RLDI 975

Chaque jour ou presque, l'actualité rapporte les heurts et malheurs des uns et des autres par rapport aux noms de domaine. Alors que les noms de domaine sont devenus un enjeu stratégique de présence sur l'internet, ils sont encore trop souvent délaissés dans le cadre des réflexions stratégiques des entreprises. Le texte qui suit propose quelques pistes pour intégrer les noms de domaine dans le périmètre stratégique en se souvenant que « prévenir vaut mieux que guérir ».

La gestion des noms de domaine et métatags au sein d'une entreprise

Par Loïc DAMILAVILLE
Consultant,
Fondateur du club Noms de Domaine

Par Étienne WÉRY
Avocat aux barreaux de Paris et de Bruxelles
Cabinet d'avocats Ulys

Quand Glaxo Wellcome fusionna avec Smith Kline pour devenir Glaxo Smith Kline, le conseil d'administration rendit la décision publique sans avoir à l'esprit la problématique du nom de domaine ; ils n'avaient aucun responsable des noms de domaine. Le jour où l'annonce eut lieu, quelqu'un enregistra le nom de domaine correspondant. Certes, tout est entretemps rentré dans l'ordre mais il n'empêche : les entreprises se passeraient bien de ce genre d'aventure.

Une telle anecdote n'est pourtant pas exceptionnelle : pareils incidents –« *l'occasion de faire des bonnes affaires* » selon les *cyber squatters*– se produisent tous les jours dans le monde.

C'est d'autant plus regrettable que moyennant quelques mesures organisationnelles et de prévention, le risque peut être sensiblement diminué.

Toute société d'une certaine taille devrait avoir un responsable des noms de domaine. Il s'agit habituellement de quelqu'un du département juridique, du département internet ou marketing et communication, voire un membre du conseil d'administration. Dans tous les cas de figure, cela doit être une personne ayant réellement accès au niveau de management où les décisions sont prises.

Dans les multinationales, le nombre de filiales et de succursales rend la situation plus complexe, d'autant plus que celles-ci bénéficient d'une liberté relative dans leur pays (dans un but de marketing par exemple). Si en plus de cela, la société opère sous un grand nombre de marques déposées (et certaines d'entre elles peuvent être spécifiques à un pays donné), la création d'un authentique groupe de travail (ou « *comité de pilotage* ») des noms de domaine est nécessaire.

Lorsque l'on crée puis gère un tel groupe, il faut se souvenir des trois principes cardinaux que sont la centralisation, la coopération et la transversalité.

Dans le cas présent, la centralisation signifie que, plus le groupe de travail pourra s'impliquer dans les décisions de business (même quand la décision en question ne cible qu'un pays spécifique), mieux cela vaudra. Il est fortement recommandé d'y nommer un président ou un secrétaire, dans tous les cas une personne en charge de la préparation des réunions et des décisions, et du suivi de leur exécution. La personne chargée du dossier « *Noms de domaine* » peut légitimement remplir ce rôle.

Le groupe de travail veillera à l'exactitude des données concernant notamment le nombre de noms de domaine actifs ainsi que leur statut et date de renouvellement, la liste de tous les noms de domaine « *proches* » liés à un nom de domaine principal (voir ci-après), les données techniques de chaque nom de domaine, etc. La centralisation peut aller jusqu'à couvrir tout ce qui concerne la facturation. En effet, lorsque c'est possible, il vaut mieux éviter d'envoyer les demandes de renouvellement et les factures qui les accompagnent au département comptable, qui pourrait être débordé et acquitter les factures avec retard. Les factures (ou au moins copies de celles-ci) devraient idéalement être envoyées au groupe de travail afin d'assurer la jouissance permanente du nom de domaine.

La coopération signifie, dans le cas présent, que le groupe de travail doit associer une bonne représentation géographique (des représentants des filiales outre un membre du siège central) et une bonne représentation des compétences (le directeur général n'est pas toujours la personne la plus apte : peuvent notamment convenir, un responsable d'exploitation ou un responsable des départements clientèle ou marketing). À côté de membres permanents, comme par exemple le directeur général, la composition du groupe de travail varie fréquemment selon les problèmes à traiter.

La transversalité est le corollaire de la coopération : l'objectif est de permettre au groupe de travail (ou comité de pilotage) d'avoir une vision globale des besoins de l'entreprise et de son portefeuille de noms de domaine, afin d'identifier le plus facilement possible les points où l'adéquation est bonne, et au contraire ceux où des améliorations doivent être apportées. De ce point de vue, la présence des diverses grandes directions ainsi que de représentants des principales filiales est particulièrement souhaitable, afin d'assurer une bonne circulation de l'information. Cette transversalité au niveau du groupe de travail peut être utilement complétée par la mise en place d'un réseau opérationnel de correspondants noms de domaine destiné à assister le responsable noms de domaine dans ses missions. Un responsable noms de domai- >

ne isolé ne peut matériellement pas garantir l'adéquation entre les besoins de l'entreprise et son portefeuille de noms de domaine.

Questions d'*outsourcing*

De plus en plus de prestataires de services se sont spécialisés dans la gestion, les enquêtes et les surveillances noms de domaine. Ces sociétés proposent des procédures d'enregistrement pour presque tous les ccTLDs (voir ci-dessous) et tous les gTLDs publics (voir ci-dessous également). Elles constituent un unique contact. Certaines d'entre elles s'occupent en outre du monitoring des noms de domaines de leur clients et ceux de leurs concurrents, ainsi que du *cybersquatting* (elles fournissent habituellement en outre à leurs clients des logiciels permettant l'accès en ligne à toute l'information disponible).

Ces sociétés (bureaux d'enregistrement) sont de précieux auxiliaires pour tous les aspects liés à la gestion opérationnelle du portefeuille : dépôts dans le monde entier, transferts, pointages, renouvellement, leurs outils et leurs compétences sont indispensables aux responsables noms de domaine. Pour autant, elles ne peuvent pas remplacer celui-ci car il est le seul à pouvoir apporter la vision « *interne* » de l'entreprise sur ses propres besoins. Si cette vision globale et homogène n'existe pas, le responsable noms de domaine est fondé à organiser les remontées d'information en interne afin de la faire émerger progressivement. Les bureaux d'enregistrement n'interviennent pas sur ces aspects où ils pourraient être juges et parties (intéressés à accroître le portefeuille de noms de leurs clients plutôt qu'à le réduire) et où leur position d'acteurs extérieurs à la société est un obstacle notable pour obtenir des diverses entités concernées des informations parfois sensibles.

I. – CHOISIR UN NOM DE DOMAINE

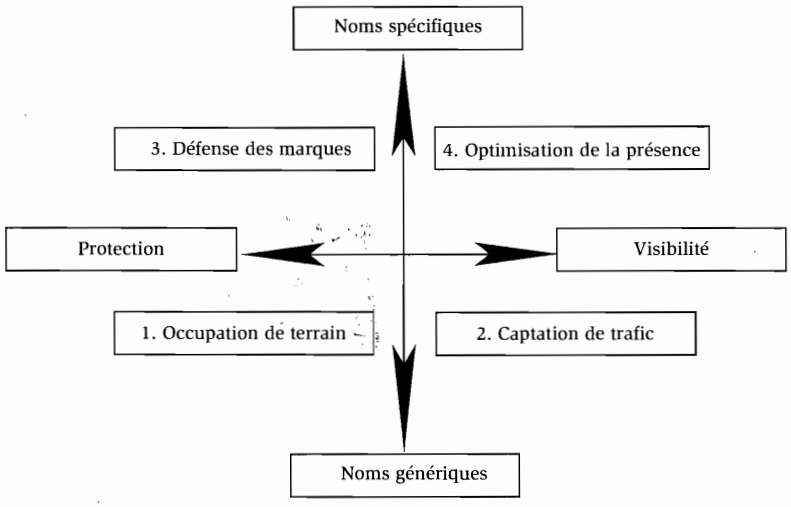
Lorsqu'elle choisit un nom de domaine, la personne qui l'enregistre doit garder à l'esprit au moins deux facteurs importants.

a) Une fois le nom de domaine « *principal* » choisi, il sera nécessaire d'analyser quels sont les noms de domaine « *proches* » qui doivent également être enregistrés, ceci afin de définir un « *périmètre de sécurité* » autour des noms sensibles. L'objectif bien compris est de limiter au maximum, dans ce périmètre, l'existence de noms de domaine déposés par des tiers de bonne ou de mauvaise foi qui viendraient perturber la présence de l'entreprise sur l'internet.

b) Bien qu'il soit souvent utile d'enregistrer des noms proches, il doit demeurer clair que le « *risque zéro* » n'existe pas. Ces actions de dépôt doivent donc être limitées à un périmètre de sécurité bien précis, englobant le « *périmètre de communication* » (ensemble des noms de domaine sur lesquels l'entreprise communique). Le dispositif doit ensuite être complété par la mise en place d'outils de veille permettant d'être alerté en cas d'enregistrements de noms de domaine sur des variantes non intégrées dans les périmètres de dépôts.

Bien que les noms de domaine ne soient pas les seuls éléments d'une bonne stratégie de présence sur internet, ils en sont des composants incontournables.

On peut résumer par le schéma reproduit ci-dessous, développé par Loïc Damilaville dans le cadre de ses activités de conseil, les différentes raisons qu'une société peut avoir de déposer des noms de domaine :



1. Occupation de terrain : la première des raisons identifiées peut être de déposer des noms de domaine génériques, donc correspondant à des mots du dictionnaire, dans le but de s'en assurer le contrôle avant que des tiers ne s'en emparent. Ces noms génériques peuvent notamment désigner des métiers ou secteurs d'activité où l'entreprise est présente.

2. Captation de trafic : une autre raison de déposer des noms de domaine, toujours génériques, peut être de chercher à capter du trafic par leur intermédiaire. L'entreprise ne communiquera jamais dessus, mais le trafic spontané qu'ils apportent peut s'avérer particulièrement précieux.

3. Défense des marques : l'entreprise, lorsqu'elle définira son périmètre de sécurité, aura à cœur de lister ses marques et de chercher à protéger celles sur lesquelles elle a engagé des dépenses en termes de création de notoriété, et/ou celles sur lesquelles elle pense investir dans l'avenir. L'approche ici sera donc de protéger des noms liés à ces marques sans nécessairement vouloir les utiliser comme capteurs de trafic.

4. Optimisation de la présence : bien que les noms de domaine ne soient pas les seuls éléments d'une bonne stratégie de présence sur internet, ils en sont des composants incontournables, ne serait-ce que pour les adresses des sites sur lesquelles l'entreprise communiquera, et pour les adresses de courrier électronique dont ils seront les supports (<xxxx@nomdelentreprise.com> par exemple).

Ce schéma appelle deux remarques complémentaires :

– en premier lieu, il peut être utile pour toute entreprise possédant des noms de domaine de « scanner » son portefeuille en essayant de qualifier ses noms de domaine en fonction de la nomenclature proposée. Cela lui permettra d'identifier les noms stratégiques et ceux qui le sont moins, les noms qu'elle a déposés et qu'elle devrait utiliser ou envisager d'abandonner ;

– en second lieu, ce shéma ne prend tout son sens que lorsque l'entreprise a pu préalablement définir ses besoins en matière de noms de domaine. On a évoqué ci-dessus les concepts de périmètres de sécurité et de communication ; ceux-ci ne peuvent être fixés que si l'entreprise a une connaissance précise des marchés sur lesquels elle intervient, des marques qu'elle exploite, ainsi que de ses diverses filiales et implantations dans le monde. Dans l'idéal, chacun de ces éléments est qualifié en termes d'importance stratégique pour l'entreprise, ce « *coefficient* » pouvant être une clef de

lecture intéressante au moment de préciser les contours des deux périmètres évoqués ci-dessus.

Le responsable noms de domaine doit garder présentes à l'esprit les diverses formes de menaces qui pèsent sur l'identité de son entreprise sur internet au travers des noms de domaine. Pour ce faire, il a intérêt à lister les principales formes de *cybersquatting*, qui comprennent notamment :

– le *cybersquatting* proprement dit (aussi appelé « accaparement de nom de domaine ») : enregistrer un nom de domaine dans le but de le revendre ultérieurement à celui –habituellement une société ou une personne bien connue– qui, intuitivement, devrait en être le titulaire ;

– le piratage de nom de domaine à l'envers : le pirate enregistre une marque déposée identique à un nom de domaine existant. Après quoi, il poursuit en justice le titulaire du nom de domaine en avançant l'argument selon lequel ce titulaire viole ses droits. Cette technique de *cybersquatting* échoue heureusement le plus souvent ;

– le *squat* de points : il s'agit d'une forme spécifique de *cybersquatting* utilisant la même adresse que celle de la victime sans point après le fameux < www > (par exemple < http://wwwcompany.com au lieu de http://www.company.com >) ;

– le *typosquatting* : autre forme spécifique de cybersquatting exploitant des « *fautes d'orthographe* » (par exemple < http://www.companny.com > au lieu de < http://www.company.com >).

Ainsi, si l'on souhaite enregistrer < worldofpleasure > comme nom de domaine principal, on pourrait considérer que les noms ci-dessous sont « *proches* » :
world-of-pleasure ; world-ofpleasure ; worldof-pleasure ; world-of-pleasures ; world-ofpleasures ; worldof-pleasures ; worlds-of-pleasure ; worlds-ofpleasure ; worldsof-pleasure ; worlds-of-pleasures ; worlds-ofpleasures ; worldsof-pleasures ; aworldofpleasure ; a-world-of-pleasure ; worldpleasure ; world-pleasure ; etc.

C'est un travail difficile et fastidieux, mais qui s'avère en réalité le meilleur moyen d'éviter de perdre du temps et de l'argent en jugements et autres procédures. Des logiciels spécifiques peuvent aider à la rédaction de la liste.

La liste non exhaustive fournie à titre d'exemple illustre parfaitement le fait qu'il est quasiment impossible de déposer toutes les variantes possibles autour d'un vocable, surtout si celui-ci est composé de plusieurs termes. Il faudrait en effet couvrir les variantes de chacun des termes au singulier et au pluriel, voire les variantes phonétiques ou orthographiques lorsqu'il existe des ambiguïtés, ces différentes possibilités étant ensuite combinées entre elles en formules avec et sans traits d'union.

Cette liste présente aussi l'intérêt de montrer le contraste assez fort entre les diverses variantes possibles en termes d'intuitivité et de « *valeur-visibilité* » pour l'entreprise. Les plus évidentes feront naturellement partie du périmètre de sécurité tandis que les plus éloignées du terme utilisé pour communiquer seront simplement mises en surveillance sans dépôts de noms de domaine. Il appartient au responsable Noms de domaine et/ou au groupe de travail noms de domaine d'apprécier les contours des différents périmètres, en s'appuyant le cas échéant sur des règles définies à l'avance et compilées dans un document de référence que l'on désigne fréquemment sous le nom de « *Charte de nommage* ».

La Charte de nommage a pour objectif essentiel de formaliser les orientations de la stratégie de nommage (que déposer et où ?), de préciser un certain nombre de règles opérationnelles (quels titulaires ?, quels contacts ?) et parfois même de fixer l'organisation et l'articulation des intervenants autour du dossier. Dans l'idéal, cette Charte est aussi un document permettant au responsable Noms de domaine de communiquer en interne autour de ce dossier et des enjeux qui y sont liés.

Pour revenir à la démarche d'enregistrement, il paraît clair qu'une société doit aujourd'hui considérer que l'enregistrement de plusieurs noms de domaine incontournable. Cette liste doit inclure au moins toutes les marques déposées (du moins, les marques exploitées et d'une certaine importance pour l'entreprise) et autres logos pour lesquels la société dispose d'une exclusivité (par exemple, une dénomination commerciale, le nom d'une compagnie, etc.).

Lorsqu'il détermine le nom de domaine principal et les noms proches, le candidat à l'enregistrement doit combiner à la fois le point de vue de la protection et celui de la cible (voir ci-après).

II. – CHOISIR DES METATAGS

Les métatags sont des codes HTML habituellement invisibles pour le visiteur, sauf si celui-ci demande à lire le code-source de la page web. Il existe plusieurs types de métatags (1), mais la catégorie la plus connue sert à permettre aux moteurs de recherché d'indexer et de classer les sites web selon leur contenu. Par exemple, un site web concernant le football comprendra au moins le mot « *football* » dans son métatag.

Les métatags sont aujourd'hui moins cruciaux qu'avant car il existe à présent d'autres techniques plus efficace d'optimisation de la présence sur les moteurs de recherche, mais ils demeurent néanmoins utiles.

L'absence de toute forme d'enregistrement constitue la grande différence entre métatags et noms de domaine : n'importe quel titulaire de site web peut librement décider quels métatags il souhaite inclure dans son code-source.

Ce *modus operandi* se voit fréquemment utilisé dans le but de :

– augmenter artificiellement le nombre de visiteurs (on peut par exemple inclure le mot « *sexe* » dans le métatag, même si le site n'a rien à voir avec le sexe afin d'apparaître dans la liste des résultats chaque fois que quelqu'un tape « *sexe* » sur un moteur de recherches) ;

– gagner des visiteurs (inclure le nom d'un concurrent dans le but de figurer sur la liste des résultats lorsque quelqu'un tape le nom du concurrent dans un moteur de recherches).

À côtés de ces usages potentiellement illégaux, le métatag peut se montrer très utile :

– un sponsor pourra l'utiliser afin de s'assurer qu'il figurera dans la liste des résultats lorsque quelqu'un essaie d'obtenir des informations concernant un évènement (par exemple, les sponsors de la Coupe du monde sont habilités à inclure « *coupe du monde* » dans leurs métatags) ;

– il permettra à une société d'obtenir des références croisées pour ses sites web (ainsi, si un même produit est vendu dans le monde sous différents noms commerciaux et s'il existe un site web par nom, il sera utile d'introduire sur tous les sites web les différents noms commerciaux comme métatags).

– il pourra être utilisé par des groupes de sociétés ou des holdings pour croiser les références de tous leurs sites web. Le groupe de travail des noms de domaine travaillera en étroite coopération avec tous les départements de la société afin d'établir la liste de tous les métatags adéquats. Par exemple, le département marketing fournira la liste de tous les évènements sponsorisés, et le groupe de travail s'assurera, avec le concours du département juridique, que le contrat liant la société à l'organisateur de l'évènement stipule que son nom (ou celui de ses produits) figure dans les métatags du site web de l'évènement.

(1) Comprenant par exemple « *nouvelle visite* », « *description* », « *mot-clé* », « *robots* », « *taux* », « *copyright* », « *auteur* », « *langue* », « *générateur* », etc.

III. – OPTER POUR UN gTLD ET/OU UN ccTLD

Après avoir choisi les différents noms de domaine, il faut considérer le « *Top Level* » pour lequel on se portera candidat à l'enregistrement. Il existe pour l'instant deux familles de « *Top Level* » :

– le *Top Level* générique (gTLD pour *generic Top Level*), qui comprend les fameux < .com >, < .net > et < .biz >. Les gTLDs sont enregistrés au niveau mondial

– le *Top Level* avec code du pays (ccTLD pour *country code Top Level*), enregistré au niveau national (< .be >, < .fr >, < .us >, etc.). Depuis peu, un ccTLD < .eu > existe qui permet de considérer l'Union européenne comme un territoire et d'insister ainsi sur le côté européen du site.

Certaines situations sont assez simples. Par exemple, toutes les marques déposées doivent au moins être enregistrées en tant que nom de domaine dans tous les pays dans lesquels la marque est déposée. Autre cas : le site d'une multinationale doit au moins être enregistré (ccTLD) dans tous les pays dans lesquels la compagnie est installée. La situation s'avère cependant souvent plus difficile à évaluer, c'est pourquoi certaines sociétés ont adopté la règle selon laquelle chaque enregistrement de nom de domaine aura lieu pour tous les ccTLDs et gTLDs pour lesquels il est disponible (Coca-Cola, la « *world company* », opère de cette façon).

Pour reprendre l'exemple de < worldofpleasure.com >, si ce site est consacré à un produit vendu uniquement en Allemagne, le groupe de travail pourrait envisager de l'enregistrer non seulement en < .com >, mais également en < .de > et même sous les ccTLDs des pays voisins de l'Allemagne (Autriche, Pologne, Pays-Bas, Belgique, etc.), car certains clients originaires de ces pays pourraient acheter le produit en Allemagne.

Afin d'éviter toute mésaventure, il sera aussi pertinent de protéger les termes « *world of pleasure* » en allemand.

Ainsi, on peut distinguer trois questions-clefs à se poser :

– au niveau du choix des vocables (marques, noms commerciaux...) ;

– au niveau des « *extensions* » (gTLDs et ccTLDs) ;

– au niveau des langues et graphies, d'autant plus que les noms de domaine en caractères naturels (IDN) tendent à se répandre de plus en plus largement. Les variantes de « *world of pleasure* » en allemand devront impérativement être déposées en caractères non accentués habituels comme en caractères allemands traditionnels, lorsque cela est techniquement possible.

Lorsqu'il aborde la question, celui qui souhaite enregistrer un nom de domaine doit par ailleurs combiner deux approches :

1. Le point de vue de la protection implique qu'il doit protéger son bien (voir le schéma ci-dessus). Par exemple, il pourrait décider que tous ses avoirs en propriété intellectuelle doivent être protégés en tant que noms de domaine dans tous les pays et sous tous les gTLDs.

Le candidat à l'enregistrement, s'étant décidé pour un gTLD (par exemple < .com >), essaiera habituellement, en application de ce point de vue d'enregistrer tous les autres gTLDs publics (< .net >, < .biz >, etc.). Les conséquences se comprennent aisément. Ayant omis de se conformer à ce principe, la Maison Blanche n'a enregistré que < http://www.whitehouse.gov > en tant que site web officiel ; très vite, deux autres personnes ont enregistré < http://www.whitehouse.org > (site satirique) et < http://www.whitehouse.com > (site à contenu pornographique revendu à une société de recrutement).

Une politique efficace en matière de noms de domaine fait partie intégrante du plan d'entreprise et doit s'appuyer sur une connaissance exhaustive de ses activités, projets, portefeuille de marques déposées, etc.

2. Le point de vue de la cible implique que le candidat doit tout d'abord, analyser la cible de son site web et ensuite, considérer comme indispensable d'enregistrer au moins tous les TLDs pertinents prenant sa cible en compte. Par exemple, si un produit est vendu sous différents noms dans différents pays, il faut au moins enregistrer tous les noms nationaux sous les ccTLDs correspondants, avec les variantes linguistiques locales adéquates.

IV. – VERIFICATIONS AVANT L'ENREGISTREMENT

Après avoir choisi les noms à enregistrer et les ccTLDS et/ou gTLDs pertinents, le candidat devrait faire une vérification préliminaire dans les bases de données publiques *Whois*, afin de s'assurer qu'il n'existe pas de problème d'antériorité. Il pourrait en effet apparaître à ce stade qu'un nom ou un *Top Level* a déjà été enregistré par quelqu'un d'autre.

Il est important de souligner qu'un résultat positif à cette vérification (le nom est encore disponible) ne signifie pas que le nom sera accepté quand on se portera candidat. En effet, un certain nombre de ccTLDs sont soumis à des règles strictes d'éligibilité (qui peut avoir quoi ?) de sorte que l'autorité qui gère cette zone pourrait refuser une demande en application de ces règles. La France (< .fr >) fait partie de ces ccTLDs restrictif. En outre, un résultat *Whois* favorable ne signifie pas non plus que l'usage du nom sera possible (par exemple, en dépit du fait qu'un nom soit accordé au candidat, un tiers pourrait s'opposer à son utilisation en raison de ses droits de propriété intellectuelle).

Le but de cette vérification est seulement de détecter l'enregistrement antérieur d'un nom de domaine identique. Elle s'avère néanmoins utile, notamment pour deux raisons :

1. à ce stade, il est habituellement encore possible pour le candidat d'amender son plan, d'abandonner un nom ou d'entreprendre une action dans le but d'en acquérir un autre ;

2. un problème d'enregistrement, ou un enregistrement interrompu constitue toujours une mauvaise publicité pour le candidat... et éventuellement une occasion pour ses concurrents.

En résumé :

– une société doit aborder sa stratégie en matière de noms de domaine à un niveau global, élevé dans sa hiérarchie décisionnelle et de façon transversale ;

– une politique efficace en matière de noms de domaine fait partie intégrante du plan d'entreprise et doit s'appuyer sur une connaissance exhaustive de ses activités, projets, portefeuille de marques déposées, etc. ;

– cela implique une collaboration étroite entre plusieurs ressources internes et externes à l'entreprise ;

– lorsqu'il s'agit de gérer plusieurs noms de domaine, cela doit signifier un haut de gré de centralisation et de coopération entre les différentes personnes, filiales et succursales ;

– la politique doit être flexible afin de pouvoir s'adapter aux besoins évolutifs de l'entreprise ;

– il existe différentes raisons de déposer des noms de domaine ; l'entreprise doit les connaître et définir des périmètres de sécurité et de communication qui lui permettront de savoir quels sont les noms importants pour elle ;

– il existe au moins trois dimensions à prendre en considération : les marchés, les pays et les marques, en intégrant les spécificités de chacun en termes linguistiques et/ou de maturité dans le cycle de vie de l'entreprise.

V. – ENREGISTREMENT D'UN NOM DE DOMAINE

A. – Informations à fournir

1. Quelles informations ?

Plusieurs informations doivent être communiquées aux unités d'enregistrement (*registrar*) ; en voici quelques unes. Nous avons également listé une série de recommandations :

Candidat à l'enregistrement * (titulaire)	Enregistrer un nom de domaine au nom d'un fournisseur, d'un employé de la société ou même au nom du président directeur général est à éviter. Il est généralement préférable de l'enregistrer au nom de la société.
Contact administratif *	Le contact administratif joue un rôle clé. Il conserve le pouvoir exécutif en permanence et doit être autorisé à prendre seul des décisions relatives au nom de domaine. Il est donc essentiel de donner ce rôle à une personne qualifiée entraînée à la gestion de noms de domaine.
Contact comptable * ou de facturation	Ce contact gère les renouvellements de noms de domaine au nom de la société. Il est important de souligner que beaucoup de problèmes surgissent pour cause de mauvais contact comptable (par exemple, l'adresse e-mail d'un employé, à laquelle on envoie l'avis de renouvellement, ne fonctionne plus et personne ne s'occupe de l'avis en question).
Contact technique *	Ce contact devrait idéalement se voir attribué au fournisseur d'accès internet (FAI) responsable de l'administration de serveurs de noms de domaine sur lesquels ces noms sont hébergés. Si la firme détient et gère elle-même ses serveurs, le responsable sert habituellement de contact technique.

* La formulation exacte peut varier en fonction du pays et/ou du fournisseur.

2. Comment fournir cette information ?

L'information délivrée doit être constante et intemporelle, indépendamment de la personne physique et du fournisseur ; il s'agit d'un point clé.

En effet, si l'information dépend d'une personne ou d'un fournisseur, elle doit être actualisée en cas de modification (un employé peut changer de société ou de département au sein de la société, un fournisseur peut en remplacer un autre). On constate qu'en pratique, la mise à jour a rarement lieu, entraînant parfois de lourdes conséquences pouvant aller jusqu'à l'effacement du nom de domaine.

B. – L'attribution du nom de domaine

Pour la plupart des gTLDS (<.com.>, <.net> et <.org> notamment), l'enregistrement se base sur le principe « *premier arrivé, premier servi* » : l'autorité qui gère l'enregistrement ne pratique pas de contrôle au moment de celui-ci. L'enregistrement est automatiquement accepté si le nom est disponible. Certains gTLDs, réservés à une catégorie limitée de candidats, constituent l'exception à la règle (par exemple <.museum> et <.aero>).

Certains ccTLDs nationaux fonctionnent selon le même principe « *premier arrivé, premier servi* » (la Belgique entre autres), mais certains (de plus en plus rares toutefois) ont une politique d'enregistrement stricte en vue d'évaluer, avant enregistrement, si le candidat a le droit de postuler pour le nom de domaine.

Sans prendre en compte l'existence d'un contrôle préliminaire, un tiers peut toujours demander au titulaire de cesser d'utiliser le nom de domaine et/ou de le lui transférer. Dans la plupart des cas, une telle action se base sur des considérations de propriété intellectuelle, pratiques équitables et droit de la concurrence (voir ci-dessous : VII).

C. – L'attribution des métatags

Une grande différence entre les métatags et les noms de domaine est l'absence de tout type d'enregistrement : n'importe quel titulaire de site web peut librement décider quels métatags il souhaite inclure dans les codes-sources.

Il va sans dire que, si l'usage d'un métatag constitue une infraction à la loi ou aux droits d'une tierce partie, le nom de domaine peut devenir l'objet d'un litige (voir ci-après : VII).

En résumé :

– il est important de préparer l'information à transmettre au moment de l'enregistrement ;

– cette information doit être logique et tenir compte de la situation de la société ; elle doit être indépendante d'une personne physique et intemporelle ;

– on veillera à harmoniser autant que possible l'information technique et comptable au sein de la société ;

– même en cas de vérification préliminaire opérée par l'autorité d'enregistrement, l'attribution d'un nom de domaine ne garantit pas qu'aucun tiers ne le revendique à l'avenir ;

– les métatags sont gratuits (pour autant évidemment, qu'ils n'enfreignent aucune loi ni ne portent atteinte aux droits d'un tiers).

VI. – UTILISATION D'UN NOM DE DOMAINE

La façon la plus naturelle d'utiliser un nom de domaine est de placer un site web à son adresse, mais ce n'est pas le seul mode d'utilisation.

On peut notamment imaginer :

– enregistrer un nom de domaine sans l'utiliser (« *enregistrement défensif* ») : c'est souvent le cas lorsqu'un *cybersquatter* enregistre un nom de domaine correspondant à une marque déposée en vue de le revendre ultérieurement, mais également lorsque le département marketing ou le département R & D sont sur le point de diffuser un nouveau produit ou d'entamer une nouvelle campagne et veulent s'assurer de l'obtention du nom le plus approprié ;

– pointer le nom vers une « *page d'attente* » : le site ne contient aucune information, excepté un message d'attente (« *site en construction* » par exemple). Les *cybersquatters* désirant dissimuler un enregistrement défensif utilisent souvent ce *modus operandi* ;

– rédiriger le visiteur vers un autre site web : il s'agit de la situation typique des noms de domaine proches.

>

VII. – APPLICATION

A. – Monitoring

Dès qu'une société considère comme importante la propriété de noms de domaine, elle doit envisager leur monitoring. Cette tâche se voit habituellement confiée à un fournisseur spécialisé équipé de services de monitoring sophistiqués parcourant le web et les noms enregistrés (parfois même à une échelle mondiale comprenant les ccTLDs) afin de détecter tous les usages potentiellement délétères. La liste des « *noms de domaine proches* » rédigées avant l'enregistrement constitue souvent une aide précieuse, mais les nouveaux logiciels emploient beaucoup d'autres outils technologiques englobant le monitoring des métatags.

Il faut souligner qu'il apparaît absurde d'organiser le monitoring des noms de domaine si l'on n'applique pas la même procédure aux métatags. En réalité, les métatags se montrent potentiellement plus nuisibles, car plus difficiles à détecter et à surveiller.

B. – Application

Dès lors que la société a décidé de combattre un usage nuisible de nom de domaine, trois attitudes sont possibles : la résolution hors tribunal, l'ADR ou la procédure légale.

1. Résolution hors tribunal

Il va sans dire que les parties peuvent se mettre d'accord sans intervention du tribunal. Le coût, bien que fréquemment élevé, s'avère très souvent moindre que celui d'une procédure judiciaire, et la démarche plus rapide.

2. Alternative Dispute Resolution (ADR)

L'ADR est un procédé de résolution de conflits pour lequel les parties acceptent de soumettre leur problème à un comité d'arbitrage.

L'UDRP *(Uniform Domain Name Dispute-Resolution Policy)* est une des procédures ADR les plus connues, qui vise essentiellement les conflits de noms de domaine gTLD, dont la rédaction résulte d'une collaboration entre l'ICANN (2) et le WIPO (3). Chaque registre de gTLD doit insérer une clause de contrat rendant l'UDRP obligatoire pour les propriétaires de gTLD.

Dans une procédure UDRP, le plaignant doit démontrer trois éléments :

– le nom de domaine est identique ou pourrait engendrer la confusion avec une marque déposée ou une marque de service pour laquelle le plaignant détient des droits ;

– le titulaire n'a ni droits ni intérêts légitimes vis-à-vis du nom de domaine en question ;

– le nom de domaine a été enregistré et/ou est utilisé de mauvaise foi. Afin de se prononcer sur la mauvaise foi, le comité d'Arbitrage tiendra compte de tous les éléments d'information disponibles, notamment :

– les circonstances indiquant que le nom de domaine a été enregistré ou acquis dans le but premier de le vendre, le louer ou de le transférer au plaignant ;

– le nom de domaine a été enregistré afin d'empêcher son dépositaire de refléter la marque, alors que c'est l'attitude habituellement adoptée par le dépositaire en question ;

L'UDRP *(Uniform Domain Name Dispute-Resolution Policy)* est une des procédures ADR les plus connues, qui vise essentiellement les conflits de noms de domaine gTLD.

– le nom de domaine a été enregistré dans le but premier de perturber la bonne marche des affaires d'un concurrent ;

– le nom de domaine a été enregistré dans l'intention de gagner des visiteurs sur internet en rendant probable la confusion avec la marque du plaignant, comme si le site web du titulaire, ou l'un de ses produits ou services, en constituait la source, le sponsor, l'affilié ou bénéficiait de son approbation. Il faut souligner que la possibilité de confusion, particulièrement en ce qui concerne le consommateur, servira de critère de base.

En dépit de l'uniformité de cette procédure de résolution de conflits, il est bien connu que certains comités d'arbitrage (le WIPO par exemple) favorisent plus les détenteurs de marques déposées que d'autres. Selon la nature des droits sous-jacents du plaignant, il pourrait s'avérer utile de « passer en revue » les différents comités d'Arbitrage et d'opérer un choix en conséquence.

Les deux principaux avantages de l'UDRP sont :

– assurer l'efficacité de la décision : si le Comité tranche en faveur du plaignant et accorde un transfert de nom de domaine, ce transfert se fera automatiquement pour autant que la partie défenderesse n'entame pas de procédure légale devant un tribunal dans un délai donné ;

– au cas où l'on se trouverait dans l'impossibilité de localiser le *cybersquatter* (par exemple parce qu'il a donné une fausse adresse au moment de l'enregistrement), il suffit de prouver à l'arbitre que, tous les efforts raisonnables ayant été entrepris, le titulaire du nom de domaine demeure injoignable.

Le coût d'un arbitrage UDRP peut varier entre 1 500 dollars et 2 000 dollars pour un litige comprenant de 1 à 10 noms de domaines et nécessitant un seul arbitre. Il n'existe pas de système de remboursement des honoraires de l'avocat.

Une procédure similaire existe pour le < .eu >, si ce n'est que les conditions cumulatives de l'UDRP perdent ce caractère, et que le champ d'application dépasse le strict droit des marques : conformément à l'article 21 du Règlement EU 874/2004, « *un nom de domaine (< .eu >) est révoqué, dans le cadre d'une procédure extrajudiciaire ou judiciaire appropriée, quand un nom de domaine enregistré est identique ou susceptible d'être confondu avec un nom sur lequel un droit est reconnu ou établi par le droit national et/ou communautaire, tel que les droits mentionnés à l'article 10, paragraphe 1, et que ce nom de domaine : a) a été enregistré sans que son titulaire ait un droit ou intérêt légitime à faire valoir sur ce nom, ou b) a été enregistré ou utilisé de mauvaise foi* ».

On peut également avoir recours à l'UDRP pour certains ccTLDs, lorsque l'autorité nationale concernée l'a adoptée (4).

Bien que l'URDP ne soit pas en vigueur dans d'autres pays en ce qui concerne les litiges de ccTLD, des principes similaires sont en général appliqués. La France a elle aussi adopté une procédure d'arbitrage appelée PARL.

En réalité, il y a trois PARL :

– PARL par « *recommandation en ligne* » administrée par le Centre de médiation et d'arbitrage de Paris (CMAP). Cela permet de confier, d'un commun accord, à un « *tiers aviseur* » désigné par le CMAP, la mission de formuler une recommandation.

Si la recommandation est acceptée par les parties elle est alors utilisée pour ré-

---

(2) *Internet Corporation for Assigned Names and Numbers.* (ICANN) : organisme sans but lucratif créé pour assurer la coordination technique de l'internet (attribution des adresses IP, gestion de la base de données administrative des extensions de premier niveau (gTLDs et ccTLDs). **(3)** *World Intellectual Property Organization :* <http://www.wipo.org>. **(4)** AC (Île de l'Ascension), <.AG> (Antigua & Barbuda), <.AS> (Samoa américaines), <.BS> (Bahamas), .BZ (Belize), <.PA> (Panama), <.PH> (Philippines), <.PN> (Île de Pitcairn), <.CY> (Chypre), <.EC> (Équateur), <.FJ> (Îles Fiji), <.GT> (Guatemala), <.LA> (Laos), <.MX> (Mexique), <.NA> (Namibie), <.NU> (Île de Niue), <.RO> (Roumanie), <.SH> (Saint-Helena), <.TT> (Trinidad et Tobago), <.TV> (Tuvalu), <.VE> (Venezuela), <.WS> (Samoa occidentales).

diger un protocole transactionnel et mettre fin au litige. La solution retenue sera alors mise en œuvre par l'AFNIC sur demande du prestataire gérant le nom de domaine.

C'est une sorte de médiation sauf que cela nécessite que les parties s'accordent aussi bien pour lancer la procédure que pour appliquer la recommandation du tiers aviseur ;

– PARL par « *décision technique* », administrée par le Centre d'arbitrage et de médiation de l'Organisation mondiale de la propriété intellectuelle (OMPI). Cette PARL est soumise à la procédure UDRP de sorte que les conditions sont *grosso modo* similaires ;

– PARL du < .fr > par « *médiation* », administrée par le Forum des droits sur l'internet. Ce dernier assure le règlement extrajudiciaire des conflits portant sur les noms de domaine en < .fr > enregistrés par des particuliers (personnes physiques).

3. Procédures judiciaires

Un plaignant a évidemment le droit de saisir un tribunal.

Il s'agit fréquemment d'un processus de longue durée, notamment à cause des implications internationales. Le plaignant doit d'abord déterminer dans quel pays il déclenchera la procédure et quelle loi le juge pourra appliquer. En outre, même si le tribunal tranche en faveur du plaignant, sa décision pourrait ne pas se voir appliquée si le titulaire réside dans un autre pays.

Ceci dit, la procédure juridique pourrait s'avérer plus avantageuse dans certaines circonstances, par exemple quand le plaignant et la partie défenderesse résident dans le même pays, ou quand le fond de l'action relève plus de la législation de la concurrence que de celle de la propriété intellectuelle (l'expérience montre que les comités d'arbitrage se montrent plus réceptifs envers les lois de la concurrence et des pratiques équitables qu'envers les lois concernant la propriété intellectuelle -en cas d'URDP, la situation devient encore plus claire puisque l'arbitre n'est compétent que si le nom de domaine est d'une similarité propre à engendrer la confusion ou identique à un nom de marque déposée ou de marque de service sur lequel le plaignant détient des droits).

Si le plaignant veut obtenir une compensation financière suite à son action, il doit en règle générale entreprendre une procédure juridique. ◆