

Wet betreffende het wederrechtelijk registreren van domeinnamen.

26 juni 2003

(B.S. 9 september 2003)

Te onthouden:

Elke domeinnaam op het internet is in beginsel uniek, wat voor gevolg heeft dat degene die als eerste een domeinnaam registreert daardoor noodzakelijkerwijs uitsluit dat iemand anders deze naam kan verwerven. Dit resulteert natuurlijk in een grote interesse voor commercieel interessante domeinnamen, die een groot aantal bezoekers zouden kunnen aantrekken.

Soms gaat deze competitiedrang echter te ver, en merkt men dat een domeinnaam werd geregistreerd door iemand die geen waardeerbare band heeft met de naam. Meestal heeft de houder van de domeinnaam enkel als bedoeling de naam door te verkopen voor een aanzienlijke som geld aan een derde die een zeer voor de hand liggende aanspraak heeft op de naam. Men kan dan onder andere denken aan gevallen waarin een gedeponeed merk als domeinnaam werd geregistreerd door iemand die niet de houder van het merk is.

Dit fenomeen noemt men in het computerjargon vaak *cybersquatting*ⁱ, en met deze wet wilde de wetgever een juridische oplossing voor dit probleem uitwerken.

De wet gebruikt echter nergens de term cybersquatting, maar spreekt over “het wederrechtelijk registreren van een domeinnaam”.

Sleutelbegrippen:

e-commerce - Intellectuele eigendom – Handelspraktijken – Eerlijke mededinging – Domeinnamen - Cybersquatting

Inhoudsopgave van de bespreking:

- A. [Inleiding](#)
 - Doel van de wetgeving
 - Schets van de problematiek
 - Begripsbepaling cybersquatting
- B. [Technische schets](#)
 - Domeinnamen en IP-adressen
 - DNS
 - Opzoeken van websites
- C. [Oplossingen vóór de wet inzake cybersquatting](#)
 - Handelspraktijkenwet
 - Benelux Merkenwet
 - Bemiddeling
- D. [Begrippen uit de wet inzake cybersquatting](#)

- Definities en omschrijvingen
- E. [Maatregelen in de wet inzake cybersquatting](#)
 - Draagwijdte
 - Vordering tot staking
 - Beperkingen
- F. [Om meer te weten](#)
 - Nuttige links

Bespreking:

A. Inleiding

Sinds zijn totstandkoming is het aantal vaste gebruikers van het internet gestaag toegenomen, waarbij men vooral sinds de vroege jaren '90 van een echte *boom* kan spreken. Eén van de voornaamste factoren hierin is de ontwikkeling en de commercialisering van het zogenaamde *World Wide Web*. Het opzetten en onderhouden van websites bleek een commerciële voltreffer van formaat: waar er begin 1993 nog maar een 500-tal *Web servers* op het internet aangesloten waren (dit zijn computers die websites huisvesten en beschikbaar maken voor bezoekers), steeg dit aantal in de loop van 2003 naar iets meer dan 42 miljoenⁱⁱ. Niet alleen privégebruikers maar ook overheden, non-profitorganisaties en natuurlijk bedrijven vindt men steeds vaker terug op het internet. Men kan zelfs stellen dat voor bedrijven het bezit van een eigen website een vereiste lijkt te zijn om ernstig genomen te kunnen worden als zakenpartner.

Vanuit technisch standpunt hoeft dit geen probleem te zijn. Het World Wide Web is immers een open architectuur, die ruimte kan bieden aan een zeer groot aantal web servers, en waaraan zonder veel moeite nieuwe systemen toegevoegd kunnen wordenⁱⁱⁱ. Elk van deze systemen moet echter geïdentificeerd worden door een uniek nummer (een zogenaamd *IP-adres*) dat verbonden is aan een unieke domeinnaam, zoals bijvoorbeeld www.internet-observatory.be. Aangezien maar één persoon de houder kan zijn van een dergelijke domeinnaam, is het dus van groot belang dat een belanghebbende 'zijn' domeinnaam tijdig opeist.

Dit 'opeisen' gebeurt via een registratieprocedure, die [elders](#) in deze tekst wordt besproken. Hierbij kan een geïnteresseerde worden geconfronteerd met het probleem dat iemand anders de gewenste domeinnaam al heeft geregistreerd, zodat deze niet meer beschikbaar is. In vele gevallen gaat het om iemand die eveneens een legitieme aanspraak op de domeinnaam kon maken, en gewoon zijn concurrenten te vlug af was. In sommige gevallen is er echter meer aan de hand. Wanneer men het geregistreerde adres bezoekt, blijkt dat er helemaal geen website terug te vinden is, of een site die geen enkele informatie over het relevante onderwerp bevat. Vaak vindt men op deze sites maar één inlichting: de contactinformatie van de huidige 'exploitant', die zich bereid verklaart de domeinnaam met een vaak aanzienlijke winst door te verkopen...

Dit fenomeen noemt men in het computerjargon vaak *cybersquatting*, en met deze wet wilde de wetgever een juridische oplossing voor dit probleem uitwerken.

De wet gebruikt echter nergens de term cybersquatting, maar spreekt over “het wederrechtelijk registreren van een domeinnaam”. Een dergelijke registratie wordt in artikel 4, 2^e lid omschreven als ”het, zonder enig recht of legitiem belang jegens die domeinnaam, en met het doel een derde te schaden of er een ongerechtvaardigd voordeel uit te halen, laten registreren door een officieel erkende instantie gemachtigd voor registratie, al dan niet via een tussenpersoon van een domeinnaam, die ofwel identiek is aan, of die zodanig overeenstemt dat hij verwarring kan scheppen met, onder meer, een merk, een geografische aanduiding of een benaming van oorsprong, een handelsnaam, een origineel werk, een naam van een vennootschap of van een vereniging, een geslachtsnaam of de naam van een geografische entiteit, die aan iemand anders toebehoort.”

Op deze uitgebreide definitie zullen we [hieronder](#) verder ingaan, maar we kunnen nu al opmerken dat het begrip hier een vrij ruime interpretatie krijgt. Het gaat immers niet enkel om domeinnamen die identiek zijn aan o.a. merknamen (vb. www.coca-cola.com), maar ook om domeinnamen die hier zodanig mee overeenstemmen dat er verwarring zou kunnen zijn (vb. www.cocacola.com)^{iv}. Deze tweede praktijk wordt op het internet soms omschreven als *cyberpiracy*, hoewel het onderscheid tussen de twee termen niet consequent wordt gemaakt. De wetgever vond het onderscheid kennelijk niet relevant genoeg om een verschillende behandeling te rechtvaardigen.

Een derde praktijk die men naast cybersquatting en cyberpiracy op het internet soms tegenkomt is het zogenaamde *typosquatting*^v. Hiervan is er sprake als men een domeinnaam laat registreren die in feite fout werd ingetikt door de gebruiker. De registrant gokt er met andere woorden op dat een internaut vroeg of laat het foute adres zal intikken, en naar zijn site zou worden geleid. Een (volledig fictief^{vi}) voorbeeld hiervan zou de registratie van de naam www.mircrosoft.com kunnen zijn. Dit fenomeen lijkt op het eerste zicht wellicht relatief onschadelijk, aangezien het niet erg waarschijnlijk is dat Microsoft alle mogelijke tikfouten van zijn naam zou willen registreren voor zijn website. Maar de situatie wordt opeens veel bedreigender als zou blijken dat een concurrent van Microsoft de domeinnaam liet registreren, en alle bezoekers zou omleiden naar de eigen site.

Op basis van de wettekst en de parlementaire voorbereiding kan niet worden opgemaakt of de wetgever ook beoogde tegen typosquatting op te treden. Om de wet te kunnen toepassen op typosquatting zou een rechter moeten oordelen dat er verwarring mogelijk is tussen Microsoft en Mircrosoft. Het is betwistbaar of een aandachtslapsus bij de internaut mag worden gelijkgesteld met een objectief verwarringsgevaar, en het is dan ook afwachten op de eerste rechtspraak hieromtrent.

Men kan zich overigens de vraag stellen of deze wetgeving niet enkele jaren te laat komt. De allergrootste *boom* in de aangroei van websites vond immers plaats in de late jaren '90, en dit is dan ook de ‘gouden periode’ van de cybersquatters geweest. Hoewel de wet zeker nog relevantie heeft en kan helpen nieuwe verwickelingen sneller te beëindigen, is het toch jammer dat er nu pas een regelgeving over dit probleem tot stand kwam. De meeste grote bedrijven beschikken immers al enige tijd over een eigen website, waardoor de interessantste doelwitten voor cybersquatters ook zonder deze wet al buiten schot waren.

B. Technische schets

Voor de volledigheid schetsen we hier even kort de basisbeginselen van de organisatie van het World Wide Web. De bedoeling hiervan is om de geïnteresseerde lezer een elementair inzicht te geven van de technische oorzaken van het probleem van cybersquatting. Voor een louter juridische analyse is het begrip van deze materie echter niet essentieel aangezien er geen juridische concepten uit de doeken zullen worden gedaan. De lezing van dit deel kan dan ook worden overgeslagen door de lezer die enkel de juridische aspecten wil analyseren.

Zoals we in [de inleiding](#) al stelden beschikt elke computer die websites huisvest (een zogenaamde *web server*) over een uniek adres en een bijbehorende unieke naam. In feite is alleen het adres noodzakelijk voor de technische overdracht van gegevens, en bestaat de naam alleen om mnemotechnische redenen. Het protocol dat de overdracht van gegevens over het internet regelt (het zogenaamde *TCP/IP*^{vii}-protocol) werkt namelijk alleen met de adressen.

Deze IP-adressen bestaan eigenlijk uit een getal van 32 bits, dat meestal wordt weergegeven als 4 groepen van 8 bits die naar een decimaal getal worden omgezet. Elke computer die permanent met het internet verbonden is beschikt over een vast IP-adres. Voor het ministerie van Economische Zaken is dit bijvoorbeeld 193.191.210.45^{viii}.

Dergelijke getallen zijn voor mensen echter niet gemakkelijk te onthouden, en het is om die reden dat er domeinnamen gebruikt worden op het World Wide Web. Deze naam moet dan wel door de computer worden omgezet naar een IP-adres, aangezien het TCP/IP-protocol alleen daarmee kan werken.

Dit gebeurt via het *Domain Name System*. Het gaat om een systeem van servers, die tabellen bijhouden met geregistreerde namen en de overeenkomstige IP-adressen. Telkens als een menselijke gebruiker zo'n naam intikt, zal de computer dus een DNS-server contacteren en het IP-adres opzoeken. Op basis daarvan kan de gezochte informatie worden teruggevonden op het internet en aan de internaut worden bezorgd.

Het zou ondoenbaar zijn om alle domeinnamen met de bijbehorende IP-adressen in één grote tabel bij te houden, omwille van het gigantische aantal ervan. Daarom werd het bijhouden van deze adressen hiërarchisch gespreid, wat men ook terugvindt in de opbouw van de domeinnamen. Alle domeinnamen eindigen immers met een groep van twee of drie letters, die een eerste indeling aangeven, namelijk een zogenaamd *top level domain*. Hierin onderscheidt men twee categorieën: nationale top level domains die indicatief zijn voor een bepaald land (zoals het belgische .be) en generieke top level domains die indicatief zijn voor een bepaald thema (zoals .com voor sites met een commercieel oogmerk). Deze top level domains bestaan niet enkel om de internaut een eerste inzicht te geven in het onderwerp van de gezochte site, maar hebben ook een technisch nut.

Stel dat men bijvoorbeeld een site moet opzoeken van de vorm [www.company-name.co.uk](#). In plaats van in één tabel deze site tussen miljoenen anderen terug te vinden zal men in theorie^{ix} enkel bij één van de zogenaamde *root servers*^x het adres van een server met de .uk-adressen moeten vinden. Deze .uk-server kan op zijn beurt doorverwijzen naar een server met de .co.uk-adressen, die uiteindelijk de gegevens

van company-name.co.uk zal bevatten. Op die manier wordt de belasting enigszins gespreid.

Om een domeinnaam in een dergelijke tabel met adressen te laten opnemen, moet de naam worden geregistreerd. De verantwoordelijken daarvoor werden aangeduid door de Amerikaanse organisatie [ICANN](#) (Internet Corporation for Assigned Names and Numbers), en variëren naar gelang het top level domain. Voor de .be-domeinnamen is de vzw [DNS](#) bevoegd, die de namen via een systeem van [erkende agenten](#) ter beschikking stelt. Tegenwoordig kent DNS de namen toe op een ‘first come, first served’-basis; m.a.w. wie als eerste een domeinnaam aanvraagt, zal hem in principe zonder een verdere legitimeitscontrole toegewezen krijgen. DNS is overgestapt naar dit eerder passieve beleid als gevolg van een reeks rechtszaken, waarbij DNS er telkens van werd beschuldigd de marktwerking te verstoren omwille van beweerde ongeoorloofde weigeringen.

Het spreekt voor zich dat dit gebrek aan controle als neveneffect heeft dat misbruiken door cybersquatters gemakkelijker worden. Deze wet kan hierbij een nuttig bestrijdingsmiddel blijken te zijn.

C. Oplossingen vóór de wet inzake cybersquatting

Zoals we hierboven al hebben aangegeven begon de periode van spectaculaire groei van het World Wide Web in de vroege jaren '90, ruim 10 jaar voor de totstandkoming van deze wet. Het spreekt voor zich dat er zich ook in deze periode problemen stelden met cybersquatters, waarvoor er een juridische oplossing moest worden gezocht^{xi}. Meestal heeft men daarbij zijn toevlucht gezocht bij de [Handelspraktijkenwet](#) en de [Merkenwet](#), die we hieronder verder zullen bespreken.

De meeste rechtspraak die voorhanden is over deze problematiek heeft echter geen betrekking op conflicten met cybersquatters, maar over vermeende onterechte weigeringen tot registratie van DNS. Hieruit mag men nochtans niet afleiden dat er in België geen conflicten met cybersquatters waren. Een verklaring vindt men daarentegen wel in de zeer goed werkende [bemiddelingsprocedure](#) die DNS voorschreef (en nog steeds voorschrijft) aan zijn klanten. Dit laat toe de meeste conflicten snel af te handelen, zonder gerechtelijke tussenkomst. Ook deze procedure zal verder nog worden behandeld.

Voordat we deze besprekingen beginnen is het belangrijk te wijzen op het basisprincipe dat geformuleerd wordt in artikel 3: “Deze wet wordt toegepast onverminderd andere wettelijke bepalingen, meer bepaald elke wettelijke bepaling tot bescherming van merken, geografische aanduidingen en benamingen van oorsprong, handelsnamen, originele werken en alle andere voorwerpen van intellectuele eigendom, namen van vennootschappen en verenigingen, geslachtsnamen, namen van geografische entiteiten, alsook elke wettelijke bepaling inzake oneerlijke mededinging, handelspraktijken en voorlichting en bescherming van de consument.” De Wet op Cybersquatting verhindert de verdere toepassing van de hieronder beschreven beschermingsstelsels dus niet.

- [Handelspraktijkenwet](#)

De Handelspraktijkenwet biedt in art. 93 bescherming tegen “elke met de eerlijke handelsgebruiken strijdige daad, waardoor een verkoper de beroepsbelangen van een of meer andere verkopers schaadt of kan schaden.” Het is een zeer ruime bepaling, die dan ook in zeer uiteenlopende materies kan worden ingeroepen.

Onder meer in de zaken van Tractebel en Cockerill-Sambre werd er een beroep gedaan op de Handelspraktijkenwet. De partijen argumenteerden hierbij dat het reserveren van een domeinnaam die overeenkomt met een handelsnaam die aan iemand anders toebehoort, in strijd is met de eerlijke handelsgebruiken. Het Hof van beroep van Brussel volgde dit standpunt^{xii}.

Hierbij is het opvallend dat de rechtspraak eveneens al heeft geoordeeld dat de registratie van een domeinnaam een schending van de eerlijke handelsgebruiken zou kunnen zijn, als er sprake is van verwarringsgevaar. Ook cyberpiracy zou dus bestreden kunnen worden met de Handelspraktijkenwet, terwijl de toepasbaarheid op typosquatting dan weer afhangt van de interpretatie van de term verwarringsgevaar^{xiii}. De Wet inzake Cybersquatting is wat betreft haar toepassingsvoorwaarden dus min of meer een codificatie van de rechtspraak in het kader van de Handelspraktijkenwet op deze problematiek.

- De Benelux Merkenwet (B.M.W.)

Het merkenrecht is een zeer gangbare bescherming voor de intellectuele eigendom in de zakenwereld. Een merk biedt de mogelijkheid om een bepaalde dienst of een bepaald product op een exclusieve manier aan het publiek te presenteren, zodat concurrenten er geen ongeoorloofd gebruik van kunnen maken. Aangezien merknamen dus een sterke identificerende werking hebben, zijn ze zeer aantrekkelijk als domeinnamen, en is zijn ze eveneens een ideaal doelwit voor cybersquatters.

De meest relevante bepaling in de B.M.W. is art.13, A., 1, d, dat enigszins ingekort bepaalt: “Het ingeschreven merk geeft de houder een uitsluitend recht. Onverminderd de eventuele toepassing van het gemene recht betreffende de aansprakelijkheid uit onrechtmatige daad kan de merkhouder op grond van zijn uitsluitend recht iedere derde die niet zijn toestemming hiertoe heeft verkregen, het gebruik van een teken verbieden (...) wanneer dat teken gebruikt wordt anders dan ter onderscheiding van waren, indien door gebruik zonder geldige reden, van dat teken ongerechtvaardigd voordeel wordt getrokken uit of afbreuk wordt gedaan aan het onderscheidend vermogen of de reputatie van het merk.”

Het criterium voor de rechtmatigheid van het gebruik is dus dat van het merk geen gebruik mag worden gemaakt waardoor een concurrent een onrechtmatig voordeel verkrijgt, of afbreuk doet aan het onderscheidend vermogen of de reputatie van het merk. Deze bepaling vormt dus een uitweg indien een cybersquatter andermans merknaam gebruikt als domeinnaam voor een website, op voorwaarde dat hierdoor afbreuk wordt gedaan aan het onderscheidend vermogen van het merk of dat de cybersquatter een ongerechtvaardigd voordeel trekt uit de registratie van de domeinnaam^{xiv}.

Het merkenrecht zal geen eenvoudige oplossing bieden bij cyberpiracy of typosquatting, aangezien er in deze gevallen geen gebruik wordt gemaakt van het gedeponeerde merk, maar enkel van een woord dat hier sterk op lijkt.

Het spreekt voor zich dat het misbruik maken van andermans gedeponeerde merknaam eveneens kan worden beschouwd als een daad die strijdig is met de eerlijke handelsgebruiken, zodat deze schending van de Merkenwet ook aanleiding kan geven tot toepassing van de Handelspraktijkenwet.

- Bemiddeling

Zoals we in de inleiding al hebben aangehaald voorzag DNS België in een beperkte oplossing voor de problematiek van cybersquatting door de inrichting van een bemiddelingsprocedure. Ook op dit moment nog stellen de algemene voorwaarden van DNS dat "alle geschillen in verband met een domeinnaamregistratie die tussen de licentienemer en een andere partij dan DNS BE ontstaan, moeten opgelost worden door rechtsgedingen, arbitrage of andere beschikbare procedures".

Wat betreft gevallen van cybersquatting wordt de huidige licentiehouders verplicht de bemiddelingsprocedure te volgen 'wanneer een derde partij beweert dat:

- de domeinnaam van de licentiehouders identiek is aan of grote gelijkens vertoont met een merk, een handelsnaam, een maatschappelijke benaming of vennootschapsnaam, een geografische aanduiding, een persoonsnaam of een benaming van een geografische entiteit op dewelke de aanklager rechten heeft; en
- de licentiehouders geen rechten of legitieme belangen heeft ten opzichte van de domeinnaam; en
- de domeinnaam van de licentiehouders te kwader trouw geregistreerd werd of gebruikt wordt.^{xv}

Voor deze alternatieve procedure doet DNS een beroep op het bemiddelingsbureau [Cepina](#), en dit leidt in de meeste gevallen tot een definitieve uitspraak voor de partijen binnen de 50 dagen voor een procedurekost van ongeveer 1.600 Euro. De bemiddelaar kan daarbij uiteindelijk beslissen om de domeinnaam te laten verwijderen of deze over te laten dragen aan de eiser.

Een reeks recente beslissingen kan [online](#) worden geraadpleegd op de site van Cepina. Uit deze beslissingen blijkt duidelijk de grote verdiensten die de bemiddelingsprocedure in het verleden heeft gehad, en ook in de toekomst ongetwijfeld nog zal blijven hebben. Toch vult de nieuwe wet een belangrijke lacune in de procedure in: de bemiddeling wordt immers ingericht door DNS België, en het spreekt dan ook voor zich dat ze enkel kan worden opgelegd aan geregistreerde .be-sites. Indien een Belgische cybersquatter echter een generieke domeinnaam zou hebben geregistreerd (bijvoorbeeld een .org domeinnaam als [www.artsenzongrenzen.org](#)^{xvi}), dan zou de bemiddelingsprocedure van DNS België vanzelfsprekend geen soelaas kunnen bieden^{xvii}.

De wet heeft wat dat betreft een wat ruimere geldingsfeer: artikel 4 laat een vordering tot staking toe voor “elk wederrechtelijk registreren van een domeinnaam door een persoon met woonplaats of vestiging in België, en van elk wederrechtelijk registreren van een domeinnaam geregistreerd onder het BE-domein.” De nieuwe wet heeft dus niet alleen betrekking op alle .be-domeinnamen, maar ook op alle andere mogelijke domeinnamen (nationale en generieke) die werden geregistreerd door een persoon met woonplaats of vestiging in België. Een erg ruime werkingssfeer dus, die zal toelaten de meeste misbruiken met een oorsprong in België te bestrijden.

D. Begrippen uit de wet inzake cybersquatting

De kernbegrippen van de wet inzake cybersquatting worden gedefinieerd in de artikelen 2 en 4. Artikel 2 bevat daarbij vooral technische definities, die blijkbaar eerder zijn bestemd om de aard van de materie op een juridisch afdoende manier af te lijnen, terwijl artikel 4 poogt het begrip cybersquatting te omschrijven (zonder daarbij deze term zelf te gebruiken).

Artikel 2 bevat twee belangrijke definities: enerzijds van het begrip “domeinnaam”, anderzijds van het begrip “domeinnaam geregistreerd onder het BE-domein”.

Een domeinnaam werd gedefinieerd als “een alfanumerieke weergave van een numeriek IP (Internet Protocol) adres dat het mogelijk maakt een op het Internet aangesloten computer te identificeren; een domeinnaam wordt geregistreerd onder een domein van het eerste niveau, dat ofwel overeenstemt met een van de generieke domeinen (gTLD) die werden bepaald door de Internet Corporation for Assigned Names and Numbers (ICANN), ofwel met een van de landcodes (ccTLD), zulks krachtens de norm ISO-3166-1”. De definitie is vrij duidelijk; voor een verdere bespreking verwijzen we naar [de technische uiteenzetting elders in deze tekst](#).

Aangezien de wet niet alleen toepasselijk is op domeinnamen die werden geregistreerd door personen met een woonplaats of vestiging in België, maar ook op domeinnamen “geregistreerd onder het BE-domein” is het niet vreemd dat dit laatste begrip wat verder wordt verhelderd. Het gaat om een “domeinnaam geregistreerd onder het domein van het eerste niveau dat overeenstemt met de landcode « .be » die krachtens de norm ISO-3166-1 werd toegewezen aan het Koninkrijk België.” Of in iets toegankelijker termen: domeinnamen die eindigen op .be.

Artikel 4 bevat zoals we [in de inleiding](#) al hebben aangehaald een definitie van cybersquatting, of in de termen van de wetgever: het wederrechtelijk registreren van een domeinnaam. Dit begrip wordt uitgelegd als “het zonder enig recht of legitiem belang jegens de domeinnaam en met het doel een derde te schaden of er een ongerechtvaardigd voordeel uit te halen, laten registreren door een officieel erkende instantie gemachtigd voor registratie, al dan niet via een tussenpersoon van een domeinnaam, die ofwel identiek is aan, of die zodanig overeenstemt dat hij verwarring kan scheppen met, onder meer, een merk, een geografische aanduiding of een benaming van oorsprong, een handelsnaam, een origineel werk, een naam van een vennootschap of van een vereniging, een geslachtsnaam of de naam van een geografische entiteit, die aan iemand anders toebehoort.”

Een behoorlijk lijvige definitie waarvan we de bestanddelen even wat verder zullen bekijken.

Globaal kunnen we drie elementen in de definitie onderscheiden. Op de eerste plaats vereist de wet dat de registratie plaatsvond met een bepaald [oogmerk](#). Ten tweede wordt de [registratiehandeling](#) zelf omschreven; en tenslotte worden er een reeks [voorwaarden](#) opgelegd waaraan de domeinnaam zelf moet voldoen vooraleer er sprake kan zijn van een wederrechtelijke registratie.

Wat betreft het oogmerk van de wederrechtelijke registratie stelt de wet dat de registratie moet gebeuren “zonder enig recht of legitiem belang jegens de domeinnaam en met het doel een derde te schaden of er een ongerechtvaardigd voordeel uit te halen.” Het oogmerk kan dus worden opgesplitst in twee aspecten, die beide aanwezig moeten zijn.

Op de eerste plaats moet de registratie betrekking hebben op een naam waarop de titularis van de domeinnaam geen rechtmatige claim heeft, doordat hij geen recht heeft op de naam, noch een legitiem belang bij de registratie. Hierbij wordt de vergoeding die de titularis hoopt te verkrijgen uit de verkoop van de naam vanzelfsprekend niet als legitiem belang beschouwd. Dit eerste aspect kan dus worden samengevat als een gebrek aan een concrete band tussen de titularis en zijn geregistreerde domeinnaam.

Het tweede aspect van het oogmerk heeft betrekking op de bedoelingen die de titularis heeft met de registratie van de domeinnaam. De registratie moet gebeurd zijn “met het doel een derde te schaden of er een ongerechtvaardigd voordeel uit te halen.” De registratie kan dus enkel als wederrechtelijk worden bestempeld indien ze gebeurde met de bedoeling zichzelf op een onrechtmatige manier te verrijken (bijvoorbeeld door de domeinnaam voor een excessief bedrag te verkopen) of om een derde te schaden (bijvoorbeeld door de domeinnaam te registreren met als enige bedoeling ze uit de handen van een concurrent te houden). Men zou dit aspect met wat goede wil kunnen omschrijven als een ‘bedrieglijk opzet’. Dit vereiste ligt redelijk voor de hand: als men geen slechte bedoelingen heeft met de domeinnaam is de registratie hoogstens zinloos, maar niet schadelijk.

De materiële registratiehandeling wordt eveneens verder omschreven in artikel 4: het gaat om een registratie “door een officieel erkende instantie gemachtigd voor registratie, al dan niet via een tussenpersoon”. Dit is een verwijzing naar de organisaties die door ICANN werden gemachtigd om domeinnamen toe te kennen, zoals DNS dat doet voor België. Voor meer details hierover verwijzen we naar [de technische uiteenzetting](#).

De verwijzing naar het gebruik van tussenpersonen kan worden verklaard door het feit dat vele domeinnaambeheerders (waaronder DNS België) niet rechtstreeks verzoeken tot registratie aannemen, maar hiervoor gebruik maken van een netwerk van erkende agenten^{xviii}. Dit systeem sluit dus de toepasbaarheid van de wet niet uit.

Tenslotte bevat artikel 4 ook nog een aantal objectieve voorwaarden waaraan de domeinnaam moet voldoen om van een wederrechtelijke registratie te kunnen spreken. Het moet gaan om een domeinnaam “die ofwel identiek is aan, of die zodanig overeenstemt dat hij verwarring kan scheppen met, onder meer, een merk, een geografische aanduiding of een benaming van oorsprong, een handelsnaam, een origineel werk, een naam van een vennootschap of van een vereniging, een

geslachtsnaam of de naam van een geografische entiteit, die aan iemand anders toebehoort.”

Net zoals bij toepassing van de Handelspraktijkenwet op deze problematiek ook al het geval was wordt er dus vereist dat de geregistreerde domeinnaam hetzij identiek is aan andermans domeinnaam, hetzij er zo sterk op lijkt dat er verwarringsgevaar dreigt. Zoals we [hierboven](#) al stelden zal de wet dus ook toepasbaar zijn op cyberpiracy, maar is de toepasbaarheid op typosquatting betwistbaar.

Bij wijze van voorbeeld geeft het artikel ook een non-exhaustieve opsomming van namen die omwille van hun aard kunnen worden beschouwd als toebehorend aan een derde belanghebbende. In deze lijst vinden we merken^{xix}, geografische aanduidingen of benamingen van oorsprong^{xx}, handelsnamen^{xxi}, originele werken, namen van vennootschappen of verenigingen^{xxii}, een geslachtsnamen^{xxiii} of namen van geografische entiteiten.

Zoals in de inleiding al gesteld werd is het toepassingsgebied van de wet dus weinig vernieuwend. Het gaat vooral om een codificatie van de criteria die al enige tijd gehandhaafd werden in bemiddelingsprocedures en bij toepassing van de Handelspraktijkenwet.

E. Maatregelen in de wet inzake cybersquatting

Uit de hierboven beschreven definities en afbakening van het toepassingsgebied blijkt dus duidelijk een sterke verwantschap met de bemiddelingsprocedures en de Handelspraktijkenwet. Het mag dan ook niet verwonderen dat de wet ook voor een gelijkaardige oplossing gekozen heeft als deze beide hulpmiddelen, namelijk een vordering tot staking, eventueel gekoppeld aan een bevel tot overdracht van de domeinnaam aan de klager. Gezien de aard van het probleem lijkt dit ook de meest gepaste oplossing.

Opvallend is wel dat de wederrechtelijke registratie van een domeinnaam niet strafrechtelijk wordt beteugeld^{xxiv}. Wellicht is dit ook niet nodig: het vooruitzicht in een potentieel kostelijke procedure te worden betrokken zal wellicht volstaan als afschrikkingsmiddel, ook zonder dat hieraan nog een strafrechtelijke sanctie wordt gekoppeld.

De basisbevoegdheid met betrekking tot de vordering tot staking wordt geregeld in artikel 4. De voorzitter van de rechtbank van eerste aanleg, of in voorkomend geval, de voorzitter van de rechtbank van koophandel wordt belast met de vaststelling van elke wederrechtelijke registratie van een domeinnaam, indien aan de hoger vermelde voorwaarden is voldaan. Indien hij oordeelt dat er inderdaad sprake is van een wederrechtelijke registratie, dan kan hij overgaan tot een bevel tot staking van de registratie (m.a.w. bevelen dat de registratie wordt doorgehaald), eventueel samen met een bevel tot overdracht van de domeinnaam (m.a.w. een bevel tot registratie ervan op naam van de klager).

De vordering tot staking van de registratie kan enkel worden ingesteld door een persoon die een legitiem belang aan toont ten opzichte van de betrokken domeinnaam, en die een recht kan laten gelden op één van de in artikel 4 vermelde tekens. Dit is een verwijzing naar de niet-exhaustieve opsomming van namen waarop men een bepaalde

claim kan hebben, zoals merken, geografische aanduidingen of benamingen van oorsprong, handelsnamen, originele werken, namen van vennootschappen of verenigingen, een geslachtsnamen of namen van geografische entiteiten.

Het artikel vereist ook dat men “een recht kan laten gelden op één van de in artikel 4 vermelde tekens”. Deze bepaling werd via een amendement toegevoegd aan het oorspronkelijke wetsontwerp, en strekte ertoe te vermijden dat “bv. ondernemingen die zelf geen merkenrechten genieten, zouden kunnen optreden tegen een domeinnaamregistratie zonder tussenkomst van de merkhouders zelf^{xxv}. Een dergelijke gang van zaken zou immers indruisen tegen het merkenrecht in het bijzonder en het intellectuele eigendomsrecht in het algemeen, dat vereist dat de rechthebbende zelf optreedt.” De bedoeling was blijkbaar ervoor te zorgen dat de nieuwe wet geen afbreuk zou doen aan de bestaande jurisprudentie binnen het intellectuele eigendomsrecht. Men kan zich echter de vraag stellen of de huidige formulering van het artikel niet te sterk is afgestemd op het klassieke intellectuele eigendomsrecht. Er is immers ook sprake van wederrechtelijke registratie bij bv. domeinnamen die een geslachtsnaam bevatten, terwijl men hier bezwaarlijk van intellectuele eigendom kan spreken.

Als de houder van de domeinnaam in het ongelijk werd gesteld, dan kan de voorzitter van de rechtbank eveneens bevelen dat het vonnis geheel of gedeeltelijk wordt bekendgemaakt in de pers of op een andere door hem bepaalde wijze (zoals bijvoorbeeld op een website), en dit op kosten van de (ex-)houder. Een dergelijke publicatie is echter alleen mogelijk als dit kan bijdragen tot de stopzetting van de registratie of de uitwerking ervan. Men kan dan denken aan een situatie waarbij een onderneming bijvoorbeeld de domeinnaam van een concurrent heeft geregistreerd, om zo klanten te kunnen wegkaperen. In zo'n geval kan het zinvol zijn de publicatie van het vonnis op de website van de kaper op te leggen, om zo de weggelokte klanten duidelijk te maken aan wie de domeinnaam eigenlijk had moeten toebehoren.

Artikelen 8 e.v. regelen de procedurele aspecten van de rechtsgang, en doen sterk denken aan de overeenkomstige bepalingen in de Handelspraktijkenwet.

Artikel 8 schrijft voor dat “de vordering wordt ingesteld en behandeld zoals in kortgeding. Zij mag ingesteld worden bij verzoekschrift.”

De precieze inhoud van de vordering en de afhandeling ervan ter griffie worden eveneens uiteengezet in de wet. Het vonnis is uitvoerbaar bij voorraad, niettegenstaande elk rechtsmiddel en zonder borgtocht.

Een laatste opmerkelijke bepaling vinden we nog terug in artikel 11. Volgens dit artikel vallen de geschillen voortvloeiend uit het recht op vrije meningsuiting niet onder de toepassing van deze wet. Het artikel wil hiermee vermijden dat domeinnamen die een mening uitdrukken op zich als onrechtmatig bestempeld zouden worden^{xxvi}. Voor dergelijke meningsuitingen geldt dus het gemene recht, zodat een naam als www.deholocaustiseenleugen.be (fictief voorbeeld) wel verboden zou kunnen worden via de wet op het negationisme, maar niet als een wederrechtelijke registratie van een domeinnaam.

- F. Om meer te weten
- Nuttige links

- [DNS](#), de officiële registrar van de .be-domeinnamen
- [ICANN](#), de internationale organisatie die verantwoordelijk is voor het beheer van de domeinnamen
- [Belgische PISA-site](#) (Providing Information about internet Security Aspects) met uitleg over cybersquatting en technische beveiligingsmaatregelen.
- [Amerikaanse site](#) over cybersquatting en bestrijdingsprocedures
- [Amerikaanse site](#) over de historiek en werking van het internet, inclusief een korte uitleg over de werking van het DNS-systeem

Bespreking opgesteld door ICRI, gecoördineerd door Hans GRAUX.

ⁱ De term cybersquatting is afgeleid van het Engelse werkwoord ‘to squat’, dat onder andere vertaald kan worden als het kraken van een pand. Daarmee is de connotatie van het woord meteen duidelijk: een *cybersquatter* is iemand die zich onrechtmatig andermans “virtuele huis” heeft toegeëigend om er zelf profijt uit te halen.

ⁱⁱ Bron: Hobbes’ internet timeline: <http://www.zakon.org/robert/internet/timeline/>

ⁱⁱⁱ Op dit moment gebruikt men voor de adressering van computers op het internet de IPv4-standaard, die 32-bits gebruikt om de adressen te omschrijven. Hierdoor zijn er in theorie ongeveer 4,3 miljard adressen beschikbaar; in de praktijk is een groot deel daarvan onbruikbaar omwille van bepaalde conventies. Daarom wordt er momenteel gedebatteerd over een uitbreiding naar de IPv6-standaard, die 128 bits gebruikt. Hierdoor zouden er meer dan voldoende nieuwe adressen bijkomen. Voor meer informatie kunt u [hier](#) klikken..

^{iv} Fictief voorbeeld. Beide sites werden geregistreerd door The Coca-Cola Company.

^v Ook hier is de etymologie redelijk evident: *typo* is namelijk een Engelse term voor ‘tikfout’.

^{vi} Op het moment van schrijven is de domeinnaam www.microsoft.com nog niet geregistreerd.

^{vii} Cette abréviation veut dire Transmission Control Protocol/Internet Protocol. Il s’agit donc en fait de deux protocoles séparés, qui garantissent ensemble la transmission de données sans erreurs par un réseau.

^{viii} Om uw eigen IP-adres te vinden, kunt u [hier klikken](#).

^{ix} En réalité les providers Internet ont leurs propres serveurs DNS locaux, qui ont mémorisé les sites visités le plus récent. De cette manière les adresses les plus populaires peuvent être retrouvées beaucoup plus vite. La procédure qui est décrit dans le texte ci-dessus sera donc seulement appliquée à des sites dont l’adresse IP n’a pas été conservée localement, soit parce qu’il s’agit d’un site tout neuf, soit parce que le site n’est que visité rarement.

^x Il y a 13 root serveurs, qui sont dispersés dans tout le monde. Bien qu’ils ne soient donc certainement pas nécessaire pour chaque recherche, ils contiennent les données qui permettent d’autres serveurs DNS de fonctionner. En ce sens elles forment le tendon d’Achille de l’Internet.

^{xi} O.m. Tractebel en Cockerill-Sambre werden met cybersquatters geconfronteerd.

^{xii} Hof Beroep Brussel, 1 april 1998, *Computerrecht* 1998, p. 176, met noot HERMAN DE BAUW; zie ook Rb. Koophandel Brussel, 27 november 1997, *Computerrecht* 1998, p. 26, met noot P. Goethals.

^{xiii} Wat typosquatting betreft is dit een voornamelijk academische discussie. We hebben in de inleiding al opgemerkt dat typosquatting vooral schadelijk is indien de fout getypte domeinnaam werd ingepikt door een concurrent met slechte bedoelingen. In dit geval zal er nagenoeg altijd sprake zijn van een daad die strijdig is met de eerlijke handelsgebruiken, ongeacht enig mogelijk verwarringsgevaar.

^{xiv} Een voorbeeld van misbruik van een gedeponeerd merk vinden we in een geschil over de domeinnaam www.novotel.be. Novotel is immers een gedeponeerd merk dat toebehoort aan de Franse S.A. Accor, terwijl de domeinnaam aanvankelijk geregistreerd werd door een onderneming die de domeinnaam gekoppeld had aan een pornografische website. Later werd de domeinnaam doorverkocht aan een particulier, die ze enkel gebruikte om haar vraagprijs voor de domeinnaam te publiceren. Na een bemiddelingsprocedure werd de domeinnaam overgedragen aan Accor. De uitspraak van de bemiddelaar dd. 30 september 2003 kan geraadpleegd worden [op de site van Cepina](#).

^{xv} Bron: informatiepagina over de Alternative Dispute Resolution (ADR) van DNS:

<http://www.dns.be/nl/DomainInfo/adrproc.htm>

^{xvi} Fictief voorbeeld; Artsen zonder grenzen vindt men in België terug op www.azg.be of www.msf.be

^{xvii} Daarbij moet er wel opgemerkt worden dat de meeste *top level domain*-beheerders een eigen bemiddelingsprocedure voorzien hebben. Dit is echter niet altijd het geval en is daarbij vaak ook niet praktisch, omdat er bij internationale disputen nogal wat kosten gepaard kunnen gaan met bemiddeling. Daarmee verdwijnt natuurlijk onmiddellijk een van de grote voorbeelden van een alternatieve afhandeling.

^{xviii} Een lijst van erkende agenten van DNS is beschikbaar op hun website:

<http://www.dns.be/info/nl/agent/registered>

^{xix} Zoals bv. in [de betwisting over de domeinnaam www.stubru.be](#)

^{xx} Zoals bv. in [de betwisting over de domeinnaam www.belgie.be](#)

^{xxi} Zoals bv. in [de betwisting over de domeinnaam www.hengstler.be](#)

^{xxii} Zoals bv. in [de betwisting over de domeinnaam www.ckzvlaanderen.be](#)

^{xxiii} Zoals bv. in [de betwisting over de domeinnaam www.filipdewinter.be](#)

^{xxiv} In de eerste versie van het wetsontwerp was dit nochtans wel het geval, en werd er in een gevangenisstraf van één maand tot vijf jaar voorzien en een geldboete van 1.000 tot 30.000 frank, of één van beide straffen alleen.

^{xxv} Hierboven haalden we reeds het voorbeeld aan van [de betwisting over de domeinnaam www.hengstler.be](#).

Hengstler is immers een Duits merk, terwijl de domeinnaam zonder succes werd opgeëist door een Belgische onderneming (nl. Hengstler Belgium BVBA). Weliswaar had deze onderneming de officiële toelating gekregen van Hengstler GmbH om haar merknaam te gebruiken, maar desondanks zou een dergelijke vordering voor deze wet niet toelaatbaar zijn zonder de inmenging van het Duitse Hengstler zelf.

^{xxvi} Een voorbeeld hiervan is de [dorsetpolice.com](#)-zaak. Een misnoegde Brit liet deze domeinnaam registreren, om vermeende corruptie bij de politie van Dorset aan de kaak te stellen. Het kwam tot een bemiddelingsprocedure, waarbij de bemiddelaar uiteindelijk oordeelde dat de registratie van de domeinnaam niet wederrechtelijk was. Volgens hem was er geen sprake van kwade trouw bij de houder, en had iedereen er een rechtmatig belang bij dergelijke descriptieve domeinnamen te kunnen registreren, o.a. om kritiek op overheidsdiensten mogelijk te maken. De uitspraak kan geraadpleegd worden op

<http://www.worldlii.org/int/cases/GENDND/2001/1356.html>