CHIOMENTI

Newsletter

Dipartimento IP, TMT e Data Protection
"Cybersquatting": quali soluzioni per i titolari dei nomi a dominio?

Marzo 2021

INDICE

I. IL *DOMAIN NAME SYSTEM*

Per un'adeguata comprensione del fenomeno del *cybersquatting* è necessario fissare alcuni concetti preliminari con riguardo al *Domain Name System* ("**DNS**")[1]. Il DNS è concepito secondo una logica "multilivello", cui corrisponde un'architettura gerarchica di deleghe, a determinati soggetti, capitanata dalla *Internet Corporation for Assigned Names and Numbers* ("**ICANN**")[2]. Da ciò deriva la stessa conformazione del nome a dominio, costituito da una stringa, da leggersi da destra verso sinistra e strutturata come segue:

- **Livello radice (*Root Level*)** – è il punto finale a destra del nome di dominio, nel verso senso del termine: si tratta di un <.>, implicito nella stringa visibile e operato dai c.d. *root name servers* (attualmente sono 13 in tutto il mondo) e amministrato dalla *Internet Assigned Numbers Authority* ("**IANA**") all'uopo istituita da ICANN.
- **Primo livello (*Top Level Domain – TLD*)** – è la sigla alfanumerica che occupa l'ultima parte visibile a destra del nome di dominio, formato da termini predeterminati e suddivisi in varie categorie, come i *Country Code Top-Level Domain* (ccTLD) tra cui <.it>, <.eu> etc., ovvero i *Generic Top-Level Domain* (gTLD) tra cui <.com>, <.net>, <.org> etc.

  È gestito dagli operatori di registro (*"**Registries**"*), quali organizzazioni delegate da IANA, cui sono assegnati uno o più TLD (*e.g.*, <.it> è gestito da *Registro.it* nell'alveo dell'*Istituto di Informatica e Telematica del CNR*) per amministrarne le politiche di assegnazione nonché il *database* di registro centrale dei relativi *domain name* registrati.

[1] Il DNS è il sistema universale di *server*, gerarchico e distribuito, che garantisce la registrazione e il funzionamento dei nomi a dominio, affinché essi siano associati a servizi *web* (*e.g.*, siti internet ed e-mail) e in grado di operarne l'accesso dell'utente attraverso la c.d. "risoluzione" del relativo indirizzo IP. I nomi a dominio (*e.g.*, <chiomenti.net>) possono essere dunque concepiti come i nomi dei "punti nodali" di *internet*, attribuiti a un soggetto che offre servizi sul *web* in senso lato – siano essi imprese, enti o privati – quindi visibili e fruibili da parte degli utenti affinché accedano alle relative risorse *web*.

[2] L'ICANN – clicca qui per visitare il sito web – è un'organizzazione senza scopo di lucro e con partecipazione globale (c.d. *multistakeholder*), fondata nel 1998 e avente sede a Los Angeles (USA). ICANN ha la funzione di salvaguardare la stabilità operativa di *internet*, di promuovere la competizione, di ampliare la rappresentanza delle comunità globali di *internet* e di sviluppare una politica appropriata al suo intento tramite processi partecipati e consensuali. In tale quadro, ha la responsabilità di assegnare gli indirizzi IP (*Internet Protocol*), gli identificatori di protocollo, di gestire il sistema dei nomi a dominio di primo livello (*Top-Level Domain*) nonché i sistemi di *root server*.

- **Secondo livello (*Second Level Domain – SLD*)** – è la sigla alfanumerica selezionata "a piacimento" – ma non per questo sempre selezionabile in concreto o, comunque, selezionata legittimamente (v. *infra*) – in sede di registrazione del nome a dominio da parte del soggetto che offre servizi sul *web*. È questa, pertanto, la porzione maggiormente "distintiva" e identificativa del nome di dominio (es. <chiomenti>).

  È gestito da appositi fornitori di servizi ("***Registrars***"), quali organizzazioni che operano generalmente sulla base di accordi contrattuali con i *Registries*, svolgendo un'attività di "vendita al dettaglio" ai soggetti richiedenti la registrazione di nomi dominio come imprese, enti, privati ("***Registrants***") talvolta offrendo anche servizi di *hosting* dei relativi siti *web*. Essi sono, dunque, gli interlocutori del mercato per la registrazione, la modifica o la cancellazione delle informazioni sui *domain name* nei *database*-registri detenuti dai *Registries*.

Dalla prospettiva che qui interessa, pertanto, il nodo principale della questione risiede nell'assegnazione dei *domain name* ai relativi *Registrants* da parte dei *Registrars*.

II. IL C.D. «*CYBERSQUATTING*»

Il *cybersquatting* è una pratica illecita (v. *infra*) che consiste nell'accaparramento speculativo, in mala fede, più o meno sistematico, di determinati segni o denominazioni da parte di *Registrants* terzi – rispetto a chi possa legittimamente vantarvi diritti di proprietà intellettuale ovvero altri diritti (*e.g.*, diritto al nome) – mediante la relativa registrazione come *domain name*, con l'obiettivo di monetizzare e/o di sfruttare altrimenti "l'esclusiva" ottenuta sul piano tecnico presso il *database* dei *Registries*.

Si deve notare, infatti, che la registrazione è operata dai *Registrars* in base a un criterio di priorità cronologica della richiesta (c.d. principio "*first come first served*")[3]. Al tempo stesso, i *Registrars* sono tenuti a verificare esclusivamente che il *domain name* oggetto della domanda sia disponibile nel *database*: generalmente non svolgono sindacato di anteriorità ad ampio spettro, in zone-porzioni del TLD gestite da altri *Registries* rispetto a quelli di riferimento (né comunque tale sindacato è paragonabile a quello svolto presso gli uffici di proprietà intellettuale).

Ottenere la registrazione di un *domain name* formalmente "libero" – ancorché di segni e/o nomi notori – ovvero di un *domain name* già registrato come secondo livello ma sotto diverso TLD, ovvero ancora con piccole variazioni o perfino refusi del *domain name* già registrato (c.d. *typesquatting*), in linea di principio non è affatto impresa ardua per i *cybersquatter*. Con il tempo, inoltre, fioriscono nuove strategie di *cybersquatting*, come quella di *"punycode"*[4]. Una volta ottenuta, fino a quando il *cybersquatter* rimane formalmente *Registrant*, il relativo *domain name* non potrà essere registrato dal titolare legittimo dei diritti, né quindi costruirvi il proprio sito *web* ovvero impiegarlo appositamente come @"dominio" in un indirizzo e-mail.

Tra le svariate conseguenze generate dal *cybersquatting*, incluse quelle di natura economica e sociale – non ultimi, in questo senso, tentativi di *phishing* piuttosto che l'immissione in rete di *fake news* o contenuti inappropriati, anche in modo credibile stante l'impiego di nomi illustri usurpati – vi è quella della violazione di diritti di proprietà intellettuale. Di seguito il quadro giuridico di riferimento, dei relativi rimedi attualmente a disposizione nonché di alcune novità normative che si profilano a livello UE.

III. QUADRO GIURIDICO, RIMEDI & MISURE PREVENTIVE

Ancor prima dell'avvento del D.lgs. 10 febbraio 2005, n. 30 *Codice della proprietà industriale* ("**CPI**") – che all'art. 22 ha esplicitamente annoverato i nomi a dominio tra i segni distintivi tipici, sancendo *inter alia* il divieto di adottare come "*nome a dominio aziendale un segno uguale o simile all'altrui marchio*" – già nel noto *"caso Amadeus"* del 1997[5] la giurisprudenza nazionale si era espressa sull'innovativa questione, ritenendo che il *domain name* costituisse un vero e proprio segno distintivo, in grado di entrare in conflitto con altri segni tipizzati dal legislatore, quindi idoneo ad assumere un ruolo giuridicamente rilevante nei fenomeni confusori del mercato.

A livello nazionale vi sono state numerose pronunce in materia di *cybersquatting*, nelle quali quest'ultima è stata ritenuta una pratica confusoria illecita "*idonea a precludere ai titolari del marchio l'utilizzo di Internet come ulteriore segno*

[3] Si guardi, a questo proposito, il punto 4. del *Regolamento di assegnazione e gestione dei nomi a dominio nel ccTLD.it* emanato da *Registro.it* per quanto concerne l'assegnazione dei nomi a dominio con <.it> quale primo livello.

[4] Ispirato dall'omonimo sistema di codifica *unicode*, è una tecnica volta a "eludere" la registrazione (già esistente) di un *domain name* utilizzando dei simboli (in luogo dei caratteri alfabetici) per ottenere graficamente il rimando alle lettere dell'alfabeto, con l'effetto di registrare un *domain name* visivamente identico ma tecnicamente diverso da quello esistente.

[5] V. ord. Trib. Milano, 10 giugno 1997.

distintivo"[6] e che "*consente al titolare del sito di accaparrarsi più facilmente contatti commerciali che, in assenza dell'utilizzo del domain name non avrebbe potuto conseguire se non a prezzo di ingenti investimenti pubblicitari e dopo anni di apprezzata attività nel settore di riferimento*"[7].

I titolari di diritti di proprietà industriale sui *domain name*, pertanto, possono anzitutto ricercare la propria protezione contro i *cybersquatter* avvalendosi dei rimedi giudiziali offerti dal CPI. In particolare, si potrà **agire in via cautelare** per ottenere non solo l'inibitoria dell'uso del nome a dominio illegittimamente registrato, ma anche il suo trasferimento provvisorio al ricorrente subordinandolo, se ritenuto opportuno dal giudice, alla prestazione di idonea cauzione (art. 133 CPI). Si potrà, inoltre, agire **in via ordinaria** per la rivendica del *domain name* registrato in violazione dell'art. 22 CPI o in mala fede, affinché venga revocato o trasferito all'avente diritto da parte della autorità di registrazione (art. 118 CPI). Rimane comunque ferma l'azione di risarcimento del danno, subito a seguito della violazione dei diritti di proprietà industriale sul *domain name* (art. 125 CPI), nonché la tutela offerta dalla disciplina della **concorrenza sleale** (art. 2598 del Codice Civile). Infine, il *cybersquatter* potrebbe risultare punibile anche sul **piano penalistico**, integrando fattispecie quali la contraffazione, l'alterazione o l'uso di marchi o segni distintivi altrui (art. 473 del Codice penale).

* * *

Ferma la tutela giudiziale, di seguito una rassegna dei principali mezzi alternativi potenzialmente a disposizione dei *brand owners* colpiti da fenomeni di *cybersquatting*.

1) Invio di **lettere cessazione e desistenza (*cease & desist*)** ai *cybersquatter* nonché agli eventuali *registrant service provider* e/o altri *internet service provider* (ISP) quali ad esempio gli *hosting provider* del sito, in particolare ove sia (anche) il contenuto di quest'ultimo a interessare il soggetto vittima dell'illecito (tenendo a mente che il D.lgs. 70/2003 prevede casi in cui l'ISP sia perseguibile anche ai fini del risarcimento dei danni).

2) Avvio di una **procedura arbitrale nell'ambito della *Uniform Domain-Name Dispute Resolution Policy*** ("**UDRP**") istituita dall'ICANN nel 1999[8] – senza necessità di un accordo con la controparte –amministrata da fornitori di servizi di risoluzione delle controversie accreditati dall'ICANN, come l'*Arbitration and Mediation Center* presso l'*Organizzazione Mondiale per la Proprietà Intellettuale* ("**OMPI**")[9].

Ove il *panel* arbitrale decida a favore del soggetto che ha presentato il reclamo (*complainant*), ordinerà al *Registrar* competente il trasferimento del *domain name* al legittimo titolare ovvero la cancellazione di quest'ultimo a seconda dei casi. Questo rimedio offre il vantaggio di una procedura agile e meno costosa rispetto a quella giudiziale – al tempo stesso non pregiudicandovi il ricorso, prima come in seguito alla procedura UDRP, posto che per l'effetto quest'ultima potrebbe essere sospesa – prescindendo dalla località del *Registrant*-*cybersquatter*, piuttosto che del reclamante ovvero del *Registrar*, oltre a rendere le decisioni pubbliche (il che può rappresentare un grande deterrente per i *cybersquatters*).

Una delle prove della diffusione del fenomeno nel *cyberworld* è proprio il numero delle decisioni emesse in seno all'OMPI in ambito UDRP dal 1999 al 2020 (oltre 48.000 casi) nonché i relativi protagonisti. Tra le altre, si possono rinvenire una serie di decisioni nel settore del *fashion* che hanno visto vittoriose alcune *maison* di alta moda[10], in cui l'OMPI, preso atto della reputazione acquisita sul mercato dai rispettivi marchi e della lesione ad essi arrecata, ha ordinato in tutti i casi il trasferimento ai ricorrenti del *domain name* contestato.

3) Avvio di una **procedura arbitrale nell'ambito dello *Uniform Rapid Suspension System*** ("**URS**") istituito dall'ICANN nel 2015[11], quale meccanismo di protezione dei diritti che integra la UDRP, offrendo un percorso più rapido e a basso costo per i titolari dei diritti che sperimentano i casi più evidenti di violazione. A differenza dell'UDRP, tuttavia, la decisione del *panel* arbitrale può ordinare al *Registrar* di operare la sospensione e/o il *redirecting* del *domain name* contestato, senza poter giungere alla relativa riassegnazione.

4) Avvio di una **procedura di opposizione dinanzi al *Registry* competente**. Per quanto concerne i *domain name* con TLD <.it>, ad esempio, è possibile avviarla dinanzi all'ente *Registro.it* da parte del soggetto che ritenga leso un suo diritto a causa del *domain name* contestato, incluse le ipotesi in cui quest'ultimo sia identico o tale da indurre

[6] Trib. Milano, 20 febbraio 2009.

[7] Trib. Torino, 26 ottobre 2007.

[8] Qui il link alla pagina informativa ICANN.

[9] In particolare, la procedura amministrativa UDRP è disponibile (solamente) per le controversie riguardanti una presunta registrazione abusiva di un *domain name*, ossia quando: *(i)* il *domain name* è identico o confondibile con un marchio sul quale il ricorrente (*complainant*) ha dei diritti; (*ii)* il relativo *Registrant* non ha diritti o interessi legittimi rispetto al nome di dominio in questione; *(iii)* il *domain name* è stato registrato e viene usato in malafede.

[10] Tra le altre si vedano *WIPO Arbitration and Mediation Center, Decision No. D2010-1743* | *WIPO Arbitration and Mediation Center, Decision No. D2016-0965* |*WIPO Arbitration and Mediation Center, Decision No. D2000-0430* | *WIPO Arbitration and Mediation Center*, *Decision No. D2020-2063*.

[11] Qui il link alla pagina informativa ICANN.

confusione rispetto a un marchio, o altro segno distintivo dell'opponente, nonché identico al proprio nome e cognome. In presenza di una valida richiesta di opposizione il *Registry* aggiunge al nome a dominio lo stato di "*challenged*" – ciò che impedisce il trasferimento ad altro *Registrant* – e, nel caso in cui la richiesta pervenuta superi tutti i passi di validazione previsti dall'apposito regolamento[12], il *Registry* provvede alla cancellazione immediata del *domain name* e alla transizione nello stato di "*inactive/toBeReassigned*" (ivi iniziando una fase per la relativa registrazione da parte dell'opponente vittorioso).

5) Avvio di un **arbitrato irrituale dinanzi al *Registry* competente**. Anche in questo caso con riferimento ai *domain name* con TLD <.it>, ai sensi del suddetto regolamento[13] è possibile avviare un arbitrato in seno all'ente *Registro.it* (sul modello UDRP, ma in questo caso è richiesto il consenso di entrambe le parti) gestito da *Prestatori del Servizio di Risoluzione delle Dispute* (PSRD), ha lo scopo di trasferire l'assegnazione del nome a dominio a chi ne ha il diritto qualora il reclamante provi che il *Registrant* non abbia titolo all'uso o alla disponibilità giuridica e che il nome a dominio sia stato registrato e mantenuto in malafede. Anche in questo caso, ove il PSRD decida a favore del reclamante, l'esito è analogo a quello esposto *sub* **4)**, ma ciò non sarà stato anticipato da un'indicazione del *domain name* come "*challenged*" nel *database*: ecco perché, ove si opti per la procedura arbitrale in menzione, è consigliato il contemporaneo avvio di una procedura di opposizione.

* * *

Si possono valutare, infine, le seguenti iniziative quali misure preventive (potenzialmente atte a ridurre l'*effort* economico e organizzativo ad avvenuto *cybersquatting*):

1) Iscrizione al *database* della ***Trademark ClearingHouse* istituito da ICANN**[14] nel 2013 in vista del programma di lancio dei nuovi nomi di dominio generici di primo livello (gTLD) che avrebbero creato, come per ogni nuovo TLD, nuovi "universi" di registrabilità. Il meccanismo di difesa si basa sulla "registrazione" del proprio marchio presso la *Trademark Clearinghouse* al fine di ottenere da quest'ultima determinati servizi, consistenti in effetti prenotativi del proprio *domain name* per i nuovi gTLD (servizio "*Sunrise*") ovvero in apposite di notifiche di *alert* in caso di tentativi di *cybersquatting* da parte di terzi (servizio "*Trademark Claims*");

2) Iscrizione ai ***Blocking Services* offerti da alcuni *Registries*** aggiuntivi rispetto a quelli offerti dalla *Trademark ClearingHouse*, generalmente sul presupposto che il richiedente sia già iscritto a quest'ultima;

3) azioni di ***brand monitoring*** per intercettare le minacce in modo proattivo (prima ancora che reattivo), nell'ottica di anticipare i rischi futuri – nella misura possibile – e mitigare i relativi rischi.

IV. NOVITÀ NORMATIVE IN VISTA?

Uno dei principali ostacoli che si possono sperimentare (*inter alia*) nel tentativo di intraprendere azioni contro i *cybersquatter* è quello della difficoltà di accedere ai dati identificativi dei *Registrants*. Ciò in quanto le *policy* in vigore presso *Registries* e *Registrars* applicano criteri di riservatezza che non parrebbero essere giuridicamente sostenibili – quantomeno non in modo generalizzato nonché uniforme rispetto a *Registrants* persone fisiche ovvero giuridiche – nella misura in cui vengano fondati sul Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (*Regolamento Generale sulla Protezione dei Dati* – "**GDPR**"), spesso richiamato dalle *policy* medesime[15]. Da un lato, infatti, con riferimento ai *Registrants*-persone giuridiche e alla pubblicazione delle informazioni che le riguardano, com'è noto il relativo trattamento non ricade nell'ambito applicativo del GDPR[16]. Dall'altro lato, con riferimento ai *Registrants*-persone fisiche e

[12] Qui il link alle *Linee Guida sulla Risoluzione delle dispute nel ccTLD.it.*

[13] Qui il link alle *Linee Guida sulla Risoluzione delle dispute nel ccTLD.it.*

[14] Qui il link alla pagina ufficiale e qui il link alla pagina informativa ICANN.

[15] A questo proposito si guardino le F.A.Q. pubblicate da ICANN (qui il link) le quali enunciano tali criteri, poi recepiti a valle dalle *policy* dei *Registries* e dei *Registrars*: «[…] *Some of your contact information associated with your domain name registration may be made publicly available in the Registration Data Directory Service (also commonly known as the WHOIS database or the Registration Data Access Protocol (RDAP)). Similar to a traditional telephone directory or book, publication of registration contact information is done to allow others to contact you about your domain name or its website information, as well as for public safety reasons. When you register a domain name, you may have the option to mask your some of your contact information using a privacy/proxy service. Contact your registrar to find out more about your options for masking your public contact information. You can use https://lookup.icann.org/ to see your domain name contact information which is publicly available.* ***Recently, new global data privacy regulations such as the European Union's Global Data Protection Regulation have restricted the amount of public information that your Registrar needs to make available, to help protect the privacy of registrants*** […]» (corsivo – grassetto aggiunti).

[16] Si guardi il *Considerando* n. 14 del GDPR: «*È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali.* ***Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto.***» (corsivo – grassetto aggiunti).

alla possibilità che terzi richiedano l'accesso alle informazioni che le riguardano, sarebbe il GDPR medesimo a fornire i presupposti per un trattamento di dati personali rispondente (*inter alia*) al legittimo interesse dei terzi richiedenti – quale potrebbe essere la difesa di un diritto leso da attività di *cybersquatting* – naturalmente nel quadro di un bilanciamento con gli interessi e i diritti fondamentali delle persone fisiche interessate[17].

In questo senso, è da accogliere con favore l'intenzione del legislatore europeo cristallizzata nella proposta di revisione della c.d. "Direttiva NIS"[18], nell'ambito della *Cybersecurity Strategy for the Digital Decade* pubblicata dalla Commissione Europea il 16 dicembre 2020. Tale proposta, infatti, sembra indirizzata a imporre agli Stati membri la previsione in capo agli attori del DNS obblighi *ad hoc*, ulteriori a quelli generalmente previsti per la qualifica di "operatori essenziali" nel quadro NIS (peraltro escludendo gli attori DNS dall'applicazione delle soglie dimensionali previste per gli operatori essenziali). In particolare, gli Stati membri dovrebbero assicurare *inter alia* che *Registries* e *Registrars*:

- raccolgano e mantengano dati di registrazione dei *domain names* **accurati e completi** per identificare e contattare i *Registrants*;
- rendano **pubblici** – senza indebito ritardo dopo la registrazione di un *domain name* – i dati che non rientrano nell'ambito di applicazione delle norme UE sulla protezione dei dati (*e.g.*, i dati che riguardano le persone giuridiche);
- forniscano un **accesso efficiente** e **senza ingiustificato ritardo** ai dati di registrazione dei *domain names* per i legittimi richiedenti;
- mettano in atto **politiche e procedure** atte a garantire quanto sopra, rendendole pubbliche.

Ciò vale a maggior ragione dal momento che la situazione pandemica sembra aver alimentato una crescita del crimine informatico e, in questo senso, la stessa OMPI ha evidenziato un aumento costante di casi di *cybersquatting* depositati in ambito UDRP nel 2020 rispetto al 2019 e, nel primo bimestre del 2021, già si contano più di 600 casi[19].

Contatti

Gilberto Nava
Partner – Chiomenti
Dipartimento IP, TMT, Data Protection
T. +39.06.46622.719
gilberto.nava@chiomenti.net

Paolo Bertoni
Of Counsel – Chiomenti
Dipartimento IP, TMT, Data Protection
T. +39.02.72157.679
paolo.bertoni@chiomenti.net

Anna Gardini
Counsel – Chiomenti
Dipartimento IP, TMT, Data Protection
T. +39.02.72157.758
anna.gardini@chiomenti.net

[17] Si guardi l'art. 6, par. 1, lett. f), del GDPR: «*Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:* […] ***f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato*** *che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.* […]» (corsivo – grassetto aggiunti).

[18] Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[19] Qui il link al portale di statistiche OMPI.