reverse domain name hijacking

publié le **18/01/2014**, vu **2596 fois**, Auteur : IPNESS

Le "reverse domain name hijacking" est une utilisation abusive de la procédure UDRP souffrant d'une absence de sanction et illustrée récemment par une décision du centre d'arbitrage et de médiation de l'OMPI

OMPI, Centre d'arbitrage et de médiation, 30 décembre 2013, n°D2013-2094, RPG Life Sciences Ltd. v. James Mathe, nom de domaine rpglife.com, expert unique M. Nicholas Weston, décision de rejet. http://www.wipo.int/amc/en/domains/search/text.jsp?case=D2013-2094

Le requérant est la société indienne RPG life sciences possédant une activité dans le domaine pharmaceutique et des biotechnologies, elle est présente dans plusieurs pays dont les Etats-Unis et titulaire des marques indiennes RPG depuis 1999 et RPG LIFE depuis octobre 2012.

Le défendeur est une personne physique habitant aux Etats-Unis, ayant enregistré le nom de domaine rpglife.com le 28 octobre 2005 et proposant un site de vente en ligne de jeux et accessoires relatifs aux « Role-Playing-Games », soit des jeux à travers lesquels des personnes prétendent être des personnages de fiction de type Dongeons & Dragons.

Cette décision continue d'illustrer la notion de « reverse domain name hijacking » ou « recapture illicite de noms de domaines » en français.

Il s'agit de l'utilisation de la procédure UDRP de mauvaise foi afin de tenter de priver un tiers du nom de domaine enregistré par ses soins.

Cet abus est définit par le paragraphe 15(e) des principes directeurs UDRP : « *[…] Si, au vu des éléments qui lui ont été soumis, la commission constate que la plainte a été introduite de mauvaise foi, par exemple dans une tentative de recapture illicite de nom de domaine, ou qu'elle l'a été principalement dans le but de harceler le détenteur du nom de domaine, la commission déclare dans sa décision que la plainte a été introduite de mauvaise foi et constitue un abus de procédure administrative* ».

Dans le cadre de cette procédure, le défendeur soulève en réponse que le requérant se livre à un acte de « *reverse domain name hijacking* ».

En l'espèce, l'expert retient que le représentant du requérant devait relever, même après un examen rudimentaire des principes UDRP, que la requête était vouée à l'échec dans la mesure ou le nom de domaine litigieux est constitué d'un acronyme (RPG) largement reconnu pour promouvoir la vente de biens et services dans le domaine des jeux « Role-Playing-Games » et utilisé comme tel par le défendeur, il n'avait donc aucun espoir raisonnable de pouvoir remplir les critères de l'article 4 (a) des principes UDRP[1].

Le paneliste conclut que le requérant savait où aurait dû savoir selon une juste interprétation des faits raisonnablement appréhendables que le défendeur n'avait ni enregistré ni utilisé le nom de domaine de mauvaise foi et que la plainte à été formée avec un mépris volontaire des principes

UDRP ce qui constitue un abus de la procédure administrative.

Dans le cadre d'une stratégie de libération des droits, des sociétés peuvent être tentées de faire pression sur des personnes physiques par le biais de la procédure UDRP afin de tenter de récupérer un nom de domaine qui les intéresse particulièrement à moindre coût, alors même qu'il est enregistré/utilisé légitimement et de bonne foi.

Les procédures qualifiées de « *reverse domain name hijacking* » ont ainsi été constituées aux regards de plusieurs éléments, tels qu'un re-dépôt de plaintes constitutives d'un harcèlement[2] voire de plaintes déposées suite au refus express ou tacite du défendeur de vendre le nom au requérant[3].

Comme l'évoque la décision du paneliste, la procédure UDRP implique un investissement en termes de temps et surtout d'argent, ce qui rend le dévoiement de la procédure à des fins de prédation inacceptable.

La notion de « *reverse domaine name hijacking* » est appréciable en ce qu'elle permet à un défendeur de mettre en exergue le caractère abusif de la procédure mais elle est critiquée depuis de nombreuses années n'étant assortie d'aucune sanction, l'expert paneliste se bornant à mentionner l'abus dans sa décision et assez paradoxalement de sorte à ce qu'elle soit bien motivée.

Certes, le requérant en sera pour ses frais (1500$ de frais de procédure minimum), mais le défendeur qui a mandaté un conseil pour répondre à la plainte n'est pas sans souffrir une absence de réparation de son préjudice.

La meilleure solution pourrait résider dans la demande par l'OMPI d'une provision destinée à réparer ce préjudice éventuel qui serait rendue au requérant à la fin de la procédure, ce qui nécessiterait une modification des principes UDRP.

L'on pourrait songer en France à une action fondée sur l'article 1382 du code civil mais le caractère international de tels litiges est très dissuasif.

Certaines procédures nationales dont la procédure DRS auprès de *Nominet UK* en Angleterre, prévoient des sanctions. La procédure DRS précitée prévoit ainsi que si trois plaintes formées par le même requérant sont constitutives de « *reverse domain name hijacking* » en moins de 2 ans, aucune de ses plaintes ne sera reçue pendant deux ans.

La procédure URS (Uniform Rapid Suspension system), prévue dans le cadre du lancement des nouvelles extensions de noms de domaine, est censée apporter une solution aux inconvénients de l'actuelle procédure UDRP (Uniform Domain Name Dispute) en sanctionnant ce type de pratiques.

Tout d'abord, le requérant peut être soumis au versement de pénalités dont le montant n'a pas encore été déterminé. Celui-ci peut également être placé sur liste noire, pendant une durée d'un an s'il a initié deux procédures abusives ou une procédure avec intention de nuire, ou de façon définitive s'il a initié deux procédures avec intention de nuire.

Un alignement des sanctions dans le cadre de la procédure UDRP serait plus protecteur des personnes physiques amenées à faire face à des stratégies prédatrices de libération des droits de grandes sociétés sans scrupules ou tout simplement peu regardantes.

L.B.V

[1] Selon lequel le requérant doit démontrer que le nom de domaine est identique ou semblable au point de prêter à confusion, à une marque de produits ou de services sur laquelle il a des droits (i) ; que le défendeur n'a aucun droit sur le nom de domaine et aucun intérêt légitime qui s'y rattache (ii) ; que le nom de domaine à été enregistré et utilisé de mauvaise foi (iii)

[2] OMPI, centre d'arbitrage et de médiation, 29 juill. 2009, n° D2009-0540, Cheung Kong (Holdings) Limited et Chueng Kong Property Development Limited c/ Netego DotCom, experts David H. Bernstein, C. K. Kwong, David E. Sorkin, rejet : www.wipo.int/amc/en/domains/decisions/html/2009/d2009-0540.html ; Propriété industrielle n° 11, Novembre 2009, alerte 141 ; Notions de plainte re-déposée et de reverse domain name hijacking, Veille par Nathalie DREYFUS**.**

[3] OMPI, centre d'arbitrage et de médiation, 20 juin 2011, n° D2011-0596, Futuris Automotive Interiors Pty Ltd c/ X9 Interactive LLC, nom de domaine , experts Andrew D. S. Lothian, Andrew F. Christie et Michael A. Albert, rejet, Propriété industrielle n° 10, Octobre 2011, alerte 75 Appréciation de la notion de reverse domain name hijacking, Veille par Nathalie DREYFUS