*) kun je in enkele zeer eenvoudige stappen (een account aanmaken, de naam en de basisweergave voor je blog kiezen) je blog aanmaken. Deze zogenaamde gebruiksklare oplossingen bieden je hosting aan en een reeds geïnstalleerd instrument, m.a.w. de noodzakelijke omstandigheden voor het online plaatsen van een blog.

5 Met een RSS-feed (Really Simple Syndication) kan je de wijzigingen van een site die geregeld verandert, zoals een blog, aan het publiek meedelen. De personen die belang hebben bij de dienst in kwestie kunnen snel worden ingelicht over wijzigingen want ze hebben de mogelijkheid om zich te "abonneren" op een RSS-feed.

41. Welke risico's zijn er verbonden aan het gebruik van een blog?

De blog is natuurlijk bestemd om te worden onderhouden door een aanzienlijk aantal internauten. Deze maakt immers deel uit van de openbare sfeer en laat iedereen zich uitdrukken door zijn bijdrage te leveren. De gegevens die er worden teruggevonden, zijn enorm gevarieerd en kunnen niet worden voorzien, wat bepaalde risico's met zich brengt waarvoor de *bloggers* en gebruikers moeten opletten.

Als je de blog voorziet van je commentaar of als je een blog aanmaakt, moet je ervoor zorgen dat je je verantwoordelijkheid opneemt en geen lasterlijke uitlatingen doet over de eer, de reputatie of het privéleven van anderen. Waak ook over het feit dat het online plaatsen van een tekst een handeling van verspreiding vormt die onderhevig is aan de wetgeving op het auteursrecht.

Het kan voorvallen dat je zelf het slachtoffer bent van bepaalde op een blog verspreide informatie (je auteursrechten worden geschonden, bepaalde uitlatingen zijn lasterlijk, je privéleven wordt niet gerespecteerd enz.). Je hebt de mogelijkheid om op te komen tegen deze informatie bij de *blogger* of bij de moderator (persoon wiens functie erin bestaat om de inhoud van de berichten te bekijken voor ze online worden geplaatst), zodat een van hen de omstreden inhoud verwijdert. Als deze poging mislukt, zijn er andere procedures. Je kunt je tot de internetprovider of webhoster wenden, de inhoud aangeven bij een politiebureau of via het internet bij het meldpunt van de gerechtelijke politie (http://www.e-cops.be). Indien je bovendien de identiteit van de auteur van de uitlatingen kent, kan je hem altijd in het openbaar aanklagen. Merk op dat het opportuun kan zijn om uitlatingen van twijfelachtige betekenis van andere internauten aan de kaak te stellen.

Op basis van de blogs waaraan je deelneemt, kunnen klantenwervers ten slotte erg gemakkelijk je commerciële profiel vastleggen. Bovendien moet je je e-mailadres meedelen om informatie op een blog te mogen verspreiden. Het is moeilijk precies te weten wat er uit informatie die op jou betrekking heeft, kan voortvloeien en wie ervan zal gebruikmaken en op welke manier. Als deze informatie het onderwerp vormt van een "verwerking", zal de wetgeving voor de bescherming van de persoonsgegevens van toepassing zijn.

42. Is de blogger verantwoordelijk voor berichten die door derden zijn gepost?

We herhalen dat je als *blogger* zoals eender welke internaut verantwoordelijk bent voor de berichten die je verspreidt op je blog.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Een delicatere vraag is of je verantwoordelijk kan worden gehouden voor de inhoud die op je blog werd toegevoegd door andere internauten. Als oprichter en beheerder van de blog beschik je over technische middelen om informatie toe te voegen, te verwijderen of te wijzigen. Vanaf dat moment word je geacht je verantwoordelijkheid te nemen wat de commentaren van derden betreft. Probeer uit voorzorg berichten van tevoren (d.w.z. vóór ze online worden verspreid) te controleren. Als je een van de berichten verdacht vindt, aarzel dan niet om het te verwijderen. Je kunt je zo beschermen tegen het risico dat je aansprakelijk wordt gesteld.

Om optimaal toezicht op de inhoud te verzekeren, kun je het beheer van de blog aan een moderator delegeren. Deze heeft als opdracht om de informatie te superviseren vóór ze te verspreiden; hij speelt de rol van bemiddelaar tussen de gebruikers; en indien nodig verwijdert hij ongeoorloofde inhoud of inhoud die schade berokkent aan anderen.

Om problemen te voorkomen, kun je een "handvest" van goed gedrag van de gebruikers opstellen, waarin je bijvoorbeeld vulgaire, beledigende of aanstootgevende uitlatingen verbiedt. Er kunnen sancties worden voorzien (zoals het verwijderen van het account van een lid) als de gebruikers hun beloften niet nakomen.

Er is ook nog een laatste radicalere oplossing: je kunt een blog aanmaken waarop de bezoekers zich niet mogen uitdrukken. De mogelijkheid bieden aan internauten om hun commentaren achter te laten is immers facultatief.

43. 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 een aantal hoffelijkheidsregels 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 ergeISDN 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 internetruimte ontwerpen

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Om je bekend te maken of om een van je interesses met anderen te delen, kun je bijvoorbeeld 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.

Overigens 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

44. 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 85.91.172.24. of de Federale Overheidsdienst Economie, K.M.O., 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 bedrijpelijke domeinnaam. Zo gaat het er trouwens meestal aan toe op het web, waar je geen 85.91.172.24. hoeft te typen, maar gewoon het voor de gebruiker transparante adres http://www.privacycommission.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)* of voor jezelf (*http://www.janssens.be of .org*). Dat adres identificeert je heel precies, waardoor internetters moeiteloos naar je webpagina kunnen surfen.

45. 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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

46. 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", ".eu" of ".be", particulieren voor ".be", ".name" of ".info", instellingen of verenigingen zonder winstoogmerk voor ".org" of ".net" en internationale organisaties voor ".int" enz.

47. 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 een domeinnaam. In het kader van de territoriale extensies bestaat er een bijzondere extensie voor de Europese Unie: ".eu". De uitbreiding ".eu" mag enkel 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 over elektronische handel en die de consument o.a. een hoge graad van bescherming bieden.

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.

48. 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".

49. Moet ik aan voorwaarden voldoen om een domeinnaam te bekomen?

Er moeten voor haast geen enkel domein – noch de generieke (".com", ".org", ".net" enz.) noch de "nationale" (bijvoorbeeld ".be") specifieke criteria in acht worden genomen, voor zover de domeinnaam beschikbaar is ("wie het eerst komt, het eerst maalt").

Zodra je domeinnaam geregistreerd is, krijg je een gebruiksvergunning voor één jaar (of soms langer). 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 voor de .be-domeinnamen), die we je aanraden vooraf te lezen.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

50. 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*[1]*, 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 kun 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).

51. 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. De wet van 26 juni 2003 voerde een nieuwe, versnelde procedure in in verband met het onrechtmatig registreren van domeinnamen. Zo'n procedure kan, door de gerechtelijke achterstand, desondanks 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 (1.620,00 euro 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 (zie http://www.cepani.be). 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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Hoofdstuk II. Mijn rechten en plichten

Als je een persoonlijke webruimte (website, blog enz.) creëert, dan moet je andermans rechten eerbiedigen.

Die rechten zijn van uiteenlopende aard.

52. Welke basisregels moet ik respecteren?

De vrijheid van meningsuiting is een fundamenteel recht dat voornamelijk wordt gegarandeerd door de Europees Verdrag voor de rechten van de mens (artikel 10). Dit recht kan echter niet onoordeelkundig worden uitgeoefend en bijgevolg moeten verschillende grenzen worden gerespecteerd. Beperkingen zijn dus toegelaten, in het bijzonder om de rechten van anderen te beschermen.

In de eerste plaats herinneren we eraan dat het verboden is om informatie te verspreiden die strijdig is met de openbare orde of met de goede zeden. Bovendien worden racistische en revisionistische uitlatingen of uitspraken die aanzetten tot het plegen van een misdaad of tot geweld strafrechtelijk gesanctioneerd.

Je moet dus voorzichtig zijn en de schijnbare legaliteit van een bericht evalueren voordat je het via je persoonlijke ruimte toegankelijk maakt voor derden.

Als je een persoonlijke ruimte aanmaakt moet je er ook op letten dat je er geen informatie of andere zaken (foto's, tekeningen enz.) op plaatst die een inbreuk zijn op de persoonlijke levenssfeer of op het recht op afbeelding van anderen.

Het is eveneens verboden informatie te verspreiden die de eerbaarheid of de reputatie van anderen schaadt.

Ten slotte moet de gebruiker van een persoonlijke ruimte ook oppassen met het verspreiden van informatie die hij niet zelf aanmaakte, om geen afbreuk te doen aan de rechten van derden (auteursrecht op een foto, merkenrecht op een logo enz.). Over het algemeen moet je er dus op letten dat je de intellectuele eigendomsrechten van anderen eerbiedigt.

De belangrijkste juridische risico's hebben betrekking op de schending van

- de persoonlijke levenssfeer van derden;
- het recht op afbeelding van derden;

- het recht op eer en op de reputatie van derden;
- de intellectuele eigendomsrechten (afdeling 4).

53. Wat zijn mijn rechten en plichten met betrekking tot de eerbiediging van de privacy van derden?

Iedereen heeft recht op eerbiediging van privé-, familie- en gezinsleven. Inmenging in het privéleven is toelaatbaar indien toegestaan bij wet en indien noodzakelijk (in het bijzonder) voor de bescherming van de rechten en vrijheden van anderen.

De vrijheid van meningsuiting bijvoorbeeld kan in bepaalde gevallen een inbreuk op het recht tot bescherming van het privéleven rechtvaardigen. Er moet een evenwicht worden gevonden tussen de vrijheid van meningsuiting en het recht op eerbiediging van het privéleven en er moet worden nagegaan of de inbreuk op het privéleven kan worden gerechtvaardigd op basis van het maatschappelijke belang van de verspreide informatie.

Het bekendmaken van informatie over het privéleven van anderen wordt gezien als een overtreding, tenzij het rechtmatige belang van het grote publiek kan worden aangetoond met betrekking tot het verspreiden van deze informatie.

De seksuele voorkeur of de religieuze overtuiging van zijn leerkracht op een blog kenbaar maken, kan niet worden gerechtvaardigd door het belang van deze informatie voor de leerlingen van de klas. De schending van de persoonlijke levenssfeer is op het eerste gezicht immers te ernstig om te worden getolereerd in naam van de vrije meningsuiting.

De rechtspraak staat echter een inbreuk op het privéleven toe

- als de verspreide informatie betrekking heeft op het privéleven van publieke personen (een politicus bijvoorbeeld) en ze verband houdt met de uitgeoefende functies; bijvoorbeeld als de pers bekendmaakt dat een staatshoofd op vakantie gaat met een belangrijke industrieel, dan heeft dit te maken met zijn functie, voor zover deze gegevens een invloed zouden kunnen hebben op het beleid van het staatshoofd;
- als de verspreide informatie betrekking heeft op een persoon die bij gelegenheid is betrokken in een actualiteitsgebeuren en als de informatie verband houdt met dit gebeuren; bijvoorbeeld als een leerkracht in een krant een blanco pagina publiceert om de gewelddadigheden tegen vrouwen aan de kaak te stellen en als een van zijn oud-leerlingen ontdekt dat hij zijn ex-vrouw sloeg. De verspreide gegevens over het privéleven van de leerkracht houden rechtstreeks verband met zijn publieke stellingname en is dus gegrond, ondanks de inbreuk op het privéleven.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

De rechtspraak staat bijgevolg de verspreiding van informatie over het privéleven toe, maar met de grootste terughoudendheid.

Je moet dus bijzonder voorzichtig zijn vóór je gegevens over het privéleven van anderen de wereld instuurt.

54. Wat zijn mijn rechten en plichten met betrekking tot het recht op afbeelding van derden?

Het **recht op afbeelding** is een persoonlijkheidskenmerk dat iedere persoon beschermt tegen het ongeoorloofd gebruik van zijn afbeelding (foto of grafische voorstelling).

In theorie is voor elk gebruik van de afbeelding van een ander zijn of haar voorafgaande toestemming noodzakelijk. Om praktische redenen is de rechtspraak van oordeel dat in bepaalde omstandigheden deze toestemming stilzwijgend kan zijn, voor zover ze zeker is:

- als een persoon een openbare functie of mandaat uitoefent, kan men ervan uitgaan dat hij zijn stilzwijgende toestemming heeft gegeven voor het gebruik van zijn afbeelding in het kader van de informatieverstrekking aan het publiek met betrekking tot de uitoefening van zijn functie (in het geval van publieke personen);

- als een persoon is betrokken in een actualiteitsgebeuren kan men ervan uitgaan dat hij zijn stilzwijgende toestemming heeft gegeven voor het gebruik van zijn afbeelding voor alle publicaties die te maken hebben met het desbetreffende actualiteitsgebeuren (personen die in de actualiteit komen);

Deze versoepeling is vanzelfsprekend aangezien er rekening moet worden gehouden met de noodzaak om het publiek informatie te verschaffen. Het is bijvoorbeeld ondenkbaar dat alle krantenuitgevers verplicht zouden zijn geweest om een voorafgaande toestemming te vragen aan alle voorbijgangers op de foto's van de ruïnes van het World Trade Center na het instorten van de twin towers.

In alle andere gevallen moet vooraf toestemming worden gevraagd aan de persoon die wordt afgebeeld, voordat zijn foto op geoorloofde wijze kan worden gebruikt.

De rechtspraak is buitengewoon streng wat het commerciële gebruik van afbeeldingen van andere personen betreft. Zo werd de publicatie van foto's van Kim Clijsters die tijdens een tennismatch werden genomen en die voor reclamedoeleinden werden gebruikt als ongeoorloofd beschouwd aangezien niet om haar voorafgaande toestemming werd gevraagd. Op dezelfde wijze moet een handelaar die een foto van zijn winkel op de

homepage van zijn website plaatst, eerst toestemming vragen aan de klanten die op de desbetreffende foto staan.

55. Wat zijn mijn rechten en plichten met betrekking tot het recht van de eer van derden?

Ieder persoon heeft recht op de eerbiediging van zijn eer en zijn reputatie.

Ook hier moet een evenwicht worden gevonden tussen de berokkende schade en het belang van de verspreide informatie.

Elke veroordeelde heeft bijvoorbeeld het recht op verwijdering van gegevens, op grond waarvan de publicatie van informatie over zijn vroegere veroordeling niet kan worden gerechtvaardigd als er geen verband is met een of ander actualiteitsgebeuren.

De juiste informatie wordt burgerlijk (schadevergoeding) en strafrechtelijk (laster: beschuldiging van precieze feiten waarvoor geen bewijs kan worden geleverd) gesanctioneerd.

Informatie over derden mag niet ondoordacht worden verspreid, ook als ze niet over het privéleven gaan.

56. Wat zijn mijn rechten en plichten met betrekking tot de eerbiediging van de intellectuele rechten van anderen?

Het auteursrecht verleent de auteurs exclusieve rechten met betrekking tot het gebruik van hun werk. Daaruit volgt dat je voor het gebruik van een werk, doorgaans de voorafgaande toestemming moet hebben van de rechthebbende van een werk (voor een reproductie zoals een fotokopie, een afdruk, om het te *kopiëren/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 worden deze exploitatiehandelingen vaak gebruikt. 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

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

mededeling van het werk aan het publiek); vervolgens konden de bezoekers van zijn site de tekst downloaden (een bijkomende reproductie) en hem eventueel afdrukken op papier (laatste reproductie). Doordat het werk via de website voor het grote publiek toegankelijk werd gemaakt, heeft er ook een mededeling aan het publiek plaatsgevonden, wat een exclusief recht van de auteur is.

Overeenkomstig de auteursrechtelijke regelgeving, had de uitbater eerst de toestemming van de rechthebbende moeten verkrijgen. Dat gold ook voor de Franse studenten die veroordeeld werden voor de digitalisering en het online plaatsen van de liedjesteksten van Jacques Brel en Michel Sardou. Voordat je een werk via het internet verspreidt, moet je dus eerst de toestemming hebben van de rechthebbende (die vaak ook de schepper van het werk is, doch niet altijd, want hij kan zijn rechten hebben overgedragen, in het bijzonder aan een collectieve beheersvennootschap voor auteursrechten).

De intellectuele eigendom kan tevens tekens beschermen die de activiteiten of producten van een onderneming onderscheiden van die van zijn concurrenten. Het merkenrecht verleent aan de eigenaar ervan een gebruiksmonopolie van het geregistreerde teken. Aan derden kan zodoende verboden worden om in het zakenleven het teken of een gelijkaardig teken te gebruiken, voor identieke of gelijkaardige producten of diensten.

Na een uiteenzetting met betrekking tot de basisprincipes van de intellectuele eigendom, worden concrete vragen over het internetgebruik beantwoord.

57. Wat is beschermd door het auteursrecht?

Elk werk dat origineel is en in een bepaalde vorm wordt uitgedrukt, is beschermd door het auteursrecht. Wat betekenen de begrippen: werk, originaliteit en uitdrukking in een bepaalde vorm?

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

- **teksten** van welke aard ook (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 van 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** (tekstverwerkingssoftware, videospelletjes).

Om beschermd te zijn, moet een werk *origineel* zijn. Dit is een abstract criterium, dat in de praktijk moeilijk te definiëren is. Het betekent dat het werk de stempel van de persoonlijkheid van de auteur moet dragen. Zonder in details te treden kan men reeds stellen dat de beoordeling van de originele aard van een werk een feitenkwestie is, die door de rechter soeverein wordt beoordeeld. Zolang de rechter zich bijgevolg niet heeft uitgesproken over het originele karakter van een werk, kan je niet weten of een werk al dan niet origineel is. Nu, de rechtspraak is zeer soepel bij de interpretatie van het begrip originaliteit. In de meeste gevallen zal een werk dus als origineel worden beschouwd. Opgelet: origineel betekent geenszins mooi! Originaliteit is een begrip dat niets te maken heeft met schoonheid. Het is niet omdat je een werk lelijk of zelfs belachelijk vindt dat het niet als origineel zal worden beschouwd.

Om beschermd te zijn, moet een werk ook gematerialiseerd worden in een bijzondere *vorm* die voor zintuiglijke waarneming vatbaar is. Die voorwaarde vormt geen probleem voor werken die online beschikbaar zijn, aangezien ze noodzakelijkerwijze, om zichtbaar te kunnen zijn, vooraf in een bepaalde vorm moeten worden uitgedrukt. Deze voorwaarde houdt a contrario in dat het auteursrecht geen bescherming biedt, noch aan ideeën (ook al zijn die *briljant* of *origineel*), noch aan werkwijzen of stijlen, ook al zijn die origineel (bij het creëren van een persoonlijke ruimte kun je je dus laten inspireren door stijlen die door anderen worden gebruikt op voorwaarde dat je geen enkel origineel formeel element kopieert).

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

NEEN, er worden geen andere voorwaarden opgelegd om van een auteursrechtelijke bescherming te kunnen genieten. Het volstaat dat het werk origineel is en in een bepaalde vorm uitgedrukt is.

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 bewijsrechtelijke maatregelen). De bescherming begint te lopen vanaf het ogenblik dat het werk gecreëerd is.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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

59. 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 persoonlijke webruimte?

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 licentie kan worden verleend;
- *morele rechten* (beschermen de integriteit van het werk, de relatie van het werk met zijn auteur en de reputatie van de auteur), die niet overdraagbaar zijn (hooguit kan er gedeeltelijk afstand van worden gedaan) en nauw verbonden zijn met de persoonlijkheid van de auteur.

60. Welke vermogensrechten heeft een auteur op zijn werk?

Samengevat, zijn de vermogensrechten de volgende:

- 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 adaptatie- en vertalings*recht*: dit recht slaat op de omzetting van het werk in een ander genre (een tekst interactief maken), het aanbrengen van allerhande 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 bepaalde tijd ter beschikking te stellen van een derde (de rechthebbende van dat recht zou bijvoorbeeld de verhuur van een cd-rom gedurende een aantal maanden na de eerste verspreiding van deze cd-rom kunnen verbieden om genoeg tijd te maken voor de verhandeling van het werk);

- Het *distributierecht*:

Dit recht geeft een auteur controlemogelijkheden over de wijze waarop zijn werk wordt gecommercialiseerd (dit recht vertoont raakpunten met het reproductierecht in enge zin);

- Het *uitvoerings- of mededelingsrecht*:

Dit recht heeft betrekking op de mededeling van een werk aan het publiek, met inbegrip van de beschikbaarstelling voor het publiek op zodanige wijze dat deze voor de leden van het publiek op een door hen individueel gekozen plaats en tijd toegankelijk zijn. Dit recht heeft betrekking op de *online*-transmissie van een werk (via het internet). Het betreft de directe mededeling aan het publiek, zonder dat een drager noodzakelijk is.

61. Welke morele rechten heeft een auteur op zijn werk?

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

De morele rechten zijn de volgende:

- het *divulgatierecht*: dit recht houdt in dat de auteur kan beslissen wanneer zijn werk voltooid is en aan de openbaarheid kan prijs gegeven worden. Zich een nog onafgewerkt 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 dit recht; de auteur had immers nog geen toestemming gegeven tot verspreiding van het werk.

- 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 de exploitatie van zijn werk moet worden vermeld of dat zijn werk anoniem moet worden gepubliceerd. Het zich toe-eigenen van andermans werk is dus een schending van dit recht, alsmede het verspreiden van het werk onder de naam van de auteur indien hij wenste dat dit naamloos zou gebeuren.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

- het *integriteitsrecht:* met dit recht kan de auteur zich verzetten tegen elke wijziging van zijn werk (het inkorten of samenvatten van een tekst, het anders in beeld brengen van een foto, het met een filter of door trucage wijzigen van een foto) evenals tegen alles wat zijn eer of reputatie schendt (hetzij door een materiële wijziging van het werk, hetzij door een wijziging van de context of de wijze waarop het werk is voorgesteld).

62. Hoe lang is een werk beschermd?

De beschermingsduur van het auteursrecht is beperkt in de tijd. De algemene regel is dat het werk beschermd is tot 70 jaar na de dood van de auteur. Dit betekent bijvoorbeeld dat de originele partituren van de concerto's van Mozart niet langer door het auteursrecht zijn beschermd. Ze mogen dus vrij gereproduceerd worden (bijvoorbeeld d.m.v. fotokopie), zonder dat de toestemming van de erfgenamen van Mozart vereist zijn (doch eventueel zal een toestemming van de uitvoerende musici en de platenfirma's, die naburige rechten genieten op de uitvoering van de werken van Mozart, moeten bekomen worden).

63. Wat is niet door het auteursrecht beschermd?

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

- Een werk dat niet origineel is! Dit begrip is echter relatief en moet door de rechter worden beoordeeld. Het wordt bijgevolg afgeraden om zelf te beslissen of andermans werk al dan niet origineel is;

- Een werk dat niet langer beschermd is, d.w.z. waarvan de auteur sedert meer dan 70 jaar overleden is (soms moet je wel een toestemming hebben van andere rechthebbenden);

- Een werk zoals bedoeld in artikel 8 van de auteurswet. Dit artikel bepaalt dat bepaalde, zelfs originele, werken niet beschermd worden door het auteursrecht: 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, zolang het niet in een bepaalde vorm is uitgedrukt en dus concreet gestalte heeft gekregen, niet beschermd door het auteursrecht.

64. Mag ik nooit een auteursrechtelijk beschermd werk reproduceren?

Er zijn gevallen waarin een auteursrechtelijk beschermd werk geheel of gedeeltelijk mag worden gereproduceerd en waarvoor de toestemming van de auteur niet vereist is. De auteurswet voorziet namelijk in enkele uitzonderingen. Deze uitzonderingen zijn sowieso niet talrijk en bovendien onderworpen aan zo'n strenge voorwaarden dat het niet altijd gemakkelijk is om er zich op te beroepen bij de creatie en het online plaatsen van een website. Hierop bestaat echter één belangrijke uitzondering in het kader van het ontwerpen van een website of een blog: m.n. het citaatrecht.

Krachtens het citaatrecht mag je korte fragmenten uit een werk reproduceren zonder dat hiervoor de toestemming van de auteur vereist is. Verscheidene voorwaarden moeten echter cumulatief vervuld zijn:

- het citaat moet afkomstig zijn van een werk dat op geoorloofde wijze werd openbaar gemaakt (je mag dus geen werk citeren zolang de auteur niet heeft beslist om het aan de openbaarheid prijs te geven);
- het citaat moet kort zijn (dit is een feitenkwestie, die door de rechter moet worden beoordeeld);
- het citaat moet worden aangehaald "ten behoeve van kritiek, polemiek, onderwijs, of in het kader van wetenschappelijke werkzaamheden" (dit sluit bijgevolg het citaat in het kader van ontspanningswebsites of louter commerciële websites uit);
- het citaat moet overeenkomstig de eerlijke beroepsgebruiken en het beoogde doel worden gebruikt;
- het citaat moet de bron en de naam van de auteur vermelden.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

65. Tot wie moet ik mij richten indien ik toestemmingen voor het gebruik van een auteursrechtelijk beschermd werk wens te verkrijgen ?

Uit het voorafgaande volgt dat de toestemming van de auteur vereist is voor de exploitatie van een werk en er bijgevolg een overeenkomst met hem moet gesloten worden. Daartoe moet je je drie vragen stellen:

- Wie is (zijn) de rechthebbende(n) van de auteursrechten op het werk?
- Is de auteur altijd de rechthebbende? Heeft hij zijn rechten niet overgedragen?
- Heeft de auteur het beheer van zijn rechten niet toevertrouwd aan een beheersvennootschap voor auteursrechten ?

Principe

In principe is de rechthebbende van de auteursrechten, de natuurlijke persoon die het werk gecreëerd heeft. Deze persoon is de "oorspronkelijke auteursrechthebbende". Om de bewijslast te vergemakkelijken, wordt de persoon van wie de naam (of een of ander teken) op het werk vermeld staat, geacht de rechthebbende 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.

Bovendien moet er steeds in gedachten worden gehouden dat met betrekking tot een website of een databank, er twee soorten auteurs kunnen zijn:

- de auteur of co-auteur van de persoonlijke ruimte: een persoonlijke ruimte zal als dusdanig, onafhankelijk van haar inhoud, immers vaak zelf een auteursrechtelijk beschermd werk zijn, door de originele rangschikking van haar diverse elementen (de structuur van de website of databank);
- de auteur(s), niet van de persoonlijke ruimte, maar van de erin geïncorporeerde elementen (foto, logo, muzieksequens) (de inhoud van de website of databank).

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 reeds een exclusieve licentie heeft verleend aan een derde. Die persoon is dan de *afgeleide auteursrechthebbende*. Er moet dus aan de auteur gevraagd worden of hij nog steeds houder is van de rechten en, als dat niet zo is, wie de verkrijger van de rechten is. Bovendien moet je eventueel de morele rechten van de oorspronkelijke auteur eerbiedigen, daar morele rechten niet overdraagbaar zijn.

Beheersvennootschappen voor auteursrechten

Een auteur die niet zelf wil instaan voor het beheer van zijn rechten kan die taak toevertrouwen aan een beheersvennootschap voor auteursrechten (SABAM, SOFAM, SESAM, SCAM, SCAM, enz.). Deze oplossing biedt onder meer het voordeel dat de gebruiker slechts met één gesprekspartner over de rechten moet onderhandelen, wat een niet te onderschatten voordeel is, indien hij verscheidene werken wil exploiteren.

66. Wat is een merk? Wat is zijn rol?

Een merk is een teken (woord, letter, kleur, stempel, cijfer, vorm van een product of van zijn verpakking, enz.) dat wordt gebruikt ter onderscheiding van producten of diensten die worden aangeboden door een onderneming (vb.: het merk "Côte d'Or" ter onderscheiding van chocolade, die verhandeld wordt door de vennootschap Kraft).

De belangrijkste functie van een merk is de garantie voor de consument van de oorsprong van verhandelde producten of diensten. Zo, biedt bijvoorbeeld, de vermelding van het merk "Côte d'Or" op de verpakkingen van chocolade de garantie aan de consument dat deze chocolade werd vervaardigd onder het toezicht van de houder van het merk (de vennootschap Kraft). Doordat een bijzondere kwaliteit van het product aan de klanten wordt gewaarborgd, heeft een merk dus een vooraanstaande rol bij de fidelisatie van klanten.

67. Wat zijn de voorwaarden om te kunnen genieten van de bescherming door een merk?

Om te kunnen genieten van een bescherming door het merkenrecht, moet er een teken worden geregistreerd bij een bevoegde overheid (bijvoorbeeld bij het Benelux-bureau voor de Intellectuele Eigendom).

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Opdat een merk geldig zou zijn, moet het teken bovendien verschillende voorwaarden vervullen:

- het moet een onderscheidend vermogen bezitten, d.w.z. in staat zijn om de oorsprong van de producten of diensten waarop het vermeld staat te identificeren (vb.: het "Apple"-teken heeft een sterk onderscheidend vermogen ter identificatie van computerapparatuur; ditzelfde teken zou echter geen enkel onderscheidend vermogen bezitten indien het werd gebruikt bij de verhandeling van appelsap); het teken mag dus niet enkel dienen om te verwijzen naar het betreffende type producten of om iets zeggen over de kwaliteiten van het product;

- het moet beschikbaar zijn, d.w.z. dat het niet het voorwerp mag zijn van concurrerende rechten van een derde (vb.: een logo dat ontworpen werd door een grafisch vormgever zal slechts in de vorm van een merk kunnen geëxploiteerd worden, indien men voorafgaandelijk de auteursrechten op het genoemde logo heeft verkregen)

- het teken moet toelaatbaar zijn, d.w.z. dat het geregistreerde teken niet strijdig mag zijn met de openbare orde of de goede zeden en het publiek bovendien niet mag misleiden m.b.t. de kwaliteit of de oorsprong van de producten en/of diensten.

68. Wat is de draagwijdte van de bescherming door een merk?

De bescherming door een merk is op twee vlakken beperkt.

Enerzijds is het merk enkel beschermd binnen het grondgebied van de registratie. Indien ik bijvoorbeeld een merk in Frankrijk registreer, zal de bescherming van het teken mij niet toelaten om een derde te verbieden hetzelfde teken in België te gebruiken. Dit is het "territorialiteitsprincipe" van een merk. De bescherming van een merk op Belgisch grondgebied wordt gegarandeerd door de registratie van een Benelux-merk dat automatisch bescherming biedt op het grondgebied van de drie Beneluxlanden (België, Nederland en Luxemburg). Het beheer van het Beneluxmerk wordt verzekerd door het Benelux Bureau voor de Intellectuele Eigendom, waarvan de site terug te vinden is op het adres <http://www.boip.int>.

Anderzijds is de bescherming van een merk beperkt tot de betrokken branche van producten of diensten. Bij de aanvraag tot registratie van het merk moet(en) de categorie(ën) van producten en/of diensten waarvoor de bescherming wordt gevraagd nauwkeurig worden omschreven. Indien een derde hetzelfde teken voor andere producten en/of diensten gebruikt, kan de houder van het merk zich daar in principe niet tegen verzetten ("specialiteitsbeginsel" van een merk).

Er moet echter worden opgemerkt dat algemeen bekende merken – onder bepaalde voorwaarden – een ruimere bescherming genieten en zodoende de houders ervan toelaten om zich te verzetten tegen het gebruik van het teken door een derde, zelfs voor verschillende producten of diensten (indien het merk Ferrari bijvoorbeeld enkel voor producten m.b.t. auto's was geregistreerd, zou door de bekendheid van het teken het gebruik van het teken voor textielproducten toch kunnen worden verboden). Om van deze ruimere bescherming te genieten, moet de houder van het algemeen bekend merk bewijzen dat derden door het teken te gebruiken een ongerechtvaardigd voordeel halen uit de bekendheid van het merk of hem schade berokkenen. In het voorbeeld van Apple, zal het echter moeilijk te bewijzen zijn dat het gebruik van het teken bij de verhandeling van fruitsap voordeel haalt uit de bekendheid van het merk of hem schade berokkent, vermits het begrip voor dit soort van producten tot het dagelijkse taalgebruik behoort. Dezelfde conclusie kan echter niet getrokken worden indien het Apple-logo zou worden gereproduceerd.

In een nog ruimere context echter, bieden sommige wetgevingen (bijvoorbeeld de Benelux Conventie inzake Intellectuele Eigendom, die het Beneluxmerk regelt) de houder van een merk de mogelijkheid, derden te verbieden een teken voor andere doeleinden te gebruiken dan om producten of diensten van elkaar te onderscheiden, wanneer het gebruik van dat teken, zonder gegronde reden, onterecht mee profiteert van het onderscheidend karakter of van de bekendheid van het merk of daaraan schade berokkent.

69. Heb ik het recht om software voor de aanmaak van webinhoud te gebruiken?

Om je persoonlijke ruimte te creëren, ga je waarschijnlijk gebruik maken van daarvoor geschikte software. Om vervolgens je persoonlijke ruimte op de server van de internetprovider op te laden, ga je ook daarvoor geschikte software gebruiken. Om je persoonlijke ruimte te raadplegen, ga je navigatiesoftware gebruiken. Heb je het recht om gebruik te maken van al die software? Of met andere woorden, zijn deze bijvoorbeeld geen illegale kopieën?

Hoewel het misschien vanzelfsprekend is, moet er toch aan herinnerd worden dat software eveneens geniet van een auteursrechtelijke bescherming. Het is niet omdat je software op een drager hebt gekocht, dat je ook houder bent geworden van de intellectuele rechten op deze software. In de praktijk brengt dit met zich mee dat het gebruik van software de toestemming van de rechthebbende van het auteursrecht op dit programma, vereist. Deze toestemming wordt in de praktijk gegeven door het sluiten van een licentie. De licentie wordt over het algemeen verleend bij de aankoop van de cd-Rom of dvd drager, waarop het programma staat.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

70. Mag ik een foto scannen om in mijn persoonlijke ruimte te plaatsen?

Om je persoonlijke ruimte aantrekkelijker te maken, zal je waarschijnlijk geneigd zijn om er één of meer gescande (gedigitaliseerde) foto's op te plaatsen. Mag je een analoge foto scannen om hem vrij op je persoonlijke ruimte te plaatsen? Op deze vraag kan geen eenduidig antwoord worden gegeven. Er moeten twee mogelijke hypotheses worden onderscheiden:

1. Ofwel heb je zelf de foto genomen (vakantiefoto, familiefoto, foto van je autoverzameling, enz.) en ben je dus zelf de rechthebbende van de auteursrechten op deze foto. In principe mag je deze foto 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, van een album van Kuifje). In dit geval, moet je de toestemming verkrijgen van de auteur van het gefotografeerde voorwerp.

   Maar opgelet: daar blijft het niet bij! Als je een persoon fotografeert, moet je ook zijn recht op afbeelding eerbiedigen. Dit recht, dat niet rechtstreeks verbonden is met het auteursrecht, laat iedere gefotografeerde persoon toe om zich te verzetten tegen elke reproductie van zijn afbeelding (onder meer via het internet) en tegen elke mededeling van zijn afbeelding aan het publiek. In dit geval moet je dus de toestemming vragen aan de afgebeelde persoon.

2. Ofwel scan (digitaliseer) je een foto uit een boek of tijdschrift met de bedoeling om ze op je persoonlijke ruimte te plaatsen. In dit geval is de kans groot dat de foto beschermd is door het auteursrecht. Het volstaat immers dat een foto origineel is om een auteursrechtelijke bescherming te genieten. Een foto als origineel bestempelen is een beoordeling die dikwijls door de rechter wordt gevolgd. Er wordt unaniem aanvaard dat het scannen (of op een andere manier digitaliseren) van een werk een reproductiehandeling is, die tot exclusieve recht van de auteur behoort. Bijgevolg mag je zulks een foto doorgaans niet scannen en ook niet op je persoonlijke ruimte plaatsen zonder de toestemming van de fotograaf (of een andere persoon aan wie de rechten zijn overgedragen). Naast de toestemming 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 de rechthebbende bent van de auteursrechten. Je moet deze rechten dus blijven eerbiedigen.

71. Mag ik een beeld (tekening) scannen en op mijn persoonlijke ruimte plaatsen?

Net zoals met foto's zal je misschien geneigd zijn enkele beelden (zoals humoristische tekeningen of striptekeningen) op je persoonlijke ruimte te plaatsen om deze aantrekkelijker te maken. Zoals voor foto's mag je enkel, zonder de toestemming van wie ook, een gescand beeld op je site plaatsen als je zelf de tekenaar bent van dat beeld en voor zover het geen herkenbare afbeelding van een persoon is.

In de andere gevallen zal het beeld beschermd zijn door het auteursrecht indien het origineel is, wat vaak het geval zal zijn. Bijgevolg zal je dan vooraf de toestemming van de auteur moeten vragen. Krachtens het recht op afbeelding moet je ook de toestemming krijgen van een getekende persoon. Onverminderd een bescherming door het auteursrecht, kan een beeld nog beschermd zijn door het merkenrecht.

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

72. Mag ik een tekst scannen en op mijn persoonlijke ruimte plaatsen?

Naast foto's en beelden wil je ook een tekst op je persoonlijke ruimte plaatsen. Deze tekst kan je bijvoorbeeld zelf schrijven of misschien verkies je om een bestaande tekst te scannen. Nadat je een programma voor tekenherkenning hebt gebruikt, plaats je vervolgens deze tekst, in de vorm van een beeldbestand of een tekstbestand, op je site. Kan je om het even welke tekst op je persoonlijke ruimte plaatsen? Ook op deze vraag is het antwoord negatief.

Op grond van de hierboven uiteengezette principes weet je reeds dat een tekst door het auteursrecht wordt beschermd indien hij origineel is. De lengte van de tekst (een slogan, enkele regels of verscheidene pagina's) of de drager waarop hij oorspronkelijk werd geplaatst (papier, cd-rom, website, enz.) spelen bijgevolg geen enkele rol.

Dit vormt geen enkel probleem indien je de auteur bent van de tekst, of m.a.w. dat je de de tekst zelf hebt gecreëerd. Het overnemen van een bestaande tekst heeft uiteraard niet tot gevolg dat je zelf de auteur van de tekst wordt.

Indien, daarentegen, de tekst beschermd wordt door het auteursrecht, mag hij niet op een persoonlijke ruimte worden gereproduceerd zonder de toestemming van de au-

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

teur ervan (tenzij men zich kan beroepen op de uitzondering van het citaatrecht). Zo beschouwde de Franse rechtspraak dat het digitaliseren van het werk van Jacques Brel en van Michel Sardou, zonder toestemming van de rechthebbenden, als namaak moet worden beschouwd. In België heeft de rechtspraak geoordeeld dat de reproductie van krantenartikels op een databank, beschikbaar op internet, een handeling is waarvoor de toestemming van de auteurs noodzakelijk is.

73. Mag ik een werk (beeld, logo, icoon, foto, tekst, videosequens, muziekbestanden) van een andere site of persoonlijke ruimte kopiëren of downloaden om het op mijn persoonlijke ruimte plaatsen?

Hier gaat het niet meer om de digitalisatie van een werk dat vastgelegd is op een analoge drager (een papieren document), maar om het downloaden door een internetgebruiker van een werk (beeld), dat zich op een site bevindt, waarbij het vervolgens op de eigen persoonlijke ruimte van de internetgebruiker wordt geplaatst. Het werk wordt zodoende (her)verspreidt op internet.

Met de bekende functie *kopiëren/plakken* (*copy/paste*), die in de meeste software zit, kun je in een mum van tijd een indrukwekkende reeks gegevens bijeenscharrelen 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 is namelijk een reproductiehandeling en het (her)verspreiden van een werk op internet is een mededeling aan het publiek. Beide handelingen vallen onder het auteursrecht. Indien het werk bijgevolg beschermd is door het auteursrecht, wat doorgaans het geval is, moet je in principe dus vooraf de toestemming van de auteur bekomen.

Als het logo dat je overneemt, bovendien als merk is geregistreerd, kan de reproductie ervan een inbreuk op het merkenrecht vormen en worden gesanctioneerd.

74. Mag ik een beeld of foto vastgelegd op een analoge drager scannen of een beeld of foto vastgelegd op een digitale drager kopiëren en op mijn persoonlijke ruimte 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 de grootte, kleuren, vormen, contrast, oriëntatie, kadrering enz.) dat het gewijzigde beeld geen enkele gelijkenis meer vertoont met het oorspronkelijke. Ben je in dit geval vrijgesteld van het moeten bekomen van de toestemming van de auteur van het originele werk (voor zover het beschermd is door het auteursrecht en dus origineel is)?

NEEN, het is niet omdat dit nieuwe beeld niet meer lijkt op het originele dat je je om het even wat mag permitteren. Om dit beeld immers te kunnen wijzigen met behulp van de geschikte software, heb je vooraf een reproductiehandeling gesteld (hetzij door het werk te scannen, hetzij met *kopiëren/plakken*), waarvoor de toestemming van de auteur nodig is. Bovendien valt het herwerken van een beeld met tekensoftware niet enkel onder het "adaptatierecht" maar ook onder het "integriteitsrecht" van het werk, welke tot de exclusieve rechten van een auteur behoren. Bijgevolg vereisen zulke wijzigingen ook een toestemming van de auteur.

Indien het herwerkte beeld helemaal niet meer lijkt op het oorspronkelijke beeld, hoe kan de auteur dan een inbreuk op zijn rechten opsporen en zich op die rechten beroepen? Het is inderdaad zo dat het dikwijls moeilijk is voor een auteur om de inbreuken op zijn rechten op te sporen. Men moet echter weten dat er tegenwoordig systemen van technische bescherming bestaan (bijvoorbeeld "tatoeëring" of "markering"). Deze systemen maken het mogelijk om een digitaal werk te identificeren, zelfs indien het sterk werd gewijzigd, en om het gemakkelijk op internet terug te vinden.

75. Mag ik muziekbestanden (bijvoorbeeld mp3's) op mijn persoonlijke ruimte ter beschikking stellen van internetgebruikers?

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

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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. Men kan onmiddellijk begrijpen wat voor mogelijkheden dit biedt op het internet: vroeger had je uren nodig om een lied van enkele minuten te downloaden, terwijl je vandaag voor een mp3-bestand slechts een paar minuten nodig hebt. Het internet puilt uit van geluidsbestanden in mp3-formaat (waarvan de meeste illegaal zijn), omdat ze van de ene internetgebruiker 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 of literaire creatie, beschermd door het auteursrecht indien het origineel 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 bijgevolg 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 internetgebruikers zonder toestemming van de rechthebbenden van de aldus gecomprimeerde werken. Dergelijke handelingen zijn namelijk reproducties en mededelingen aan het publiek, die onder het exclusieve recht van de auteur vallen. Belgische en buitenlandse rechtbanken hebben deze principes reeds toegepast en sommige personen tot verschillende maanden gevangenisstraf veroordeeld. Deze 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 vennootschappen (*zoals Napster ea.*) kregen het ook aan de stok met het gerecht omdat ze software en een platform ontwikkelden waardoor internetgebruikers (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 bijgevolg gevallen waarin het plaatsen van een mp3-bestand op een website niet strafbaar is:

- hetzij omdat het werk niet origineel is en bijgevolg dus niet beschermd wordt door het auteursrecht (zo'n geval komt wel zelden voor);
- hetzij omdat je zelf het werk hebt gecomponeerd, uitgevoerd en opgenomen. In dit 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: al moet je geen toestemming vragen aan de componist van het muziekstuk of lied, toch kan het zijn dat je de toestemming van de muzikanten (de artiesten die het werk uitvoeren) en de fonogramproducenten,(de platenmaatschappijen) nodig hebt. Bovendien moet je voorzichtig zijn, daar er verscheidene werken bestaan die niet meer door het auteursrecht worden beschermd, maar waarvan de bewerking nog beschermd is;
- hetzij omdat de mp3-bestanden de auteursrechten eerbiedigen.

76. Mag ik hyperlinks die verwijzen naar sites met mp3-bestanden, op mijn persoonlijke ruimte plaatsen?

Het antwoord hierop is onzeker. 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 hebben gekozen voor een minder soepele oplossing. 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.

77. Mag ik beschermde werken (muziek, films, enz.) verspreiden via peer-to-peersystemen?

Zich inschrijven in een uitwisselingssysteem voor bestanden van het *peer-to-peer*type is geen ongevaarlijke handeling m.b.t. de intellectuele eigendom.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Toelaten aan derden om werken te downloaden waarvan kopieën op je computer (op de harde schijf of op een andere drager die erop is aangesloten) zijn opgeslagen, is een terbeschikkingstelling aan het publiek, die het auteursrecht schendt.

Het gebruik van peer-to-peersystemen om bestanden aan te bieden is alleen toegestaan in de veronderstelling dat een voorafgaande toelating van de auteur van de aangeboden werken werd gegeven of als de aangeboden werken eigen creaties zijn. In dit laatste geval mogen in de eigen creaties geen bestaande werken van derden zijn verwerkt (vb.: als je een gedubde Vlaamse versie van een aflevering van de televisieserie "Prison Break" ter beschikking stelt, schend je de auteursrechten op het originele werk, en meer bepaald op de desbetreffende aflevering).

De rechtspraak heeft herhaaldelijk privépersonen veroordeeld voor het gratis aan derden aanbieden van van beschermde werken, die kunnen gedownload worden via peer-to-peersystemen.

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

Neen, niet noodzakelijk. Het vermelden of ontbreken van een *"copyright"* betekent niet dat het werk beschermd is door het auteursrecht of juist niet beschermd is. Wij hebben immers reeds gezien dat een werk beschermd is door het auteursrecht door het loutere feit van het creëren van het werk. Het werk moet – en dit zijn de enige voorwaarden - origineel zijn en in een bepaalde vorm worden uitgedrukt. 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.

Omwille van bewijsrechtelijke maatregelen, raden wij echter aan de vermelding *"copyright Janssens* – 2000" aan te brengen, indien je een - waarschijnlijk door het auteursrecht beschermd - werk van jou (tekst, foto, enz.) op je site wilt plaatsen. Overeenkomstig artikel 6 van de auteurswet wordt iemand verondersteld houder te zijn van het auteursrecht als zijn naam of een of ander teken als dusdanig op het werk is vermeld.

79. En wat met de werken die worden verspreid met de vermelding "zonder auteursrechten" (copyright free), "open access", "vrije licentie", "freeware" of "shareware"?

Bekommerd om een gemakkelijke en gratis toegang tot hun werken te verzekeren, wilden bepaalde auteurs hun werken verspreiden volgens een bepaalde formule, die soms wordt voorgesteld als een alternatief op het auteursrecht en met verschillende benamingen wordt aangeduid: een vrije licentie, open access, creative commons, enz.

Bij de meeste van deze licenties mag iedereen het werk "vrij" (binnen de voorwaarden van de licentie) gebruiken, reproduceren, verspreiden en wijzigen. Deze viervoudige vrijheid is verbonden aan de voorwaarde dat de van het originele werk afgeleide werken zelf worden verspreid volgens identieke voorwaarden (dit is wat men de besmettelijkheid van de vrije licenties noemt: het virus verspreidt zich van het oorspronkelijke werk naar alle werken die ervan zijn afgeleid).

Vanuit een juridisch oogpunt blijft het auteursrecht van toepassing op deze exploitatiewijze van werken. De werken blijven immers beschermd door het auteursrecht. Door het gebruik van deze exploitatiewijze drukken de rechthebbenden hun wil uit dat ze "op een andere manier" hun rechten willen uitoefenen. De nuance is van belang.

Het betekent immers dat de maker van de onder vrije licentie verdeelde werken de rechthebbende van de auteursrechten blijft en dus kan beslissen om deze rechten uit te oefenen wanneer hij zich, bijvoorbeeld, wil verzetten tegen bepaalde gebruiksvormen van zijn creatie.

Vóór elk gebruik van een werk dat wordt aangeboden onder vrije licentie of als open access, moet **de gebruikerslicentie grondig worden gelezen** (deze neemt dikwijls de vorm aan van algemene voorwaarden). Het is deze licentie die bepaalt wat je kunt doen met het op een dergelijke wijze verspreidde werk. Het is bijvoorbeeld gebruikelijk dat deze licenties het gebruik van werken voor commerciële doeleinden verbieden.

Een vrije licentie betekent dus geen totale vrijheid!

Bovendien wordt de verspreiding onder een vrije licentie soms als een tijdelijke exploitatiewijze gebruikt, waarbij je enkel een zeker aantal werken kunt uitproberen. Zo vind je op internet vaak databanken of *"shareware"* software. Na een proefperiode moet de gebruiker een licentie aanvragen of ophouden met het gebruik van de software of de databank. De tijdelijke vrije licenties van het "shareware"-type zijn over het alge-

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

meen veel beperkter m.b.t. de gebruiksmogelijkheden van de tijdelijk ter beschikking gestelde werken onder de zogenaamde "vrije" licentie. Ook hier, is het onontbeerlijk om de voorwaarden van de licentie aandachtig te lezen om elk later probleem met de rechthebbende(n) te vermijden.

80. Wanneer ik met een hyperlink verwijs naar een andere website, moet ik dan de toestemming vragen aan de eigenaar van die site?

Als je een eigen website creëert, zal je waarschijnlijk een of meer links naar andere sites (of naar een specifieke pagina van een andere site) plaatsen. Moet je dan de toestemming vragen aan de eigenaar van de site waarnaar je een hyperlink legt?

Het antwoord blijkt negatief te zijn. Over het algemeen vormt dit soort van handeling geen probleem m.b.t. het auteursrecht. Zelfs al is deze vraag nog het voorwerp van discussies onder juristen, is de tendens om aan te nemen dat elke persoon die verantwoordelijk is voor een website geacht wordt om de andere operatoren van het netwerk stilzwijgend de toestemming te hebben gegeven om een hyperlink naar zijn site te plaatsen. Deze link moet wel eenvoudig zijn en doorverwijzen naar de homepage van de site (en niet naar een andere bepaalde pagina van de website). Wel wordt aangeraden om zich te onthouden van het plaatsen van hyperlinks naar sites met een illegale of schadelijke inhoud (revisionistische of pornografische sites bijvoorbeeld).

Indien je daarentegen andere hyperlinktechnieken gebruikt, die niet als "eenvoudig" worden beschouwd, moet je aandachtig blijven voor de eventuele juridische gevolgen die eruit kunnen voortvloeien. Bijvoorbeeld: men vermeldt hyperlinks die bestaan uit de titels van krantenartikels (die beschermd zijn door het auteursrecht!) en waarbij systematisch wordt verwezen naar de site die deze artikels publiceert. Deze praktijk kan worden beschouwd als een oneerlijke concurrentie (*parasitisme*) en/of een schending van het auteursrecht. Ook het gebruik van een "diepe link" kan voor problemen zorgen. Dit soort van hyperlink verwijst naar een interne pagina van de site, zonder aldus via de homepage van de desbetreffende site te moeten passeren.. Bepaalde verantwoordelijken van websites hebben erop gewezen dat deze praktijk voor hen schadelijk is, oa. wanneer de homepage de enige is die reclame bevat en aldus door het toedoen van de "diepe" link niet kon gezien worden door verscheidene internetgebruikers. Waakzaamheid is ook geboden voor het gebruik van de *framingtechniek* (kaders, vensters) gecombineerd met hyperlinks. Je moet vermijden dat het publiek in verwarring wordt gebracht omtrent de echte eigenaar van de site. Men kan zich inderdaad inbeelden dat je een hyperlink plaatst in een venster (*frame*) die verwijst naar een prachtig gedicht op een andere site.

Bij het aanklikken van deze link kan het gebeuren dat de pagina waarop het 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 jouw gedicht is. Onthoud je van dergelijke praktijken of zorg ervoor dat je de toestemming hebt van de persoon die verantwoordelijk is voor de site waarnaar verwezen wordt.

81. Kan ik mij verzetten tegen het plaatsen van een hyperlink naar mijn site?

Zoals uitgelegd in het voorafgaand antwoord wordt er over het algemeen aangenomen dat de verantwoordelijke van een website geacht wordt stilzwijgend toestemming te hebben verleend aan de andere operatoren van het netwerk om een hyperlink te leggen naar zijn site.

Dit principe moet echter sterk genuanceerd worden. Je zal je steeds kunnen verzetten tegen een hyperlink naar je site, indien deze link wordt geplaatst op een zodanige wijze dat het je schade kan berokkenen. Dit zou het geval kunnen zijn bij een hyperlink die naar jouw site verwijst en die om de een of de andere reden geplaatst wordt op een website met een pornografische of revisionistische karakter, of waarbij de link deel zou uitmaken van een zin die een onterend of beledigend karakter heeft. De hyperlink zou ook, naar gelang van de context, kunnen beschouwd worden als bedrieglijke reclame (wat verboden is) of vergelijkende reclame (die echter niet het geheel van de door de wet opgelegde voorwaarden zou naleven). Zou ook als schadelijk worden beoordeeld, de hyperlink die overmatig voordeel haalt uit jouw werk (je hebt een site gecreëerd die niet uitgegeven foto's publiceert m.b.t. de bergbeklimming en een andere gebruiker creëert een inhoudsloze site, doch verwijst met een hyperlink stelselmatig naar foto's op jouw site, dit alles met een zeer verwarrend karakter).

Gezien de schadelijke gevolgen die kunnen voortvloeien uit het gebruik van hyperlinks, vermelden bepaalde sites in hun algemene voorwaarden de volgende clausule: "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".

82. Welke zijn de sancties i.g.v. niet naleving van het auteursrecht ?

De niet naleving van de hierboven vermelde principes kan aanleiding geven tot het nemen van strafrechtelijke sancties (gevangenisstraf of boete) en/of burgerrechtelijke straffen (bijvoorbeeld de betaling van een schadevergoeding).

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Er moet benadrukt worden dat namaak geen oogmerk tot het berokkenen van schade vereist, noch een kennis over het bestaan van andermans recht. Het zal dus onmogelijk zijn om je te beroepen op je onwetendheid of goede trouw om aan een veroordeling te ontsnappen.

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.

Deze 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 collectieve beheersvennootschappen voor auteursrechten alles in het werk om de rechten van hun leden te doen eerbiedigen. Tenslotte werden al tal van personen door onder meer Belgische en Franse rechtbanken veroordeeld wegens namaak omdat zij op hun site auteursrechtelijke beschermde werken hadden geplaatst. Een goed verstaander heeft maar een half woord nodig...

83. Mag ik het merk van een derde op mijn persoonlijke ruimte gebruiken?

Zoals hierboven werd aangetoond, is het gebruik van een merk dat aan een derde toebehoort in principe verboden. Concreet wordt de omvang van de bescherming van een merk bepaald door de gelijkenis tussen de tekens, de gelijkaardigheid van de producten of diensten en het soort gebruik dat van het merk wordt gemaakt. Zelfs al zijn de betrokken producten of diensten niet gelijk aan die van de houder van een bekend merk, of zelfs als wordt het teken niet gebruikt om mijn eigen producten of diensten te onderscheiden (ik verkoop niets met dit teken), dan is het gebruik van andermans teken verboden, als het gebruik van dat teken onterecht voordeel haalt uit het onderscheidend karakter of de bekendheid van het merk, of daaraan schade berokkent.

Er is met andere woorden een inbreuk op het merk, als het gebruik van het teken op een persoonlijke ruimte:

- van die aard is dat het een ongerechtvaardigd voordeel haalt uit de bekendheid van het merk (bijvoorbeeld het gebruik van het merk "Comme chez soi" als de restaurateur op zijn persoonlijke ruimte aangeeft dat zijn recepten zijn geïnspireerd op die van het bekende Brusselse restaurant)

- van die aard is dat het schade berokkent aan de reputatie van het merk (als de keuken van het betreffende restaurant in het voornoemde voorbeeld van erbarmelijke kwaliteit is);

In bepaalde gevallen is het gebruik van het merk van een derde mogelijk:

- als het is gecreëerd om het publiek te informeren over het doel van de producten of diensten die je verkoopt (bijvoorbeeld als je Zanussi-wasmachines herstelt, is het toegestaan om dit merk te gebruiken om het doel van je diensten aan te geven);

- als je informatie wilt verspreiden m.b.t. een merk, is het toegestaan om het merk te gebruiken. Dit wordt toegestaan door het principe van vrije meningsuiting. Zo heeft de rechtspraak bijvoorbeeld geoordeeld dat de Franse vakbonden van de Danone-groep een website mogen creëren die een oproep doet tot het boycotten van de Danone-producten, als reactie op een ontslagplan van de Franse fabrieken van de multinational (het gebruik van het merk Danone werd als rechtmatig beschouwd). Men moet echter voorzichtig blijven en elke ongerechtvaardigde kritiek op het merk vermijden. Deze kritiek zou immers als een inbreuk op het merk kunnen beschouwd worden en het voorwerp kunnen zijn van een gerechtelijke sanctie. Zo werd Greenpeace veroordeeld voor opzettelijke laster aan het merk Areva (groep die in Frankrijk actief is in de kernenergie) dat ze in verband hadden gebracht met foto's van dode vissen, gezichten van doden enz.

Rekening houdend met de complexiteit van het onderwerp en in het bijzonder met het vage karakter van de grenzen tussen de rechtmatige uitoefening van de vrije meningsuiting en de opzettelijke laster, is het aan te bevelen om met de grootste omzichtigheid om te springen met het gebruik van het merk van een derde op uw persoonlijke ruimte.

84. Hoe kan ik mijn persoonlijke ruimte optimaliseren voor zoekmachines zonder de rechten van derden te schenden?

De positionering van een persoonlijke ruimte hangt vaak af van de manier waarop ze is geïndexeerd in de zoekmachines. In dit opzicht moet de keuze van de trefwoorden of de positioneringstermen met de grootste voorzichtigheid gebeuren.

Als je hemden verkoopt, is het verleidelijk om termen als "Lacoste" of "Ralph Lauren" te gebruiken om internetgebruikers aan te trekken. Dergelijke praktijken moeten niettemin worden vermeden.

Het gebruik van het merk van een derde – *a fortiori* van een concurrent – vormt immers in de meeste gevallen een ongeoorloofd gebruik dat een inbreuk is op het merkrecht. De rechtspraak heeft reeds verscheidene malen websitebeheerders bestraft die het merk van hun voornaamste concurrent bij hun trefwoorden hadden gevoegd, voor een optimalere indexering van hun site.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Er zijn niettemin omstandigheden waarin het gebruik van het merk van een derde geoorloofd is. Als je vervangingsonderdelen verkoopt, is het toegestaan om gebruik te maken van het merk van de producten waarvoor de stukken die jij verkoopt, zijn bestemd.

Gezien de uitzonderingen op het verbodsprincipe zeer beperkt zijn, wordt aangeraden om een specialist raad te plegen vóór elk gebruik van het merk van een derde ter indexatie van je persoonlijke ruimte.

85. Is mijn persoonlijke ruimte beschermd door het auteursrecht of door een ander recht?

We hebben reeds gezien dat wanneer je een persoonlijke ruimte creëert, je dit moet doen met eerbiediging van de rechten van derden en onder meer de auteursrechten. Omgekeerd kan je belang hebben bij de bescherming van je eigen persoonlijke ruimte en de inhoud ervan. Indien je bijvoorbeeld amateur-fotograaf bent en je andere internetgebruikers de mogelijkheid wil bieden je foto's raad te plegen, heb je niet noodzakelijkerwijze zin dat een derde het geheel van je foto's zou kopiëren. Wat voor foto's geldt, geldt ook voor gedichten, muziekstukken, wetenschappelijke publicaties en dergelijke meer. Anderzijds kan de structuur van je persoonlijke ruimte op zich, ook origineel zijn en zou je er graag het vaderschap erop willen behouden.

Daar het hier om een complexe aangelegenheid gaat, treden wij niet in details. Je moet evenwel weten dat de inhoud van je persoonlijke ruimte (teksten, beelden, foto's, enz.) door het auteursrecht kan worden beschermd voor zover je de auteur bent van de inhoud. Bovendien kan de persoonlijke ruimte zelf (d.w.z. zijn voorstelling, lay-out, typografie, tekeningen, structuur van de elementen) ook door het auteursrecht worden beschermd, zoals we hierna zullen zien. De enige voorwaarde is dat de persoonlijke ruimte en de inhoud ervan origineel zijn, wat meestal wel het geval is. Hierdoor zal je je dus kunnen verzetten tegen elke reproductie van deze elementen door een derde.

Voorts wordt door een Europese richtlijn van 11 maart 1996, omgezet in Belgisch recht bij wet van 31 augustus 1998 (*BS*, 14 november 1998, p. 36914), een dubbele bescherming ingesteld voor databanken, enerzijds via het auteursrecht en anderzijds via een specifiek recht, *sui generis* recht genaamd.

Het auteursrecht beschermt originele databanken (een website kan namelijk als een databank worden beschouwd of kan tenminste een databank bevatten). Originele databanken zijn databanken die, door de keuze of de rangschikking van de stof, een eigen intellectuele schepping van de auteur vormen. Deze bescherming heeft niet betrekking op 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 oorspronkelijke rechthebbende is de persoon die de databank ontworpen heeft. Hij kan zijn rechten wel overdragen aan een natuurlijke of rechtspersoon, zoals bijvoorbeeld de producent van de databank. 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 indien ze niet origineel zijn) genieten ook van een bescherming door een *sui generis* recht, dat van toepassing is op alle databanken, waarvan het verkrijgen, het nakijken of het voorstellen van de inhoud getuigt van een aanzienlijke kwantitatieve of kwalitatieve investering. De rechthebbende is de producent van de databank, d.i. de natuurlijke of rechtspersoon die het initiatief en het investeringsrisico nam. Op grond van dit recht mag hij de opvraging en/of het hergebruik van de gehele databank of van een substantieel deel ervan, verbieden (of tegen betaling toestaan). Dit recht heeft een beschermingsduur van 15 jaar te rekenen vanaf de voltooiing van de databank. Elke substantiële wijziging van de databank geeft recht op een nieuwe beschermingstermijn van 15 jaar.

Vergeet niet dat als de structuur en de voorstelling van de persoonlijke ruimte door het auteursrecht worden beschermd, dit bepaalde voorzorgsmaatregelen vergt als je beroep doet op een derde om je persoonlijke ruimte aan te maken. Inderdaad, vermits een derde deze persoonlijke ruimte aanmaakt, is hij immers de rechthebbende van de auteursrechten op de ruimte. Er moet dus in het contract voor het ontwerp van een persoonlijke ruimte worden voorzien dat de auteursrechten aan jou worden overgedragen. Bovendien is het waarschijnlijk dat de ontwerper van de persoonlijke ruimte gebruik maakt van reeds bestaande elementen (foto's, iconen, enz.). In dit opzicht moet hij je de garantie geven dat hij de toestemming heeft gekregen van de derde rechthebbende(n) op deze elementen en moet hij er zich toe verbinden om je schadeloos te stellen in geval van een geschil met een derde. Deze contractuele voorzorgsmaatregelen zijn onontbeerlijk om je persoonlijke ruimte vrij en in alle wettelijkheid te kunnen beher.

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

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Hoofdstuk I. Inbreuken op het privéleven

Afdeling 1. Indringingstechnieken

86. In hoever wordt mijn privéleven 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* 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.

Op het vlak van 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. Sommige technieken, zoals *spyware* (spionagesoftware), zijn nog indringender en kunnen zelfs achter persoonsgegevens komen die op je harde schijf staan.

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 - http://www.privacycommission.be).

87. 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. Ze worden opgeslagen in het werkgeheugen van je computer 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 pa-

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

gina 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. Zij worden op de harde schijf van je computer weggeschreven.

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).

88. Waartoe dient een cookie?

Cookies doen je opzoekingen 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 onderneming 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 opzoekingen 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 goederen en diensten 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.

89. Moet ik op mijn hoede zijn voor cookies?

In principe verschaffen cookies geen informatie die je niet voordien op een of anderre manier hebt doorgespeeld. 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 (permanente) cookie een spoor nalaat op de harde schijf van je computer en aangeeft welk traject je op het internet hebt gevolgd. Houd je dus een sessie op een andere computer dan de jouwe en je niet wil dat de volgende gebruiker alles te weten komt over dat bezoek, neem dan je voorzorgen en wis je “sporen” uit. De meeste internetbrowsers bieden aan om uw sporen onmiddellijk te wissen na elke sessie (in het bijzonder in Mozilla Firefox door de toetsen ALT + SHIFT + DEL in te drukken). Voor andere browsers kunt u het tabblad “opties” aanklikken en “internet opties” selecteren en de knop “Cookies verwijderen”.

90. Hoe kan ik mij beschermen tegen cookies?

Afhankelijk van je ergelSDN over die intrusie in je privéleven, 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 (Firefox en Microsoft Explorer) melden de komst van cookies "in real time" of

blokkeren ze zelfs automatisch (Mozilla Firefox). 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 parametreren.

Sommige browserversies bieden de mogelijkheid automatisch cookies te weigeren. Je kunt je browser zodanig instellen dat hij systematisch de indringing van cookies weigert. Die radikale 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.

91. Hoe kan ik mij juridisch beschermen?

De Belgische wet regelt het gebruik van je persoonsgegevens. 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.

92. Wat is spionagesoftware?

Spionagesoftware (ook spionsoftware of *spyware* genoemd) is een klein informaticaprogramma dat ongemerkt alles wat je op je computer of op internet doet volgt en 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. Spyware verschilt van een cookie, omdat je niet noodzakelijk een website moet hebben bezocht om hem op je computer te krijgen.

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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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 bezoekfrekwentie te meten.

93. 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).

94. 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. Extra waakzaamheid is geboden met software om bestanden uit te wisselen.

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 geregistreerd als een virus en glipt vaak door de mazen van deze filters.

Vermijd tevens om op berichten te klikken die je willen doen geloven dat de computer in gevaar is, dat hij is besmet met een virus of dat u een loterij heeft gewonnen.

De doeltreffendste 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 antispywareprogramma'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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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

95. 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 internetsessies (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, automatische verrichtingen om een klant een profiel toe te kennen 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).

96. 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 inzamelen 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.

97. Wat zijn de algemene principes van de gegevensverwerking door de verantwoordelijke?

Elke fysieke persoon of rechtspersoon moet bij een verwerking van persoonsgegevens de volgende onderlinge afhankelijke principes respecteren:

- het legitimiteitprincipe schrijft voor dat er voldoende wettige redenen moeten zijn om de verwerking te rechtvaardigen (bijvoorbeeld de uitvoering van een contract, het naleven van een wettelijke verplichting, het levensbelang van de betrokkene, enz.);

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

- het oogmerkprincipe schrijft voor dat het gebruik van verzamelde gegevens streng moet worden beperkt tot één of meerdere doeleinden die moeten worden bepaald alvorens te beginnen met de verwerking van de gegevens;
- het noodzakelijkheids- en proportionaliteitsprincipe houden in dat de verwerking van gegevens moet worden beperkt tot de gegevens waarvoor een direct verband bestaat met het aanvankelijke doel van de gegevensverwerking;
- het principe van de nauwkeurigheid van gegevens wil de overlast vermijden die personen zouden kunnen ondervinden omwille van onnauwkeurige of onvolledige gegevens. Het gaat hierbij om een verplichting tot zorgvuldigheid die de verantwoordelijke oplegt om omzichtig te werk te gaan bij de gegevensverwerking;
- het eerlijkheidsprincipe houdt transparantie van daden in met betrekking tot de verwerking van persoonsgegevens;
- het principe van veiligheid en vertrouwelijkheid schrijft voor dat de verzamelde gegevens moeten worden verwerkt op een vertrouwelijke manier en moeten worden opgeslagen op onaantastbare en veilige plaatsen.

98. 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 privételefoonnummer 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

- recht op directe 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. Je kunt hem dan een fax of een brief sturen met een kopie van je identiteitskaart in bijlage, of eventueel een elektronisch ondertekende e-mail (elektronische handtekening – zie woordenlijst). De verantwoordelijke moet, op straf van boete, ten laatste 45 dagen na ontvangst van het verzoek antwoorden.

- recht op indirecte toegang

Bepaalde delen van je gegevens mogen niet vrij worden geconsulteerd. Dat is het geval voor gegevens die worden bewaard in het kader van de bescherming van het land, van de openbare veiligheid, van de landsverdediging of de preventie of de bestraffing van misdrijven (bijvoorbeeld als er een gerechtelijk onderzoek tegen jou wordt geleid op basis van je gedragingen als internaut).

Je kunt niettemin indirect toegang krijgen tot deze gegevens door je tot de Commissie voor de bescherming van de persoonlijke levenssfeer te wenden. Meer nog dan in het raam van je recht van directe toegang, moet je je identiteit bewijzen, ofwel door bij je brief een kopie van je identiteitskaart te voegen of door een elektronisch ondertekende e-mail te sturen.

De Commissie treedt dan op als bemiddelaar en kan je gegevens in jouw plaats consulteren. Vervolgens brengt ze je ervan op de hoogte dat ze de gegevens heeft gecontroleerd en eventueel dat ze ze heeft laten wijzigen zonder de inhoud openbaar te maken.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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 inroepen die verband houden met je bijzondere toestand.

Bovendien is het gebruik van persoonsgegevens voor marketingoperaties streng gereglementeerd. De wet biedt je steeds de mogelijkheid je, zonder verantwoording en kosteloos, te verzetten tegen de geplande verwerking wanneer persoonsgegevens voor directe marketing worden ingewonnen.

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.

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

Als je problemen ondervindt om je rechten uit te oefenen of als je ziet dan een verantwoordelijke persoon zijn plichten niet nakomt, kun je je gratis richten tot de *Commissie voor de Bescherming van de Persoonlijke Levenssfeer* (hierna CBPL genoemd), die de zaak zal onderzoeken. Als je een klant indient, zal de CBPL trachten te bemiddelen om de zaak in der minne te regelen. Deze procedure is gratis. Inlichtingen over die instelling vind je op het volgende adres: http://www.privacycommission.be.

Lukt dat niet, dan kan de CBPL de inbreuk melden aan de Procureur des Konings of een klacht indienen bij het gerecht. Je kunt zelf ook klacht neerleggen bij de Procureur des Konings.

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

100. 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 opneming 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 over 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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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

101. 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 privéleven 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 privésector.

Bij de controle van elektronisch meegedeelde gegevens (men spreekt ook van "verkeersgegevens" – niet te verwarren met de inhoud van de mededelingen -, zoals de naam van de verzender of van de bestemmeling van een elektronische zending, de datum en het uur van verzending, de aard (tekstbestand, beeld, audio) en de grootte van een eventueel bijgevoegd bestand, het adres van een bezochte website, het tijdstip en de duur van de inzage, het feit of er al dan niet werd gedownload,enz.) 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 *evenredigheid*sprincipe 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.

Bovendien 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.

Ten slotte is de naleving van CAO nr. 81, die werd verplicht bij koninklijk besluit, met het wettelijk verbod om kennis te nemen van elektronische communicaties, echter onderworpen aan controverse. Het is dan mogelijk dat de CAO nr. 81 niet over een toereikende legale basis beschikt om de werkgever inbreuk te laten maken op de vertrouwelijkheid van de elektronische communicaties.

Een andere collectieve arbeidsovereenkomst (CAO nr.85) die betrekking heeft op het telethuiswerk heeft deze mogelijkheid van "cybertoezicht" weer mogelijk gemaakt indien

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

de werkgever beschikt over een machtiging voor toezicht en controle op het werk van de werknemer, overeenkomstig de gezagsverhouding die de werkrelatie kenmerkt.

In het kader van het telethuiswerk kan de werknemer normaal gezien alleen nog gecontroleerd worden op een indirecte manier. Als directere controletechnieken hun intrede hebben gedaan de laatste tijd, neemt dat niet weg dat de werkgever verplicht is om de werknemer voorafgaand in te lichten en dat hij voorafgaandelijk toestemming moet krijgen van de werknemer om een dergelijke controle te mogen invoeren.

102. 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 privéleven 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 privéleven. Het afstaan van een fundamenteel recht is onderworpen aan een aantal voorwaarden, gelet op de onvervreemdbare 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 privéleven afstaat in het arbeidscontract, die afstand meestal moet worden bevestigd bij elke nieuwe inmenging.

103. 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 "gereglementeerd".

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 geheim van elektronische communicatie en inbreuken daarop worden strafrechtelijk vervolgd.

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.

104. 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 privéleven van zijn werknemers.

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.).

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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 en de verwerking van de verzamelde gegevens moet aangeven bij de CBPL.

Hoofdstuk II. De oplichters en ongewenste e-mail

105. Wat zijn de meeste verspreide vormen van ongewenste e-mail?

Er bestaan vele vormen van ongewenste e-mail, die soms gepaard gaan met oplichterij en fraude. De courantste vormen worden hieronder kort uitgelegd, maar je zult ook andere concrete voorbeelden en praktische raadgevingen vinden op de site www.spamsquad.be. Veel informatie staat ook in de brochure "Spamming in vraag – Geïllustreerde voorbeelden en praktische tips" in te kijken op het adres: http://economie.fgov.be/information_society/spamming/home_nl.htm

- Spamming

In ruime zin betekent *spamming* (of kortweg *spam*) 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 bestemmelingen.

Gegeven het feit dat deze berichten van commerciële of publicitaire aard zijn, zijn ze onderworpen aan de specifieke reglementering van reclameberichten via e-mail.

- Phishing

Phishing is fraude door zich over het algemeen onder de valse identiteit van een dienstverlener of een erkende instelling (een bank, ene portaal enz.) voor te stellen om van de geadresseerde vertrouwelijke gegevens te ontfutselen, zoals zijn bankrekeningnummers, zijn gebruikersnaam en wachtwoord, zijn nummer van de sociale verzekering, zijn geboortedatum, het nummer van zijn rijbewijs, het nummer en de vervaldatum van zijn kredietkaart enz.

Phishing gebeurt het vaakst door middel van een (valse) officiële website of een (valse) e-mail afkomstig van de zogenaamde dienstverlener of instelling. Als hij eenmaal in het bezit is van de persoonsgegevens van de slachtoffers, kan de auteur dan misbruik

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

maken van hun identiteit en bijvoorbeeld bankverrichtingen uitvoeren in hun naam, betalingen uitvoeren, hun e-mails lezen enz. Phishing is strafbaar.

- Scam

Scam betekent 'oplichting' in het Engels. In het internetuniversum verwijst deze term naar verschillende bijzondere vormen van oplichting. Hieronder enkele voorbeelden.

De "Nigerian scam" (ook 'scam 419', 'Nigeriaanse brieven' of 'Afrikaanse scam' genoemd) heeft betrekking op e-mails waarvan het doel is om goedgelovige internauten geld afhandig te maken door ze te vragen als tussenpersoon op te treden voor de transfer van aanzienlijke sommen geld (zogenaamd geblokkeerd in het buitenland in moeilijke politieke context) in ruil voor een percentage van de getransfereerde som. Als het slachtoffer aanvaardt, zal het over het algemeen een rekening openen en geld voorschieten (voorgewende notaris- of advocaatkosten, steekpenningen enz.) zonder ooit in ruil de beloofde som te krijgen.

Met de "werkaanbiedingscam" wordt gestolen geld gesleten. Een pseudobedrijf (of een bestaand bedrijf waarvan de identiteit wordt misbruikt) verstuurt een e-mail om werk aan te bieden. Vaak gaat het om thuiswerk in de sector van de elektronische betalingen, die erop is gericht om geld te transfereren. In werkelijkheid gaat het om een vorm van oplichterij waarbij de bankrekening van de internaut wordt gebruikt om sommen geld te versassen, om op die manier gestolen geld "wit te wassen" ten voordele van de verschillende oplichters.

De "loterijscam" verwijst naar een vorm van oplichting met voorschotten op kosten die worden verhaald op het slachtoffer. Gewoonlijk krijgt het "doelwit" een ongevraagde e-mail, die hem erover inlicht dat hij een groot lot heeft gewonnen bij een loterij, zelfs als hij er niet heeft aan deelgenomen. Om het bedrag te krijgen, moet de zogenaamde winnaar verschillende stappen uitvoeren (een formulier invullen waarin persoonsgegevens worden gevraagd, een nieuwe rekening openen enz.) en instemmen met verschillende voorschotten op fictieve kosten (overschrijvingskosten, taksen, zegelrechten enz.).

Deze zwendels zijn allemaal vormen van phishing (zie hierboven).

- Hoaxen

Zie nr. 29.

106. Hoe komen verzenders van ongevraagde e-mails aan mijn elektronisch adres?

Ze 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 goed of dienst aan te kopen of een bestand te downloaden, als je je inschrijft op een mailinglijst of deelneemt aan een wedstrijd of 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 tal van gratis product- of dienstenaanbiedingen dat je in ruil daarvoor aanvaardt reclame- of andere e-mails 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 om 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, aanbieding van gratis webruimten...).

- Ten slotte bestaat er een ware markt van (al dan niet legaal verzamelde) 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.

107. Moet is spam vrezen?

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 ongewenste berichten 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).

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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

108. 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 overzendingswijze van de e-mail kan worden nagegaan te vervalsen of te verbergen.

Door de invoering van die wettelijke vereisten, ook al zijn die niet van toepassing op reclame, zal de programmering van filters volgens het gekozen criterium worden vergemakkelijkt.

Filters geprogrammeerd volgens de oorsprong van de berichten blokkeren e-mail afkomstig van geïdentificeerde IP-adressen. Filters die geprogrammeerd zijn volgens de inhoud van e-mails elimineren berichten 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 e-mailprovider of op je eigen computer worden geïnstalleerd.

Filtering bij je e-mailprovider is de handigste oplossing omdat de provider zelf de ongewenste berichten 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.

En omgekeerd, als er een filter op je computer staat, dan komt alle ongewenste e-mail 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 berichten te verliezen dus minder groot, vermits je zelf de selectiewijze hebt ingesteld.

Je vindt nog meer concrete voorbeelden en praktische tips door te surfen naar www.spamsquad.be.

109. Zijn er technische mogelijkheden om me te beschermen tegen oplichters?

Het beste is om zo waakzaam mogelijk te blijven ten opzichte van aanlokkelijke of vreemde voorstellen. Hierbij enkele raadgevingen (surf voor meer informatie naar www.spamsquad.be en www.oplichters.be):

- Laat je onder geen enkel voorwendsel verleiden om geld te storten aan een (on)bekende.
- Reageer nooit op een e-mail die je vertelt dat je een loterij hebt gewonnen.
- Antwoord nooit op een e-mail die je om persoonsgegevens vraagt, zelfs al gaat het om een dienstverlener die je kent. Geen enkele ernstige dienstverlener zou je vragen om hem gevoelige gegevens mee te delen via e-mail. In geval van twijfel, is het best om de (echte) dienstverlener rechtstreeks te contacteren, zonder daarbij de (valse) adresgegevens te gebruiken uit de (valse) e-mail.

Als je je e-mailadres op een website plaatst, denk er dan aan om het te camoufleren door bijvoorbeeld het "@"-teken te vervangen door "at". Je adres naam@domeinnaam.be wordt op die manier naam(at)domeinnaam.be.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Hoofdstuk III. Illegale en nadelige sites

110. 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. 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 met bepalingen voor de strijd tegen kinderporno nieuwe wapens aan om pedofilie te bestrijden:

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, zijn volgens de wet strafbaar.

Toegepast op het internet opent die wet nieuwe perspectieven: iedere persoon die op het Belgische grondgebied woont en met kennis van zaken van het internet gedownloade 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.

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

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

Uiteraard moet je vermijden informatie van pedofiele aard te raadplegen (een ministeriele 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 meldpunt van het Belgisch overheidsmeldpunt voor internetmisbruik (http://www.ecops.be). Indien de aangifte bij de provider werd gedaan, stuurt deze ze door naar het meldpunt.

- Het meldpunt voert een sortering uit. Indien *duidelijk* blijkt dat de informatie *niet* illegaal is, wordt het dossier geseponeerd. 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 het Belgisch overheidsmeldpunt voor internetmisbruik (http://www.ecops.be).

3. Ten slotte kun je je richten tot *Child Focus*, hetzij telefonisch (op nummer 116 000), 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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

- 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.
- 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.

112. 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.

113. 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.

114. Zijn filtersystemen efficiënt?

De waarde en de doeltreffendheid van op lijsten gebaseerde systemen hangen af van de keuze van de ondernemingen. 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. Door het succes van dit initiatief moeten echter heel wat websites worden geëvalueerd. Het aantal geëvalueerde websites is momenteel nog klein.

115. Wat moet ik doen als ik op het web een illegale of voor mij 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 privéleven, ...?

Vooreerst moet je je wenden tot je internetprovider of tot de *hoster* 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 politiecommissariaat. 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. Je kunt de inhoud elektronisch aangeven, bij het Belgisch overheidsmeldpunt voor internetmisbruik (zie www.ecops.be).

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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 privéleven), dan kun je steeds schadevergoeding eisen. Wij raden je dan ook aan je klacht in te dienen met burgerlijkepartijstelling.

Buiten elke rechtsvordering kun je tevens vergoeding eisen voor geleden schade door een vordering over 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 kwestieuze site laten blokkeren of hem onmiddellijk doen verwijderen.

116. 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 overzenden 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 kwestieuze 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 kunt hoe dan ook altijd de aansprakelijkheid van de auteur van de betwiste informatie aan de kaak stellen, voor zover je hem natuurlijk kunt identificeren.

Hoofdstuk IV. Cybercriminaliteit

Afdeling 1. Informaticavervalsing

117. 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* en zelfs aan informaticabedrog indien de operatie je een voordeel kan opleveren. We spreken dan van "ideale samenloop van overtredingen", d.w.z. dan eenzelfde daad diverse misdrijven inhoudt. In dat geval wordt enkel de grootste strafmaat toegepast.

118. Voorbeelden van informaticavervalsing

Valsheid in informatica is onder meer: namaak of vervalsing van kredietkaarten; valsheid op het vlak van 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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

119. 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.

De wet voorziet tevens dat hij die gebruik maakt van de gegevens die op die manier werden verkregen terwijl hij weet dat ze vals zijn, wordt gestraft alsof hij de auteur ervan is. Het hergebruik van verkregen gegevens door middel van bedrog is dus op dezelfde wijze strafbaar als het bedrog zelf!

120. 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 veranderd zijn. Het begrip gegevens wordt door de wet in ruime zin opgevat en deze laatste bevat alle voorstellingen van informatie die kunnen worden opgeslagen, verwerkt en verstuurd door middel van een computersysteem.
- Door de manipulatie moet de juridische draagwijdte van de gegevens veranderen. De rechter bepaalt of een dergelijke verandering daadwerkelijk heeft plaatsgevonden.
- Het misdrijf moet gepleegd zijn met bedrieglijk opzet of met het oogmerk te schaden. Daaruit volgt dat de vervaardiging van valse kredietkaarten of valse digitale handtekeningen voor wetenschappelijke doeleinden bijvoorbeeld niet strafbaar is op basis van de inbreuk van valsheid in informatica.

Afdeling 2. Informaticabedrog

121. Wat is informaticabedrog?

Volgens de wet wordt "informaticabedrog" gepleegd door iemand die, met frauduleus oogmerk voor zichzelf of voor een ander tracht een illegaal economisch voordeel te verwerven, via een informaticasysteem opgeslagen, verwerkt of overgedragen gegevens in een informaticasysteem invoert, wijzigt, wist of op enige andere technologische wijze de normale aanwending van gegevens in een informaticasysteem verandert.

Met andere woorden bestaat computerfraude erin gegevens te manipuleren ten opzichte van een machine om zich een onwettig voordeel te bezorgen (deze inbreuk leunt aan bij oplichterij; traditionele oplichterij heeft echter betrekking op het misleiden van een persoon en niet van een machine).

122. 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 wijziging van programma's of computerbestanden om onrechtmatige financiële voordelen te bekomen of de uitvoering van onrechtmatige manipulaties van klantenrekeningen door een bankbediende.

Een andere recentere vorm van computerfraude is phishing. *Phishing* op zich vormt niet het voorwerp van een specifieke strafbepaling, toch is het gebruik van persoonsgegevens van het slachtoffer met de bedoeling om handelingen te verrichten in naam van het slachtoffer strafbaar uit hoofde van computerfraude en zelfs van bedrog als een valse website of een vals e-mailadres werd gebruikt.

123. 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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

124. 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

125. 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:

- De eerste is ongeoorloofde toegang tot het informaticasysteem van een derde of er zich handhaven. Dat noemen we *externe hacking;*
- De tweede is voor iemand die reeds rechtmatig toegang heeft tot een computersysteem, overschrijding van zijn bevoegdheid voor toegang tot dit systeem. Dat noemen we *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. Indien het misdrijf wordt gepleegd met een dergelijk opzet of doel, dan wordt de straf enkel verzwaard. Er is sprake van het zich handhaven in het informaticasysteem zodra de indringer er zich gedurende een bepaalde tijd in verplaatst, ook al is het systeem niet beveiligd (met een wachtwoord of firewall) of al omzeilt de indringer geen enkele beveiligingsmaatregel.

In het tweede geval moet de dader, die beschikt over de rechten voor toegang tot een systeem maar die bevoedheid 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).

126. 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 informaticasyseem 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. In het geval dat een persoon gebruik maakt van de onbeveiligde Wi-Fi-toegang van zijn buur zonder daarvoor de toestemming te hebben gekregen kan de volgende vraag worden gesteld: moest hij noodzakelijkerwijs weten dat hij geen toestemming had om ge-

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

bruik te maken van de draadloze verbinding of kon hij daarentegen echt denken dat de eigenaar van het Wi-Fi-netwerk impliciet aan derden de toestemming had gegeven om er gebruik van te maken door het niet te beschermen tegen toegang van buitenaf?

127. Wat met hulpmiddelen en apparatuur om gemakkelijker te kunnen hacken?

Personen die eender welke voorzieningen, met inbegrip van computergegevens, die hoofdzakelijk ontworpen zijn of aangepast om te *hacken*, onrechtmatig bezitten, vervaardigen, verkopen, verschaffen voor gebruik, importeren of ter beschikking stellen onder een andere vorm worden door de wet bestraft met een boete of een gevangenisstraf. Deze bepaling heeft betrekking op het gebruik, het bezit of de verdeling van *hackertools*, d.w.z. de hulpmiddelen of software die hacking vergemakkelijken, maar tevens de verboden handel in toegangscodes of valse licenties waarmee je in een computersysteem kan binnendringen zonder ertoe te zijn gemachtigd.

We merken op dat om het vrije verkeer van algemene informatie op het gebied van beschermingstechnieken (in het bijzonder via het web) niet te belemmeren, de wet bepaalt dat de inbreuk niet heeft plaatsgevonden tenzij dit bezit of gebruik van een hackertool is verbonden aan het oogmerk om te bedriegen (of is op zijn minst *ongegrond,* om de exacte juridische term te gebruiken). Zo kregen de bedrijven het recht om hun computerbeveiliging te kunnen testen en de wetenschappers of professoren om de werking van apparatuur voor beveiligingsomzeiling te kunnen uitleggen en te testen. In deze veronderstelling is het gebruik of de communicatie van informatie om te kunnen *hacken* toegestaan en dus een niet-strafbaar feit.

128. 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 informaticasys-

teem 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 tot *hacking* of ertoe aanzet. Zo straft de wet ook iemand die via *hacking* bekomen data heelt, onthult of er enig gebruik van maakt. Met andere woorden, heling van gehackte informatie is eveneens strafbaar.

129. 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 zogenoemd *Intrusion Detection System* of IDS, een soort inbraakalarm).

Bovendien zorgt de toename van Wi-Fi-netwerken voor bijkomende beveiligingsproblemen als deze netwerken van buitenaf toegankelijk zijn. De golven reiken immers verder dan het normale gebruiksveld van de het netwerk. Het is dus noodzakelijk om je Wi-Fi-netwerk te beschermen, te weten door gebruik te maken van apparatuur die voor de codering, legalisatie en identificatie zorgen van de werkstations die het Wi-Fi-netwerk betreden en van de gegevens die er circuleren. Beveiligingsprotocollen zoals WPA2 (Wi-Fi Protected Access 2) helpen het netwerk te beveiligen en zijn drie functies te leren kennen. Aangezien geen enkele beveiliging volmaakt is, wordt aangeraden om voldoende

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

informatie in te winnen bij een verkoper van Wi-Fi-routers of je internetprovider en de installatiegidsen goed te lezen die worden meegeleverd met het materieel om zo de beveiliging van je Wi-Fi-netwerk te optimaliseren.

Afdeling 4. Computersabotage

130. Wat is computersabotage?

Personen die rechtstreeks of onrechtstreeks in een computersysteem gegevens invoeren, wijzigen of verwijderen, of die door middel van eender welke technologie het normale gebruik van gegevens in een computersysteem wijzigen, bewust van het feit dat ze er geen toestemming voor hebben, worden door de wet bestraft met een gevangenisstraf en/of boete.

De wet heeft betrekking op computersabotage, bijvoorbeeld schadelijke handelingen zoals het binnenbrengen van een virus, de vernietiging van een computerbestand of het onbruikbaar maken van een harde schijf of computersysteem.

Een computervirus overdragen kan bijvoorbeeld worden ondergebracht bij computersabotage, zelfs als dit virus niet werd binnengebracht als gevolg van *hacking* of computerfraude. Het virus zorgt er immers voor dat het normale gebruik van een computer wordt bemoeilijkt door de gegevens die hij verwerkt te beschadigen.

Het uitwissen van computergegevens waartoe men toegang heeft, kan tevens als strafbaar aan sabotage worden beschouwd als het niet was toegestaan.

De wet voorziet dat poging tot computersabotage wordt bestraft met dezelfde straffen als sabotage zelf.

131. Zijn er verzwarende omstandigheden?

De wet schrijft voor dat als er computersabotage wordt gepleegd met het oogmerk om te bedriegen of om schade te berokkenen, de gevangenisstraf wordt verzwaard.

Zwaardere straffen zijn eveneens bij wet voorzien als de sabotage effectieve schade veroorzaakt (bijvoorbeeld de corruptie van een database, de onmogelijkheid om nog commerciële diensten aan te bieden via het gesaboteerde systeem, de verspreiding van een

virus enz.) of het computersysteem volledig of gedeeltelijk belemmert (onbeschikbaarheid van de computer, verlies van noodzakelijke software om een toepassing te laten functioneren enz.) wat vaak het geval is.

Ten slotte schrijft de wet voor dat bij herhaling van de feiten de straffen worden verdubbeld.

132. Wat met sabotagehulpmiddelen?

Net zoals *hackertools* bij wet zijn verboden, schrijft de wet voor dat personen die voorzieningen, met inbegrip van computergegevens, hoofdzakelijk ontworpen of gebruikt om gegevens te beschadigen of het volledige of gedeeltelijke correcte gebruik van een computersysteem te verhinderen, onrechtmatig bezitten, vervaardigen, verkopen, verschaffen voor gebruik, importeren, verdelen of ter beschikking stellen onder een andere vorm, worden veroordeeld tot dezelfde straffen als deze in geval van computersabotage.

De wet heeft betrekking op de hulpmiddelen en voorzieningen die systemen van derden kunnen beschadigen. De creatie of het gewone bezit van een virus, als dat niet is toegestaan en als de houder zich bewust is van de gevaarlijke kenmerken ervan, kan strafrechtelijk worden gestraft.

Afdeling 5. Verzending/ontvangst van virussen

133. Wat is een computervirus?

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

Het woord "virus" wordt vaak gebruikt in een ruime zin en verwijst in dit geval naar elke vorm van kwaadwillige programma's (*malware* in het Engels). De virussen in enge zin, zoals wormen, *spywareprogramma's* en "Trojaanse paarden" zijn voorbeelden van kwaadwillige programma's.

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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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.

De kwaadwillige programma's kunnen tevens veel schadelijkere gevolgen hebben: *spywareprogramma's* zijn gevaarlijke programma's die als bijzonder kenmerk hebben dat ze persoonsgegevens verzamelen op de hostcomputer en versturen naar instellingen van derden, zonder dat de computer er zich rekenschap van geeft.

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.

134. Welke levensloop heeft een computervirus?

Computervirussen hebben, net als biologische virussen, een levenscyclus die loopt van de schepping tot de uitroeiing. Na de schepping, dus de ontwikkeling van het virus, wordt het virus gekopieerd naar een strategische plaats om het zo breed mogelijk te verspreiden. Als het eenmaal is verspreid, zal het zichzelf kopiëren op alle geïnfecteerde computers. Het kan dan zichzelf activeren op een ogenblik dat alle voorwaarden daarvoor vervuld zijn: een virus kan dus gedurende een zekere tijd "slapen" op een besmet systeem.

Een virus kan meestal worden opgespoord en geïsoleerd. Zodra dat gebeurd is, wordt het nieuwe virus over het algemeen doorgezonden naar de ICSA (*International Computer Security Association*) in Washington DC, waar documentatie over het virus wordt verzameld en nadien verdeeld onder de ontwerpers van antivirusprogramma's.

Zo kunnen de software-ontwikkelaars hun programma's om de aanwezigheid van een nieuw virus te kunnen vaststellen en van het systeem te kunnen verwijderen, maar ook om te beletten dan andere systemen worden besmet.

135. 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 cd in je computer steken is meestal ongevaarlijk, *zolang je geen software lanceert of geen bestand opent!*

Meestal is het door een besmette toepassing of een besmet bestand te openen dat het virus zich verspreidt over andere toepassingen en bestanden. Op die manier kunnen programma's of bestanden die je met vrienden of collega's deelt via een cd, dvd, USB-sleutel, het internet of een lokaal netwerk eveneens besmet worden en kun je het virus dus overbrengen op andere computers.

Je computer kan onmogelijk door een virus besmet worden als je alleen maar een e-mail in tekstformaat leest. Een tekstformaat kan geen virus bevatten. Het is daarentegen 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 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. Het is echter mogelijk het risico te beperken door de opties in uw e-mailprogramma aan te passen.

136. 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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

137. 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.

- Mijd programma's van twijfelachtige oorsprong en bestanden die worden meegestuurd met berichten;
- Wees voorzichtig met het openen van bestanden van externe bronnen (USB-sleutel, internet, cd-rom);
- Scan je harde schijf en je systeem geregeld op virussen,
- Maak geregeld back-ups van belangrijke bestanden op je harde schijf nadat je bent nagegaan of er geen virussen in voorkomen en eventuele virussen hebt verwijderd;
- Blijf op de hoogte van het opduiken van nieuwe virussen. Sommige websites bieden je die service gratis aan door het afkondigen van "besmettingsgevaar" als een virus zich sterk aan het verspreiden is. Dat doet onder meer de site www.secuser.com/alertes, dat diverse recent ontdekte virussen bespreekt.

138. Is het verzenden van virussen strafbaar?

Zoals we eerder al zagen, beteugelt de wet niet alleen het gebruik van een virus, dat wordt beschouwd als computersabotage, maar ook 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.

139. 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).

140. 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...

141. 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 web circuleren.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Je moet tevens weten dat de site van het BIPT (Belgisch Instituut voor Postdiensten en Telecommunicatie – www.ibpt.be) een rubriek bevat die informatie over de recentste virussen geeft en de mogelijkheid biedt om zich op een nieuwsbrief in te schrijven om op de hoogte te worden gebracht van de recentste ontwikkelingen.

Afdeling 6. Andere vragen die je je stelt

142. 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 dragers of zelfs je hele informaticamaterieel, voor zover zij een huiszoekingsbevel hebben.

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

Ja. Wanneer inbeslagname van informaticamaterieel of -dragers niet nodig is, mogen de kwestieuze 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.

144. 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...

145. Kan een huiszoeking worden uitgebreid naar de elektronische gegevens buiten mijn eigen systeem?

Ja. De wet schrijft uitdrukkelijk voor dat de onderzoeksrechter kan gelasten om in het kader van een huiszoeking, het onderzoek uit te breiden naar een computersysteem of een deel ervan dat zich op een andere plaats bevindt dan waar het onderzoek wordt uitgevoerd. Op grond van deze bepaling zou de rechter dus toegang kunnen krijgen tot het e-mailaccount of de bankgegevens van de persoon die het voorwerp is van het onderzoek door middel van software die op zijn computer is geïnstalleerd.

Deze uitbreiding van het onderzoek zal echter alleen mogelijk zijn onder de dubbele voorwaarde dat de uitbreiding noodzakelijk is om de waarheid met betrekking tot de inbreuk die het voorwerp uitmaakt van het onderzoek aan het licht te brengen en dat andere maatregelen zijn uitgeput of dat er een risico bestaat dat bewijselementen verloren zouden gaan zonder deze uitbreiding.

De wet bepaalt dat de uitbreiding van het onderzoek naar een computersysteem niet verder mag gaan dan de computersystemen waartoe de personen die gemachtigd zijn om het systeem te gebruiken dat het voorwerp is van de maatregel, specifiek toegang hebben. De autoriteiten mogen er dus niet van profiteren om sites of systemen te bezoeken waartoe de persoon die het voorwerp van het onderzoek is geen toegang heeft, wat logisch lijkt.

Als zou blijken dat de gegevens zich buiten het Belgische grondgebied bevinden, verplicht de wet om de autoriteiten van de derde staat te contacteren en is enkel het kopiëren van de gegevens toegestaan.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

146. 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 decoderingssoftware, vertrouwensderden (bijvoorbeeld een verstrekker van certificatiediensten), zelfs van deskundigen over informaticaveiligheid die het cryptosysteem voor de beveiliging van de kwestieuze 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.

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

Ja! De wet verplicht de operatoren (telefoonnetwerk- en –dienstenoperatoren voor vaste en mobiele telefonie, internetproviders, e-mailproviders enz.) je verkeer- en identifi-

catiegegevens te registreren en te bewaren tijdens een periode van ten minste twaalf maanden en maximaal zesendertig maanden.

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

De wet vermeldt niet wat ze onder "verkeergegevens" of "identificatiegegevens" verstaat; ze zegt ook niet welke providers specifiek aan die bewaarplicht onderworpen zijn. Waarschijnlijk omvatten de gegevens het uur en de duur van de verbindingen, de herkomst van de oproepen, het IP-adres van je computer... Een Europese richtlijn, die nog niet in België werd omgezet, bepaalt de categorieën van gegevens die moeten worden bewaard voor elke dienst van elektronische communicatie.

Een koninklijk besluit zou de voorwaarden voor de gegevensbewaring, de lijst van de betreffende gegevens, en de precieze duur van de bewaring moeten bepalen. Dit koninklijk besluit werd echter nog niet bekrachtigd. Bovendien is het regelen van deze kwestie bij koninklijk besluit aanvechtbaar in die zin dat de Grondwet voorschrijft dat de beperkingen voor het privéleven moeten worden geregeld door een wet.

Deze ruime en onduidelijke verplichting om gegevens te bewaren wordt voorzien met het doel om het onderzoek en het vervolgen van strafrechtelijke inbreuken te vereenvoudigen. Een ander koninklijk besluit bepaalt in dit opzicht de regels en voorwaarden waarvoor de operatoren moeten samenwerken met de gerechtelijke autoriteiten om het toezicht op de belgegevens van de gebruikers en de communicatie ervan mogelijk te maken.

Deel 5.
Een overeenkomst sluiten op het web

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Hoofdstuk I. Reclame, wedstrijden en promotionele aanbiedingen op internet

148. 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 goederen of diensten.

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

Dit betekent dat elke publiciteit duidelijk als dusdanig naar voren moet komen. Is dat niet het geval, dan moet de vermelding "reclame" in het bericht staan.

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. Het volstaat dat zijn identificatiegegevens via een hyperlink kunnen worden geraadpleegd.

149. 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 goed of dienst recht geven op een kortingbon, een geschenk, een gratis goed of dienst, of aanbiedingen die de aankoop van goed of een dienst linken aan de aankoop van andere goederen of diensten, 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 product- of dienstenverstrekker, bij prijsvermindering, duidelijk vermelden :

- ofwel de referentieprijs (dit is de laagste prijs die voor dat goed of die dienst werd toegepast in de loop van de maand die voorafging) naast de verminderde prijs;
- ofwel enkel de nieuwe prijs, met de nodige informatie (toegekend kortingpercentage) die het de consument mogelijk maakt die referentieprijs onmiddellijk en gemakkelijk te berekenen.

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.

150. Hoe moet ik denken over aanbiedingen voor gratis goederen of diensten?

Deze vorm van aanbiedingen neemt toe, zowel op het web als elders. Denk er steeds aan dat als de dienstverlener je iets gratis aanbiedt hij er op een andere manier wel voordeel uithaalt. Je moet in ieder geval waakzaam blijven en de voorwaarden goed lezen om een dergelijke aanbieding te kunnen genieten. Als je in de informatie die wordt gegeven een gebrek aan transparantie bemerkt, wees dan wantrouwig. Hierna volgen enkele basisraadgevingen die je verder kan aanvullen door te surfen op de site www.oplichters.be:

- Let op voor inbreuken op het privéleven:

  Om een gratis goed of dienst te krijgen, moet je soms een aantal persoonlijke gegevens meedelen over jezelf of over je verwanten. Het idee dat erachter zit, is om van jou zo veel mogelijk gegevens los te krijgen om voor marketingdoeleinden te gebruiken of door te verkopen aan anderen. Hoe beter je consumentenprofiel is vastgelegd, hoe meer waarde het zal hebben.

  De wetgeving ter bescherming van de persoonlijke levenssfeer is natuurlijk op deze praktijken van toepassing. Je moet in het bijzonder worden ingelicht over het gebruik van al deze gegevens en over de identiteit van de verantwoordelijke voor de gegevensverwerking. Bovendien moet de dienstverlener je om toestemming vragen om je e-mailadres te mogen gebruiken voor reclamedoeleinden en je de mogelijkheid bieden om je te verzetten tegen enig ander commercieel gebruik van je gegevens.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Voor wat de gegevens van je verwanten betreft, ben jij in principe niet gemachtigd om deze mee te delen zonder ze daarvan vooraf op de hoogte te stellen en er mag hen geen enkele publicitaire e-mail worden gestuurd als ze daar zelf geen toestemming voor hebben gegeven.

- Let op voor abonnementen:

  In bepaalde gevallen zijn de gratis goederen of diensten gebonden aan een abonnementsformule: ofwel moet je je abonneren om een gratis welkomstgeschenk te ontvangen, ofwel is het abonnement zelf gedurende een bepaalde testperiode gratis, ofwel brengt alleen al het verzoek om een gratis goed of dienst een automatisch abonnement met zich voor gelijkaardige en... betalende goederen en diensten. Alvorens de minste stap te ondernemen, moet je de voorwaarden om van een dergelijke aanbieding te kunnen profiteren en om het abonnement op te zeggen, goed lezen.

- Ga na wat gratis is:

  Soms is enkel het verzoek om informatie over het goed of de dienst werkelijk gratis en niet het goed of de dienst zelf! Het gebeurt tevens dat de aanbieding slechts gedeeltelijk gratis is en dat erbovenop tal van betalende diensten worden aangeboden (en zelfs opgelegd).

- Let op voor twijfelachtige downloads:

  Er kunnen tal van bestanden gratis worden gedownload van het internet (software, spelletjes, muziek, films, achtergrondafbeeldingen...). Merk echter op dat bepaalde van deze bestanden twijfelachtige software bevatten, die inbreuk zouden kunnen maken op je privéleven (spyware) of op je computer (virus, Trojaans paard enz.).

- Pas op voor communicatiewijzen waarbij een toeslag moet worden betaald:

  Om een gratis goed of dienst te kunnen krijgen, moet je soms een telefoonnummer bellen, een sms sturen of je met het internet in verbinding stellen via een speciaal nummer, het zijn allemaal communicatiewijzen waarbij een toeslag moet worden betaald (van het type 09xx). De dienstverlener is verplicht om je in te lichten over deze bijkomende kosten. Je moet tevens ook nagaan of dit gesprek je niet doet overgaan naar een formule van een automatisch abonnement met andere gelijkaardige diensten (zie hierboven). Aarzel bij problemen niet om de ombudsdienst voor telecommunicatie te contacteren (www.ombudsmantelecom.be).

Als je denkt dat je het slachtoffer bent van een misleidende of oneerlijke reclame, kan je klacht indienen bij de bemiddelaar op de site www.ecops.be.

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

Behoudens uitzonderingen mag je geen enkele reclame per e-mail worden toegezonden zonder je voorafgaande, vrije, specifieke en geïnformeerde toestemming. Vaak vraagt men je om je toestemming te geven door een vakje aan te vinken bij een vermelding in de trant van "Ik aanvaard om via e-mail promotionele boodschappen te ontvangen" als je een onlineformulier invult om een goed of dienst te bestellen.

Je toestemming moet in alle *vrijheid* zijn gegeven. U een voordeel ontzeggen als u er niet mee instemt om reclame te ontvangen, is bijvoorbeeld een drukkingsmiddel.

Je toestemming moet *specifiek* zijn, wat betekent dat enkel jij die kan geven en dat die specifiek betrekking moet hebben op het feit via e-mail reclame te ontvangen van de dienstverlener, of daarnaast eventueel van commerciële partners van deze laatste.

Je toestemming moet *geïnformeerd* zijn, d.w.z. dat het duidelijk moet zijn dat je via e-mail reclame zult ontvangen als je het vakje aanvinkt.

Bij betwisting is het overigens de dienstverlener die zal moeten bewijzen dat hij wel degelijk je toestemming heeft verkregen binnen de wettelijke vereisten.

Je vindt talrijke informatie over deze vraag in de brochure « Spamming in 24 vragen en antwoorden », op het volgende adres : http://economie.fgov.be/information_society/spamming/home_nl.htm

152. Zijn er uitzonderingen op het principe van voorafgaande toestemming?

Er zijn niettemin uitzonderingen op het principe van voorafgaande toestemming. De voornaamste is dat een adverteerder je onder de volgende voorwaarden ongevraagde reclame mag sturen via e-mail als je een van zijn klanten bent:

- hij heeft je e-mailadres rechtstreeks van jou gekregen, in het kader van de verkoop van een goed of een dienst en met eerbied voor de wet voor de bescherming van de persoonlijke levenssfeer;

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

- hij mag je alleen reclame sturen voor gelijkaardige goederen en diensten die hij zelf levert (en niet van andere of door derden geleverde goederen of diensten);
- op het moment waarop je hem je e-mailadres hebt meegedeeld, moet hij je de mogelijkheid hebben geboden om je gratis en op een eenvoudige manier te verzetten tegen het ontvangen van dergelijke reclameberichten. In ieder geval heb je altijd het recht om je te verzetten tegen het ontvangen van dergelijke reclameberichten in de toekomst.

Je vindt talrijke informatie over deze vraag in de brochure " Spamming in 24 vragen en antwoorden ", op het volgende adres : http://economie.fgov.be/information_society/spamming/home_nl.htm

153. 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 in de toekomst;
- je een geschikt middel aanreiken om via de computer efficiënt gebruik te maken van dat recht.

Als je bovendien je recht op verzet uitoefent, heeft de betreffende dienstverlener de verplichting:

- om je binnen een redelijke termijn via elektronische weg een bericht van ontvangst te sturen waarbij hij je bevestigt dat hij je verzoek goed heeft geregistreerd (deze ontvangstbevestiging mag vanzelfsprekend geen reclameboodschap meer bevatten);
- om binnen een redelijke termijn de nodige maatregelen te nemen om aan uw wil te voldoen;
- om zijn verzetlijst bij te werken.

154. 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 aangesloten bij het Belgisch Direct Marketing Verbond (BDMV), kun je je inschrijven op de Robinson-e-maillijst van dit verbond (surf naar http://www.bdma.be, of rechtstreeks naar pagina http://www.robinsonlist.be/). De doorgegeven gegevens (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. Je kan je trouwens afvragen wat het nut is van die Robinsonlijst, vermits het sinds maart 2003 bij wet verplicht is op voorhand in te stemmen met elke verzending van e-mailreclame!

155. Geldt dit alles ook voor sms-berichten en pop-ups?

In de praktijk gebruikt de wet nergens de term "e-mail", maar "elektronische post", die bijzonder ruim is en zeker ook sms'en omvat. Reclame-pop-ups vallen echter niet onder de reglementering op de verzending van reclame via elektronische post.

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).

Die lijst is in alle opzichten vergelijkbaar met de e-maillijst.

Weet ook dat gelijkaardige regels gelden voor alle reclame die per fax en automatisch oproepautomaat wordt verzonden.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Hoofdstuk II. De sleutel van het vertrouwen: goede informatie

Krachtens de wet moet de dienstverlener op zijn website een aantal gegevens vermelden met betrekking tot zijn activiteiten, contractvoorwaarden, aangeboden goederen en diensten, je bestelling enz.

156. Met wie heb ik te maken? Op welke informatie over de dienstverlener en zijn activiteiten heb ik recht?

Om een bepaalde transparantie te verzekeren in de contractuele relaties die worden gesloten op het net, moet de dienstverlener aan al zijn bezoekers een minimum aan informatie bieden betreffende zijn activiteiten, te weten:

- zijn naam of zijn bijnaam;
- het geografische adres waar hij is gevestigd;
- zijn persoonlijke gegevens, met inbegrip van zijn e-mailadres, waardoor je snel met hem in contact kan komen en rechtstreeks en efficiënt met hem kan communiceren;
- indien van toepassing, het handelsregister waarbij hij is ingeschreven en zijn registratienummer (dit nummer werd sinds 2003 vervangen door het ondernemingsnummer);
- indien van toepassing, zijn btw-nummer ; dit nummer werd sinds 2003 vervangen door het ondernemingsnummer);
- de gedragscodes waaraan hij eventueel is onderworpen alsook de gegevens met betrekking tot de wijze waarop de codes via elektronische weg kunnen worden geconsulteerd;
- in het geval dat de activiteit van een dienstverlener onderhevig is aan een autorisatiebeleid, de gegevens van de bevoegde toezichtautoriteit;
- en ten slotte, voor de dienstverleners die een gereglementeerd beroep uitoefenen (bv. vrije beroepen):

- de professionele vereniging of de professionele organisatie waarbij de dienstverlener is ingeschreven,
- de professionele titel en het land waar hij is vergund,
- een referentie naar de professionele regels die van toepassing zijn en naar de mogelijkheden om toegang te krijgen tot de regels.

Deze gegevens moeten voorhanden zijn bij elke veronderstelling, indien het nu gaat om een e-commercesite, een informatiesite, een zoekmachine, een internetprovider, een e-mailprovider, een discussieforum enz.

De toegang tot deze gegevens moet eenvoudig, rechtstreeks en permanent zijn, bijvoorbeeld door te klikken op een hyperlink die onderaan elke pagina wordt geplaatst, verwijzend naar een specifieke pagina die deze gegevens bevat.

Deze gegevens moeten worden geleverd door elke dienstverlener die een activiteit van economisch karakter op het internet uitvoert, en niet alleen door de dienstverleners waarbij je online een bestelling kan plaatsen. Met andere woorden, zelfs de dienstverlener die zich beperkt tot het promoten van zijn diensten via een website moet zijn identiteit meedelen voor meer transparantie.

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

Als je op het internet een overeenkomst sluit, zijn er twee problemen: ernerzijds heb je geen rechtstreeks en concreet contact met het aangeboden product of de aangeboden dienst, 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 goederen of diensten die hij levert, alsook over de voorwaarden van de overeenkomst, d.w.z.:

- gegevens over zijn identiteit en beroepsactiviteit;
- essentiële kenmerken van het goed of de dienst;

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

- prijs van het goed of de dienst, met aanduiding of de belasting en leveringskosten inbegrepen zijn;
- eventuele leveringskosten;
- wijze van betaling, levering of uitvoering van de overeenkomst;
- het al of niet bestaan van een herroepingsrecht;
- wijze van terugneming of teruggave van het goed, 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 goederenlevering, 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;
- wijze waarop eventueel verkeerd ingevoerde gegevens kunnen worden gecorrigeerd voordat de bestelling wordt doorgegeven;
- eventuele archivering van de gesloten overeenkomst en, in voorkomend geval, voorwaarden voor toegang tot dit archief na plaatsing van de bestelling.

Die informatie moet duidelijk, begrijpelijk en ondubbelzinnig zijn.

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

158. 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.

159. 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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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

- identiteit en geografisch adres van de onderneming;
- prijs van het goed 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 goederenlevering of dienstverlening, minimumduur van de overeenkomst;
- de identificatie van het goed of de dienst;
- geografisch adres waar je een klacht kunt indienen;
- inlichtingen over 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 nr. 176) 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 herroepingsrecht hebt: "De consument heeft het recht aan de onderneming mee te delen dat hij van de aankoop afziet, zonder een boete te betalen en zonder een reden op te geven, gedurende... kalenderdagen (ten minste 14 dagen) vanaf de dag die volgt op de levering van het goed of op het sluiten van de dienstverleningsovereenkomst".
- indien je geen herroepingsrecht hebt: "De consument beschikt niet over het recht om van een aankoop af te zien".

Als je een goed 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 herroepingstermijn (minimum 14 kalenderdagen), 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 dowloaden.

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 (herroeping van 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. De vekoper moet je die gegevens op een duurzame informatiedrager bezorgen, zodat je ze kunt bewaren en nadien raadplegen. Dit kan een papieren versie 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.

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

De verlener is niet verplicht je toegang te geven tot een gearchiveerde kopie van je bestelling. Biedt hij je die mogelijkheid wel, dan moet hij je dat duidelijk meedelen vóór je bestelt.

Zo laten sommige verleners 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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Hoofdstuk III. Het sluiten van een overeenkomst op het internet

161. 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. 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 goed of de gewenste dienst misschien vinden in de onlinecatalogus van de verkoper waarin per rubriek alle te koop gestelde goederen 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.

Let wel : voortaan verbiedt de wet default-opties op het internet. De onderneming mag vanaf nu niet langer de mogelijkheid van default-opties bieden bij het sluiten van een overeenkomst via het web; die praktijk bestond erin, dat je voorhand bepaalde opties moest "uitklikken" (weigeren) om te vermijden dat je een of meer extra producten zou moeten betalen (praktijk die onder meer werd toegepast door luchtvaartmaatschappijen). Tijdens transacties op het internet gebeurt het immers vaak, dat de onderneming extra producten aanbiedt en reeds op voorhand de daarvoor bestemde vakjes aanvinkt, zodat de consument, als hij niet alert is of het kruisje vergeet uit te vinken, ongewild die extra producten meebestelt, die hij in feite niet wenst. Om dergelijke praktijk te vermij-

den, werd een opt-insysteem ingevoerd voor deze producten. De consument zal voortaan zelf kunnen kiezen of hij al dan niet een bijkomend product wenst mee te bestellen, zodat hij een weldoordachte keuze kan maken zonder te worden misleid.

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.

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.

162. 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. 161) gezien hebben, wordt de verkoop vaak afgesloten met een bevestigingspagina waarop je de juistheid van de ingebrachte gegevens kunt nagaan alvorens alles te valideren.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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 herroepingsrecht.

163. Vanaf wanneer ben ik contractueel verbonden?

Het antwoord op die vraag verschilt volgens het recht dat op de overeenkomst van toepassing is, 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 herroepingsrecht uitoefenen als je nadien van mening verandert.

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

164. 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. 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 IV. Bewijs en elektronische handtekening

Je hebt een overeenkomst gesloten op het internet en je hebt erop gelet dat de voorgeschreven 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 het contract gemakkelijk kunt bewijzen.

In principe wel. Zeker als je een procedure met elektronische handtekening hebt gebruikt. Twee recente wetten (van 20 oktober 2000 en van 9 juli 2001) erkennen immers 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 onderneming 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 onderneming.

165. 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 onderneming-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 kopie van je bestelbon en van de bevestiging van je bestelling die je van de onderneming 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 kopie van je bestelbon en van de bevestiging van de onderneming!
- 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).

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

166. Hoe kan de onderneming bewijzen dat ik iets via het internet heb besteld?

Voor alle duidelijkheid: de onderneming zal het moeilijker hebben dan jij om het bestaan van de overeenkomst te bewijzen (tenzij je de onderneming hebt betaald! In dat geval zal zij 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 euro.

In het eerste geval valt de onderneming onder het stelsel van de bewijsvrijheid. Zij 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 onderneming 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 online-onderneming zonder onverantwoorde vertraging en op elektronische wijze de ontvangst moet melden van de bestelling, ongeacht het bedrag van de bestelling. Bij betwisting moet hij het bewijs leveren dat hij effectief de ontvangst van de bestelling heeft gemeld.

167. 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 euro 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 clausule 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 onderneming geen overeenkomst ondertekend hebt waarin zo'n bepaling voorkomt!

168. 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 juridisich 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 certificatiedienstverlener die voldoet aan een aantal wettelijke voorwaarden (bijlage II van dezelfde wet);

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

- 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.

Praktisch moet je weten, dat de gegevens van de handtekening die op je elektronische identiteitskaart zijn opgeslagen aan deze voorwaarden beantwoorden, en je dus in staat stellen om met een grote juridische betrouwbaarheid te ondertekenen.

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 certificatiedienstverlener 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.

169. 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 authentificatie 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 (PKI) 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 privésleutel, 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 privésleutel 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 privésleutel. Met je privésleutel kun je een bericht "ondertekenen". De ontsleuteling gebeurt volgens het principe van de complementariteit van het sleutelpaar: een bericht dat versleuteld werd met een privésleutel kan enkel worden ontsleuteld met de bijbehorende openbare sleutel. De identiteit van de ondertekenaar wordt bevestigd door een certificaat, dat wordt uitgegeven door een certificatiedienstverlener (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 privésleutel 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 privésleutel 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 certificatiedienstverlener) bevestigt dat die openbare sleutel wel degelijk aan Alice toebehoort. Dankzij de hashfunctie en een

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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 openbaresleutelcryptografie 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 certificator ("certificatiedienstverlener", ook "certificerende autoriteit" of CA genoemd).

170. Wat is een certificatiedienstverlener?

De certificatiedienstverlener (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 privésleutel 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 privésleutel. 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 ver-

volgens de openbare sleutel van Alice gebruiken om de handtekening in het door haar verstuurde 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 privésleutel 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.

171. 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 certificatiedienstverlener 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 *gekwalificeerd 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 op het vlak van 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 gekwalificeerde 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.

De lijst van erkende in België gevestigde dienstverleners die gekwalificeerde certificaten afleveren vindt u op op de site van de Federale Overheidsdienst Economie, KMO, Middenstand en Energie: http://economie.fgov.be/information_society/e-signatures/lis_e_signature_nl.pdf).

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

172. 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 privésleutel). Meer concreet is dat bijvoorbeeld software waarmee je de gegevens voor het aanmaken en verifiëren van de handtekening kunt genereren (privésleutel/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.

173. 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 privésleutel 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;

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

- hij tekent het certificaat door middel van zijn privésleutel, 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 de recente versies van Windows bevatten 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.*

174. 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.

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

Als je van plan bent een overeenkomst te sluiten via elektronische weg, 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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Hoofdstuk V. Herroepingsrecht

176. Wat is het herroepingsrecht?

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 goed 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 14 kalenderdagen (met inbegrip van zaterdag); deze termijn begint, voor de goederen, op de dag na de dag van levering en voor de diensten, op de dag na de dag van sluiting van het contract. Dit recht kan discretionair worden uitgeoefend: als je aan de overeenkomst verzaakt, moet je daarvoor geen reden opgeven.

177. Voor welke soort aankopen beschik ik over een herroepingsrecht?

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

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

- indien je de uitvoering van de dienst vraagt vooraleer de herroepingstermijn afgelopen is (bijvoorbeeld wanneer je toegang wil tot een databank en onmiddellijk de gevraagde informatie wenst te raadplegen, zonder het einde van de herroepingstermijn af te wachten);
- indien je goederen bestelt die volgens jouw wensen vervaardigd zijn of die voor jou werden gepersonaliseerd (bijvoorbeeld een op bestelling vervaardigd kledingstuk, een met je naam erop, op maat gemaakte inbouwmeubelen voor je keuken, ...);
- indien de gekochte goederen niet kunnen worden teruggestuurd of snel kunnen bederven of verouderen (bijvoorbeeld aan bederf onderhevig voedsel, verse producten enz.);
- indien de goederen (voedingswaren, drank en huishoudproducten) worden geleverd ten huize van de consument, in zijn verblijfplaats of op zijn arbeidsplaats, door verdelers tijdens frequente en geregelde rondes;

- indien je kranten, tijdschriften of magazines koopt;
- indien je online weddingschappen aangaat of loterijbriefjes koopt;
- indien je een muziek- of video-opname of informaticabestanden ontzegelt (bv. dvd, cd, cd-rom, videocassette, ...). Als je daarentegen niet aan het veiligheidssysteem raakt, dan kun je aan de overeenkomst verzaken en het goed 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 over een herroepingsrecht van 14 kalenderdagen, op voorwaarde dat je de overeenkomst zonder beroepsdoeleinden hebt gesloten. Je beschikt echter niet over dit herroepingsrecht :

1° wat de diensten betreft waarvan de prijs afhankelijk is van schommelingen op de financiële markt waarop de dienstverlener geen enkele invloed heeft (bijvoorbeeld: wisselverrichtingen, aankoop van aandelen, aandelen in collectieve beleggingsondernemingen, enz.);

2° als je vraagt om de overeenkomst uit te voeren voor de herroepingstermijn is verstreken;

3° wat betreft de overeenkomsten aangaande hypothecair krediet, die onder de wet betreffende het hypothecair krediet vallen.

178. Hoe kan ik weten of ik over een herroepingsrecht beschik?

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

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 goed is gevoegd).

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

179. Wat kan ik doen als ik niet werd ingelicht over mijn herroepingsrecht?

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

Indien de verkoper je, vóór het sluiten van de overeenkomst, of nadien, niet meldde dat je over *geen verzakingsrecht* beschikt, bedraagt de herroepingstermijn 3 maanden.

Indien de verkoper je, vóór het sluiten van de overeenkomst niet meldde dat er een herroepingsrecht bestaat, dan bedraagt de verzakingstermijn 3 maanden in plaats van 14 kalenderdagen.

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

Indien je overeenkomst de aankoop van financiële diensten betreft, en je werd niet ingelicht over het feit dat er al dan niet een herroepingsrecht bestaat, kan je de overeenkomst opzeggen per aangetekende en gemotiveerde brief, binnen een redelijke termijn vanaf het tijdstip waarop je kennis had of kennis had moeten hebben van het niet naleven van deze informatieplicht.

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

In principe beschik je over een herroepingstermijn van minimum **14 kalenderdagen**. Dat betekent dat je de verkoper vóór het verstrijken van die termijn moet verwittigen dat je de bedoeling hebt de overeenkomst op te zeggen.

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 goed of van een dienst betreft:

- voor goederen 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 draalt om de overeenkomst uit te voeren en je aan de overeenkomst wil verzaken om een bestelling te plaatsen bij een andere verkoper);
- voor goederen 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 (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 herroepingstermijn 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 herroepingstermijn mag echter met **drie maanden** worden verlengd vanaf de dag na de levering van het goed of na het sluiten van de dienstverleningsovereenkomst. In die gevallen, indien de ontbrekende informatie je vervolgens werd meegedeeld, binnen de termijn van 3 maanden, begint de gewone termijn van 14 kalenderdagen opnieuw te lopen. Je kan dan enkel binnen de **7 kalenderdagen** aan de overeenkomst verzaken, vanaf de dag na ontvangst van deze ontbrekende informatie.

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

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

Ja. Als je je herroepingsrecht doet gelden, moet de verkoper je de gestorte bedragen kosteloos terugbetalen. Die terugbetaling moet ten laatste binnen 30 dagen na je herroeping gebeuren.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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

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

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

In twee gevallen moet je zelfs geen terugzendingskosten betalen:

- indien het geleverde goed of de verleende dienst niet beantwoordt aan de beschrijving van het aanbod;
- indien de onderneming haar verplichting van informatie vóór of na het sluiten van de overeenkomst niet nakwam (zie nrs. 157 en 159).

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

Ja, je mag aan een op afstand gesloten overeenkomst verzaken, zelfs indien je een lening aanging om de betaling van de prijs van het goed 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 verstrekker van het goed of de dienst 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 goederen of diensten te zorgen.

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

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

De wet schrijft voor dat je de herroeping van je contract moet meedelen op een of andere duurzame drager waarover de verkoper beschikt en die toegankelijk voor hem is. Je kunt dus om het even welk middel gebruiken om de verkoper mee te delen dat je aan de overeenkomst verzaakt : via gewone brief, fax of e-mail, of voor alle veiligheid, via aangetekende zending.

Daar de herroeping 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 de herroeping van je overeenkomst mee te delen. Weet dat de certificatiedienstverleners tegenwoordig diensten voor elektronische aangetekende brieven aanbieden.

185. Welke zijn mijn verplichtingen als ik de overeenkomst herroep?

Wanneer je beslist aan de overeenkomst te verzaken, moet je dit gewoon meedelen aan de verkoper en hem het geleverde goed terugsturen (de verkoper kan je ook goederen leveren ter uitvoering van een dienstverleningsovereenkomst).

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

- het geleverde goed of de verleende dienst niet overeenstemt met de beschrijving van het aanbod;
- de onderneming haar informatieplicht niet nakwam voor of na het sluiten van de overeenkomst.

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

Indien je je herroepingsrecht uitoefent, moet de verkoper je een reeds betaalde prijs of voorschot terugbetalen. Die terugbetaling moet worden uitgevoerd binnen 30 dagen na de herroeping. Van die terugbetaling mogen geen kosten worden afgehouden.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Hoofdstuk VI. Betaling

187. Ben ik verplicht te betalen bij de levering?

Ja, als de verkoper je daartoe verplicht, wat hij volgens de wet kan. Je beschikt echter wel – behoudens uitzondering - over een herroepingsrecht van minstens 14 kalenderdagen, vanaf de dag na de dag waarop het goed werd geleverd of het dienstverleningscontract werd gesloten. Als je je herroepingsrecht uitoefent, moet je alle bedragen die je zou hebben gestort binnen 30 dagen terugbetaald krijgen.

188. 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.

In de hierna volgende vragen 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.

189. Kan ik met een kredietkaart betalen?

Natuurlijk, dat is het meest praktische en meest verspreide onlinebetaalmiddel. Als je de bestelbon invult, moet je de onderneming meestal het nummer en de vervaldatum van je kredietkaart meedelen. Bij ontvangst van je bestelling neemt de onderneming 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 meestal 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. De uitgevers van kredietkaarten hebben echter doeltreffende technische methodes uitgewerkt om onlinebetalingen te beveiligen. 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.

190. 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: het nulrisico bestaat niet, noch op netwerken, noch in de echte wereld.

Het eerste probleem met kredietkaartbetalingen is dat het nummer en de vervaldatum van je kaart vaak 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. Zelf zou je een aantal voorzorgsmaatregelen moeten respecteren om je te beschermen tegen *phishing*. Dit type van oplichterij heeft immers vaak als doel je je bankgegevens te ontfutselen.

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. 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. 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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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.

191. 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.

Deze beveiligingsvoorzieningen evolueren voortdurend en zijn zeer verschillend. Ze worden toegepast door de onlinehandelaar zelf, die zijn toevlucht neemt tot een systeem dat wordt aangeboden door een leverancier van een beveiligde betaaloplossing. De meeste van deze betaalsystemen beschermen de gegevens door ze te coderen bij de overdracht ervan op de netwerken. Voor een grotere beveiliging wordt de betaling en/of de identificatie eventueel niet op de website van de onderneming uitgevoerd, maar tevens op een beveiligd platform, dat wordt beheerd door de leverancier van de betaaloplossing of door een bankinstelling.

Visa en MasterCard hebben zelf hun eigen beveiligingsmechanisme voor onlinebetalingen ontwikkeld, dat overal ter wereld wordt erkend: "Verified by Visa en MasterCard SecureCode ". Enkel de onlinehandelaars die officieel zijn erkend door Visa et MasterCard kunnen gebruik maken van deze mechanismen. Daarvoor moeten ze beantwoorden aan een groot aantal vereisten die betrekking hebben op hun onlinebetalingsbeleid en op de specifieke technologie de moet worden gebruikt. In aansluiting hierop hebben bepaalde banken hulpmiddelen ontwikkeld die de online-identificatie van hun klanten mogelijk maken als ze hun kredietkaart gebruiken via deze betaaloplossingen. Ga bij je bank te rade voor meer informatie.

192. 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 annulering aanvragen van een betaling die werd uitgevoerd ten gevolge van bedrieglijke praktijken. 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 op het vlak van de bescherming van overgedragen bankgegevens werd de jongste jaren flink wat technische vooruitgang geboekt onder impuls van de uitgevers van kredietkaarten.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

193. 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. Na een snel onderzoek betaalt hij je de onrechtmatig geïnde bedragen zo spoedig mogelijk terug.

194. 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 draalt om je bestelling uit te voeren, hoef je niet te panikeren! Neem eerst contact op met hem om uitleg te vragen.

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 toe te sturen. Bij ontvangst van je betwisting neemt de uitgever van je kredietkaart zelf contact op met de verkoper om hem uitleg te vragen.

195. Mag ik met mijn debetkaart van Bancontact / Mister Cash betalen?

Een groeiend aantal Belgische websites hebben er samen met Banksys voor gezorgd dat je nu met je Bancontact/Mister Cash-kaart kan betalen.

Alle banken die deelnemen aan dit betaalsysteem hebben hun eigen aan de kaart verbonden onlinebeveiligings- en identificatievoorzieningen opgezet en passen de voorzieningen geregeld aan de evolutie van de technologieën aan. In een groot aantal gevallen zijn de voorzieningen verbonden aan *home banking*. Vergewis je er bij je bank van dat ze ook bij dit onlinebetaalsysteem is aangesloten en vraag haar om de te volgen procedure om ervan te kunnen gebruikmaken.

Je kunt op de site van Banksys (www.banksys.be) tevens meer informatie vinden over de werking van dit systeem, alsook de banken en de e-commercesites die eraan deelnemen.

196. 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 overboeking gebeurt tijdens het bestelproces, zodat de onderneming de zekerheid heeft dat zij betaald wordt.

Om dat betaalsysteem te kunnen gebruiken, moet je computer uitgerust zijn met een *homebanking*systeem, dat je bank je kan leveren. Met om het even welke *homebanking*software kun je thuis overschrijvingen maken, op dezelfde manier als met de *selfbanking*toestellen. Je kunt echter niet met alle softwareprogramma's *rechtstreeks* een elektronische overschrijving maken *op een website.* Daartoe moet je bank je die dienst verschaffen.

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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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.

197. Hoe betaal ik met behulp van mijn telefoon?

Op bepaalde websites kan je kleine aankopen vereffenen (download van muziek, beltonen, spelletjes, informatie enz.) door middel van de telefoon. Het volstaat een telefoonnummer te bellen (van het type 09xx) dat op het scherm wordt weergegeven en de instructies te volgen om een toegangscode te verkrijgen. Je moet dan enkel de code invoeren op de website om je aankoop te betalen. Er bestaat een analoog betaalsysteem per sms met toeslag. In werkelijkheid wordt een deel van het bedrag dat je voor de communicatie met toeslag aan je gsm-operator betaalt, doorgestort aan de onlinehandelaar. In alle gevallen moet de kost van de communicatie worden aangegeven op de website.

198. Hoe doe ik online aankopen met een voorafbetaalde kaart?

De voorafbetaalde internetkaart doet intussen zijn intrede, in het bijzonder voor kleine aankopen, zoals het betaald downloaden van muziek of gsm-beltonen. De werking ervan is vergelijkbaar met de voorafbetaalde kaart voor gsm's. Het gaat om een kaart (tastbaar of virtueel) die online (bv. met je kredietkaart), per telefoon of in bepaalde winkels kan worden gekocht en waaraan een unieke code is verbonden. Dit type kaart vertegenwoordigt een zekere waarde (vaak tussen vijf en vijftig euro).

Je kunt deze kaart alleen gebruiken op de websites die deze vorm van betaling aannemen. Het volstaat om op het moment van de betaling de code op de kaart in te voeren en het bedrag van je aankopen wordt afgetrokken van de waarde van je kaart. Het voordeel van deze kaart is dat er geen bankgegevens aan te pas komen.

199. Kan ik met een bankoverschrijving betalen?

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. Weet dat je, als je vooraf wenst te betalen, over een herroepingsrecht beschikt.

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). Vergeet niet het referentienummer van de bestelling duidelijk te vermelden. Ook in dit geval beschik je over een herroepingsrecht.

Die formule is trouwens niet voordelig voor grensoverschrijdende aankopen, gezien de hoge bankkosten die soms gepaard gaan met internationale overschrijvingen.

200. Kan ik bij de levering betalen?

Sommige verkopers geven je de mogelijkheid het goed 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.

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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Hoofdstuk VII. Levering van het goed of dienstverlening

201. 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. Anderzijds kan ook de verkoper een kortere termijn voorstellen, waartoe hij zich verbindt.

202. Wat moet ik doen wanneer de verkoper draalt 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 goed tijdelijk niet voorradig. Ofwel is het goed bij de verzending zoekgeraakt; daarvoor is de verkoper dan volledig verantwoordelijk.

Indien de verkoper na de wettelijke termijn van 30 dagen (of de met jou afgesproken termijn) je bestelling nog niet uitgevoerd heeft, heb je het recht om de ontbinding van de overeenkomst te vragen. 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. 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 herroepingsrecht uitoefenen, nog vóór de levering van het goed of binnen 14 kalenderdagen na het sluiten van de dienstverleningsovereenkomst.

203. Wordt de overeenkomst online of offline gesloten?

Indien de bestelling betrekking heeft op een goed of een immateriële dienst (software, video of film op verzoek, raadpleging van een informatiedienst...), kan die onmiddellijk online worden uitgevoerd (bijvoorbeeld het downloaden van software).

Indien de bestelling een materieel goed betreft (boek, kledingstuk, elektrisch huishoudapparaat...) of een dienst die bestaat in de levering van een goed (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.

204. Moet ik betalen als het product zoek raakt of tijdens het transport beschadigd raakt?

Neen. Het sturen van goederen of van stukken die diensten vertegenwoordigen gebeurt steeds op risico van de verkoper.

Bijgevolg kan van jou geen betaling geëist worden indien het goed niet aankomt. Indien je reeds de volledige prijs of een voorschot betaald hebt, moeten die bedragen worden terugbetaald.

Indien het goed in slechte staat toekomt, moet de verkoper daarvan de gevolgen dragen. In de praktijk mag je het goed houden en aan de verkoper een prijsvermindering vragen. Je mag het goed ook terugsturen naar de verkoper, die je een nieuw product in perfecte staat moet leveren. Controleer indien mogelijk de staat van het goed bij levering, in aanwezigheid van de leverancier, om elke betwisting te vermijden.

205. Wat moet ik doen indien het geleverde goed niet beantwoordt aan de beschrijving op de site?

Je mag de overeenkomst opzeggen binnen 14 kalenderdagen vanaf de dag na de leveringsdag en het niet-conforme goed naar de verkoper terugsturen. In dat geval zijn de verzendkosten ten laste van de verkoper.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

206. 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 goederen.

Het betreft de volgende gegevens:

- identiteit en geografisch adres van de onderneming;
- prijs van het goed 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 herroepingsrecht 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 herroepingsrecht hebt): "De consument heeft het recht aan de onderneming mee te delen dat hij van de aankoop afziet, zonder een boete te betalen en zonder een reden op te geven, gedurende... kalenderdagen (ten minste 14 dagen) vanaf de dag die volgt op de levering van het goed of op het sluiten van de dienstverleningsovereenkomst";
- (indien je geen herroepingsrecht 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, bij de bevestiging van de bestelling), moet ze je bij de levering niet meer worden verstrekt.

207. 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 14 kalenderdagen om aan de verkoper mee te delen dat je de overeenkomst opzegt.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Hoofdstuk VIII. Terugbetaling en Klantenservice

208. 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 herroepingsrecht;
- als de overeenkomst niet uitgevoerd werd.

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.

209. 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 *bpost* 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.

210. 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 herroeping plaatsvinden.

Wordt de overeenkomst niet uitgevoerd binnen 30 dagen na verzending van je bestelling, dan heb je het recht om de ontbinding van je overeenkomst te vragen 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.

211. Geldt er voor de goederen en diensten die ik op het internet koop een waarborg of klantenservice?

Ja, je aankopen worden gedekt door een waarborg en eventueel ook door klantenservice, zowel in traditionele winkels als op het web.

Vaak geldt op het gekochte goed een commerciële waarborg die de onderneming geeft gedurende een door haar bepaalde termijn. De onderneming 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 en uiterlijk bij levering. Dat soort waarborg is heel praktisch, aangezien je zo het defecte goed kunt laten vervangen of herstellen zonder tussenkomst van een rechtbank.

Naast deze commerciële waarborgen die door de onderneming worden geboden, voorziet het Burgerlijk Wetboek een wettelijke waarborg tegen verborgen gebreken, die van toepassing is op alle verkopen, of het nu gaat om professionelen of om privépersonen.

Een andere wettelijke waarborg is tevens van toepassing op de aankoop van consumptiegoederen tussen een onderneming en een consument, in het geval dat het goed niet aan het contract zou voldoen.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Voor zover het toepassen van deze waarborgen relatief complex is raden we je aan om de hulp van een specialist in te roepen om je ervan te vergewissen dat je aan de voorwaarden voldoet om ervan te kunnen gebruikmaken. Je vindt ook talrijke informatie op de site http://economie.fgov.be/protection_consumer/warranty/home_nl.htm.

Wat de dienst naverkoop betreft, moet worden gepreciserd dat de wet sinds december 2006 duidelijk verbiedt, dat de onderneming telefonische oproepen (over)factureert (in het kader van een "hotline" bijvoorbeeld) waarvoor de consument de inhoud van het bericht moet betalen, bovenop het oproeptarief, wanneer die oproepen betrekking hebben op de uitvoering van een reeds gesloten verkoopovereenkomst.

Let wel, als je geen klant bent en informatie vraagt over een goed, dan wordt dat niet beschouwd als een naverkoopdienst, en is het mogelijk dat de oproep wordt gefactureerd tegen een hoger tarief dan het klassieke.

Hoofdstuk IX. Minderjarigen en e-commerce

Er zijn steeds meer kinderen en tieners, die zich bijzonder vlot op het internet bewegen, die online verschillende goederen en diensten kopen (software, spelletjes, muziek, gsm-beltonen enz.), soms zelfs zonder medeweten van hun ouders. Het gebeurt ook dat een jongere via platforms als eBay goederen te koop aanbiedt op het internet. Op het moment dat de bedragen aanzienlijk worden of het goed ongeschikt is, zouden de ouders in bepaalde gevallen de door het kind gesloten overeenkomst willen kunnen verbreken. Hierna zien we of dit mogelijk is of niet.

212. Kan mijn kind zelf geldige aankopen doen op het internet?

In principe kan een kind of adolescent jonger dan achttien jaar zelf geen overeenkomsten afsluiten. Op dit principe zijn er echter een aantal uitzonderingen die door de wet of door hoven en rechtbanken zijn ontwikkeld.

Er bestaan een aantal stappen die een minderjarige op een geldige manier alleen kan uitvoeren. In het bijzonder kan een kind normaal gezien enkel kleine aankopen doen (boeken, snoep, spelletjes, magazines enz.). Daarnaast hebben bepaalde rechters "in de echte wereld" al de geldigheid van gewichtigere aankoopovereenkomsten die betrekking hadden op gewone consumptiegoederen (een hifiketen, een tweedehandsmotorfiets, meubelen, een reisje met vrienden enz.) erkend. Ze hielden hierbij wel rekening met de leeftijd en de financiële situatie van de minderjarige. Als de rechter echter acht dat de aankoop te gewichtig is of niet beantwoordt aan de vereisten, zal hij de aankoop ongeldig verklaren.

We kunnen ons dus afvragen of bepaalde rechters in de toekomst niet geneigd zullen zijn om op dezelfde manier de geldigheid van bepaalde overeenkomsten die door minderjarigen op het internet werden afgesloten, te erkennen. Toch zou de overeenkomst hier ook misschien moeten overeenkomen met de persoonlijke situatie van de minderjarige, met zijn leeftijd en zijn financiële situatie. Zo zou een zestienjarige in principe meer autonomie moeten hebben dan een kind van twaalf jaar. Over deze betrekkelijk recente kwestie werd door de hoven en rechtbanken nog geen duidelijke beslissing genomen en er bestaat nog relatief veel twijfel in dit opzicht.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

213. Kan ik onlineaankopen van mijn kind annuleren?

Alles hangt af van de aankoop een de persoonlijke situatie van de minderjarige. Minderjarig zijn op zich houdt niet in dat de overeenkomst automatisch nietig is. Daarvoor moet je naar de rechter stappen en aantonen aan de rechter dat de overeenkomst schadelijk is voor je kind.

Meerdere factoren zullen door de rechter in overweging worden genomen. Natuurlijk kan een te hoge prijs ten opzichte van het goed of de geleverde dienst worden beschouwd als schadelijk als zodanig. Maar de wet houdt ook rekening met de persoonlijke situatie van je kind. Zo kan een overeenkomst die op het eerste gezicht correct is, worden geannuleerd als het als ongepast wordt beschouwd met betrekking tot het goed of de geleverde dienst (nutteloos product, luxeproduct, aankoop van te grote omvang zoals een auto enz.), zijn financiële situatie of de maturiteit van het kind.

Deze principes gelden niet alleen voor een afzonderlijke aankoop, maar tevens in een hypothese waarbij je kind tal van aankopen heeft gedaan die door de opeenstapeling ervan leiden tot buitensporige of nutteloze uitgaven of aankopen. Als je erin slaagt om aan te tonen dat het geheel van de operaties nadelig is voor je kind, is het in dit geval mogelijk om te verzoeken dat alle overeenkomsten nietig worden verklaard, zelfs als ze bij verschillende dienstverleners werden afgesloten.

214. Kan een onderneming eisen dat een overeenkomst die mijn kind heeft afgesloten nietig wordt verklaard omwille van zijn minderjarigheid?

Nee. Enkel de minderjarige, de ouders of zijn voogd kan volgens de voorwaarden hierboven verzoeken om een overeenkomst nietig te verklaren. De onderneming kan de minderjarigheid van de koper niet aangrijpen om terug te komen op de overeenkomst als die eenmaal is afgesloten.

215. Kan de onderneming bij annulering van een overeenkomst een schadevergoeding eisen van de ouders?

Hij kan proberen om een schadevergoeding te krijgen door een rechtsvordering in te stellen, maar hij zal moeten bewijzen dat hij daadwerkelijk schade heeft geleden en dat het kind een fout heeft begaan. De normale gevolgen van de annulering van een overeenkomst zullen niet worden beschouwd als voldoende bewijs van schade. De onderneming zou echt bijkomstig onrecht moeten hebben ondergaan, bijvoorbeeld als je zijn reputatie schaadt.

216. En als mijn kind heeft gelogen door zich uit te geven voor een volwassene?

Het feit dat het kind gewoon heeft gelogen over zijn leeftijd door een valse geboortedatum op te geven op de bestelbon, verhindert niet dat de overeenkomst kan worden geannuleerd. Je kind zou echt kunstgrepen en oneerlijke verhullingen moeten hebben gebruikt met de bedoeling om de handelaar te misleiden, bijvoorbeeld door wederrechtelijk gebruik te maken van de creditcard van een volwassene en door de eventuele technische middelen om de leeftijd van de klant te controleren, te omzeilen.

Een valse geboortedatum opgeven in een bestelbon kan niettemin wel strafrechtelijke gevolgen hebben. Bepaalde dienstverleners deinzen er immers niet voor terug om bij de ouders te dreigen dat ze tegen hun kind gerechtelijke vervolgingen zullen instellen voor valsheid in informatica of informaticabedrog. Om tot een strafrechtelijke veroordeling te komen, moeten echter alle elementen om van een strafbaar feit te kunnen spreken, aanwezig zijn en met name moet de frauduleuze intentie van het kind of zijn eventuele intentie om te schaden, worden aangetoond. Opdat er sprake zou zijn van computerfraude, moeten we bovendien herhalen dat de fraudeur de bedoeling moet hebben om er onwettig economisch voordeel uit te halen, wat zal afhangen van het goed of de dienst die op een frauduleuze manier werd verkregen. We merken nog op dat een minderjarige in geen enkele geval tot een gevangenisstraf of boete kan worden veroordeeld, maar dat de wet op de jeugdbescherming voorziet in specifieke sancties, aangepast aan de leeftijd en de ernst van het misdrijf. Het feit dat uw minderjarige kind daadwerkelijk een strafrechtelijk misdrijf heeft gepleegd, zou echter tot de betaling van schadevergoeding en interesten kunnen leiden, zelfs als het dossier wordt geseponeerd of wordt afgesloten met een eenvoudige berisping van de rechter, op voorwaarde dat de onderneming kan aantonen dat zij door de leugen van uw kind schade heeft geleden. Tracht uw kind in elk geval verantwoordelijkheidsgevoel bij te brengen door het te informeren over de gevolgen van dergelijke leugens.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Anderzijds moeten de handelaars eveneens voor hun verantwoordelijkheden worden geplaatst. Als ze geen overeenkomsten willen sluiten met minderjarigen, of als ze goederen of diensten aanbieden die verboden zijn onder de achttien jaar, behoren zij ook voorzieningen te treffen om de leeftijd van hun klanten te kunnen controleren. In dat opzicht kunnen we ons afvragen of de gewone vermelding "Je moet achttien jaar zijn om een bestelling te kunnen plaatsen" of "Deze site is verboden onder de achttien jaar" volstaat.

217. Kan ik het herroepingsrecht van mijn kind inroepen om terug te komen op onlineaankopen?

Ja, als de aankoop van je kind de voorwaarden om van dit recht te kunnen gebruikmaken, verenigt: de herroepingstermijn mag nog niet zijn verstreken en het goed of de dienst mag geen deel uitmaken van de uitzonderingen die door de wet zijn voorzien.

218. Kan ik me verzetten tegen betalingen die mijn kind heeft gedaan met mijn kredietkaart?

Nee. Als je kind zonder je medeweten gebruikmaakt van je kredietkaart, is het niet mogelijk om de betaling te betwisten onder op grond van het feit dat je daarvoor je toestemming niet hebt gegeven want je bent verantwoordelijk voor de daden van je kind. Als je je kind de toelating geeft om gebruik te maken van je kredietkaart, of als je slordig omgaat met je kaart, moet je des te meer de uitgaven aanvaarden.

Je kunt de gestorte sommen echter eventueel terugkrijgen via het herroepingsrecht, of een rechtsvordering om de overeenkomst te annuleren, als je aan de voorwaarden voldoet om hiervan gebruik te maken.

219. Hoe kan ik de aankopen van mijn kind op het internet in goede banen leiden?

Het is van belang om op een preventieve manier met je kind te spreken, regels te stellen en zijn aandacht te vestigen op een aantal punten om het kind verantwoordelijkheidsbesef bij te brengen. Bepaalde websites, zoals www.saferinternet.be of www.oplichters.be kunnen je hierbij helpen.

Bovendien kunnen er aan de hand van het gebruikte betaalmiddel op voorhand een aantal voorzorgsmaatregelen worden genomen. De banken bieden de mogelijkheid om een maximumbedrag vast te leggen dat de minderjarige met zijn debetkaart per week of per maand kan uitgeven. Voor de betalingen per telefoon, kan je eveneens je operator contacteren om de gesprekken naar telefoonnummers met een toeslag te blokkeren.

220. Ik heb op het web een goed gekocht dat door een minderjarige te koop werd aangeboden. Kunnen zijn ouders de overeenkomst annuleren?

Ja, als het verkoopscontract nadelig is voor de minderjarige, ofwel wegens een te lage prijs, ofwel wegens zijn gebrek aan maturiteit of wegens het bijzonder nuttige of belangrijke karakter van het goed voor de minderjarige. De voorwaarden die hierboven werden uiteengezet zijn van toepassing.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Hoofdstuk X. Veilingen en handel tussen privépersonen

221. Kan je je kost verdienen door voorwerpen te verkopen op het internet?

Er bestaat een groot aantal sites waar iedereen diverse goederen en diensten kan verkopen, via opbod of voor een vaste prijs. eBay is een bekend voorbeeld. Bepaalde mensen slagen er zelfs in om aanzienlijke verdiensten te halen uit de handel die ze drijven op dit soort platform.

Maar, let op! Als wordt beschouwd dat deze handel een commercieel karakter heeft, zal dat gevolgen hebben op het sociale en fiscale vlak: je zult een ondernemingsnummer en een btw-nummer moeten aanvragen, sociale lasten moeten betalen en de verdiensten uit je activiteit moeten aangeven bij de belastingdienst. Bovendien ben je als je beroepsmatig handel drijft op het internet onderhevig aan een reeks verplichtingen wat de verstrekking van informatie betreft.

De grens tussen commerciële activiteit en strikt private activiteit is niet duidelijk. Bovendien moet het commerciële karakter van een activiteit geval per geval worden beoordeeld. Bij wijze van voorbeeld kan het feit dat je voorwerpen koopt om opnieuw te verkopen met winst, of het feit dat je voorwerpen verkoopt die je zelf vervaardigt of verwerkt (bijvoorbeeld een artiest die zijn werken verkoopt), worden beschouwd als een commerciële activiteit. Daarentegen is het feit dat je persoonlijke voorwerpen verkoopt, zelfs als dat min of meer geregeld gebeurt of kort nadat ze werden verworven, in principe geen activiteit met commercieel karakter maar valt dit eerder onder beheer van privébezit.

222. Kan je alles verkopen en aankopen op het internet?

Nee. Eerst en vooral zijn bepaalde goederen, zoals namaakgoederen of gestolen goederen onwettig. Dergelijke goederen verkopen of aankopen is een strafrechtelijk misdrijf. Vervolgens is het leveren van bepaalde goederen (alcohol, tabak, medicijnen, wapens enz.) of diensten (bank, verzekeringen, georganiseerde reizen, huwelijksbemiddeling enz.) gereglementeerd. Zorg er dus voor dat je er goed over geïnformeerd bent of je het recht hebt om dergelijke goederen of diensten te verkopen of aan te kopen.

223. Welke regels zijn van toepassing op de veilingen en de handel tussen privépersonen op het internet?

Alle verkopen zijn onderworpen aan de traditionele regels van het Burgerlijk Wetboek, of ze nu op het internet of elders plaatsvinden en van welke vorm ze ook zijn (per opbod of met een vaste prijs), onafhankelijk van de website waar de handel wordt gedreven (persoonlijke website, platform of sociale netwerken), of de hoedanigheid van de partijen in het verkoopscontract (beroepsmatig of consument). In alle gevallen moeten beloften worden nagekomen en eerlijk en te goeder trouw worden gehandeld. Weet ook dat de koper onder bepaalde voorwaarden geniet van een vordering tot vrijwaring tegen de verkoper.

Bovendien zijn de personen die zich als een onderneming gedragen onderworpen aan een reeks regels met betrekking tot het verstrekken van informatie en moeten ze aan de koper-consument herroepingsrecht toekennen en een aantal regels betreffende de levering, de betaling en de terugbetaling respecteren.

Ten slotte beschikken de meeste sociale netwerk- of veilingplatforms tevens over een reglement dat door alle gebruikers, koper of onderneming, moet worden gerespecteerd. Elke inbreuk op het reglement houdt meestal in dat het account waarmee op het platform verkopen of aankopen kunnen worden gedaan, wordt verwijderd.

224. Kan ik me tot de verantwoordelijke van de site wenden als de verkoop slecht afloopt?

Aarzel niet om de verantwoordelijke van de site te contacteren als je tijdens de verkoop of aankoop een probleem ondervindt met een gebruiker van de site. Als je het slachtoffer bent geworden van zwendel, zal de verantwoordelijke van de site verplicht zijn om mee te werken met de autoriteiten om ze de schuldige te helpen vinden. Bovendien zullen ze de nodige maatregelen nemen zodat deze gebruiker geen gebruik meer kan maken van hun dienst en andere gebruikers kan benadelen.

De rol van de siteverantwoordelijken stopt soms hier. Bepaalde dienstverleners beschouwen zich immers soms als derde ten opzichte van de op hun platform gesloten overeenkomsten, in die mate dat ze genoegen nemen met het in verbinding stellen van ondernemingen en potentiële kopers, zonder tussen te komen in het sluiten of het uit-

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

voeren van de overeenkomst. In dat geval zijn ze in principe niet verantwoordelijk voor de slechte uitvoering van een overeenkomst en zijn ze niet verplicht de sommen terug te betalen die je afhandig werden gemaakt, of voor jou het goed dat nooit werd betaald, te recupereren.

Andere dienstverleners mengen zich meer in de verkopen op hun platform, doordat ze zich als vertegenwoordiger van de onderneming beschouwen. Soms ontvangt dit soort dienstverlener in de hoedanigheid van een vertrouwensderde de betalingen voor rekening van de onderneming. Als de koper ontevreden is, kan hij zich dus rechtstreeks tot de dienstverlener wenden die dan onder bepaalde voorwaarden kan overgaan tot terugbetaling.

Op bepaalde platforms kunnen de Belgische partijen zich voortaan identificeren aan de hand van hun elektronische identiteitskaart. Dat biedt in geval van betwisting zekerheid over het bestaan en de identiteit van de partijen, en in het bijzonder van de onderneming.

Hoofdstuk VIII. Gedragscodes en labeling

225. 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 "privéregulering" 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 hypertekstlink die naar deze gedragscode verwijzen. De site kan de code ook opnemen in zijn algemene voorwaarden.

226. Kan ik vertrouwen hebben in een gedragscode?

In het digitale landschap worden gedragscodes gekenmerkt door een grote verscheidenheid, zowel wat de auteurs betreft als over inhoud en doelpubliek. Een webstek met een gedragscode is niet noodzakelijk meer betrouwbaar dan een andere.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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...

227. 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 onderneming op haar 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.

228. 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 aanging.

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".

229. 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.

Deel 6.
Regeling geschillen op internet

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

230. Wat te doen bij geschillen?

Op het internet doen zich gemakkelijk en regelmatig conflictsituaties voor van allerlei aard: een slechte uitvoering van een onlinebestelling, lasterlijke en aanstootgevende berichten, pesten, schending van de privacy, schending van het auteursrecht enz.

Of je nu het slachtoffer bent van deze problemen of als je ze net zelf hebt veroorzaakt, er moet zonder enige twijfel in de eerste plaats met de rechtstreeks betrokken personen worden overlegd om tot een oplossing te proberen komen.

Zo nodig kan je je wenden tot een eventuele bemiddelaar die evenzeer bij het probleem is betrokken, zoals de hoster van de omstreden site, de moderator van het forum waarin de misplaatste uitlatingen werden gebruikt, de provider van de blogservice of van het netwerkplatform waarop de ongeoorloofde inhoud werd gepost, of de internetprovider waarlangs de illegale bestanden werden gedownload. Wees er echter van bewust dat een dergelijke bemiddelaar geen geschillen moet oplossen, noch vervolgingen moet instellen en dat hij misschien niet tot een oplossing kan komen. Het kan echter wel bevorderlijk zijn om hem op de hoogte te brengen van je geschil, zodat hij contact kan opnemen met de tegenpartij.

Als een schikking onmogelijk blijkt of als de tegenpartij niet reageert, kan je een organisatie voor consumentenbescherming of andere autoriteiten (zie in het bijzonder de site www.ecops.be) inlichten over je geschil.

Je kunt er ook voor kiezen om het geschil voor het gerecht te brengen, waarbij je natuurlijk de hulp moet inroepen van een advocaat. Als je liever niet naar de rechter stapt, kan je overgaan tot alternatieve manieren van geschillenregeling zoals arbitrage, bemiddeling of verzoening.

231. Wat te doen bij geschillen met een persoon of een bedrijf in het buitenland?

Het is mogelijk dat je op het internet een conflict krijgt met een persoon of een bedrijf in het buitenland. Om enkel voorbeelden van online afgesloten overeenkomsten te noemen, het is bijzonder gemakkelijk om een bestelling te plaatsen op een website bij een onderneming die in Groot-Brittannië is gevestigd. Als je in geval van een geschil een rechtsvordering wilt instellen, wie is dan de bevoegde rechter: de Belgische of de Britse rechter? En welke wetgeving zal hij toepassen om het conflict op te lossen: de Belgische of de Britse?

Om deze vragen te beantwoorden kan je je beroepen op de regels van het internationaal privaatrecht. Elk land heeft logischerwijs zijn eigen regels om de bevoegde rechtbanken en de wetten die van toepassing zijn, aan te duiden, maar er bestaan ook uniforme regels op Europees en internationaal vlak. Bovendien verschillen de wetten die van toepassing zijn naargelang je ageert als consument of als beroeps en naargelang de aard van het geschil en in het geval van een overeenkomst, zelfs volgens de aard van de overeenkomst. Vergeet ten slotte niet dat als een gerechtelijke beslissing wordt uitgesproken in België, deze nog moet kunnen worden uitgevoerd in het land van de tegenpartij.

Gezien de complexiteit van de zaak en van de criteria waarmee moet worden rekening gehouden, raden we je aan om de hulp van een deskundige in te roepen als je een rechtsvordering wilt instellen.

232. 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. Dat noemen we ODR (Online Dispute Resolution).

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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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. In het geval van een bemiddeling, laten de partijen zich bijstaan door een derde bemiddelaar om tot een oplossing te komen die voor hen beiden het beste uitkomt. Een verzoening wordt over het algemeen voorzien in het kader van een gerechtelijke procedure (vaak als poging tot een minnelijke schikking voorafgaand aan een dergelijke procedure) en daarbij komt een conciliator tussenbeide die naar de partijen luistert en hen een voorstel doet voor de regeling van het geschil, in tegenstelling tot de bemiddelaar.

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.

233. 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 BELMED : onlineplatform voor consumentengeschillenbemiddeling : http://economie.fgov.be/nl/geschillen/Consumentengeschillen/Belmed/).

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.

234. Wat zijn de voordelen van ADR?

Vrijheid: als het geschil grensoverschrijdend is, kun je via ADR de klassieke problemen over rechtsbevoegdheid en toepasselijke wet omzeilen. 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 uitsluitsel 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.

235. 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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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.

Sinds enkele jaren omkadert de wet de bemiddelingsprocedures door meerdere principes in te voeren waaraan het bemiddelingsproces zal worden onderworpen. De wet biedt de partijen met name de mogelijkheid om door een rechter akte te laten nemen van hun akkoord om het verbindend te maken (d.w.z. de bemiddeling de waarde geven van een vonnis).

Bovendien kan de bemiddeling die plaatsheeft in het kader dat door de wet werd bepaald, niet gebeuren zonder de voogdij van een bemiddelaar die werd goedgekeurd door de federale bemiddelingscommissie, wat in het bijzonder de bevoegdheid en de onafhankelijkheid van de aangeduide bemiddelaar waarborgt.

Ten slotte onderstrepen we het bestaan van het EEC-Net (*European Consumer Centers networ*k), waarvan de site kan worden bezocht op het volgende adres: http://ec.europa.eu/consumers/redress_cons/index_en.htm en dat de Europese consumenten voorstelt te helpen bij het oplossen van hun geschillen, de verwerking van hun klachten of het opzoeken van informatie over hun rechten.

De site van het EEC-Net vermeldt een lijst van centra die in de verschillende lidstaten een ADR-procedure aanbieden (de lijst kan worden gevonden op het adres http://ec.europa.eu/consumers/redress_cons/adr_en.htm).

Tussen deze centra, willen we de Ombudsdienst voor telecommunicatie (www.ombudsmantelecom.be) vermelden, dat bevoegd is voor de hele telecomsector en die wordt gevraagd om tussen te komen als de gebruiker ontevreden is over de contacten met zijn telecomaanbieder.

Naast deze dienst willen we tevens de Geschillencommissie Reizen, of ook nog de Bemiddelingsdienst Banken-Krediet-Beleggingen vermelden, die elk tussenbeide komen bij geschillen die betrekking hebben op hun specifieke activiteitensector.

236. 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 clausule 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 clausule kan worden bepaald vóór het ontstaan van het conflict. Die geschillenregelingsprocedures zijn namelijk minder dwingend.

237. 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. Een bemiddeling of verzoening sluit immers de mogelijkheid om naar de rechtbank te stappen niet uit.

De partijen kunnen in het kader van de door de wet georganiseerde en hierboven vermelde bemiddelingen aan de rechter vragen om het overeengekomen onderlinge akkoord goed te keuren om er de waarde van een vonnis aan te geven. In dat geval kunnen de partijen geen beroep meer doen op een rechter om hun geschil op te lossen, aangezien hun akkoord de waarde heeft van een rechterlijke beslissing.

Je kunt 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.

Glossarium

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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 webvertentie

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

Blog

Een blog is een gezellige en interactieve website die door een internaut (de blogger) wordt onderhouden die er inhoud op levert onder de vorm van berichten die hij geregeld plaatst, waarop internauten kunnen reageren door er hun commentaar aan toe te voegen. Een blog wordt vaak vergeleken met een dagboek.

bps

Zie bit per seconde

brandmuur

Zie firewall

Browser (navigator)

Software waarmee de internetgebruiker informatie op het internet kan zoeken en raadplegen. De meest bekende zijn Firefox en Internet Explorer.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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 certificatiedienstverleners.

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 privéleven 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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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 handtekening

Een elektronische handtekening is een geheel van computergegevens, vastgehecht aan of logisch geassocieerd met andere elektronische gegevens, die worden gebruikt als authentificatiemiddel.

Een dergelijke handtekening kan worden gebruikt om de ondertekenaar(s) van een rechtshandeling die via elektronische weg werd uitgevoerd, te identificeren. Wettelijk gezien kan ze niet worden geweigerd op het stuk van haar juridische doeltreffendheid of haar ontvankelijkheid als gerechtelijk bewijsmiddel. Niettemin wordt ze slechts erkend als equivalent van de handgeschreven handtekening als ze beantwoordt aan een aantal technische veiligheidscriteria; in dat geval, zeggen we dat de elektronische handtekening is gekwalificeerd.

Geavanceerde elektronische handtekening

De geavanceerde elektronische handtekening is een geheel van computergegevens, vastgehecht aan of logisch geassocieerd met andere elektronische gegevens, die worden gebruikt als authentificatiemiddel en aan de volgende eisen voldoet:

a) zij 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.

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

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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

hackertools

Technische of softwarematige hulpmiddelen die hacking vereenvoudigen.

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.

herroepingsrecht

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.

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

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

hotline

Zie helpdesk

Hotspot

Wi-Fi-toegangspunt waarmee computers en terminals in de zone die door een Wi-Fi-hotspot wordt gedekt een draadloze verbinding kunnen maken. Deze zone is vaak een drukbezochte plaats, zoals een station, een luchthaven, een restaurant, een hotel of een café.

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.

I

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)

Strafbare handeling waarbij een persoon wordt bestraft die zichzelf of iemand anders met bedrieglijke opzet een onwettig economisch voordeel wil verschaffen door in een computersysteem gegevens in te voeren, te wijzigen of gegevens te wissen die worden opgeslagen, verwerkt of overgedragen door een computersysteem, of door met behulp van alle mogelijke technische middelen het normale gebruik van gegevens in een computersysteem wijzigen.

Informaticabedrog kan bijvoorbeeld het gebruik zijn van een gestolen kredietkaart om geld te halen uit een bankautomaat, de onwettige overschrijding van het krediet verbonden aan je eigen kredietkaart, de verandering van programma's of computerbestanden om 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 rechtscollege 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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

internetprovider

Zie Internet Service Provider

internetter

Internetgebruiker.

Internet Service Provider (ISP, internetprovider)

Organisatie die particulieren en ondernemingen toegang biedt tot het internet.

intranet

Privénetwerk 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 **mo**dulator/**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.).

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

moderator

Persoon die verantwoordelijk is voor het beheer van een discussieforum of een mailing-lijst. Hij filtert de door de leden verzonden berichten en verwijdert 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 op het vlak van goederen of diensten gesloten tussen een onderneming en een consument in het kader van een door de onderneming 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 2, 21° van de wet op de marktpraktijken).

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.

Peer-to-peer

"*Peer to peer*" ("gelijke naar gelijke" in het Nederlands), vaak afgekort als "p2p", verwijst naar een netwerk dat is opgebouwd uit een aantal computers die op een gegeven moment met elkaar in wisselwerking staan. De wisselwerking tussen de computers is gebaseerd op het delen van informatie die vaak de vorm heeft van muziekbestanden, maar ook van multimediastreaming zoals films (*streaming*).

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.

Phishing

Fraudetechniek die wordt gebruikt door derden met slechte bedoelingen om persoonlijke gegevens van de internauten los te krijgen (zoals bankgegevens, toegangscodes enz.).

PIN

Personal Identification Number. Persoonlijke geheime code.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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

Browservenster dat boven elk hoofdvenster wordt geopend. Talrijke sites nemen reclame op in dergelijke vensters.

portaal

Internetsite van waaruit de gebruiker zijn opzoekingen 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.

RSS-feed

Met een RSS-feed (*Really Simple Syndication*) kan je aan het publiek de wijzigingen van een site meedelen die geregeld evolueert, zoals een blog. Personen die zijn geïnteresseerd in de dienst in kwestie kunnen snel op de hoogte worden gebracht van wijzigingen want ze kunnen zich "abonneren" op de RSS-feed.

S

Gegevenssabotage

Strafbare handeling waarbij een persoon wordt bestraft als hij, zich bewust van het feit dat hij er niet toe is gemachtigd, rechtstreeks of onrechtstreeks gegevens in een computersysteem invoert, gegevens wijzigt of wist, of met eender welke technische middelen het normale gebruik van gegevens in een computersysteem wijzigt.

De wet heeft betrekking op computersabotage, bijvoorbeeld schadelijke handelingen zoals het binnenbrengen van een virus, de vernietiging van een computerbestand of het onklaar maken van een harde schijf of een computersysteem.

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.

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.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Sociaal virtueel netwerk

Een sociaal virtueel netwerk verwijst naar een groep entiteiten (individuen of organisaties) die virtueel in wisselwerking met elkaar samenwerken door middel van het internet, om een groep vrienden, een professionele kring of een sociale organisatie van commerciële, gevoelsmatige enz. ontmoetingen te vormen.

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.

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, decomprimeert 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 transmissie-controle) 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 op het vlak van 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

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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.

virus

Een virus is in de strikte zin van het woord een programma dat de werking van informaticasystemen verstoort of erger nog, de daarin opgeslagen gegevens wijzigt, vervalst, ja zelfs vernietigt. Het woord "virus" in de ruime zin slaat op elke vorm van kwaadwillig bedoeld programma (*malware*) zoals met name virussen in de strikte zin, *spyware* en Trojaanse paarden.

W

web

Verkorte naam voor *World Wide Web*. Zie aldaar.

Web 2.0

Web 2.0 verwijst naar de tweede generatie van onlinediensten die de samenwerking en het delen van informatie tussen internauten willen vereenvoudigen.

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.

Wi-Fi

Wi-Fi is een draadloze communicatietechnologie waarmee tegen een hoge snelheid via een bepaalde frequentie kan worden gecommuniceerd tussen computers en andere terminals die met elkaar zijn verbonden, draadloos of zonder kabel.

Wiki

Een wiki is een inhoudbeheersysteem voor websites waarvan de pagina's vrij en gemakkelijk kunnen worden gewijzigd door elke bevoegde bezoeker. De wiki's zijn opgevat om kennis gemakkelijker te kunnen verdelen en om de redactie van documenten in samenwerking te vereenvoudigen.

WiMax

WiMAX is een draadloze communicatietechnologie via hertzgolven met hoge verbindingssnelheid. Het bereik ervan is hoger dan dat van Wi-Fi, aangezien het verscheidene kilometers ver reikt.

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

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

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 hypertekstdocumenten 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

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Nuttige teksten

Bescherming van de consument

- Wet van 6 april 2010 betreffende marktpraktijken en consumentenbescherming, B.S..12 april 2010.

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.
- Collectieve arbeidsovereenkomst nr. 81 van 26 april 2002, gesloten in de Nationale Arbeidsraad, tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische on-linecommunicatiegegevens.
- Collectieve arbeidsovereenkomst nr. 85 van 9 november 2005 betreffende het telewerk, BS van 5 september 2006.

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.
- Wet van 26 juni 2003 met betrekking tot het wederrechtelijk registreren van domeinnamen, BS van 9 september 2003.

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 certificatiediensten, 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.
- Wet van 15 mei 2007 die een juridisch kader vastlegt voor sommige verleners van vertrouwensdiensten, BS van 17 juli 2007.
- Koninklijk arrest van 4 april 2003 die het versturen van reclame via e-mail moet reglementeren, BS van 25 mei 2003.

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.
- Wet van 16 juli 2004 gesteund op het Wetboek van internationaal privaatrecht, BS van 27 juli 2004.

Elektronische Communicaties

- Wet van 13 juni 2005 betreffende de elektronische communicatie, BS van 20 juni 2005.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Nuttige adressen

- Website van de Federale Overheidsdienst Economie, KMO, Middenstand en Energie:

  http://economie.fgov.be

- Algemene Directie Controle en Bemiddeling: om een klacht in te dienen:

  http://economie.fgov.be/nl/geschillen/klachten/waar_hoe_klacht_indienen/index.jsp

- BELMED : onlineplatform voor consumentengeschillenbemiddeling :

  http://economie.fgov.be/nl/geschillen/Consumentengeschillen/Belmed/

- Belgisch Centrum voor Arbitrage en Mediatie:

  http://www.cepani.be

- Website van de Federale Overheidsdienst Informatie- en Communicatietechnologie (FEDICT):

  http://www.fedict.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

- e-w@llonie.net:

  http://www.e-wallonie.net/

- 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

- Meldpunt van de gerechtelijke politie: om illegale informatie op het internet aan te geven

  E-mail: contact@gpj.be

- Meldpunt van de Belgische overheid voor internetmisbruiken:

  www.ecops.be

- De Belgische portaalsite in de strijd tegen spam:

  www.spamsquad.be

- Ombudsdienst voor Telecommunicatie:

  http://www.ombudsmantelecom.be/

- Child Focus:

  Tel.: 116 000

  www.childfocus-net-alert.be

- Website van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer:

  http://www.privacycommission.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

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

- Test-Aankoop:

  http://www.test-aankoop.be/

- Onderzoeks- en Informatiecentrum van de Verbruikersorganisaties (OIVO):

  http://www.OIVO.be

- Gezinsbond:

  http://www.gezinsbond.be

- Informatiewebsite tegen oplichters (ontwikkeld door de OIVO):

  http://www.consumentenbedrog.be/

- De veiligheid van minderjarigen online (ontwikkeld door Child Focus en de OIVO):

  http://www.saferinternet.be

- Robinsonlijst van de Belgische Direct Marketing Verbond:

  http://www.robinsonlist.be

economie
FOD Economie, K.M.O., Middenstand en Energie

Vooruitgangstraat 50
1210 Brussel
Ondernemingsnr.: 0314.595.348
http://economie.fgov.be