Spyware

Juridisch bestrijden of praktisch oplossen?

Sandra H.O. Schaapherder
Begeleid door mevr. mr. A.M. Klingenberg

Scriptie

Spyware

Juridisch bestrijden of praktisch oplossen?

Sandra H.O. Schaapherder
Studentnummer 1217046

Begeleid door mevr. mr. A.M. Klingenberg
Rijksuniversiteit Groningen, Faculteit der Rechtsgeleerdheid

Groningen 26 augustus 2005

Inhoudsopgave

Inleiding

"Poing, geachte gebruiker, zojuist is spyware deze computer binnengedrongen. Spyware kan informatie die zich op deze computer bevindt, informatie die u invoert of informatie die door middel van deze computer wordt opgevraagd, doorgeven aan derden. Dit kan grote gevaren met zich meebrengen. Klik op OK om de spyware te verwijderen."

Eén klik later is het probleem opgelost, de spyware verdwenen en zijn alle gevaren geweken.

Helaas laat het probleem spyware zich in werkelijkheid niet zo makkelijk oplossen. Besturingssystemen en/of computerprogramma's geven geen "poing" en geen melding wanneer spyware de computer van de gebruiker binnenkomt. Laat staan dat spyware met één muisklik kan worden verwijderd. Oplossingen, voorzover mogelijk, zowel juridische als praktische, zijn veel ingewikkelder dan een simpele muisklik.

Spyware is één van de plagen die tegenwoordig het internet teistert en vooral veel problemen oplevert voor de internetgebruikers. Steeds vaker lijkt men te beseffen dat spyware een probleem kan vormen. De kranten, tijdschriften, internetbronnen; via al deze media wordt de consument en computergebruiker in toenemende mate gewezen op de gevaren van spyware. Inmiddels zijn er zelfs kamervragen gesteld over spyware. Oftewel, de maatschappelijke onrust rond spyware is begonnen en neemt toe.

Spyware wordt doorgaans beschouwd als kwalijk en alles dat als kwalijk wordt beschouwd, wordt door mensen bestreden. Wat is de juiste wijze van bestrijden van spyware? Moet er een praktische oplossing worden gezocht voor de problemen die spyware met zich mee brengt of ligt de oplossing op juridisch gebied, bijvoorbeeld in wet- en regelgeving? Dat is de hoofdvraag van deze scriptie; *"Spyware, juridisch bestrijden of praktisch oplossen?"*

Om deze hoofdvraag te kunnen beantwoorden zal ik deze eerst opdelen in onderdelen en al deze onderdelen in hoofdstukken behandelen.

Allereerst zal ik behandelen wat volgens mij onder het begrip spyware valt. Daarna zullen de technische oplossingen aan bod komen. Vervolgens zal ik in gaan op de privacywetgeving met betrekking tot spyware van dit moment. In het volgende hoofdstuk zal de overige huidige wetgeving die men in het kader van spyware kan hanteren aan bod komen (computercriminaliteit en oneerlijke mededinging). Dan volgt een hoofdstuk over de toekomstige wetgeving, althans de initiatieven daartoe. Vervolgens zullen, alvorens ik zelf tot een conclusie kom, een aantal experts aan het woord komen over spyware en de daaraan gerelateerde onderwerpen en problemen.

Hoofdstuk 1: Spyware

Voor we naar eventuele oplossingen gaan kijken is het goed om vast te stellen wat spyware is. De media spreken geregeld over spyware, maar wat is nu echt spyware en wat niet?

1.1 Definitie spyware

Allereerst is het belangrijk vast te stellen dat spyware deel uit maakt van een veel groter probleem, namelijk malware. Hoepman definieerde malware als volgt: "Malware is alle software die zonder expliciete toestemming van de gebruiker op de computer van de gebruiker wordt geïnstalleerd, die tot doel heeft de functie van de computer in het nadeel van de gebruiker en/of in het voordeel van de maker te veranderen."[1] Ik kan me goed in deze definitie vinden en wat betreft malware zal ik zijn definitie dan ook aanhouden.

Er bestaat op dit moment niet één duidelijke (juridische) definitie van spyware. Aangezien spyware een redelijk nieuw onderwerp is, is er op het gebied van spyware weinig juridische literatuur. De aandacht van IT-juristen is tot op heden vooral uitgegaan naar Peer2Peer (KaZaA), SPAM, de status van software et cetera. Eén van de weinige juridische auteurs die zich wel aan een definitie van spyware heeft gewaagd, is Kleve. Hij omschrijft spyware als: "Software die wordt "meegeïnstalleerd" met andere software, met de bedoeling informatie te verkrijgen in verband met het gebruik van die andere software."[2]

De media geven spyware inmiddels veel aandacht, regelmatig verschijnen artikelen over spyware in kranten, (consumenten- of computer)tijdschriften[3] en (consumenten)programma's op TV.[4] In de media worden vaak veel verschillende definities gegeven van spyware. In de meeste gevallen gaat het dan om een veelomvattende, zeer brede definitie voor spyware. Over het algemeen rekent men in de media onder spyware alle software(onderdelen) en tools die de computer van de gebruiker vertragen en vervuilen met allerlei ongewilde software(onderdelen), zonder daarbij te kijken naar wat deze software(onderdelen) daadwerkelijk doen.
Internetbronnen besteden ook veel aandacht aan spyware, voornamelijk vanuit het oogpunt van voorkomen en genezen. Ook op internet circuleren veel verschillende definities van spyware. Deze definities zijn wat mij betreft vaak nauwkeuriger dan de definities die in de media worden gegeven. De meeste internetbronnen duiden spyware als software die informatie verzamelt over de gebruiker en deze doorspeelt. Maar ook deze definities zijn vaak niet compleet.

Allereerst wil ik kort de bovenstaande definitie van Kleve bespreken. Deze definitie luidt: "Software die wordt "meegeïnstalleerd" met andere software, met de bedoeling informatie te verkrijgen in verband met het gebruik van die andere software."[5] De definitie lijkt mij wat aan de magere kant. Volgens mij is spyware een breder begrip dan de definitie van Kleve. Hij geeft aan dat spyware wordt gebruikt om informatie te verkrijgen die wordt gebruikt in verband met de software waar de

---

[1] Gesprek met J.H. Hoepman op 14 juli 2005.
[2] Kleve 2004, p. 291.
[3] *Spyware onuitroeibaar* 2005, p. 30 en *Spyware* 2005, p. 22-23.
[4] 'TROS Radar', TROS Nederland 2, 25 oktober 2004.
[5] Kleve 2004, p. 291.

spyware bij werd meegeïnstalleerd. Spyware kan echter voor meerdere doeleinden worden gebruikt dan slechts om samen te werken met de software waarmee de spyware werd meegeïnstalleerd.[6] Tevens geeft Kleve aan dat spyware op de computer van de gebruiker komt bij het installeren van software, als een ongewenst bijproduct. Dit is zeker mogelijk, maar spyware kan ook op andere manieren op de computer van gebruikers komen, niet alleen bij het installeren van software.[7]

Strikt genomen is mijns inziens niet alle software, die (door de media) als spyware wordt aangeduid, spyware en wordt spyware in veel gevallen te breed en onnauwkeurig gedefinieerd. De reden voor deze ruime omschrijving zou kunnen liggen in het feit dat de term spyware voornamelijk wordt gebruikt in een niet-juridische context, maar in de context van het verwijderen van ongewenste "rommel en overlast" van de computer. Die "rommel en overlast" wordt dan voor het gemak spyware genoemd, daar waar malware bijvoorbeeld wellicht een betere benaming zou zijn geweest. Bij het beschrijven van spyware in die context is het niet noodzakelijk om nauwkeurig af te bakenen wat wel en wat geen spyware is.

Een voorbeeld hiervan kan men vinden bij anti-spywareprogramma's. Deze zelfbenoemde anti-spywareprogramma's verwijderen niet alleen dat wat volgens mij "echte" spyware is, maar ook adware, browser-hijackers en andere vervelende software(onderdelen) en tools.[8] Overigens is dat ook logisch, de consument is niet gebaat bij een systeem dat slechts de spyware verwijdert en andere hinderlijke software(onderdelen) laat zitten, maar wel de juiste definitie van spyware hanteert.[9] In dit licht zou het in de open source wereld gebezigde "anti-intrusion" wellicht een betere naam voor deze systemen zijn, daar het in veel gevallen gaat om programma's die de gebruiker proberen te beschermen tegen alle vormen van indringing via de computer. Dit zou verwarring rond de definitie van spyware kunnen voorkomen.

Ook ziet men bij het definiëren van spyware, dat het *doel* waarvoor spyware wordt gebruikt veelvuldig in de definitie wordt vermeld. Bij vermelding van het doel van spyware gaat men vaak louter uit van commerciële doelen. Uiteraard is dit in de meeste gevallen ook sprake van een commercieel doel, dit zal ook het belangrijkste gevaar opleveren voor gebruikers. Echter niet in alle gevallen is sprake van een commercieel doel, dat maakt dat de definitie met vermelding van één of meerdere doeleinden onvolledig is. De vermelding van het doel waarvoor spyware wordt ingezet lijkt mij in dit geval ook overbodig. Verklaring voor de vermelding van die doeleinden in veel huidige definities is dat spyware vaak wordt omschreven vanuit een voorlichtingsfunctie. Voor de voorlichting aan bijvoorbeeld consumenten is het belangrijker de gevaren van spyware te duiden, dan een juridisch sluitende omschrijving van spyware geven die consumenten wellicht te ingewikkeld vinden.

Uit het bovenstaande blijkt dat spyware zich moeilijk laat definiëren. In het kader van deze scriptie is het echter wel belangrijk vast te stellen wat ik onder spyware versta, derhalve waag ik me toch aan het definiëren van spyware. Onder spyware versta ik het volgende:

---

[6] Zie 1.2.
[7] Zie 1.5.
[8] Zie 1.3.2.
[9] *Spyware onuitroeibaar* 2005, p. 30.

Spyware zijn computerprogramma's (software) die zich zonder toestemming van de gebruiker in de computer van de gebruiker verschuilen en die informatie zonder toestemming van deze gebruiker, van zijn/haar computer verzamelen en deze zonder toestemming van de gebruiker doorgeven aan anderen of zelf gebruiken.

Spyware kan op vele verschillende manieren op de computer van de gebruiker komen, derhalve blijft de wijze waarop de spyware binnenkomt in deze omschrijving onvermeld, mede met het oog op de toekomst.

Ik heb er bewust voor gekozen om "en zonder medeweten (van de gebruiker)" niet te vermelden daar waar wel (tweemaal) "zonder toestemming" is vermeld. Wanneer er geen sprake is van medeweten, is er ook geen toestemming verleend en vallen de gevallen "zonder medeweten" sowieso onder de gevallen "zonder toestemming". "of zonder medeweten (van de gebruiker)" Leek mij ook om die reden geen zinnige aanvulling. Onder toestemming versta ik overigens, net als Alberdingk Thijm[10], "Een vrije, specifieke, en op basis van volledige informatie berustende wilsuiting".

1.2 Spyware en haar functies

Wat doet spyware nu eigenlijk precies? Als we bovenstaande definitie bekijken kunnen we dat wat spyware doet als volgt samenvatten: "Spyware verzamelt gegevens en speelt deze door." Om te kijken hoe spyware functioneert kijken we eerst naar de verschillende soorten spyware. Daarna zal kort worden ingegaan op de gegevens die spyware verzamelt. De wijze van functioneren en de gegevens die spyware verzamelt, zullen uiteindelijk afhangen van het doel dat de spyware nastreeft.

1.2.1 Welke soorten spyware zijn er?

Verschillende soorten spyware hebben verschillende functies, daarom worden hier kort de bekendste soorten spyware behandeld. De soort spyware die gebruikt wordt hangt nauw samen met het doel dat de verspreider van de spyware uiteindelijk wil bereiken.

Keylogger (of keystroke logger)

Een keylogger is een programma dat alle toetsenbordaanslagen registreert en doorspeelt. Een keylogger wordt bijvoorbeeld gebruikt om inlognamen en wachtwoorden te achterhalen.

Dataminers

Dataminers zijn programma's die gegevens over de gebruiker van een computer verzamelen door de gebruiker op het internet te volgen. Dit is de meest voorkomende soort spyware. Dataminers worden vaak in één adem genoemd met (tracking) cookies, maar zijn dit niet, cookies volgen de gebruiker niet over het hele internet, maar zijn over het algemeen gerelateerd aan één bepaalde locatie op het internet. Bovendien zijn cookies geen software en zijn dataminers dit wel. Dataminers en (tracking) cookies kunnen wel samenwerken.

[10] Gesprek met C. Alberdink Thijm op 17 augustus 2005

1.2.2 Welke gegevens verzamelt spyware?

Welke gegevens spyware verzamelt, hangt zeer nauw samen met het doel waarvoor spyware wordt ingezet. In de meeste gevallen zal spyware worden ingezet om uiteindelijk financieel gewin op te leveren voor de producenten van spyware en hun "klanten" en zal de spyware erop gericht zijn om alleen die gegevens te verzamelen die voor dat doel belangrijk zijn en zal bijvoorbeeld privé-correspondentie buiten schot blijven. Spyware kan echter *alle* gegevens achterhalen die op de computer van de gebruiker staan, die worden ingevoerd of worden opgevraagd door middel van de computer.

Soms verwerken en gebruiken de bedrijven van wie de spyware afkomstig is zelf de gegevens. Maar in veel gevallen wordt de informatie doorverkocht aan derden die deze informatie gebruiken om bijvoorbeeld gericht reclame te maken. Spammers vinden deze informatie uitermate interessant. Het gaat dan bijvoorbeeld om e-mailadressen of gegevens over het (online)koopgedrag van gebruikers. Of bepaalde gegevens zoals inlognamen, wachtwoorden en ip-adressen persoonsgegevens zijn blijft een punt van discussie. Wat mij betreft hangt dat van de omstandigheden van het geval af en kunnen daarover geen eenduidige uitspraken worden gedaan. Alberdingk Thijm geeft aan dat hij e-mailadressen wel als persoonsgegevens beschouwt omdat men indirect (door tussenkomst internetprovider) identificeerbaar is.[11] SPAM is overigens in Nederland wettelijk geregeld.[12]

Niet alle gegevens die spyware verzamelt zijn persoonsgegevens, maar veel gegevens zullen dit wel zijn vanwege hun herleidbaarheid.[13] Voor het verzamelen en verwerken van persoonsgegevens geldt specifieke regelgeving in verband met de privacy van de persoon van wie deze gegevens afkomstig zijn. De Nederlandse wetgeving met betrekking tot persoonsgegevens kan men vinden in de Wet bescherming persoonsgegevens. Volgens die wet is een persoonsgegeven: "Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon". Hierop zal in hoofdstuk 3 worden ingegaan.[14]

1.3 Wat is geen spyware?

Spyware is niet het enige gevaar dat loert op het internet. Hier volgt een korte behandeling van menselijk handelen, software(onderdelen) en bestanden die vaak worden verward met spyware, het gevolg kunnen zijn van spyware en/of dezelfde gevolgen of vergelijkbare gevolgen kunnen hebben als spyware.

1.3.1 Menselijk handelen

Er zijn twee belangrijke dingen die onder menselijk handelen vallen die dezelfde (kwalijke) gevolgen kunnen hebben als spyware. Het gaat dan om phishing en hacking. Aangezien menselijk handelen niet onder software(onderdelen) valt, gaat het mijns inziens niet om spyware.

Hacking

Hacking houdt in dat personen door middel van (sofware)tools en/of social engineering (sociaal smeerwerk; je voordoen als iemand anders, hier is de lijn tussen

---

[11] Alberdingk Thijm 2004, p. 57.
[12] Art. 11.7 Telecommunicatiewet (Tw).
[13] Gesprek met J.H. Hoepman op 14 juli 2005.
[14] Zie hoofdstuk 3.

hacking en phishing heel dun) wachtwoorden en andere gegevens achterhalen. Sommige hackers zullen deze gegevens ook gebruiken om de computer van de gebruiker te frustreren of andere (financiële) schade aan te richten in het (digitale) leven van de gebruiker.

Phishing

Phishing is het "vissen" naar gegevens van gebruikers door mensen die bijvoorbeeld een valse identiteit aannemen. Een bekend voorbeeld is een e-mail sturen naar een gebruiker met de mededeling dat men van de bank van de gebruiker is en dat men wil controleren of de gegevens correct in de bankbestanden zijn, met de vraag of de gebruiker ter controle al zijn creditcardgegevens terugmailt. Ook phishing kan zeer ernstige gevolgen hebben. Phishing gebeurt over het algemeen door middel van e-mail.[15] In sommige gevallen wordt in de e-mail een hyperlink geplaatst naar een nepsite waar de gegevens moeten worden ingevoerd.

Een bijzondere vorm van phishing vindt plaats wanneer de site van bijvoorbeeld een bank wordt "gekaapt" en de bezoekers van de echte site van de bank automatisch worden doorgestuurd naar een nepsite die lijkt op de echte site, zonder deze ooit te zien. Dit is mogelijk door zwakheden in de Domain Name System Software en men spreekt dan van pharming.[16] Wanneer men de gebruiker zijn gegevens door mededelingen op deze nepsite ontfutselt is er sprake van phishing door middel van pharming.

1.3.2 Software(onderdelen) en bestanden

Zoals al eerder gesteld trekt men in de media de omschrijving van spyware vaak erg breed. De volgende software(onderdelen) en/of bestanden worden ook vaak onder spyware gerekend. Ze zullen kort omschreven worden en tevens zal ik aangeven waarom deze onderdelen en/of bestanden volgens mij geen spyware zijn en waarom en op welke wijze zij wel verbonden zijn met spyware. De software(onderdelen) die hieronder worden beschreven vallen wel onder de definitie die Hoepman van malware geeft.[17]

Cookie

Een cookie is een klein bestandje dat bij een bezoek aan een internetpagina door deze pagina wordt achtergelaten op de computer van de gebruiker om per bezoeker een surfgeschiedenis bij te houden teneinde de gebruiker beter en sneller te bedienen. Cookies zorgen dat het internet sneller en beter kan functioneren en vallen niet onder mijn definitie van spyware, omdat cookies geen software zijn.

Tracking cookies

Tracking cookies dienen niet onder spyware te worden gerekend. Over het algemeen worden cookies achtergelaten om het bezoek aan deze site de volgende maal te vergemakkelijken, dit kan omdat zij informatie over het vorige bezoek hebben opgeslagen en doorspelen (de surfgeschiedenis). Tegenwoordig bestaan er echter ook cookies die verder gaan dan dit en informatie doorspelen die geenszins nodig is om een bezoek aan de site waar het cookie vandaan komt de

---

[15] XS4ALL (Wat is phishing?)
XS4ALL, *Wat is phishing?* WWW <http://www.xs4all.nl/veiligheid/phishing/> (geraadpleegd 12 mei 2005)
[16] *Phishing & pharming 2005,* p. 23.
[17] Gesprek met J.H. Hoepman op 14 juli 2005.

volgende keer makkelijker en sneller te maken.[18] Die cookies bestaan alleen om informatie door te geven, zodat de verzamelaar meer weet over de gebruiker van de computer/bezoeker van zijn site. Tracking cookies zijn echter net als cookies geen software en ze passen daarom niet in mijn definitie van spyware.

Adware

Een programma dat er, zonder de toestemming van de gebruiker, voor zorgt dat de gebruiker allerlei reclameboodschappen krijgt voorgeschoteld in de vorm van hinderlijke pop-ups wanneer de gebruiker zich op het internet begeeft. Adware zelf speelt geen informatie door.

Strikt gezien is adware geen spyware, het kan wel samenhangen met spyware. De spyware verzamelt specifieke informatie over de gebruiker (bijvoorbeeld zijn over zijn surfgedrag) en de adware wordt daarop aangepast zodat er gericht reclame kan worden gemaakt.

Browser hijacker

Browser hijackers, die vaak in één adem genoemd worden met spyware, voegen extra favorieten toe aan je internet-favorieten, voegen allerlei icoontjes toe op je bureaublad en vaak worden allerlei toolbars aan je internetbrowser of besturingssysteem toegevoegd. Een bekend voorbeeld is het zeer moeilijk te verwijderen Cool Web Search, dat meekomt bij het gratis programma MSN Messenger Plus. Overigens heeft de gebruiker in het geval van MSN Messenger Plus wel toestemming voor de installatie van Cool Web Search gegeven en is er geen sprake van een illegale toepassing. Nu moet wel gezegd worden dat de gebruiker die vaak onoplettend doorklikt op internet teneinde een gratis programma (zoals MSN Messenger Plus) te bemachtigen, vaak voorbijgaat aan algemene voorwaarden en licentieovereenkomsten, door eenvoudigweg snel door te klikken. Hierdoor zal een gebruiker wanneer hij/zij niet erg oplettend is toch snel aan ongewenste browser hijackers komen, alhoewel hij/zij daarmee wel zelf heeft ingestemd.

Browser hijackers vallen strikt genomen niet onder spyware aangezien zij geen informatie verzamelen en doorspelen, bovendien worden ze vaak met toestemming van de (ietwat onoplettende) gebruiker geplaatst. Browser hijackers worden in veel gevallen wel vergezeld van spyware.

Ongewenste toolbar/werkbalk

Zoals ik hierboven reeds vermeld heb is een ongewenste toolbar vaak onderdeel van een browser hijacker. Onder de toolbar van de internetbrowser van de gebruiker of boven de toolbar van het besturingssysteem nestelt zich een ongewenste toolbar, die moeilijk tot zeer moeilijk te verwijderen is. Vaak bevat deze toolbar snelkoppelingen naar commerciële websites.

De reden waarom deze toolbars geen spyware zijn in dezelfde als bij browser hijackers, ook de toolbar verzamelt zelf geen informatie en speelt dus ook geen informatie door.

---

[18] De Schrijver & Schraeyen 2005, p. 3-11.

Dialer

Een dialer is een tool die een modem, zonder dat de gebruiker hierom heeft gevraagd, opdracht geeft om te bellen met een duur (telefoon)nummer, vaak in het buitenland. Sommige websites werken legaal met dialers. Deze websites leggen de gebruiker vooraf de keuze voor om gebruik te maken van dialers. In die gevallen is er dus wel sprake van toestemming.[19] Legale dialers vindt men veel bij sites waar men moet betalen voor de tijd dat men de site bekijkt. Dialers kunnen alleen werken wanneer de gebruiker een analoog inbelmodem gebruikt.[20]

Ook dialers zijn strikt genomen geen spyware, zij speuren niet naar informatie over de gebruiker van de computer en spelen ook geen informatie door. Dialers kunnen wel een gevolg zijn van spyware, in die zin dat zij kunnen functioneren door de informatie die door middel van spyware is ingezameld.

Drive by download

Op sommige sites begint de browser van de gebruiker spontaan met het downloaden van bestanden. De drive by download is ook niet zozeer software als wel een spontane actie van de computer bij het bezoeken van bepaalde internetsites. De downloads die op deze wijze plaatsvinden zijn meestal gevaarlijke plug-ins voor de browser, maar kunnen werkelijk van alles zijn.

Strikt genomen is een drive by download geen spyware. Zoals al gezegd is een drive by download geen software(onderdeel). Er wordt niet gezocht naar informatie over de gebruiker, derhalve wordt er ook niets doorgegeven over die gebruiker. Drive by downloads kunnen echter wel een gevolg zijn van spyware die zich reeds op de computer van de gebruiker bevindt. Spyware heeft dan bijvoorbeeld informatie over de gebruiker verzameld die de drive by download nodig heeft om te kunnen functioneren. De meeste drive by downloads hebben informatie over de gebruiker niet nodig om te kunnen functioneren. Deze drive by downloads zullen spontaan gaan werken op het moment dat de gebruiker een bepaalde site bezoekt. Drive by downloads maken bijvoorbeeld gebruik van lekken in besturingssystemen en internetbrowsers.

Overigens kan de software die wordt geïnstalleerd door de drive by download wel spyware zijn, maar de actie die we drive by download noemen is zelf geen spyware, de drive by download is dan slechts de methode om de spyware op de computer te krijgen.

Virus/worm/trojan

Sommige spyware gaat zelfs vergezeld van een virus, worm of trojaans paard (ook wel trojan genoemd).

Het gaat hier volgens mij niet om spyware, wel kunnen virussen, wormen en trojans reisgenoten zijn van spyware en samenwerken met spyware. Bijvoorbeeld: met de informatie die via de spyware wordt aangetroffen in de computer van de gebruiker kan het virus, de worm, of de trojan schade aanrichten en op deze wijze samenwerken met spyware. Door De Schrijver en Schraeyen worden trojans als een variant van spyware gezien.[21] Dit lijkt me niet correct. Voor zover het virus, de worm

---

[19] *Spyware* 2005, p. 22-23.
[20] *Spyware* 2005, p. 22-23.
[21] De Schrijver & Schraeyen 2005, p. 3-11.

of de trojan niet verantwoordelijk is voor het verzamelen van gegevens en het doorsturen hiervan, beschouw ik deze als een vervelende reisgenoot van sommige spyware en niet als een (onderdeel van) spyware. Virussen, wormen en trojans vormen een heel ander, complex probleem of beter gezegd nog drie andere complexe problemen.

1.4 Het gevaar spyware

Zo langzamerhand begint het in onze gedigitaliseerde maatschappij door te dringen dat spyware een bedreiging vormt. De aandacht voor spyware neemt toe. De media; internetbronnen, (consumenten)tijdschriften, tv en kranten berichten steeds vaker over spyware. Spyware wordt veelvuldig omschreven als gevaarlijk tot zeer gevaarlijk. Waarom eigenlijk?

Zoals ik in mijn definitie van spyware heb aangegeven verzamelt spyware informatie die op de computer van de gebruiker staat, die in de computer wordt ingevoerd of via de computer wordt opgevraagd. Vaak staat er op computers vertrouwelijke informatie (bijvoorbeeld met betrekking tot het privé-leven van de gebruiker, (vertrouwelijke), informatie over het werk van de gebruiker, die wanneer deze informatie in de openbaarheid wordt gebracht, tot problematische situaties kan leiden.[22]

Spyware kan ook grote financiële schade aanrichten voor een gebruiker, omdat spyware ook wachtwoorden die men voor telebankieren gebruikt en creditcardnummers kan achterhalen. Kwaadwillenden kunnen deze nummers en wachtwoorden dan bijvoorbeeld gebruiken om de bankrekening van de gebruiker (van telebankieren) te plunderen. Door de gegevens die de spyware heeft verzameld is het mogelijk om de (digitale) identiteit van een ander aan te nemen.

Kortom in het ergste geval kan spyware, wanneer het de gegevens die het verzamelt doorspeelt aan kwaadwillenden, ervoor zorgen dat een gebruiker zijn baan kan verliezen, zijn privé-leven op straat komt te liggen en financieel aan de grond komt te zitten.

Het gevaar voor gebruikers is dus niet onaanzienlijk. Spyware vormt ook een gevaar voor de maatschappij in het algemeen, al is dit gevaar niet zo groot als bijvoorbeeld bij SPAM en virussen. SPAM en virussen hinderen het de internetcommunicatie op een directe manier, spyware doet dat niet.[23] Het "maatschappelijke gevaar" ligt vooral in de extra tijd en de extra kosten die het bestrijden van spyware met zich meebrengt. De maatschappij is tegenwoordig in verregaande mate gedigitaliseerd en als we de berichten in de media moeten geloven is een groot deel van de computers over de hele wereld met spyware geïnfecteerd. De schattingen lopen uiteen van één derde[24] tot negentig procent van de computers.[25] Uiteraard zijn deze schattingen moeilijk te controleren. Bovendien wordt vaak niet vermeld wat bij het maken van deze schattingen wel of niet tot spyware is gerekend. Vaak wordt

---

[22] Denk bijvoorbeeld aan alle informatie (zowel privé als werkgerelateerd) op de computer van Officier van Justitie Tonino.
[23] Gesprek met C. Alberdink Thijm op 17 augustus 2005
[24] Verhagen 2004
L. Verhagen, *Eén op de drie pc's besmet met spyware*, WWW <http://www.webwereld.nl/articles/12833>, publicatie 16 juni 2004
[25] De Schrijver & Schraeyen 2005, p. 3-11.

overigens betoogd dat spyware computers vertraagt en het internet vervuilt en dat door de gegevens te gebruiken die spyware verzamelt, spyware bijdraagt tot de verspreiding van SPAM. In hoeverre spyware daadwerkelijk computers vertraagt is onbekend. Er is ook veel spyware die dat zeker niet doet en ongemerkt op de computer van de gebruiker verblijft. Het vertragen en vervuilen van computers wordt in de media echter vaak aangehaald als één van de schadelijke bijwerking van spyware. Tevens is, met betrekking tot spyware in combinatie met SPAM, ook wel betoogd dat de gegevens die spyware verzamelt worden gebruikt om spyware gerichter te maken en zo de SPAM-overlast doen afnemen in plaats van toenemen.[26]

Wel kunnen we concluderen dat het verwijderen van zowel spyware als SPAM de maatschappij veel geld en tijd kost, al is spyware in vergelijking met SPAM meer een "gebruikersprobleem", dan een probleem dat de internetcommunicatie als geheel bedreigt. Extra lastig is dat spyware zich niet beperkt tot een probleem van één land, maar een internationaal, wereldwijd probleem is (net zoals de andere internetplagen zoals virusverspreiding en SPAM).

1.5 Hoe komen gebruikers aan spyware?

Spyware kan op diverse manieren de computer van de gebruiker binnenkomen, dit is in grote mate afhankelijk van de soort spyware en derhalve van het doel dat de spyware heeft.

In de definitie heb ik bewust niet de wijze behandeld waarop de spyware op de computer van de gebruiker komt, omdat de manieren waarop spyware de computer van de gebruiker binnen kan komen talrijk zijn. Het is niet altijd zo dat spyware stiekem binnenkomt, in sommige gevallen had de gebruiker van de spyware kunnen weten en heeft deze hier zelfs mee "ingestemd". Vaak zal de gebruiker echter niet weten dat hij/zij heeft ingestemd met spyware en is er wat mij betreft geen sprake van toestemming. Hieronder zal ik vijf methoden bespreken waardoor spyware op de computer van gebruikers terecht kan komen.

Drive by download

De drive by download is een actie die wordt ondernomen door de computer van de gebruiker bij het bezoek aan bepaalde websites. Dit kan de gebruiker overkomen door gewoon onschuldig surfen. De gebruiker komt op een bepaalde site en zijn/haar computer begint automatisch te downloaden. Het programma dat wordt gedownload kan spyware zijn.[27]

Freeware

In de meeste gevallen komt spyware mee met freeware. Freeware zijn gratis programma's die men op internet kan vinden. Erg aanlokkelijk voor gebruikers om te downloaden omdat ze gratis zijn. Een voorbeeld is hier bijvoorbeeld KaZaA, een populair mp3 uitwisselingsprogramma dat gratis is maar ook vol spyware zit.[28]
In sommige gevallen stemt de gebruiker zelfs in met de spyware, meestal zonder dit zelf te weten en te willen. Ergens in de algemene voorwaarden die men moet

---

[26] Gesprek met J.H. Hoepman op 14 juli 2005.
[27] Zie 1.3.2.
[28] Koelman 2002
K.J. Koelman, *noot bij Hof Amsterdam 28 maart 2002 (Kazaa/Buma),* WWW <http://www.ivir.nl/publicaties/koelman/noothofkazaa.html> (geraadpleegd 12 mei 2005)

accorderen alvorens de freeware te kunnen downloaden, wordt de spyware dan vermeld. De meeste gebruikers lezen de voorwaarden echter niet en klikken automatisch op "ja, ik stem in met algemene voorwaarden", hiermee hebben zij dan zonder het te weten ingestemd met de spyware. Wat mij betreft is in dit geval overigens geen sprake van toestemming.[29] De algemene voorwaarden waarmee wordt ingestemd zijn vaak erg ondoorzichtig en men weet dat gebruikers nauwelijks de moeite nemen om hiervan kennis te nemen, daarmee is wat mij betreft niet voldaan aan het vereiste van "op basis van volledige informatie". Gebruikers weten over het algemeen niet waar ze mee instemmen. De informatie over de software die eventueel wordt meegeïnstalleerd moet in mijn ogen duidelijker dan in een vage bepaling in de algemene voorwaarden worden vermeld.

Hiermee is overigens nog niets gezegd over de juridische correctheid van het plaatsen van software die informatie verzamelt en doorspeelt wanneer het duidelijk wordt vermeld in de algemene voorwaarden of op een andere wijze duidelijk wordt gemaakt aan de gebruiker dat software wordt geplaatst die informatie verzamelt en doorspeelt.

Onder vals voorwendselen/vermomd als iets anders

Soms downloaden gebruikers programma's die iets anders zijn dan ze beloven. Het meest extreme voorbeeld is in dit geval Spyware Nuker. Gebruikers die dit downloaden zijn in de veronderstelling een anti-spywareprogramma te downloaden. Het tegendeel is echter het geval, het gaat hier juist om spyware.

Met een virus, worm of trojan mee

Sommige spyware komt op de computer van de gebruiker omdat deze is "meegereisd" met een virus, worm of trojan.

Software?

Er wordt van sommige (besturings)programma's en internetbrowsers gesuggereerd dat ze spyware zouden bevatten. De spyware zou de maker van deze programma's dan informatie kan toespelen over die gebruikers. De (besturings)programma's waarvan dit wordt gesuggereerd zijn allemaal closed source software. Bij open source zou men de spyware zeer snel kunnen ontdekken, daar de broncode openbaar is. Het blijft echter bij suggesties want aangezien het closed software betreft, is de broncode niet bekend en kan er hieromtrent ook niets bewezen worden.[30] Over closed- en open software meer in hoofdstuk 2.[31]

---

[29] Zie 1.1.

[30] Het zou voor gebruikers te controleren zijn wanneer zij hun eigen netwerkverbinding "afluisteren" en zodoende kunnen zij ontdekken of er informatie wordt verstuurd die daarvoor niet bestemd is. Gesprek met J.H. Hoepman op 14 juli 2005. Overigens wordt dit weer lastig als het besturingssysteem zelf "fout" is en dit "afluisteren" saboteert. Gesprek met J.J. Dijkstra op 25 april 2005.

[31] Zie hoofdstuk 2.

Hoofdstuk 2: Technische oplossingen

2.1 Anti-spywareprogramma's/Intrusion detection

Spyware is een probleem en om dit probleem te bestrijden maken gebruikers vaak gebruik van anti-spywareprogramma's. Dit zijn computerprogramma's die spyware op de computer opsporen en deze spyware verwijderen en in sommige gevallen voorkomen zij dat spyware de computer binnenkomt. Intrusion detection is een term die in de open source wereld wordt gebruikt voor het voorkomen van ongewenste indringing in computers.

Er zijn veel verschillende soorten spyware, derhalve zijn er ook veel verschillende anti-spywareprogramma's. Een aantal van deze programma's kan men gratis downloaden op het internet. Voorbeelden zijn Spybot, Ad-aware en Hitman-pro. Men hoeft dus niet te betalen voor deze programma's. Vaak staat op de site waar de gebruiker een dergelijk programma kan downloaden wel een oproep aan deze gebruiker om geld te doneren. Het kost de makers namelijk wel veel tijd en moeite op de programma's up to date te houden. Verder is het ook vaak mogelijk een meer luxe versie van het programma te downloaden, bijvoorbeeld een versie die automatisch update en dan moet men voor die versie wel betalen.

Afbeelding 2.1 Screenshot Ad-Aware

Afbeelding 2.2 Screenshot Spybot

Spyware is big business. Makers van spyware krijgen goed betaald voor hun "product" en het levert informatie op die derden weer om kunnen zetten in winst. Maar ook met de bestrijding van spyware valt geld te verdienen. De makers van anti-virus pakketten hebben dat inmiddels ook ontdekt. De traditionele anti-virusreuzen zoals Norton en McAfee bieden tegenwoordig ook anti-viruspakketten met anti-spywaremodules aan.[32] Er bestaan ook losse anti-spywareprogramma's. De bekendste hiervan is wellicht Spy Sweeper, afkomstig van Webroot (ook bekend van diverse onderzoeken naar spyware). Tevens zijn er programma's zoals Hitman-pro die diverse programma's afkomstig van anderen combineren. van Norton en McAfee en programma's die meerdere anti-spywareprogramma's combineren. Er zijn ook anti-spywareprogramma's die zich specifiek op een soort spyware richten, zoals een spywareprogramma dat er op gericht is het zeer moeilijk te verwijderen Cool Web Search te elimineren. Ook Microsoft maakt tegenwoordig een anti-spyware programma.

[32] *Spyware onuitroeibaar* 2005, p. 30-33.

Er is geen overeenstemming over wat het beste programma is, hoewel het programma van Microsoft op de meeste functionaliteiten (voorkomen van spyware, verwijderen van spyware) goed scoorde in een test van de Consumentenbond. Een algemene uitkomst uit diezelfde test waarin dertien anti-spywareprogramma's werden getest was overigens dat veel programma's slecht zijn in het herkennen van spyware en nog slechter in het verwijderen van spyware. Vaak wordt geadviseerd om meerdere anti-spywareprogramma's naast elkaar te gebruiken. Anti-spywareprogramma's kan men zowel in closed als in open source vinden. De voordelen van een open source anti-spywareprogramma zullen in de paragraaf over open source worden besproken.

Onder intrusion detection zou men ook het controleren van eigen uitgaande communicatie en het beter beveiligen van netwerken kunnen rekenen. Het controleren van de uitgaande communicatie kan aantonen dat er meer informatie de computer verlaat dan door de gebruiker is beoogd. Dit duidt op een "ongewenste indringer" in de computer die deze informatie doorspeelt aan derden. Het beveiligen van netwerken kan leiden tot meldingen van "ongewenste indringers". "Ongewenste indringing" van computers wordt door deze maatregelen opgespoord en kan dan worden bestreden.

2.2 Open Source

Strikt gezien is open source geen technische oplossing. Open source software is namelijk software waarvan de broncode vrij beschikbaar is. Een ander belangrijk kenmerk van open source is dat met betrekking tot de intellectuele eigendom van de software en de broncode in het licentiemodel is geregeld dat de licentienemer de broncode mag inzien, gebruiken, verbeteren, aanvullen en distribueren.

Open source draagt bij aan de betrouwbaarheid en veiligheid van systemen omdat het de gebruiker in de gelegenheid stelt om de exacte werking na te kijken, zodat deze ook in zeer kritische omgevingen kan worden ingezet. Ook de duurzaamheid van software wordt groter. Omdat de broncode beschikbaar is, kan deze altijd worden aangepast zowel voor onderhoud als beheer, ook door andere leveranciers. Hierdoor worden innovatie en keuzevrijheid bevorderd en is men niet afhankelijk van één softwareleverancier.[33]

Bovenstaande kenmerken van open source zijn geen technische kenmerken. Door het gebruik van open source kan men wel voorkomen dat spyware binnenkomt of controleren of software spyware bevat, dit vloeit voort uit de mogelijkheden die open source biedt om een kijkje te nemen in de techniek van computerprogramma's en de mogelijkheden om deze eventueel technisch aan te passen vandaar dat open source toch in dit hoofdstuk wordt besproken.
De overheid stimuleert overigens het gebruik van open source binnen overheidsorganen en heeft daar zelfs een eigen programma voor OSOSS (Open Standaarden en Open Source Software) dat onderdeel is van ICTU, het ICT Uitvoeringsorgaan van de overheid.[34]

---

[33] Ososs 2005
Ososs, *FAQ*, WWW< http://www.ososs.nl> (geraadpleegd 12 mei 2005)
[34] Ososs
Ososs WWW <http://www.ososs.nl> (geraadpleegd 9 augustus 2005)

2.2.1 Open source in de strijd tegen spyware in closed source software

Er is een mogelijkheid dat grote closed source-softwaremakers spyware in hun software inbouwen, omdat zij informatie willen inwinnen over de gebruikers van hun software(pakketten) zodat zij deze nog beter op maat kunnen maken. Helaas is dit niet controleerbaar omdat de broncode die achter de software zit niet openbaar is.
Als gebruikers ervoor kiezen om met open source software te werken kunnen zij zelf controleren of er spyware in is gebouwd door de softwarefabrikant of zij kunnen dit laten controleren wanneer zij zelf niet deskundig genoeg zijn om spyware te detecteren. Mocht men in het geval van open source iets op het spoor komen dat de gebruiker niet zint, dan mag men het aanpassen of laten aanpassen. Open source-licenties geven de gebruiker die mogelijkheid, closed source biedt de gebruiker die mogeljkheid niet.

2.2.2 Open source in de strijd tegen lekken in closed source software die spyware binnenlaten

Omdat de broncode bij closed software niet openbaar is, zijn niet alle lekken zichtbaar. Aangezien perfecte software niet bestaat is er altijd een risico dat kwaadwillenden die deze lekken ontdekken gebruik maken van die lekken en spyware maken die door deze lekken ongedetecteerd de computer van de gebruiker binnendringt.
Als men gebruik maakt van open source loopt men deze gevaren niet, omdat dan de lekken zichtbaar zijn en men deze lekken kan en mag dichten.

2.2.3 Open source anti-spywareprogramma's

Ook de open source community heeft anti-spywareprogramma's voortgebracht. Vaak staan ze niet onder die naam bekend, maar onder de naam intrusion detection en vaak maken ze ook deel uit van anti-viruspakketten.

2.3 Bewustwording

Bewustwording lijkt ook in de eerste plaats niet een technische oplossing. Het gaat hier eigenlijk om het bewust maken van gebruikers wat betreft het fenomeen spyware, zodat zij zelf preventieve en reactieve maatregelen kunnen nemen. Daar deze maatregelen voornamelijk technisch zal bewustwording hier worden behandeld.

2.3.1 Algemeen voorlichting internet en dergelijke

Op allerlei fora en sites op internet zelf kan men inmiddels ook veel informatie vinden over onder andere spyware. Sites van internetproviders zijn daar een mooi voorbeeld van, deze sites hebben allemaal wel een deel waar aan de gebruikers wordt uitgelegd wat de gevaren van het internet zijn en wat men er tegen kan doen. Maar ook veel consumentensites zoals www.radar.nl of www.consumentenbond.nl lichten computergebruikers tegenwoordig in over zowel de mogelijkheden als de gevaren van het internet. Ook voorlichting over de maatregelen die men kan nemen tegen spyware horen bij die voorlichting. Het gaat dan bijvoorbeeld om het aanschaffen van de anti-spywareprogramma's die al besproken zijn, maar ook om het beter beveiligen van netwerken en het controleren van uitgaande informatie.

Wanneer men kijkt naar de antwoorden die minister Donner gaf op de kamervragen van kamerlid Gerkens van SP betreffende spyware, dan kan men concluderen dat minister Donner de algemene voorlichtingsfunctie van internetbronnen, zoals

internetfora, zeer belangrijk acht. [35] De minister lijkt aan te geven dat de burgers zelf ook eigen verantwoordelijkheid hebben met betrekking tot voorlichting over spyware. Als informatie beschikbaar is, bijvoorbeeld op het internet, moeten burgers deze informatie zelf zoeken en aan de hand van die informatie zelf maatregelen nemen. De overheid dicht hij maar een kleine rol toe op dit punt. Hij vindt in ieder geval niet dat de rol van de overheid groter moet worden.

2.3.2 Rol van de overheid bij bewustwording

Behalve het reguleren van de digitale wereld is er ook een andere rol voor de overheid weggelegd met betrekking tot de digitale wereld. Het gaat om de rol van het bewust maken van burgers met betrekking tot de gevaren en mogelijkheden die onze digitale samenleving met zich meebrengt. Deze taak van de overheid mag niet onderschat worden, zeker omdat de overheid zelf ook in toenemende mate op digitale wijze met de burger communiceert via en met behulp van elektronische loketten, e-formulieren, sms, internet in het algemeen et cetera. Het is dan ook niet meer dan logisch dat de overheid de burger voorlicht over het gebruik en de gevaren van deze middelen.

De overheid heeft inmiddels enkele initiatieven ontwikkeld om de burger bewust te maken van alle gevaren en mogelijkheden van de digitale snelweg. Binnen ICTU een stichting die is opgericht door het Ministerie van Binnenlandse Zaken en de Vereniging voor Nederlandse Gemeenten (VNG) bevinden zich bijvoorbeeld Gov.cert en de Waarschuwingsdienst. Tevens is vanuit het Ministerie van Economische Zaken de campagne "Surf op safe" opgestart.[36]

Zoals al eerder gezegd is Minister Donner niet van plan meer aandacht te besteden aan voorlichting van burgers en in antwoord op de kamervragen omtrent spyware, wees hij op de eigen verantwoordelijkheid van burgers. Opvallend is wel dat hij in zijn antwoord als voorbeeld wel de campagne "Surf op Safe" aanhaalde, maar niet de Waarschuwingsdienst. Dit terwijl de experts van de Waarschuwingsdienst (en Gov.cert) verantwoordelijk waren voor het technische deel van het antwoord van de minister op de kamervragen over spyware. Bovendien lijkt mij dat een initiatief als de Waarschuwingsdienst zeer lovenswaardig en nuttig is en bij uitstek een middel om mevrouw Gerkens duidelijk te maken dat de overheid zich reeds in voldoende mate met de voorlichting van de burgers bezighoudt.

Gov.cert

Gov.cert valt onder het Ministerie van Binnenlandse Zaken. Gov.cert is het computer emergency reponse team (cert) van en voor de Nederlandse overheid. Gov.cert is een overheidsorganisatie die zich richt op andere overheidsorganisaties op alle niveaus. Gov.cert licht hen in over de gevaren van het internet, beantwoordt hun vragen en helpt hen met het opzetten van een fatsoenlijke beveiliging.

Gov.cert behandelt het thema spyware wel, maar er ligt geen nadruk op. Wanneer Gov.cert concrete vragen krijgt rond spyware zullen zij overheidsorganen helpen met het oplossen van die problemen. Overheidsorganen hebben overigens vaak eigen netwerkbeheer. Gov.cert mag de netwerkbeheerders geen producten aanraden. Zij mogen slechts globaal zeggen dat het belangrijk is de organisatie te

---

[35] Zie 5.1.1.

[36] Surf op safe
Surf op safe, WWW < http://www.surfopsafe.nl/> (geraadpleegd 9 augustus 2005)

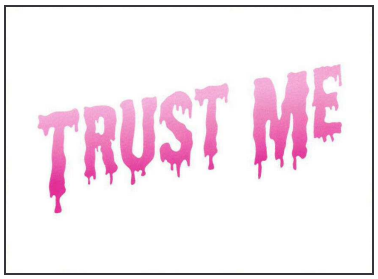
beveiligen. Daarbij mogen ze wel namen van producten noemen, zolang maar niet één product wordt gepromoot.

De Waarschuwingsdienst

De Waarschuwingsdienst valt onder het Ministerie van Economische Zaken. Dit ministerie is tevens verantwoordelijk voor de campagne "Surf op safe". De Waarschuwingsdienst is een overheidsorganisatie die zich richt op burgers. De Waarschuwingsdienst licht het voor over de gevaren van het internet en beantwoordt hun vragen.

De voorlichting vindt plaats op de meest uiteenlopende wijzen. De Waarschuwingsdienst is bijvoorbeeld aanwezig op computerbeurzen, verspreid voorlichtingsmateriaal onder scholieren en verspreid "boomerang"-kaarten[37].

Afbeelding 2.3 Boomerang-kaart
"To protect and surf"
van de Waarschuwingsdienst



Afbeelding 2.4 Boomerang-kaart
"Trust me" van de Waarschuwingsdienst

Ook stond de Waarschuwingsdienst op de huishoudbeurs en licht zij gebruikers van seniorweb voor. De doelgroep van de Waarschuwingsdienst zijn computergebruikers wiens computergebruik is te omschrijven als licht tot normaal. De gebruikers die hun computer veel gebruiken en zich vaak online bevinden zijn over het algemeen wel op de hoogte van de risico's die zij lopen en hebben zich hier ook wel tegen beschermd.

Surf op safe

Surf op safe is zoals al eerder gezegd een initiatief van het Ministerie van Economische Zaken. Surf op safe biedt voorlichting voor diverse doelgroepen aan op haar site (kinderen, ouders, docenten, bedrijven en senioren)[38] en verspreidt folders over internetproblemen zoals dialers.

2.4 Encryptie

Vermeer geeft aan dat ook encryptie, een voorbeeld van PET (Privacy Enhancing Technology) kan helpen de privacy van de internetgebruiker te beschermen. Of dit ook geldt met betrekking tot de *bestrijding* van spyware valt nog te bezien. Het

---

[37] Kaarten op ansichtkaartformaat die gratis worden verspreid in cafés, universiteiten, bioscopen et cetera, meestal met een reclameboodschap of als voorlichtingsmateriaal.

[38] Surf op safe
Surf op safe, WWW < http://www.surfopsafe.nl /index/voor_wie/index.html/> (geraadpleegd 9 augustus 2005)

gevolg zou wel kunnen zijn dat de gegevens die door de spyware worden verzameld onbruikbaar zijn.[39]

Bij encryptie worden boodschappen/gegevens die gebruikers elkaar zenden versleuteld voor ze worden verstuurd om daarna door de ontvangende partij weer ontsleuteld te worden. [40] Het nadeel is wel dat de gebruikers/instantie die met elkaar communiceren over software moeten beschikken om te ver- en te ontsleutelen. Bovendien kost het ver- en ontsleutelen ook weer tijd en moeite. Dit zou ten koste kunnen gaan van de snelheid waarmee het internet zo wordt geassocieerd.

[39] Omdat encryptie mijns inziens niet rechtstreeks bijdraagt tot de bestrijding van spyware zal ik het hier niet verder behandelen.
[40] Vermeer 2000, p. 196-197.

Hoofdstuk 3: Bestaande privacywet- en regelgeving met betrekking tot spyware

3.1 Grondrecht op privacy (met betrekking tot spyware)

Welke grondrechten er precies onder de paraplu van het grondrecht op privacy vallen is niet geheel duidelijk. Er bestaat op dit punt veel discussie. Ik zal me niet ook niet aan een antwoord op deze vraag wagen, maar slechts de privacygrondrechten behandelen die in het kader van het probleem spyware van belang zijn.

De oorsprong van het grondrecht op privacy is klassiek. In het verleden vond men dat de burger moest worden beschermd tegen de overheid. De overheid zou kunnen indringen in de persoonlijke levenssfeer van de burger en dit werd als zeer onwenselijk beschouwd. Hoewel privacy in de verhouding tussen de overheid en de burger doorgaans een zeer belangrijke rol speelt, al was het alleen al vanwege de machtsverhouding, ligt dat met betrekking tot dit onderwerp (spyware) anders. Er is hier eerder sprake van burgers die tegen elkaar beschermd moeten worden, dan burgers die tegen de overheid beschermd moeten worden. De overheid zal spyware niet zo snel inzetten, vanwege de eventuele juridische bezwaren en de zorgplicht die de overheid heeft. Wellicht zou de overheid spyware kunnen inzetten bij opsporingsmethoden, als elektronisch equivalent van telefoontaps. De informatieverstrekking daaromtrent is echter zeer miniem. Het blijft dus slechts bij gissen over de toepassing van spyware door de overheid.

Het grondrecht op privacy komt in dit kader voornamelijk ter sprake daar waar het gaat om de verhouding tussen burgers onderling. Het is denkbaar dat het recht op privacy horizontale werking verkrijgt bij een zekere vorm van machtsafhankelijkheid.[41] Als men bij het toetsen van machtsafhankelijkheid de volgende toets hanteert: "Kan men de inbreuk op de privacy tegen houden (door bijvoorbeeld een verzoek om gegevens te negeren of iemand niet toe te laten in de woning)?", dan kan de verhouding tussen de producent van spyware en de gebruiker van de computer waarop de spyware staat zeker als een machtsafhankelijk worden bestempeld. De gebruiker heeft immers geen enkele macht of zeggenschap over welke gegevens hij/zij wil verschaffen. Rechtspraak op dit punt is nog niet aanwezig, maar het lijkt waarschijnlijk dat horizontale werking van het grondrecht op privacy mogelijk is, zowel voor de grondwettelijke grondrechten als voor de verdragsgrondrechten. Bovendien heeft de Wet bescherming persoonsgegevens gezorgd dat dit grondrecht horizontaal werkt, zie daarvoor artikel 10 lid 2 van de Wbp.

Er zijn drie soorten privacy, het huisrecht, de relationele privacy en de informationele privacy.

Het huisrecht, oftewel het recht op fysieke privacy in de eigen woning is het oudst en meest verbonden met de reële wereld. De relationele privacy wordt door de Amerikanen ook wel "The right to be let alone" genoemd en heeft betrekking op de relaties die een persoon met anderen heeft. Overigens wordt door sommige auteurs het huisrecht ook wel onder de relationele privacy getrokken. [42]

---

[41] Kleve 2004, p. 289.
[42] Alberdingk Thijm 2004, p. 11.

De informationele privacy werd vanaf de jaren 60/70 steeds belangrijker. De controle over de eigen gegevens, informatie en de beslissingen die daarop zijn gebaseerd vallen volgens Alan F. Westin onder de informationele privacy. [43] Westin was één van de eersten die expliciet aandacht vroeg voor de bescherming van persoonsgegevens. [44] Dan kunnen wij bijvoorbeeld denken aan verhoudingen en communicatie van mensen en persoonsgegevens. Dit zijn de onderdelen van privacy die het meest belangrijk zijn bij het bespreken van spyware.

3.1.1 Nederland, de Grondwet

De privacygrondrechten in de grondwet die in het kader van spyware van belang zijn, zijn: Recht op eerbiediging van de persoonlijke levenssfeer, artikel 10 lid 2 Grondwet en artikel 13 Grondwet, dat het briefgeheim en het telefoon- en telegraafgeheim regelt..

Artikel 10 Grondwet, het artikel over bescherming van de persoonlijke levenssfeer, ziet onder andere op persoonsgegevens, die wanneer men naar spyware kijkt zeer belangrijk zijn. Wat persoonsgegevens zijn en dergelijke komt aan de orde in de paragraaf over de Wbp. In de Wbp is het grondrecht op privacy en de bescherming van persoonsgegevens namelijk uitgewerkt.

Is het grondwetsartikel over het briefgeheim van belang bij de bespreking van spyware? Spyware onderschept elektronische communicatie en geen stoffelijke brieven. Het briefgeheim spreekt zich niet uit over de elektronische variant van de brief, de e-mail, maar het briefgeheim lijkt me ook op e-mail van toepassing. Artikel 13 is ook niet zo gesteld dat e-mail duidelijk niet onder dit artikel valt. Doorgaans worden "brieven" opgevat als communicatie in ruime zin.[45] Toch kan men uit kamerstukken destilleren dat de bedoeling van de bepaling toch de bescherming van meer stoffelijke communicatie is, aangezien er wordt gesproken over gesloten enveloppen of verpakkingen met hetzelfde oogmerk. Als men dit meeneemt, lijkt het moeilijk te verdedigen dat een e-mail daarmee vergelijkbaar is.

In HR 29 maart 1994, lijkt de HR echter te kiezen voor het verlaten van de techniekafhankelijke standaard voor het vaststellen van het briefgeheim. In dit arrest ging het over gegevens die in een zakcomputer waren opgeslagen. Om te kijken of deze onder het briefgeheim vielen gebruikte de HR het criterium "de adressering van de mededeling", niet de vorm of de techniek van de mededeling.[46] Toch is deze kwestie ook met dit arrest nog niet opgehelderd, al lijkt het nu beter te verdedigen dat elektronische communicatie ook onder het briefgeheim zou vallen nu niet zozeer wordt vastgehouden aan de "techniek" van de verzending van stoffelijke brieven.

E-mail en andere gegevens die elektronische communicatie betreffen (bijvoorbeeld chat-logs, "logboeken" van chatgesprekken die de gebruiker van de computer met andere computergebruikers voert) worden in ieder geval beschermd door artikel 10 Grondwet. Nu deze gegevens te herleiden zijn tot een "geïdentificeerde of identificeerbare natuurlijke persoon" (terminologie van de Wet bescherming

---

[43] Westin 1967, p. 7.
[44] Van Bruggen, Van Dun & De Lange 2000, p.79.
[45] Asscher 2002, p. 84.
[46] Asscher 2002, p. 85.

persoonsgegevens), is er namelijk sprake van persoonsgegevens en zoals gesteld worden die beschermd door artikel 10 Grondwet.

Het huisrecht, artikel 12 Grondwet is niet van toepassing bij spyware, immers spyware treedt het huis niet fysiek binnen, spyware treedt slechts de computer binnen en doet dat op elektronische wijze. Nu staat het vereiste van "fysiek" binnentreden niet letterlijk in de Grondwet en zou men kunnen betogen dat men ook elektronisch zou kunnen "binnentreden". Echter dan is men nog steeds niet in de woning, maar slechts in de computer. De redenering dat men door het "binnentreden" van de computer automatisch de woning waarin de computer zich bevindt binnentreedt, gaat wat mij betreft te ver. Wel zou ik me kunnen voorstellen dat rechters deze bepaling gebruiken bij de interpretatie in een spywarezaak of dat er een bepaling zou komen voor computers die lijkt op de huisrechtbepaling, net zoals er inmiddels een computervredebreukbepaling in het strafrecht bestaat in navolging van een huisvredebreukbepaling. De gevolgen van het "binnentreden" van een computer zullen in de huidige maatschappij en met het huidige gebruik van computers net zo'n grote inbreuk kunnen vormen op de privacy van een gebruiker als het binnentreden van zijn/haar huis.

3.1.2 Europa/EVRM

De Europese wetgeving met betrekking tot het grondrecht op privacy kan men in het Europese Verdrag voor de Rechten van de Mens (hierna te noemen: EVRM) vinden en wel in artikel 8 EVRM. Dit artikel beschermt privé-, familie- en gezinsleven, ook de bescherming van briefwisseling en woning vallen onder dit artikel.
De toetsing van het EVRM vindt plaats bij het Europees Hof voor de Rechten van de Mens (hierna te noemen: EHRM).

3.1.3 Verenigde staten

In de Verenigde staten wordt het communicatiegeheim beschermd in het Vierde Amendement dat de privacy van de burgers beschermd. Echter het traditionele Vierde Amendement schiet tekort bij de bescherming van de privacybelangen bij nieuwe media. Rechters in de Verenigde staten lossen dit probleem veelal op door analoog te interpreteren. Dit biedt echter weinig rechtszekerheid.[47]

3.1.4 Overige

In het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (hierna te noemen: IVBPR) staat ook een bepaling die het grondrecht op privacy beschermt. Het gaat hier om artikel 17 IVBPR. Dit artikel beschermt privé- en gezinsleven en ook briefwisseling en huis worden door dit artikel beschermd. Tevens beschermt het artikel eenieder tegen aantasting van zijn/haar eer en goede naam.

Mocht men vinden dat een IVBPR-recht is geschonden, dan kan men zich wenden tot het Comité voor de Rechten van de Mens. Het gaat hier niet om een rechterlijke instantie, uitspraken van het Comité zijn niet rechtens bindend.[48] Wel hebben uitspraken van het comité gezag en invloed.

---

[47] Asscher 2002, p. 219.
[48] Akkermans, Bax en Verhey 1999, p. 191.

3.2 Nederlandse privacywet- en regelgeving met betrekking tot spyware

In Nederland bestaat nog geen wet- en/of regelgeving specifiek op spyware gericht. Inmiddels is men zich in Den Haag wel bewust van het probleem spyware en zijn er kamervragen gesteld door A. Gerkens van de SP. Deze zullen worden behandeld in hoofdstuk 5. Wel zou men reeds bestaande wetgeving kunnen gebruiken in de strijd tegen spyware. In deze paragraaf zal de privacywetgeving aan de orde komen die men zou kunnen inzetten in de juridische strijd tegen spyware.

3.2.1 Wet bescherming persoonsgegevens (hierna te noemen: Wbp), algemeen

De Wbp is op 1 september 2001 in werking getreden. Deze wet is de implementatie van een Europese richtlijn, namelijk de Europese richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.[49] *Deze wet beoogt duidelijk te stellen wat wel en niet is toegestaan met betrekking tot de verwerking van persoonsgegevens.*

Persoonsgegevens

Om te zien of de Wbp van toepassing is, is het belangrijk te weten wat een persoonsgegeven is. De Wbp is alleen van toepassing op als het om de verwerking van *persoonsgegevens* gaat. Welke gegevens persoonsgegevens zijn, kan men vinden in art. 1 Wbp onder a. Een persoonsgegeven is een gegeven dat herleidbaar is tot een "geïdentificeerde of identificeerbare natuurlijke persoon". Dat betekent dat de naam van een persoon op wie de gegevens betrekking hebben bekend is, dan wel dat die persoon kan worden achterhaald. Een voorbeeld van een persoonsgegeven is een naam van een persoon of een huisadres, maar ook e-mailadressen en zelfs ip-adressen kunnen persoonsgegevens zijn voorzover deze gegevens herleidbaar zijn tot natuurlijke personen. Wanneer dit het geval is, is zeer afhankelijk van de omstandigheden van het geval. Dommering geeft wel een aantal regels met betrekking tot de herleidbaarheid met betrekking tot de Wbp:
a. Het maakt niet uit om wat voor soort gegevens het gaat.
b. De herleidbaarheid moet niet onevenredig veel tijd en moeite kosten.
c. Gegevens over groepen zijn op zichzelf niet herleidbaar tot individuele personen.
d. De Wbp heeft betrekking op gegevens over natuurlijke personen.
e. Het verband tussen persoon en gegeven moet, mede gelet op de strekking van de wet, rechtens relevant zijn (aldus de regering).[50]

Verwerking van (elektronische) persoonsgegevens

Een ander vereiste om binnen het toepassingsbereik van de Wbp te vallen is dat het moet gaan om *verwerking* van persoonsgegevens. Wat onder verwerking wordt verstaan kan men lezen in art. 1 Wbp onder b. Uit deze bepaling kan men afleiden dat elke handeling met betrekking tot persoonsgegevens vanaf de verzameling van deze gegevens tot en met de vernietiging onder verwerking valt. Berkvens en Prins geven bovendien aan dat verwerking zeer ruim geïnterpreteerd moet worden.[51]

Uitzonderingen op verwerking

Er zijn onder de Wbp een aantal uitzonderingen gemaakt met betrekking tot de verwerking van persoonsgegevens. Een aantal verwerkingen valt bijvoorbeeld niet

---

[49] Richtlijn nr. 95/46 EG, (PbEG L 281)
[50] Dommering 2000, p. 410-411.
[51] Berkvens & Prins 2001, p.359-360.

onder de Wbp, het gaat dan onder andere om verwerking van persoonsgegevens in het kader van politietaken, journalistiek, of kunst.

Gronden voor verwerking van persoonsgegevens

Art. 8 Wbp geeft een limitatieve opsomming van gronden om gegevens te mogen verwerken. Vereist is de ondubbelzinnige toestemming van de betrokkene (degene wiens gegevens worden verwerkt) of de verwerking moet noodzakelijk zijn onder één van de in de sub b tot en met f genoemde gronden.

Overige voorwaarden

Valt de verwerking onder de Wbp en is de verwerking toegestaan, dan moet men aan allerlei eisen voldoen die in de Wbp worden gesteld. Deze eisen houden onder andere in dat de persoon van wie de gegevens worden verwerkt daarvan op de hoogte moet worden gesteld. Tevens moet hij/zij de mogelijkheid krijgen deze gegevens in te zien en wanneer de gegevens foutief zijn moeten ze worden gewijzigd. Ook moet er een mogelijkheid zijn tot verzet. In art. 11 Wbp wordt bovendien geëist dat de gegevensverwerking proportioneel is.

Bijzondere persoonsgegevens

In de Wbp is in artikel 16 een verbod opgenomen op de verwerking van bijzondere, ook wel gevoelige persoonsgegevens. Het gaat dan om persoonsgegevens over iemands godsdienst, levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, het lidmaatschap van een vakvereniging (vakbond), stafrechtelijke persoonsgegevens en gegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

Ook op het algehele verbod op de verwerking van bijzonder persoonsgegevens zijn uitzonderingen gegeven in de Wbp. Deze uitzonderingen gelden bijvoorbeeld voor kerkgenootschappen en ziekenhuizen. Deze instellingen mogen de persoonsgegevens wel verwerken, maar de verwerking moet wel proportioneel zijn.

3.2.2 Wet bescherming persoonsgegevens met betrekking tot spyware

Kan de Wet bescherming persoonsgegevens ook worden toegepast met betrekking tot spyware?

Persoonsgegevens

Binnen de omschrijving van persoonsgegevens zoals deze gegeven is door de Wbp vallen veel, zo niet alle gegevens die verzameld worden door spyware. Dit hangt nauw samen met het doel van spyware. Als gegevens niet te herleiden zijn tot een natuurlijk persoon, maar een soort algemeen feit zijn, is de commerciële waarde miniem. De commerciële waarde bestaat in dat geval alleen uit bijvoorbeeld algemene gegevens over gebruikers van een bepaald softwareprogramma, hoeveel mensen het programma gebruiken bijvoorbeeld, voor de meeste producenten van spyware of derden die spyware gebruiken zal deze informatie niet toereikend zijn. De softwareleverancier wil liever weten wie zijn programma gebruiken, mannen/vrouwen, in welke leeftijdscategorie, wat hun e-mailadressen zijn et cetera, zodat hij daar zijn marketing op kan afstemmen en hij de gebruikers direct kan benaderen. De Wbp zal dus bij spyware vrijwel altijd van toepassing zijn, daar de combinatie van al die feiten al snel zal leiden tot herleidbaarheid.[52]

---

[52] Sauerwein & Linnemann 2001, p. 15.

Verwerking

Bij het gebruik van spyware zo heb ik net gesteld is er bijna altijd sprake van persoonsgegevens. Al eerder is gesteld dat voor toepassing van de Wbp er ook sprake moet zijn van verwerking. Is er bij spyware sprake van verwerking? Mijns inziens is dat inderdaad het geval, aangezien de term verwerking heel breed is en alles inhoudt vanaf de verzameling tot en met de vernietiging van persoonsgegevens. De verwerkingen die bij spyware en het gebruik daarvan in het oog springen zijn: het verzamelen van de informatie door de spyware zelf, de opslag van deze gegevens, de ordening van deze gegevens, het doorverkopen van deze gegevens en het gebruiken van deze gegevens voor diverse (al dan niet commerciële) doeleinden.

Uitzonderingen op verwerking

Er zijn uitzonderingen voor toepassing van de Wbp bij het verwerken van persoonsgegevens. Spyware valt wat mij betreft echter met geen mogelijkheid onder die uitzonderingen te brengen. Spyware wordt bijvoorbeeld in het algemeen niet ingezet voor politietaken. Mocht dit wel zo zijn, dan moet de politie zorgvuldig met de persoonsgegevens omgaan en zich bovendien aan de voor hen geldende regels houden. Dit maakt spyware in voornoemd geval niet verboden.

Spyware streeft over het algemeen ook geen artistiek, journalistiek of literair doel na, doet zij dit wel dan moet zij (dat wil zeggen de verwerking van persoonsgegevens) proportioneel zijn. Dit lijkt welhaast onmogelijk gezien het overwegend stiekeme karakter en de grofheid van de inbreuk van spyware.

Gronden voor verwerking van persoonsgegevens

In artikel 8 worden de gronden genoemd op grond waarvan een verwerking van persoonsgegevens is toegestaan. Eén van deze gronden is "ondubbelzinnige toestemming". De persoonsgegevens mogen in het kader van deze grond worden verwerkt mits daar ondubbelzinnig toestemming voor is verleend, zo is in artikel 8 Wbp te lezen, in dat geval valt gegevensverzamelende/verwerkende software ook niet binnen mijn definitie van spyware. In de meeste gevallen van gegevensverzamelende/verwerkende software zal dit niet het geval zijn en zal er in mijn ogen sprake zijn van spyware. Weinig gebruikers zullen instemmen met spyware en daarmee met de verwerking van hun gegevens via deze spyware. In uitzonderlijke gevallen misschien wanneer het om freeware gaat en de gebruiker heel slecht heeft opgelet. Dan komen we bij de overige gronden voor gegevensverwerking, in hetzelfde artikel 8 wordt namelijk aangegeven dat de verwerking tevens is toegestaan wanneer deze noodzakelijk is voor of de uitvoering van een overeenkomst tussen partijen, of voor de nakoming van een wettelijke verplichting, of voor de vrijwaring van een vitaal belang van de betrokkene (gebruiker) of voor de goede vervulling van een publiekrechtelijke taak, of voor de behartiging van gerechtvaardigd belang van de verantwoordelijke (verwerker/spywareproducent) of een derde aan wie de gegevens worden verstrekt. [53] Bij spyware lijkt in de meeste gevallen deze noodzakelijkheid niet aanwezig te zijn en voldoet spyware derhalve niet aan de eisen die worden gesteld aan verwerking voor persoonsgegevens.

---

[53] Sauerwein & Linnemann 2001, p. 21-22.

Wel lastig is de zesde grond, namelijk de noodzakelijkheid voor de behartiging van een gerechtvaardigd belang. Reclameboodschappen kunnen hier onder omstandigheden onder vallen, vooral omdat het versturen van reclameboodschappen een relatief lichte inbreuk op de persoonlijke levenssfeer van de gebruikers oplevert.[54] We hebben het dan niet over gerichte reclame waarvoor de producent van spyware veel informatie nodig heeft van de gebruiker, dan is er al snel sprake van overschrijding van het noodzakelijkheidsvereiste.

Overige voorwaarden

De verwerking van persoonsgegevens in relatie tot spyware is veelal niet toegestaan. Feit is dat die verwerking in de praktijk vaak wel plaatsvindt. Als de verwerking op zichzelf was toegestaan, hoe zou het dan gesteld zijn met de overige voorwaarden van de Wbp, de voorwaarden waar de verwerking aan moet voldoen. Voldoet spyware wel aan die voorwaarden?

Wordt er bij spyware bijvoorbeeld de mogelijkheid geboden om de eigen gegevens in te zien, te laten corrigeren en verzet aan te tekenen? Neen, deze mogelijkheden worden de betrokkene niet geboden. In veel gevallen weet hij/zij overigens niet eens dat zijn gegevens worden verzameld en zullen deze rechten dus sowieso onaangeroerd blijven, dat er dan dus ook geen toestemming is gegeven voor de verwerking laten we hier even buiten beschouwing. Bovendien staat in art. 11 Wbp nog het proportionaliteitsvereiste. Aan dit vereiste zullen de meeste spywareproducenten ook niet voldoen.

Spyware is mijns inziens juist gemaakt om wet- en regelgeving zoals de Wbp te ontduiken. Door te opereren zonder dat de gebruiker het door heeft en de verdere verwerking zoveel mogelijk aan het oog te onttrekken ontduikt men de eisen en de voorwaarden die in wet- en regelgeving worden gesteld aan gegevensverwerking. De naam spyware duidt het eigenlijk al aan: spy, spion, iemand die aanwezig is zonder dat een ander het merkt en die zonder dat de ander daar toestemming voor geeft informatie inwint. Zo gaat het ook met spyware, stiekem. Immers, als men open kaart had willen spelen met de gebruiker had men geen gebruik gemaakt van het middel spyware, maar bijvoorbeeld gewoon toestemming gevraagd voor de verwerking van bijvoorbeeld adresgegevens en vragenformulieren verstuurd met betrekking tot overige gegevens van de gebruiker. Aan de overige voorwaarden voor gegevensverwerking wordt dus ook niet voldaan.

Bijzondere persoonsgegevens

Leveren bijzondere persoonsgegevens specifieke problemen op bij de behandeling van het probleem spyware? Jazeker, er zijn vele verschillend soorten spyware. Niet alle soorten zullen onderscheid maken in de gegevens die zij van de computer van de gebruiker halen. Het is mogelijk dat er soorten zijn die dat wel doen. Er zijn wellicht ook soorten die juist op zoek zijn naar bijzondere (gevoelige) persoonsgegevens omdat de producenten of opdrachtgevers van de spyware daar nu eenmaal belang bij hebben. Bijvoorbeeld exploitanten van erotische sites, zij willen graag dingen over de seksuele voorkeur van gebruikers, zodat zij hun diensten en producten zo goed mogelijk op de gebruiker kunnen afstemmen. Het is dan ook niet denkbeeldig dat de exploitant van een erotische site bij het beschikbaar stellen van bijvoorbeeld gratis afbeeldingen een programma meestuurt dat een kijkje neemt in het de surfgeschiedenis van de gebruiker en deze doorspeelt aan deze exploitant

[54] Sauerwein & Linnemann 2001, p. 25-26.

(zodat deze de gebruiker bijvoorbeeld een speciaal op hem gerichte aanbieding kan doen). Het is vervolgens mogelijk dat in die surfgeschiedenis allerlei erotische sites te vinden zijn die iets zeggen over het seksuele leven van de gebruiker en die nu duidelijk aan de gebruiker te koppelen zijn. Volgens art. 16 Wbp is dit eenvoudigweg niet toegestaan. Tevens zijn er geen specifieke uitzonderingen op "seksueel leven", zoals deze er wel zijn op "godsdienst" en "gezondheid". Ook de algemene uitzondering van artikel 23 is niet van toepassing.

De uitzonderingen die voor het verbod op de verwerking van bijzondere/gevoelige persoonsgegevens gelden zullen hier niet van toepassing zijn. De Wbp geeft een beperkt aantal instellingen aan die deze gegevens wel mogen verwerken mits ze de proportionaliteit in het oog houden. De instellingen waar het om gaat zijn bijv. kerken en ziekenhuizen, spywareproducenten zal men niet (snel) onder deze instellingen kunnen scharen, bovendien zou de proportionaliteit de meeste spywareproducenten parten spelen, daar de meeste spyware gericht is op commercieel gewin en dat onder de Wbp niet als proportioneel wordt beschouwd. Ook spywaremakers die er op uit zijn een ander het leven zuur te maken op grond van de door hen verzamelde informatie over bijvoorbeeld het privéleven van een gebruiker vallen dus niet onder deze uitzonderingen.

Artikel 23 geeft een algemene uitzondering voor de verwerking van bijzondere/gevoelige persoonsgegevens die ook niet van toepassing zal zijn. Op het persoonsgegevens omtrent het "seksueel leven van de betrokkene" zijn zelfs helemaal geen uitzonderingen gemaakt. Verwerking is dan in alle gevallen verboden.

Conclusie met betrekking tot spyware en de Wbp

Gezien de regels die de Wbp aan de verwerker van persoonsgegevens stelt is de huidige spyware vrijwel allemaal verboden, ofwel omdat men zich niet aan de regels houdt die voor de verwerking van "gewone" persoonsgegevens geldt, ofwel omdat het om de verwerking van bijzondere/gevoelige persoonsgegevens gaat, ofwel men zich niet aan de voorwaarden houdt wanneer men eenmaal aan het verwerken is geslagen.

Het lijkt welhaast onmogelijk voor een spywareproducent om zich aan de regels van de Wbp te houden en spyware te produceren die dat doet waar men belang bij heeft, namelijk zoveel mogelijk interessante informatie verzamelen over computergebruikers. In plaats van de hele "vooraf melden van de verwerking en het doel van de verwerking" kan men de informatie die men uiteindelijk van de gebruiker wil, beter bij de gebruiker zelf proberen in te winnen. Dat kost waarschijnlijk net zoveel moeite als de waarschuwing die men vooraf moet geven aan de persoon waarvan men de persoonsgegevens wil verwerken en bovendien loopt men niet de kans in overtreding te zijn. Wel moet men de gebruiker in dat geval nog steeds op de hoogte stellen van het doel van de verwerking, de mogelijkheid bieden zijn gegevens te wijzigen en zich te verzetten. In ieder geval kan men concluderen dat spyware en de Wbp, voor zover mij bekend, zeer slecht samen gaan en is de meeste spyware op grond van de Wbp verboden. Het middel spyware impliceert als het ware een inbreuk op de privacywet- en regelgeving.

3.2.3 Besluit universele dienstverleners en eindgebruikersbelangen

Het besluit staat niet in directe relatie met de Wbp, het besluit is een algemene maatregel van bestuur en is een aanvulling op de Telecommunicatiewet.[55] Dit besluit van 7 mei 2004 implementeert onder andere een aantal bepalingen uit de richtlijn "privacy en elektronische communicatie" (Richtlijn 2002/58 EG). Dit is ook de reden dat het besluit in het hoofdstuk met privacywetgeving wordt behandeld en niet in het hoofdstuk met overige wetgeving.

Artikel 4.1 van dit besluit bepaalt dat ieder die via elektronische communicatiemiddelen toegang wil tot gegevens die zijn opgeslagen op apparatuur van gebruikers, of daar informatie wenst op te slaan, de gebruiker dient te informeren over het doel van de toegang en/of opslag. Tevens moet de mogelijkheid worden geboden om de toegang of opslag te weigeren. Er wordt ook een uitzondering op deze regel gemaakt. Deze wordt gemaakt voor de gevallen waar de toegang of opslag noodzakelijk is om technische redenen, met name om de communicatie mogelijk te maken of te vergemakkelijken, of om een dienst te kunnen leveren waar de gebruiker om heeft gevraagd. Dit betekent bijvoorbeeld voor cookies dat ze wel zijn toegestaan, mits de gebruiker de gelegenheid krijgt om het cookie te weigeren en hem/haar het doel wordt duidelijk gemaakt van desbetreffende cookie.

Voor spyware betekent deze bepaling dat vooraf de gebruiker duidelijk en nauwkeurig moet worden geïnformeerd over de spyware, het doel ervan en dat de gebruiker de mogelijkheid moet krijgen te weigeren, een soort opt-outconstructie.[56] Dit betekent dat een ondoorzichtige bepaling in de algemene voorwaarden mijns inziens niet voldoet aan deze bepaling en spyware veelal op grond van deze bepaling niet is toegestaan.

3.3 Buitenlandse privacywet- en regelgeving met betrekking tot spyware

In de huidige maatschappij, waarin veel is gedigitaliseerd en het internet een belangrijke rol speelt is het internationale aspect zeer belangrijk geworden daar waar het (elektronische) communicatie betreft. Dat geldt bijvoorbeeld voor regulering omtrent SPAM, maar ook met betrekking tot (de regulering van) spyware.

In het buitenland denkt men ook druk na over spyware. Dat is gunstig, want spyware is immers een internationaal probleem, wetgeving in één of twee landen zal niet substantieel bijdragen aan de juridische strijd tegen spyware, aangezien spywareproducenten dan uitwijken naar andere landen. Bovendien heeft internet en daarmee ook privacy in een digitale omgeving geen grenzen. Wanneer naar aanleiding van door spyware verzamelde e-mail-adressen bijvoorbeeld e-mails worden verstuurd worden deze niet door landsgrenzen tegengehouden of bij landsgrenzen gecontroleerd.

3.3.1 EU/EG

Er zijn geen verdragen die duidelijkheid bieden over de combinatie spyware en privacy. Er zijn wel EG richtlijnen. Richtlijn 1995/46 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens bijvoorbeeld, dit is de richtlijn waarop

[55] Kaspersen 2005, p. 12
[56] Kaspersen 2005, p. 13

onze Wbp is gebaseerd. Tevens is richtlijn 2002/58 privacy en elektronische communicatie van belang, deze is in Nederland geïmplementeerd door het besluit universele dienstverleners en eindgebruikersbelangen.

3.3.2 Verenigde staten

Er is reeds anti-spywarewetgeving in Californië en Utah[57], en sinds kort (mei 2005) ook in Washington. Van de wet in Washington kan worden gezegd dat deze voornamelijk ziet op het doorspelen van e-mailadressen en andere adresgegevens.[58] Op de anti-spywarewetgeving in Utah is veel kritiek. De meeste kritiek is gericht op het feit dat de definitie van spyware in de wet te breed is en dat er zo ook vele "goede" en "nuttige" dingen/toepassingen/technieken verbiedt.[59]

Hoe het met de status van andere informatie staat die door spyware wordt opgehaald is niet duidelijk. Met andere informatie kan men namelijk ook veel schade aanrichten, bijvoorbeeld correspondentie over iemands sexleven, men kan aannemen dat deze informatie (net zoals in Nederland) door andere wetgeving wordt beschermd. Pluspunt van de regeling is wel dat het strafbaar is wanneer spyware anti-spywaresoftware saboteert. In vele andere staten zijn ook initiatieven voor anti-spywarewetgeving. De status van deze initiatieven is zeer lastig te achterhalen. De federale initiatieven (voorstel in het huis van afgevaardigden) zal ik in hoofdstuk 5 behandelen. Verder is er wetgeving op het gebied van privacy die men ook zou kunnen toepassen met betrekking tot spyware.

De Verenigde staten kennen wel de Electronic Communications Privacy Act (hierna te noemen: ECPA). De ECPA verbiedt om communicatie te onderscheppen zonder goedkeuring van een rechtbank of toepassing van een betrokkene.[60] De ECPA is van toepassing op spyware, maar veel heeft ze niet gebracht behalve het toestemmingsvereiste voor het onderscheppen van communicatie. De ECPA gaat niet specifiek op spyware in.

3.4 Handhaving

Al deze privacywet- en regelgeving moet natuurlijk ook gehandhaafd worden, de diverse landen en overkoepelende organisaties hebben hier allemaal hun eigen methode voor.

3.4.1 Nederland

In Nederland wordt de handhaving van de Wbp overgelaten aan een speciaal orgaan namelijk het College Bescherming Persoonsgegevens. Naast dit college kan men natuurlijk altijd met bij de "gewone" burgerlijke rechter terecht wanneer men zich niet specifiek beroept op bepalingen uit de Wbp en bijvoorbeeld schadevergoeding vordert op grond van onrechtmatige daad (6:162 BW).

---

[57] De Schrijver & Schraeyen 2005, p. 7.

[58] Pasveer 2005

L. Pasveer, *Amerikanen leggen spyware aan banden*, WWW < http://www.zdnet.nl/print.cfm?id=45778>, publicatie 23 mei 2005.

[59] Ramasastry 2004

A. Ramasastry, *Can Utah's New Anti-Spyware Law Work?* WWW < http://writ.news.findlaw.com/ramasastry/20040601.html>

[60] De Schrijver & Schraeyen 2005, p. 4.

OPTA (Onafhankelijke Post en Telecommunicatie Autoriteit)

De OPTA houdt toezicht op het Besluit universele dienstverlening en eindgebruikersbelangen. In geval van een overtreding van het besluit heeft de OPTA de bevoegdheid om een bestuurlijke boete van maximaal 450.000 Euro op te leggen. Ook kan de OPTA gebruik maken van een last onder dwangsom. Onder druk van een last onder dwangsom kan de OPTA bijvoorbeeld de eis stellen dat er geen spyware meer wordt geplaatst zonder toestemming van de gebruiker, zoals artikel 4.1 van het Besluit universele dienstverlening en eindgebruikersbelangen vereist.

College Bescherming Persoonsgegevens

Het College bescherming persoonsgegevens (hierna te noemen: CBP) ziet er, op grond van artikel 51 van de Wbp, als onafhankelijke instantie op toe, dat persoonsgegevens zorgvuldig worden gebruikt en beveiligd en dat de privacy van burgers ook in de toekomst gewaarborgd blijft.

Het CBP houdt toezicht op de naleving van wetten die het gebruik van persoonsgegevens regelen. Het CBP houdt dus toezicht op de naleving en toepassing van de Wbp, de Wet politieregisters (Wpolr) en de Wet gemeentelijke basisadministratie (Wet GBA).

Bij het CBP moet het gebruik van persoonsgegevens worden gemeld, tenzij hiervoor een vrijstelling geldt. Of er een vrijstelling geldt kan men nalezen in het vrijstellingsbesluit Wet bescherming persoonsgegevens.

Het kader voor de uitvoering van deze taak is dus in de Wbp en daarmee samenhangende andere wetgeving vastgelegd. Het instellen van het CBP is een gevolg van art. 28 van de Europese Privacyrichtlijn 95/46/EG. In dit artikel van de privacyrichtlijn wordt lidstaten de verplichting opgelegd een toezichthoudend orgaan in te stellen dat volledig onafhankelijk dient te opereren.

Bij deze taken van het CBP gaat het soms om verplichtingen, maar meestal om bevoegdheden over de uitoefening waarvan het CBP, met inachtneming van de wet en het oordeel van de rechter, zelf kan beslissen. Andere taken, zoals het geven van voorlichting en het doen van onderzoek naar nieuwe ontwikkelingen, vloeien voort uit de algemene toezichthoudende taak.[61]

Het CBP mag bestuurlijke boeten opleggen (art. 66 Wbp) en kan bestuursdwang uitoefenen (art. 65 Wbp) en kan last onder dwangsom opleggen (art. 5:32 Awb).

Strafrechter op grond van de Wbp

Ook de strafrechter kan straffen op grond van de Wbp. Art. 75 Wbp biedt de strafrechter de mogelijkheid om boetes en zelfs gevangenisstraffen op te leggen. Uiteraard kan geen vervolging worden ingesteld wanneer het CBP reeds een boete heeft opgelegd, dit vanwege het *Ne bis in idem*-beginsel. In de praktijk maakt de strafrechter zelden gebruik van zijn bevoegdheid op grond van de Wbp.

---

[61] College Bescherming Persoonsgegevens
College Bescherming Persoonsgegevens, WWW <http://www.cbpweb.n/ indexen/ind_cbp.stml> (geraadpleegd 10 april 2005)

"Gewone" rechter

Als schending van een grondrecht wordt aangevoerd (en niet specifiek schending van de Wbp) samen met bijvoorbeeld een onrechtmatige daad en de vraag om schadevergoeding kan men de gewone privaatrechtelijke rechtsgang volgen.

3.4.2 EU/EG

Er bestaan geen instanties die op EU/EG niveau louter privacyzaken afhandelen. Wel is er de artikel 29 werkgroep, deze werkgroep adviseert de Europese Commissie op het gebied van privacy, tevens stemmen zij nationale en internationale privacywetgeving op elkaar af.[62] Uiteraard zijn er voor de EU/EG het Europese Hof van Justitie (EHvJ), bijvoorbeeld wanneer inbreuk wordt gemaakt op een richtlijn. Voor het EVRM is het het Europese Hof voor de Rechten van de Mens (EHRM) in het leven geroepen.

3.4.3 Verenigde staten

De Verenigde staten kennen verschillende staten met verschillende rechtssystemen en elk met andere wetten en andere rechtbanken. Er is geen apart overkoepelend landelijk orgaan dat toeziet op de bescherming van persoonsgegevens zoals bij ons. Het gaat te ver om hier op alle rechtssystemen van alle verschillende staten in te gaan.

De hoogste instantie in de Verenigde staten is de Supreme Court, deze instantie oordeelt ook over grondrechten. Gezien spyware voor een groot deel met het grondrecht privacy is verbonden, is deze instantie ook van belang voor de handhaving van privacywet- en regelgeving met betrekking tot spyware.

---

[62] College Bescherming Persoonsgegevens
College Bescherming Persoonsgegevens, WWW <http://www.cbpweb.n /indexen/ind_cbpint.stml> (geraadpleegd 8 juni 2005)

Hoofdstuk 4: Overige bestaande wet- en regelgeving met betrekking tot spyware

4.1 Computervredebreuk

Tegenwoordig is het Wetboek van strafrecht een bepaling opgenomen die computervredebreuk verbiedt. Hierna volgt een bespreking van deze bepaling; art. 138a Wetboek van strafrecht (hierna te noemen Sr) en de mogelijkheden om deze bepaling toe te passen bij de bestrijding van spyware. Traditioneel wordt computervredebreuk vooral gebruikt om hacking[63] aan te pakken.

4.1.1 Oorsprong wet- en regelgeving op het gebied van computervredebreuk

Computervredebreuk is de virtuele/digitale variant van huisvredebreuk. Huisvredebreuk (art. 138) straft degene die, kort samengevat, wederrechtelijk in een ruimte (die niet is bestemd voor openbare diensten)[64] binnendringt. Zodoende wordt de ruimtelijke (fysieke privacy) van de bewoner of gebruiker van die ruimte beschermd.

In 1985 werd de commissie computercriminaliteit (ook wel commissie Franken genoemd) ingesteld door het Ministerie van Justitie. In 1987 publiceerde deze commissie haar rapport "Informatietechniek en Strafrecht". In dit rapport stelde de commissie 29 wetswijzigingen voor. Deze wijzigingen vormden de basis voor de Wet computercriminaliteit 1. Op 1 maart 1993 trad de Wet computercriminaliteit in werking.[65]

Met de komst van de Wet computercriminaliteit I werd art. 138a Sr ingevoerd. Deze bepaling werd ingevoerd omdat er blijkbaar behoefte was niet alleen de ruimtelijke (fysieke) ruimte van burgers te beschermen maar ook hun informationele privacy[66] , hun virtuele ruimte en hun financiën (tegen financiële schade die bijvoorbeeld door hackers kan worden aangericht). Aanleiding daartoe waren onder andere de technische ontwikkelingen met betrekking tot onder andere internet en het toenemende gebruik van computers en internet door burgers.

Burgers gebruiken hun PC steeds meer en steeds vaker voor communicatie met anderen, bijvoorbeeld door middel van e-mail of chat. Deze communicatie valt onder de informationele privacy. Inbreuk op dit deel van de privacy werd onder het "oude" strafrecht niet gestraft en zodoende bood het strafrecht de burger op dit punt geen bescherming.

4.1.2 Nederlandse wet- en regelgeving op het gebied van computervredebreuk met betrekking tot spyware

Computercriminaliteit

Er bestaat geen overeenstemming over een definitie voor computercriminaliteit. Het Korps Landelijke Politiediensten (KLPD) heeft inmiddels wel een definitie van het

---

[63] Zie 1.3.1.

[64] Hier is reeds een andere bepaling voor namelijk art. 139 Sr dat lokaalvredebreuk strafbaar stelt.

[65] Wiemans 2004
F.P.E. Wiemans, *Samenvatting,* WWW <http://www.vidya.nl/_boeken/9058500780_wiemans/samenvatting_wiemans.pdf> (geraadpleegd 20 juli 2005)

[66] Zie 3.1.

begrip computercriminaliteit of cybercrime opgesteld. Deze definitie luidt: "Computercriminaliteit is elke strafbare en strafwaardige gedraging voor de uitvoering waarvan het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is." Onder computercriminaliteit worden zowel verschijningsvormen verstaan waarbij de computer het *doel* is van strafbare gedragingen (bijvoorbeeld bij hacking en het verspreiden van computervirussen) als verschijningsvormen waarbij de computer als *middel* wordt gebruikt (bijvoorbeeld fraude, verspreiding van kinderpornografie, schendingen van het auteursrecht etc). Omdat ook andere technologieën kunnen worden ingezet om strafbare feiten te plegen, spreek men tegenwoordig ook wel van high-tech crime in plaats van computercriminaliteit.[67]

Ook Wiemans waagt zich aan het definiëren van computercriminaliteit. Wiemans onderscheidt een materieelrechtelijke benadering en een strafvorderlijke benadering van de definitie van computercriminaliteit. Wat betreft de materieelrechtelijke benadering sluit hij zich aan bij de vertaling van Kaspersen en Charbon van de defenitie die is opgesteld door de OECD (Organisation for Economic Co-operation & Development). Deze (vertaalde) definitie luidt: "Elk in Nederland begaan strafbaar feit, voor de uitvoering waarvan de geautomatiseerde verwerking en overdracht van gegevens van overwegende betekenis is." De strafvorderlijke definitie van computercriminaliteit volgens Wiemans luidt: "alle illegale handelingen waarvoor kennis van de informatietechniek nodig is om ze op te sporen of te vervolgen."[68] Het strafvorderlijke aspect van computercriminaliteit zal in deze scriptie overigens niet aan de orde komen.

Wet computercriminaliteit I

Is art. 138a ook te gebruiken om spywaremakers en verspreiders aan te pakken? Vereist is dat een persoon opzettelijk (en[69]) wederrechtelijk binnendringt in een geautomatiseerd werk voor de opslag of verwerking van gegevens, of een deel daarvan, indien hij:
a. daarbij enige beveiliging doorbreekt of
b. de toegang verwerft door een technische ingreep, met behulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid.
In de leden 2 en 3 van dit artikel zijn dan nog strafverzwarende omstandigheden vastgelegd. Lid 2 houdt in dat wanneer de dader gegevens die zijn opgeslagen in een geautomatiseerd werk waarin hij zich bevindt, overneemt en voor zichzelf of een ander vastlegt.
Lid 3 behandelt de tussenkomst van een openbaar telecommunicatienetwerk. Voorwaarden voor computervredebreuk zijn dan:
a. dat de dader met het oogmerk zich wederrechtelijk te bevoordelen gebruik maakt van de verwerkingscapaciteit van een geautomatiseerd werk;
b. dat de dader door tussenkomst van het geautomatiseerd werk waarin hij is binnengekomen de toegang verwerft tot het geautomatiseerd werk van een derde.

---

[67] E-Jure 2005
E-Jure, *Dossier computercriminaliteit*, WWW
<http://www.ejure.nl/f_dossier/language=nl/dossier_id=175/dossier.html>, (geraadpleegd 20 juli 2005)
[68] Wiemans 2004, p. 8-12.
[69] "en" is nog niet opgenomen in de huidige wetsbepaling, "en" is wel opgenomen in het wetsvoorstel computercriminaliteit II, maar men mag aannemen dat de opzet hier niet op "wederrechtelijk" ligt, maar op het feit en derhalve kan men "en" min of meer inlezen.

Spyware kan mijns inziens zeker onder dit artikel vallen. Vaak zullen gebruikers een anti-spywareprogramma op hun computer hebben. Wanneer spyware zich dan toch doorzet, ondanks dit programma, is er volgens mij sprake van het doorbreken van enige beveiliging. Men zou ook kunnen betogen dat spyware een vals signaal is. Vaak komt spyware immers mee met freeware en wordt het verpakt als iets anders. Doorgaans denkt de gebruiker dat hij iets anders binnenhaalt of de gebruiker denkt dat hij helemaal niets binnenhaalt, ook dan is er volgens mij sprake van een vals signaal. Het signaal is "niets", maar er komt immers spyware binnen.

Ook kunnen in sommige gevallen artikel 139b, tweede lid, artikel 139c, en artikel 139d worden toegepast bij het bestrijden van spyware. Deze Strafrechtbepalingen, die als achterliggende gedachte de bescherming van de persoonlijke levenssfeer hebben, verbieden onder bepaalde voorwaarden het aftappen of opnemen van gegevens zoals dat kan gebeuren met behulp van spyware. Minister Donner vindt ook dat art. 350a Sr. een rol kan spelen.[70] Artikel 350a Sr verbiedt het opzettelijk en wederrechtelijk veranderen, wissen en het onbruikbaar of ontoegankelijk maken van computergegevens dan wel het toevoegen van andere gegevens daaraan. Dit laatste zou men bijvoorbeeld bereiken door de gegevens die spyware heeft achterhaald te gebruiken. Aangezien ik spyware loskoppel van de acties die men onderneemt met de informatie die men met spyware heeft verzameld, zal ik hier in deze scriptie verder geen aandacht aan besteden.

Wet computercriminaliteit II

Hier zal ik alleen het in mijn ogen belangrijkste aspect van de Wet Computercriminaliteit II bespreken. Voor een meer uitgebreide bespreking verwijs ik naar hoofdstuk 5 van deze scriptie over toekomstige wet- en regelgeving met betrekking tot spyware. Immers de Wet computercriminaliteit II is nog steeds niet in werking getreden. Deze is inmiddels wel aanhangig gemaakt als het wetsvoorstel "Aanpassing aan het Cybercrimeverdrag". Op 15 maart 2005 werd het wetsvoorstel dat dateert uit 1998 in gewijzigde vorm verzonden naar de Tweede Kamer.[71]

In de wet Computercriminaliteit II worden enkele dingen gewijzigd aan art. 138a Sr. In mijn ogen is de belangrijkste wijziging dat de eisen die nu in sub a en b worden gesteld in lid 1 van het artikel verdwijnen. In de nieuwe bepaling worden er slechts nog voorbeelden genoemd van wat in ieder geval onder 138a valt, dit is geen uitputtende opsomming. Dit moet het nog makkelijker maken om spyware onder art. 138a te trekken. Wiemans had een dergelijke constructie al voorgesteld in zijn artikel in JAVI.[72]

---

[70] Ministerie van Justitie 2004
Ministerie van Justitie, *Kamervragen van het lid Gerkens (SP) aan de ministers van Justitie en van Economische Zaken over spyware,* WWW http://www.justitie.nl/pers/kamerstukken/include.asp?bestand=/extern/documentportal/Kamerantwoorden/20040817_A%202030416730%20spyware.doc.c>, publicatie augustus 2004.

[71] E Jure 2005
E-Jure, *Dossier wetsvoorstel computercriminaliteit II,* WWW < http://www.ejure.nl/articles/dossier_id=175/id=190/show.html>

[72] Wiemans 2004, p. 200.

4.1.3 Buitenlandse wet- en regelgeving op het gebied van computervredebreuk met betrekking tot spyware

EU/EG

In heel Europa is men gebonden aan het Cybercrimeverdrag. Zie: *Overige*

Verenigde staten

Computervredebreuk wordt zoals al eerder gezegd ook wel hacking genoemd. Hacking is in vele staten strafbaar gesteld. Ook bestaat er op federaal niveau de CFAA (oftewel: Computer Fraud and Abuse Act). In de Verenigde staten is men net zoals in Europa ook gebonden aan het Cybercrimeverdrag.

Overige

In november 2001 is het Cybercrimeverdrag van de Raad van Europa (ook wel Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken genoemd) in werking getreden toen 30 landen het ondertekenden.[73] In het Cybercrimeverdrag hebben de landen die zijn aangesloten bij de Raad van Europa afgesproken om tot een gemeenschappelijk beleid te komen met betrekking tot de bescherming van de samenleving tegen strafbare feiten verbonden met elektronische netwerken, vooral door het tot stand brengen van passende wetgeving en het versterken van de internationale samenwerking.[74] In het Cybercrimeverdrag is het artikel 2 dat over computerbreuk gaat, volgens Wiemans *noopt* dit artikel echter niet tot de nu voorgestelde wetswijziging, maar stelt het de landen in staat om aanvullende eisen op dit vlak te stellen.[75]

4.1.4 Handhaving van wet- en regelgeving op het gebied van computervredebreuk

Computervredebreuk valt in alle landen onder computercriminaliteit. Computercriminaliteit is in alle landen behalve een onderdeel van het ICT-recht een deel van het strafrecht. Handhaving van bepalingen omtrent computerbreuk zullen dan ook volgens het strafprocesrecht van het betreffende land verlopen.

Nederland

De opsporing van computervredebreuk ligt "gewoon" bij de politie. De politie en het KLPD (Korps Landelijke Politiediensten) worden daarbij geassisteerd door het National Hightech Crime Center (NHTCC) een projectorganisatie die ontstaan is op initiatief van het KLPD, het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het Ministerie van Justitie.[76] De strafrechter oordeelt over strafrechtbepalingen zoals art. 138a. Er is geen gespecialiseerde (straf)rechterlijke instantie waar vooral ICT-zaken worden afgehandeld.

EU/EG

Van een Europese strafrechter (bijvoorbeeld bij internationale gevallen) geen sprake. De Europese landen zullen anti-spywarewetgeving voorzover deze onder het strafrecht valt allemaal binnen hun eigen straf(proces)rechtelijk systeem berechten.

---

[73] Wiemans 2004, p.198.

[74] E-Jure 2005

E-Jure, *Dossier computercriminaliteit*, WWW <http://www.ejure.nl/exturls/dossier_id=175/id=92/show.html >, (geraadpleegd 20 augustus 2005)

[75] Wiemans 2004, p.200.

[76] National Hightech Crime Center

National Hightech Crime Centrer, WWW < http://www.nhtcc.nl/> (geraadpleegd 9 augustus 2005)

Verenigde Staten

De staten zullen de handhaving volgens hun eigen strafprocesrecht indelen en afhandelen.

4.2 Oneerlijke handelspraktijken

Wanneer het niet mogelijk is om spyware via privacywet- en regelgeving of computercriminaliteitbepalingen te bestrijden, grijpt men soms oneerlijke concurrentie aan om spyware te bestreden. Dit lijkt wat vergezocht, toch gebeurt dit vaker, bijvoorbeeld wanneer men auteursrechtinbreuken wil aanpakken. Immers de intentie van anti-spywarewet- en regelgeving moet mijns inziens de bescherming van de burger zijn. Deze intentie ziet men ook terug in zowel privacywet- en regelgeving als in computercriminaliteitwet- en regelgeving met betrekking tot spyware. Oneerlijke handelspraktijkenwetgeving wordt doorgaans gebruikt om bedrijven te beschermen tegen andere bedrijven. Toch zijn er situaties mogelijk waar men zich kan indenken dat deze wetgeving een rol kunnen spelen daar waar het om spyware gaat. Ik denk dat het dan wel om uitzonderlijke situaties gaat waar één bedrijf spyware inzet duidelijk gericht op zijn concurrenten, bijvoorbeeld op het computernetwerk van zijn concurrent om vertrouwelijke informatie van die concurrent te verkrijgen. Ik vind dat het ver gaat om oneerlijke concurrentiebepalingen te gebruiken wanneer de spyware louter op consumenten of cliënten van het bedrijf dat de spyware inzet is gericht. Uiteraard kunnen gegevens die de spyware aanlevert een voordeel op de concurrent opleveren, maar het lijkt me hier logischer om hier andere wet- en regelgeving te gebruiken, bijvoorbeeld op het gebied van computercriminaliteit of privacy.

In de Verenigde staten heeft een rechter in Maryland echter al eens beslist dat oneerlijke handelspraktijkenwetgeving zeker een basis kan bieden om "spyware" [77] te bestrijden. In de zaak FTC (ook wel: Federal Trade Commission) vs. D Squared Solutions werd de laatste schuldig geacht aan oneerlijke handelspraktijken. Het ging in die zaak voornamelijk om de overlast die de "spyware" opleverde voor gebruikers[78] Ook een andere zaak in de Verenigde staten trok op dit punt de aandacht, het ging hier om het zonder toestemming weigeren van homepages van internetgebruikers, wederom ben ik van mening dat het hier echter niet om spyware gaat, maar om een vorm van malware, daarom zal ik de zaak niet behandelen.[79]

In Nederland wordt de wet- en regelgeving omtrent oneerlijke handelspraktijken gehandhaafd door de NMa (Nederlands Mededingingsautoriteit)[80].

In Nederland zijn nog geen rechterlijke uitspraken met betrekking tot spyware, dus ook niet op basis van oneerlijke handelspraktijken. Wellicht biedt onze wet en de Europese wet- en regelgeving daar wel mogelijkheden toe in de toekomst. De Europese richtlijn oneerlijke handelspraktijken die is opgesteld om bij te dragen aan de goede werking van de interne markt en om een hoog niveau van

---

[77] Er lijkt hier echter geen sprake te zijn van spyware zoals door mij gedefinieerd. Er lijkt eerder sprake te zijn van malware, zie 1.1 De Schrijver en Schraeyen vatten deze vorm van overlast echter wel onder spyware.

[78] De Schrijver en Schraeyen 2005, p. 6

[79] FTC vs. MailWiper

[80] NMa

NMa, *Nederlandse Mededinginsautoriteit,* WWW <http://www.nmanet.nl/nederlands/home/index.asp> (geraadpleegd 18 augustus 2005)

consumentenbescherming tot stand te brengen door de wettelijke en bestuursrechtelijke bepalingen van de lidstaten inzake oneerlijke handelspraktijken die de economische belangen van de consumenten schaden, te harmoniseren[81], biedt wellicht een basis voor een dergelijke uitspraak.

De werkelijke waarde van oneerlijke handelspraktijkenwetgeving bij de bestrijding van spyware moet nog blijken. Het lijkt mij echter dat deze wetgeving alleen aan bod komt als noodgreep of om moeilijkheden uit privacy of computercriminaliteitwetgeving te omzeilen. Oneerlijke handelspraktijkenwetgeving is wat mij betreft niet de meest logische en effectieve wijze om spyware te bestrijden. Voor bepaalde andere vormen van malware ligt dit wellicht anders.

[81] Richtlijn nr. 2005/29/EG (*PbEG* L149/23)

Hoofdstuk 5: Toekomstige wet- en regelgeving met betrekking tot spyware

Inmiddels hebben we kunnen waarnemen dat de bestrijding van spyware niet via één lijn verloopt daar waar het wetgeving betreft.

5.1 Nederlandse initiatieven

Gezien de media-aandacht voor spyware heeft spyware wellicht ook de aandacht getrokken van Den Haag en kunnen we binnenkort nieuwe regelgeving verwachten…

5.1.1 Kamervragen

Op 29 juni 2004 werden door Ada Gerkens kamervragen gesteld over spyware. Gerkens stelde deze vragen aan de Minister van Justitie en de Minister van Economische Zaken. Op 17 augustus 2004 antwoorde Donner (Minister van Justitie), ook namens zijn collega van Economische Zaken op de vragen van het SP-kamerlid.

Het probleem spyware

Op de vragen wat de mening van de minister was over de sterk gegroeide spyware-infecties en over de nieuwsberichten dat één derde van de computers besmet zou zijn met spyware, antwoordde de minister slechts dat hij dit een ongewenste ontwikkeling vond.

Websites sluiten of betere voorlichting?

Op de vraag wat zijn mening was over methodes om spyware te bestrijden door websites die spyware verspreiden te sluiten en door betere voorlichting antwoordde hij dat het afsluiten van websites geen effectief middel is. Ook benadrukt hij dat het vaak praktisch onmogelijk is omdat websites vanuit andere landen dan Nederland worden geëxploiteerd. Een wettelijke regeling op dit punt ziet Donner dan ook niet zitten. Met betrekking tot de voorlichting is hij niet van plan om meer te investeren. Hij wijst op de voorlichting op internet zelf en in computertijdschriften. Tevens wijst hij mevrouw Gerkens op de campagne Surf op Safe (een initiatief van het Ministerie van Economische Zaken).[82] De burgers moeten de informatie zelf maar vinden want deze is reeds voorhanden, daar lijkt het op neer te komen.

Nieuwe wet- en regelgeving op het gebied van spyware?

Mevrouw Gerkens vraagt vervolgens of er een mogelijkheid is dat de Minister een wetsvoorstel indient, dat net zoals de Spy Act in de Verenigde staten er op neer komt dat consumenten vooraf toestemming moeten geven voor een (computer)programma informatie over hen mag verzamelen en/of door sturen. Tevens vraagt ze de Minister zich op Europees niveau hard te maken voor een dergelijk wetsvoorstel. De minister acht wet- en regelgeving echter al in voldoende mate aanwezig zowel op nationaal als Europees niveau. Hij verwijst uitdrukkelijk naar artikel 4.1 lid 1 van het Besluit universele dienstverlening en eindgebruikersbelangen.[83] Op Europees niveau noemt hij de richtlijn 2002/58 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie.

---

[82] Opmerkelijk is dat de Waarschuwingsdienst (meer hierover in 2.2) niet wordt genoemd. De Waarschuwingsdienst licht burgers in over internet en de gevaren daarvan en is tevens een initiatief van het Ministerie van Economische Zaken.

[83] Zie 3.2.3 en 3.4.1.

Tevens geeft de Minister aan dat spyware in bepaalde gevallen onder het strafrecht kan vallen. Hij noemt als voorbeeld artikel 138a van het Wetboek van strafrecht, oftewel computervredebreuk. Ook kunnen volgens hem in sommige gevallen artikel 139b, tweede lid, artikel 139c, en artikel 139d worden toegepast. Deze Strafrechtbepalingen verbieden onder bepaalde voorwaarden het aftappen of opnemen van gegevens zoals dat gebeurt met behulp van spyware. Artikel 350a Sr verbiedt het opzettelijk en wederrechtelijk veranderen, wissen en het onbruikbaar of ontoegankelijk maken van computergegevens dan wel het toevoegen van andere gegevens daaraan.[84] Minister Donner geeft aan dat de toepasselijke bepalingen uit het Wetboek van strafrecht in het kader van de komende goedkeuring van het Cybercrimeverdrag worden gewijzigd en aangevuld waar dat nodig is, waarbij onder meer als strafbaar feit zal worden voorgesteld de verspreiding van apparaten of technische middelen -waaronder computerprogramma's zoals spyware- met het oogmerk dat daarmee een computerdelict wordt begaan. Aangezien genoemde bepalingen onderdeel vormen van het Cybercrimeverdrag zal in de nabije toekomst ook kunnen worden opgetreden tegen buitenlandse aanbieders die zich op het grondgebied van de verdragsstaten bevinden. Toch bestaat er veel discussie over het voornemen om de verspreiding van apparaten en technische middelen – waaronder computerprogramma's zoals spyware- met het oogmerk dat daarmee een computerdelict wordt begaan.

Verder noemt hij wederom de eigen verantwoordelijkheid van gebruikers om (technische) maatregelen te nemen.[85]

Conclusie

Het ziet er dus niet naar uit dat we verrassende nieuwe maatregelen kunnen verwachten op het gebied van spyware. Minister Donner zorgt gewoon dat Nederland aan haar internationale verplichtingen voldoet (qua invoering regelgeving bijvoorbeeld op basis van Europese richtlijnen), maar meer lijken we niet te kunnen verwachten.

5.1.2 Wet computercriminaliteit II

Computervredebreuk

De Wet computercriminaliteit brengt een wijziging van het Wetboek van strafrecht mee. Het is de langverwachte aanvulling van de al in 1993 in werking getreden Wet computercriminaliteit I. Het wetsvoorstel dat al onderweg is sinds 1999 ligt nu eindelijk bij de tweede kamer.[86] Het wetsvoorstel bevat ook een aanpassing van de bepaling over computervredebreuk. Computervredebreuk kan men gebruiken om spyware aan te pakken, vandaar dat de Wet computercriminaliteit II belangrijk is om hier te behandelen. Vaak wordt in de literatuur aangegeven dat het Cybercrimeverdrag de wetgever verplicht stelde op art. 138a Sr te wijzigen. Wiemans is het hier niet mee eens. Volgens hem biedt het cybercrimeverdrag mogelijkheden om de

---

[84] Zie 4.1.2.

[85] Ministerie van Justitie 2004
Ministerie van Justitie, *Kamervragen van het lid Gerkens (SP) aan de ministers van Justitie en van Economische Zaken over spyware,* WWW
http://www.justitie.nl/pers/kamerstukken/include.asp?bestand=/extern/documentportal/Kamerantwoorden/20040817_A%202030416730%20spyware.doc.c>, publicatie augustus 2004.

[86] E-Jure 2005
E-Jure, *Dossier wetsvoorstel computercriminaliteit II,* WWW <
http://www.ejure.nl/f_dossier/language=nl/dossier_id=265/dossier.html>, (geraadpleegd 20 juli 2005)

strafbepaling te wijzigen maar brengt zij geen verplichting met zich mee. Die verplichting kan volgens Wiemans wel worden gevonden in art. 2 van het Kaderbesluit van de Raad van Europa inzake Aanvallen op informatiesystemen. Dit kaderbesluit is op 24 februari 2005 aangenomen.[87]

In de wet Computercriminaliteit worden enkele dingen gewijzigd aan art. 138a Sr. Zo verdwijnen de eisen die nu in sub a en b worden gesteld in lid 1 van het artikel. Dit moet het nog makkelijker maken om spyware onder art. 138a Sr te trekken. Voorheen werd er wel gezegd dat spyware door deze vereisten (het doorbreken van enige beveiliging of een technische ingreep, met behulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid) niet onder art. 138a Sr viel. Nu deze vereisten er niet meer zijn wordt het makkelijker om feiten onder de delictsbeschrijving van art. 138a Sr te brengen. Er worden geen vereisten meer gesteld aan het doel van het binnendringen in een geautomatiseerd werk. Tevens wordt het woordje "en" toegevoegd aan lid 1 (tussen opzettelijk en wederrechtelijk).[88] Ook de maximumstraf is verhoogd. Deze is van 6 maanden en een geldboete van derde categorie gegaan naar één jaar en een geldboete van de vierde categorie. Lid 2 e 3 van art. 138a Sr heeft men gelaten zoals zij waren.[89]

Computerspionage

Computerspionage, kan betrekking hebben op bedrijfsgeheimen en staatsgeheimen. In de praktijk zal het waarschijnlijk niet zo vaak voorkomen dat spyware zich op deze geheimen richt. Over het algemeen wordt spyware ingezet om consumentengedrag, consumentengegevens en consumentenvoorkeuren bloot te leggen. Om deze reden zal ik hier niet heel uitgebreid op computerspionage ingaan.

Wiemans ziet er wel iets in een anti-spywarebepaling op cybercrimegebied. Hij wil dat de wetgever het verboden stelt om opzettelijk, wederrechtelijk van afstand systeemfuncties uit te voeren, zoals spyware dat doet.[90]

De Wet computercriminaliteit II biedt een dergelijke bepaling nog niet, maar spyware kan onder het mom van computervredebreuk of computerspionage toch worden aangepakt. Bovendien, wie weet staat er in de volgende Wet Computercriminaliteit wel een dergelijke bepaling.

---

[87] Europees Bureau Eerste Kamer 2005
Europees Bureau *Eerste Kamer, Kaderbesluit over aanvallen op informatiesystemen*, WWW <http://www.europapoort.nl/9345000/1f/j9vvgy6i0ydh7th/vg5fcc4jpyqn> (geraadpleegd 9 augustus 2005)

[88] Koops, de Roos & Van Dijk 2004, p.35.

[89] Ejure 2005
Ejure, *wijzigingen cc II in strafrecht*, WWW <http://www.ejure.nl/downloads/language=nl/id=303/show.html> publicatie 25 juli 2005

[90] TROS Radar 2004
TROS Radar, *Justitie kansloos tegen spionagesoftware*, WWW <http://www2.trosradar.nl/?url=PHP/news/28/830/dossier> publicatie 23 november 2004

5.2 Buitenlandse initiatieven

EU/EG

Hoewel er wel op aan wordt gedrongen is er nog geen specifieke anti-spywarewet- en regelgeving. Men gaat er veelal vanuit dat de huidige wet- en regelgeving voldoet. Uiteraard speelt ook het Cybercrimeverdrag hier een rol. Hoewel dit strikt genomen geen Europese wet- of regelgeving is zijn de Europese lidstaten wel allemaal gebonden aan dit verdrag. Het is zelfs een Europees initiatief (initiatief van de Raad van Europa).

Verenigde staten

Er is anti-spywarewetgeving in de maak in diverse staten. De Spy Act (Securely Protect Yourself Against Cyber Tresspass Act) wil spyware op federal niveau aan banden leggen, dat geldt ook voor de Internet Spyware Prevention Act. Deze wet zou de CFAA (Computer Fraud and Abuse Act) wijzigen.

De Spy Act vereist dat de spywareleverancier de gebruiker informeert omtrent de spyware, maar ook dat deze zijn naam, adres en e-mailadres aan de gebruiker bekend maakt in de gebruikersovereenkomst. Directe acties op grond van niet naleving van deze bepalingen worden niet bestreken door de Spy Act.

De Internet Spyware Prevention Act zou wel in die strafsancties voorzien., dit zou moeten gebeuren via het Ministerie van Justitie en via de deelstaten. De Schrijver en Schraeyen geven aan uit diverse bronnen te hebben vernomen dat de voorstellen waarschijnlijk zullen worden samengevoegd.[91]

[91] De Schrijver en Schraeyen 2005, p. 7.

Hoofdstuk 6: Diverse meningen over spyware

Voor dit hoofdstuk heb ik diverse experts geïnterviewd. Hen is gevraagd naar hun mening over spyware, privacy op in internet, de huidige aanpak van spyware en de toekomst van deze aanpak.

6.1 Christiaan Alberdingk Thijm

Mr. Christiaan Alberdingk Thijm is advocaat bij SOLV advocaten in Amsterdam, tevens is hij één van de oprichters van dit kantoor dat gespecialiseerd is in technologie, media en communicatie. Hij is gespecialiseerd in auteursrecht, databankenrecht, merkenrecht, privacy, vrijheid van meningsuiting en e-commerce. Dit alles met name in de context van het internet.
Alberdingk Thijm is ook docent auteurs- en informatierecht aan de Hogeschool van Amsterdam. Verder geeft hij regelmatig lezingen en cursussen, onder meer aan advocaten en rechters.
Alberdingk Thijm publiceert regelmatig over de juridische aspecten van internet[92] *Het gesprek met dhr. Alberdingk Thijm vond plaats op17 augustus 2005.*

Het risico en de gevaren van spyware

Alberdingk Thijm ziet spyware wel als een gevaar, maar voornamelijk een gevaar voor de (eind)gebruiker. SPAM en virussen bedreigen het internet (en de internetcommunicatie) als geheel, spyware doet dat niet.

Oplossingen/manieren van bestrijden

Een juridische definitie van spyware is nog niet aanwezig. Dit maakt het moeilijk de omvang van wet- en regelgeving met betrekking tot spyware vast te stellen, het is niet geheel duidelijk welke regels betrekking hebben op spyware.

Het (beter) reguleren van informatieverplichtingen en toestemmingsbepaling (bijvoorbeeld opt-in/opt-out) vindt Alberdingk Thijm, kan een bijdrage leveren in het terugbrengen van spyware.

De oplossing ligt niet alleen in wetgeving, deze kan waarschijnlijk eerder worden gezocht in de techniek. Met betrekking tot de techniek moeten we wel oppassen. De belangen van de makers van anti-spywareprogramma's kunnen conflicteren met het doel om spyware (die zonder toestemming is geïnstalleerd) te verwijderen. De programma's kunnen bijvoorbeeld een programma van een concurrerende softwaremaker, dat met toestemming is geïnstalleerd, wel als spyware aanmerken en verwijderen, terwijl ze "eigen" programma's die zonder toestemming zijn geïnstalleerd niet detecteren en verwijderen. Onder toestemming verstaat Alberdingk Thijm: een vrije, specifieke, en op basis van volledige informatie berustende wilsuiting.

Bewustwording is erg belangrijk, de consumentenbond en andere consumentenorganisaties zouden daar een belangrijke rol in kunnen spelen. Er is op dat vlak ook wel een rol voor de overheid. Hoe groot die rol moet zijn is een politieke vraag waar Alberdingk Thijm zich niet over uit laat.

---

[92] SOLV (Christaan Alberdink Thijm)
SOLV, *Christiaan Alberdink Thijm,* WWW <http://www.solv.nl/Mensen-2.pagina?m=3&lang=nl> (geraadpleegd 9 augustus 2005)

Regelgeving

Spyware is meer dan SPAM een privacyprobleem, de meest voor de hand liggende manier van juridisch bestrijden is dan ook via de privacywetgeving. Maar ook de strafrechtbepalingen, oneerlijke handelspraktijken- en telecomwetgeving moeten we natuurlijk niet vergeten. Ook onrechtmatige daad biedt wellicht mogelijkheden. Wel moet goed worden gekeken naar de doeleinden van de regeling. Wie of wat beoogt de regeling te beschermen? Ook moeten we ons afvragen of we het strafrecht (zwaar middel) wel moeten inzetten, wellicht is het beter om eerst op een lager niveau spyware(makers/verspreiders) aan te pakken.

Tevens moet men oppassen met te specifiek willen reguleren wanneer men nieuwe regels opstelt, het gevaar dat het net zo afloopt als met de regulering van SPAM (die door Alberdingk Thijm wordt bekritiseerd vanwege de gevolgen voor mensen zonder kwade bedoelingen) ligt op de loer. Voorlopig is het een goed idee om eerst te proberen te roeien met de riemen die we hebben. Overhaaste wetgeving moet worden voorkomen, zie wederom de SPAM-wetgeving.

Handhaving en opsporing

Alberdingk Thijm geeft aan dat handhaving een probleem is. Tevens geeft hij aan dat het vanuit het oogpunt van het internationale karakter van het internet het ook niet heel zinvol is om in Nederland allerlei bepalingen te maken (met betrekking tot spyware) als er in het buitenland niets gebeurd qua regelgeving op dat vlak. Wellicht dat Nederland dan een voorbeeldfunctie zou kunnen vervullen, maar effectief helpt het de handhavingsmogelijkheden weinig. Vergelijk het bijvoorbeeld met de regelgeving rond SPAM.

6.2 Anton Ekker

Mr. Anton Ekker is als onderzoeker verbonden aan het IViR (Instituut voor informatierecht). Momenteel werkt hij als projectonderzoeker aan een proefschrift over Anonimiteit en Uitingsvrijheid.
Ekker studeerde Nederlands Recht aan de Universiteit van Amsterdam.
Ekker publiceert regelmatig over de juridische aspecten van internet, met name over privacygerelateerde zaken.[93] *Het gesprek met dhr. Ekker vond plaats op 12 juli 2005.*

Allereerst benadrukt dhr. Ekker dat hij geen techneut is maar een jurist.

Het risico en de gevaren van Spyware

Ekker ziet spyware als een probleem dat voortvloeit uit de techniek. Het inschatten van het gevaar van spyware vindt hij moeilijk. Spyware bedreigt de privacy van computergebruikers. Dat is wat hem betreft belangrijker dan het nauwkeurig onderscheiden van spyware van andere problemen zoals phishing, pharming, SPAM en computervirussen. Oftewel spyware maakt deel uit van een groter probleem en staat niet op zichzelf.

Oplossingen/manieren van bestrijden

De oplossing van spyware is volgens Ekker niet eenduidig. De oplossing is veelal technisch, bijvoorbeeld door software. Ekker haalt hier Lassik aan (regulering door middel van software) en benadrukt dat software zelf ook de kracht heeft te

---

[93] IViR (Anton Ekker)
IViR, *Anton Ekker,* WWW <http://www.ivir.nl/medewerkers/ekker.html> (geraadpleegd 9 augustus 2005)

normeren. Ook een verbetering van de archituur van het internet zou de problemen rond spyware wellicht kunnen verlichten.

Regelgeving

Over de rol van regelgeving bij het oplossen van het probleem spyware zegt hij: "Spyware is juridisch gezien niet op te lossen zeker niet op korte termijn."

Ekker geeft aan dat de virtuele wereld anders is dan de reële wereld en in bepaalde gevallen specifieke regelgeving behoeft. Als we in dat verband naar de Wbp kijken, zien we dat de Wbp een zeer algemene wet, met veel vage termen is die wellicht niet specifiek genoeg is. Aan de andere kant brengt dit ook een voordeel met zich mee, namelijk dat de Wbp techniekonafhankelijk is. Dit voorkomt dat regelgeving achter de feiten aanloopt wanneer er veel technische ontwikkelingen plaatshebben. Spyware zou men met behulp van de Wbp kunnen aanpakken, een mooie oplossing vindt Ekker dat niet.

Hij legt nadruk op de strafrechtelijke mogelijkheden om spyware aan te pakken omdat deze wellicht het meet effectief zouden kunnen zijn. Wanneer de bepaling met betrekking tot computervredebreuk ter sprake komt trekt hij de analogie met de reële wereld en het plaatsen van afluisterapparatuur in de reële wereld.

De bepaling 4.1 Besluit universele dienstverleners en eindgebruikersbelangen.[94] hij helder gesteld. Wel vindt hij dat er wellicht in de toekomst ruimte is op een dergelijke bepaling in het Wetboek van strafrecht op te nemen vanwege de mogelijkheden tot handhaving. Ook de Telecommunicatiewet leent zich voor (meer specifieke) anti-spywarebepalingen.

Handhaving en opsporing

Ekker benadrukt ook dat hij problemen rond de handhaving van regelgeving met betrekking tot spyware ziet.

6.3 Jaap Henk Hoepman

Dr. Jaap Henk Hoepman is als senior-onderzoeker "security en cryptografie" verbonden aan de Radboud Universiteit Nijmegen.
Voorheen was hij als docent verbonden aan de Universiteit van Twente.
In 1996 promoveerde hij aan de Universiteit van Amsterdam.[95]
Hoepman publiceert regelmatig. Het gesprek met dhr. Hoepman vond plaats op 14 juli 2005.

Dhr. Hoepman benadrukt dat hij geen jurist is maar meer technicus.

Het risico en de gevaren van Spyware

Het risico van spyware is moeilijk in te schatten aangezien spyware veelal niet zichtbaar is. De risico's liggen vaak in de applicaties, bijvoorbeeld bij telebankieren. De makers van telebankieren zijn dan ook de aangewezen personen om deze risico's te bestrijden, zoals dat nu reeds gebeurt.

---

[94] Zie 3.2.3.

[95] Radboud Universiteit (Jaap Henk Hoepman)
Radboud Universiteit, *Jaap Henk Hoepman,* WWW < http://www.cs.ru.nl/~jhh/about.html> (geraadpleegd 9 augustus 2005)

Hoepman benadrukt dat spyware een onderdeel is van een groter probleem namelijk malware. Alleen spyware bestrijden zou dan ook zinloos zijn, aangezien het probleem veel breder is. De definitie van malware die Hoepman hanteert, luidt als volgt: Malware is alle software die zonder expliciete toestemming van de gebruiker op de computer van de gebruiker wordt geïnstalleerd die tot doel heeft de functie van de computer in het nadeel van de gebruiker en/of in het voordeel van de maker van de malware te veranderen.[96]

Vaak wordt beweerd dat één van de gevaren van spyware is dat het computers vertraagd en zodoende veel verlies van tijd (en geld) veroorzaakt. Over het algemeen vertraagt spyware computers niet aldus Hoepman, dat is een misverstand, ook lang niet alle malware vertraagt computers.

Oplossingen/manieren van bestrijden

Er zijn volgens Hoepman diverse oplossingen/manieren om spyware te bestrijden.
Code-signing (Alleen software installeren van betrouwbare bronnen)
Trusted Computing Platform (TCPA) (TCPA zorg voor controle over wat wel draait en wat niet op een computer en kan ook de toegang tot bijvoorbeeld bepaalde documenten regelen.)
(technisch)
Bewustwording
(niet technisch)
Samenhang tussen de technische en de niet-technische oplossingen/manieren van spywarebestrijding is zeer belangrijk. Wanneer men zich niet bewust is van het gevaar van spyware en de mogelijkheden die men zou kunnen nemen komt men nooit bij code-signing en TCPA uit.

De meeste spyware komt met freeware mee. Mensen moeten zich bewuster gedragen met betrekking tot freeware, dan kan kunnen een hoop spywareproblemen voorkomen worden. Tevens moeten mensen hun browsers beter instellen. Ook de aanschaf van "betere" software (in plaats van freeware met onbekende herkomst bijvoorbeeld) kan helpen voorkomen dat spyware op de computer van de gebruikers komt. Ook zouden gebruikers zich bewust moeten worden van en moeten investeren in het veilig maken van systemen, netwerken en browsers.

Bewustwording is zeer belangrijk het is de enige manier om op dit vlak iets te bereiken. De bewustwording is niet zo zeer een taak voor de overheid. Meer voor bedrijven die schade ondervinden of voor opvoeders en onderwijsinstellingen. Hoepman ziet wel een rol voor de overheid met betrekking tot de groep die zelf geen onderwijs heeft gekregen op dit punt maar wel actief gebruik maakt van internet (bijvoorbeeld senioren of werkenden die geen onderricht krijgen met betrekking tot computers omdat ze er niet mee werken).

Overheidscampagnes zoals Surf op safe vindt hij te algemeen, ze dragen niet echt bij tot bewustwording bij het grote publiek. Op een gegeven moment worden mensen immuun voor dit soort campagnes.

---

[96] Zie 1.1.

Uiteraard vormt spyware ook een internationaal probleem, maar volgens Hoepman is het probleem nog niet groot genoeg voor een grote internationale regelgevingsoperatie.

Open source kan wat betreft Hoepman geen echte bijdrage leveren bij de bestrijding van spyware. Wel erkent hij dat open source wel kan voorkomen dat spyware zich ongezien in software verbergt. Ook zouden patches sneller kunnen worden ontwikkeld dan in de closed Source wereld.

Regelgeving

Waar de juridische wereld niet overeen komt met de realiteit is dat de fout van de juridische wereld. De juridische wereld moet immers de codificatie zijn van de realiteit. Virtueel vs. Reëel.

Regelgeving lijkt volgens Hoepman niet de oplossing voor spyware. Vergelijk het maar eens met SPAM, ook op dat gebied bestaat inmiddels in Nederland regelgeving, maar in de praktijk helpt het maar weinig.

Hoepman haalt wel de Wet computercriminaliteit aan en meer specifiek de bepaling over computervredebreuk; bij het bestraffen van het maken en gebruiken van spyware en malware zou men moeten kijken naar de analogie met huisvredebreuk. Wanneer straks in de Wet computercriminaliteit II (onder andere) de eis om een beveiliging te doorbreken verdwijnt uit de delictsbeschrijving van computervredebreuk wordt het makkelijker om spyware hieronder te brengen. Hoepman geeft wel aan dat spyware nu volgens hem wel degelijk al strafbaar is, maar dat het met de komst van de Wet computercriminaliteit II wel makkelijker wordt. Volgens Hoepman kan het strafrecht een rol spelen bij de juridische bestrijding van spyware.

De vraag of er misschien toch ruimte is voor *nieuwe* wet- en regelgeving om bijvoorbeeld meer duidelijkheid te bieden dan de huidige wet- en regelgeving, vindt hij moeilijk om te beantwoorden omdat hij geen exact inzicht heeft in de duidelijkheid van de huidige wet- en regelgeving.

Hij is wel van mening dat er in de huidige wetgeving veel onduidelijk is. Wat is een persoonsgegeven is, is volgens Hoepman, die hoewel hij geen jurist is zeer goed op de hoogte is van wet- en regelgeving rond ICT, zeer onduidelijk. Wanneer is een gegeven herleidbaar (tot een natuurlijk) persoon (criterium van de Wbp met betrekking tot "persoonsgegeven"). Is een IP-nummer, een creditcardnummer, surfgedrag of een password een persoonsgegeven. Omstandigheden van het geval lijken belangrijk. Wellicht moet de definitie van persoonsgegeven worden opgerekt of moet er een alternatieve definitie komen van persoonsgegeven meer gericht op de virtuele wereld, die definitie zou dan kunnen bestaan naast de huidige definitie van persoonsgegeven.

Handhaving en opsporing

Het heeft geen zin om regels op te stellen die men niet kan handhaven. Dus er moeten dan serieuze maatregelen worden genomen en resources worden vrijgemaakt om echt te kunnen handhaven. Op de vraag hoe dit moet geschieden heeft Hoepman geen antwoord.

Problemen en nieuwe vragen

Wie is de verspreider/computervredebreukmaker? De maker, de opdrachtgever, degene die per ongeluk verspreid? Een analogie met KaZaA (KaZaA wordt voor meerdere doeleinden gemaakt en de makers blijven derhalve buiten schot) is niet mogelijk. Spyware wordt met één purpose gemaakt, KaZaA kan voor meerdere doeleinden te worden gebruikt.

In beperkte mate eens met de stelling wat offline geldt, moet ook online gelden, maar hij erkent wel dat de virtuele wereld soms zulke afwijkende situaties kan meebrengen dat nieuwe specifieke regelgeving wel is vereist.

Hoofdstuk 7: Conclusie

Centraal in deze scriptie stond de hoofdvraag: "Spyware, juridisch bestrijden of praktisch oplossen?" Met de experts concludeer ik dat de oplossing voor spyware voorzover schadelijk niet eenduidig is, er is niet één juiste manier van bestrijden. Wel is bewustwording in alle gevallen van belang, wanneer men zich niet bewust is van een probleem, kan men het immers ook niet bestrijden. Dit geldt zowel voor bewustwording op het technische als op het juridische vlak.

Het is belangrijk om vast te stellen dat spyware deel uit maakt van een breder probleem, namelijk malware. Tevens is het belangrijk dat spyware een relatief beperkt begrip is dat niet overeenkomt met de definities die men over het algemeen in de media vindt. Dit heeft vooral te maken met het doel van die berichten in de media. Dat doel is namelijk het waarschuwen van consumenten en gebruikers. Deze mensen moeten zo breed mogelijk worden ingelicht en dan doen (jurdisch) sluitende definities er niet echt toe.

Er zijn zeker mogelijkheden om spyware op technische wijze te bestrijden. Oplossingen kunnen worden gezocht in anti-spywareprogramma's/anti-intrusion, open source, betere systemen, betere beveiligingen en encryptie. Wel is hiervoor erg belangrijk dat consumenten en gebruikers zich bewust zijn van het feit dat spyware gevaarlijk kan zijn. Deze bewustwording kan plaatsvinden door het raadplegen van de vele media op dit gebied. De overheid probeert de consumenten en gebruikers ook enigszins actief bewust te maken van de gevaren van internet, waaronder spyware.

De privacywetgeving kan veelal worden gebruikt om spyware te bestrijden. Wel interessant zijn de handhavingsmogelijkheden op dit gebied. Het College bescherming persoonsgegevens kan wel bestuursdwang uitoefenen, bestuurlijke boeten opleggen en last onder dwangsom opleggen, maar of dit echt helpt is nog maar de vraag. Bovendien vormt de opsporing een probleem omdat spyware slecht zichtbaar is. Ook het internationale aspect van spyware maakt het er niet makkelijker op zowel wat betreft opsporing als handhaving. In de praktijk blijkt de strafrechter nauwelijks gebruik te maken van de bevoegdheid die hem op grond van de Wbp toe komt.

Andere wetgevingsgebieden bieden ook mogelijkheden om spyware aan te pakken. Vooral het strafrechtelijk gebied is erg interessant. De bepaling die gebruikers beschermt tegen computervredebreuk springt dan direct in het oog, spyware kan goed onder deze delictsomschrijving worden gebracht. Tevens wordt in diverse landen gebruik gemaakt van oneerlijke handelspraktijkenwetgeving om spyware te bestrijden. Dit vind ik zelf wat vergezocht. Bovendien gaat het daar vaak om zaken die ik niet als spyware zou beschouwen. Ook hier geldt overigens dat de opsporing een probleem blijft vanwege de slechte zichtbaarheid van spyware en dat het internationale aspect de opsporing en handhaving ook nog eens bemoeilijkt.

Op spyware toegespitste wettelijke bepalingen zitten er waarschijnlijk voorlopig niet in. Minister Donner lijkt erg tevreden met de huidige regels en vind dat deze genoeg

waarborgen bieden tegen spyware. Hij benadrukt de eigen verantwoordelijkheid van gebruikers.

De experts verschillen op een aantal punten van mening, maar zijn het op veel punten ook met elkaar eens. Zij zijn het eens over het feit dat de oplossing voor spyware niet eenduidig is. Regelgeving kan zeker bijdragen aan bestrijding van spyware, maar is niet de enige oplossing. De techniek kan een zeer belangrijke rol spelen bij het bestrijden van spyware. Naar zowel regelgeving als techniek moet kritisch worden gekeken.

Persoonlijk vind ik de huidige wetgeving niet echt een oplossing die de schoonheidsprijs verdient, de wetgeving is op dit moment zeer verspreid (een euvel dat overigens ook moeilijk te verhelpen is vanwege de aard van het probleem) en betrekkelijk vaag. De huidige wet- en regelgeving laat producenten en opdrachtgevers van spyware in mijn ogen veel ruimte. Minister Donner is zich wel bewust van de problemen rond spyware, maar hij wil geen nieuwe spywarewetgeving maken, omdat hij vindt dat de huidige wetgeving voldoende mogelijkheden biedt. Wellicht is daadwerkelijk het geval, dat zal de toekomst nog moeten uitwijzen, echte spywarerechtszaken hebben tot op heden nog niet plaatsgevonden. Ik denk wel dat er wel ruimte is voor nieuwe wetgeving rond spyware. Toch ben ik met Alberdingk Thijm eens dat bij de invoering van nieuwe wet- en regelgeving *zeer* kritisch moet worden gekeken naar die regelgeving en de toegevoegde waarde daarvan. Met nieuwe "slechte" regelgeving is niemand geholpen. Bovendien is spyware maar een klein deel van een groot probleem (malware), iets dat bij eventuele nieuwe regelgeving ook goed in het oog moet worden gehouden.

Mijns inziens zal wetgeving, hoe perfect dan ook, nooit een volledige oplossing kunnen bieden voor dit door de techniek in het leven geroepen probleem. Wat betreft spyware zal er ook altijd behoefte blijven aan technische bestrijdingsmiddelen, al was het alleen maar omdat technische bestrijdingsmiddelen zich sneller (mee-)ontwikkelen dan wet- en regelgeving en de internationale aspecten van spyware. Het is wel belangrijk dat gebruikers zich bewust zijn van de gevaren van spyware en ook daadwerkelijk een technisch bestrijdingsmiddel toepassen. Voor mij is overigens ook duidelijk dat het internet en alle internetgerelateerde problemen wel regelgeving behoeven. De techniek kan niet alles oplossen, zonder regels wordt internet een onveilige en onprettige omgeving.

Daarom blijft de bestrijding van spyware wat mij betreft een samenspel tussen alle mogelijkheden die techniek ons biedt en wet- en regelgeving. Wat de perfecte balans tussen die twee is zal de toekomst moeten uitwijzen.

Literatuurlijst

Akkermans, Bax en Verhey 1999
P.W.C. Akkermans, C.J. Bax, L.F.M. Verhey, *Grondrechten, Grondrechten en grondrechtsbescherming in Nederland*, Deventer: W.E.J. Tjeenk Willink 1999.

Alberdingk Thijm 2004
C. Alberdingk Thijm, *Het nieuwe informatierecht, Nieuwe regels voor het internet*, Den Haag: Academic Service 2004.

Asscher 2002
L.F. Asscher, *Communicatiegrondrechten, Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving*, Amsterdam: Otto Cramwinckel Uitgever 2002.

Van Bruggen, Van Dun & De Lange 2000
R.D. Van Bruggen, H.A.A. Van Dun & E. De Lange, *Juridische aspecten van de informatievoorziening, Schoonhoven*: Academic Service 2000.

College Bescherming Persoonsgegevens
College Bescherming Persoonsgegevens, WWW <http://www.cbpweb.n/indexen/ind_cbp.stml> (geraadpleegd 10 april 2005)

College Bescherming Persoonsgegevens
College Bescherming Persoonsgegevens, WWW <http://www.cbpweb.n /indexen/ind_cbpint.stml> (geraadpleegd 8 juni 2005)

Dommering 2000
E.J. Dommering, Informatierecht, *Fundamentele rechten voor de informatiesamenleving,* Amsterdam: Otto Cramwinckel Uitgever 2000.

E-Jure 2005
E-Jure, Dossier computercriminaliteit, WWW <http://www.ejure.nl/f_dossier/language=nl/dossier_id=175/dossier.html>, (geraadpleegd 20 juli 2005)

E-Jure 2005
E-Jure, *Dossier computercriminaliteit*, WWW <http://www.ejure.nl/exturls/dossier_id=175/id=92/show.html >, (geraadpleegd 20 augustus 2005)

Ejure 2005
Ejure, *wijzigingen cc II in strafrecht*, WWW <http://www.ejure.nl/downloads/language=nl/id=303/show.html>, publicatie 25 juli 2005.

E Jure 2005
E-Jure, *Dossier wetsvoorstel computercriminaliteit II,* WWW <http://www.ejure.nl/articles/dossier_id=175/id=190/show.html>, publicatie 27 juli 2005.

E-Jure 2005
E-Jure, Dossier wetsvoorstel computercriminaliteit II, WWW <http://www.ejure.nl/f_dossier/language=nl/dossier_id=265/dossier.html>, (geraadpleegd 20 juli 2005)

Europees Bureau Eerste Kamer 2005

Europees Bureau *Eerste Kamer, Kaderbesluit over aanvallen op informatiesystemen*, WWW < http://www.europapoort.nl/9345000/1f/j9vvgy6i0ydh7th/vg5fcc4jpyqn> (geraadpleegd 9 augustus 2005)

Franken, Kaspersen & De Wild 2001
H. Franken, H.W.K. Kaspersen & A.H. De Wild (red.) *Recht en Computer*, Deventer: Kluwer 2001.

Geerts & Rijnders 2003
P.G.F.A. Geerts & J.R.M. Rijnders, *Wettenpocket ICT-recht,* Deventer: Kluwer 2003.

Grosheide 2000
F.W. Grosheide (red.) *Communicatie- & Mediarecht*, Nijmegen: Ars Aequi Libri 2000.

IViR (Anton Ekker)
IViR, Anton Ekker, WWW <http://www.ivir.nl/medewerkers/ekker.html> (geraadpleegd 9 augustus 2005)

Kaspersen 2005
H.W.K. Kaspersen, `Nederlandse wetgeving tegen cookies en spyware. Enkele aantekeningen vanuit Nederlands perspectief' , *Computerrecht* 2005-2, p. 12-14.

Kleve 2004
P. Kleve, *Juridische iconen in het informatietijdperk,* Deventer: Kluwer 2004.

Koelman 2002
K.J. Koelman, noot bij Hof Amsterdam 28 maart 2002 (Kazaa/Buma), WWW <http://www.ivir.nl/publicaties/koelman/noothofkazaa.html> (geraadpleegd 12 mei 2005)

Koops 2004
B.J. Koops (red.), *Strafrecht en ICT,* Den Haag: Sdu Uitgevers 2004.

Ministerie van Justitie 2004
Ministerie van Justitie, Kamervragen van het lid Gerkens (SP) aan de ministers van Justitie en van Economische Zaken over spyware, WWW http://www.justitie.nl/pers/kamerstukken/include.asp?bestand=/extern/documentportal/Kamerantwoorden/20040817_A%202030416730%20spyware.doc.c>, publicatie augustus 2004.

National Hightech Crime Center
National Hightech Crime Centrer, WWW < http://www.nhtcc.nl/> (geraadpleegd 9 augustus 2005)

NMa
NMa, *Nederlandse Mededingingsautoriteit,* WWW <http://www.nmanet.nl/nederlands/home/index.asp> (geraadpleegd 18 augustus 2005)

Ososs
Ososs WWW <http://www.ososs.nl> (geraadpleegd 9 augustus 2005)

Ososs 2005
Ososs, FAQ, WWW< http://www.ososs.nl> (geraadpleegd 12 mei 2005)

Pasveer 2005
L. Pasveer, Amerikanen leggen spyware aan banden, WWW <http://www.zdnet.nl/print.cfm?id=45778>, publicatie 23 mei 2005.

Phishing & pharming 2005

`Phishing & pharming', Digitale Consument 2005-4, p. 21-23.

Radboud Universiteit (Jaap Henk Hoepman)
Radboud Universiteit, Jaap Henk Hoepman, WWW < http://www.cs.ru.nl/~jhh/about.html> (geraadpleegd 9 augustus 2005)

Ramasastry 2004
A. Ramasastry, Can Utah's New Anti-Spyware Law Work? WWW <http://writ.news.findlaw.com/ramasastry/20040601.html> (geraadpleegd 9 augustus 2005)

Sauerwein & Linnemann 2001
L.B. Sauerwein & J.J. Linnemann, *Handleiding voor verwerkers van persoonsgegevens, Wet bescherming persoonsgegevens,* Den Haag: Ministerie van Justitie 2001.

De Schrijver & Schraeyen 2005
S. de Schrijver & J. Schraeyen, `"Spyware": onschuldige spionage in cyberspace?', *Computerrecht* 2005-2, p. 3-11.

SOLV (Christaan Alberdink Thijm)
SOLV, Christiaan Alberdink Thijm, WWW <http://www.solv.nl/Mensen-2.pagina?m=3&lang=nl> (geraadpleegd 9 augustus 2005)

Spyware 2005
`Spyware', *Consumentengids,* mei 2005 p. 22-23

Spyware onuitroeibaar 2005
`Spyware onuitroeibaar', *Digitale Consument* 2005-3, p. 30-33.

Surf op safe
Surf op safe, WWW < http://www.surfopsafe.nl/> (geraadpleegd 9 augustus 2005)

Surf op safe
Surf op safe, WWW < http://www.surfopsafe.nl /index/voor_wie/index.html/> (geraadpleegd 9 augustus 2005)

TROS Radar 2004
TROS Radar, *Justitie kansloos tegen spionagesoftware*, WWW <http://www2.trosradar.nl/?url=PHP/news/28/830/dossier> publicatie 23 november 2004

Verhagen 2004
L. Verhagen, Eén op de drie pc's besmet met spyware, WWW <http://www.webwereld.nl/articles/12833>, publicatie 16 juni 2004

Westin 1967
A.F. Westin, *Privacy and Freedom,* London: The Boldley Head 1967.

Wiemans 2004,
F.P. E. Wiemans, `Computervredebruek nieuwe stijl en strafbare voorbereidingshandelingen', *JAVI* 2004 p.198-204.

Wiemans 2004
F.P.E. Wiemans*, Onderzoek van gegevens in geautomatiseerde werken*, Nijmegen: Wolf legal publishers 2004.

XS4ALL (Wat is phishing?)
XS4ALL, Wat is phishing? WWW <http://www.xs4all.nl/veiligheid/phishing/> (geraadpleegd 12 mei 2005)

Nawoord

Deze scriptie is tot stand gekomen met de hulp van vele mensen. Bij deze wil ik al die mensen bedanken.

Allereerst bedank ik mevr. mr. Aline Klingenberg die mij bij het schrijven van deze scriptie heeft begeleid.

Tevens wil ik de geïnterviewden, die hun tijd en kennis ter beschikking stelden en de experts, die mij met raad en daad hebben bijgestaan, bedanken.

Voor de zeer welkome hulp bij de opmaak van zowel de papieren als de digitale versie bedank ik Peter Breedijk.

Tevens wil ik alle mensen in mijn omgeving bedanken voor hun interesse, goede raad en steun.

Groningen, 26 augustus 2005