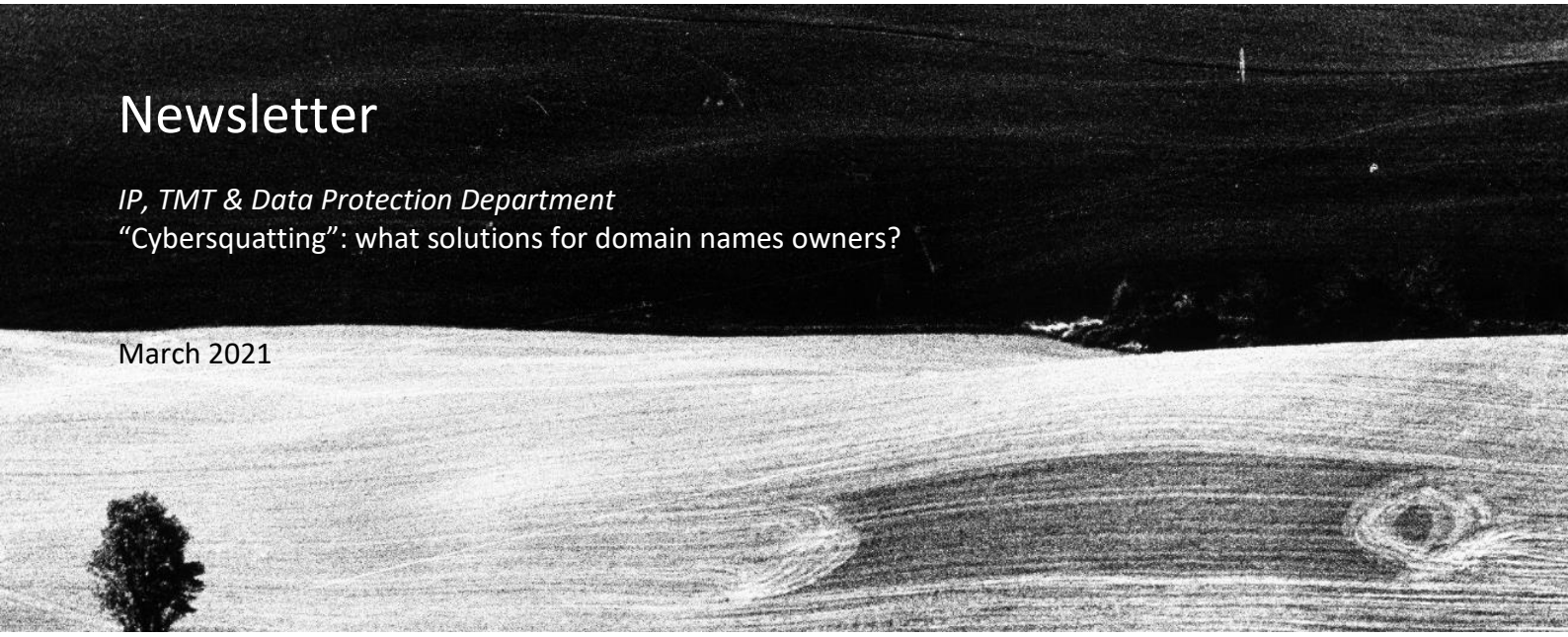
CHIOMENTI



Newsletter

IP, TMT & Data Protection Department

"Cybersquatting": what solutions for domain names owners?

March 2021

TABLE OF CONTENTS

I. THE *DOMAIN NAME SYSTEM*

For a proper understanding of the cybersquatting phenomenon, it is necessary to establish some preliminary concepts with regard to the Domain Name System ("**DNS**")[1]. The DNS is conceived according to a "multi-level" logic, which corresponds to a hierarchical architecture of delegations to certain subjects, headed by the *Internet Corporation for Assigned Names and Numbers* ("**ICANN**")[2]. Hence the very conformation of the domain name, consisting of a string, to be read from right to left and structured as follows:

- **Root Level** – it is the final point to the right of the domain name, in the true sense of the term: it is a <.>, implicit in the visible string and operated by the so-called "root name servers" (currently they are 13 in the world) and administered by the *Internet Assigned Numbers Authority* ("**IANA**") set up for this purpose by ICANN.
- **Top Level Domain** ("**TLD**") – it is the alphanumeric abbreviation occupying the last visible part to the right of the domain name, made up of predetermined terms and divided into various categories, such as *Country Code Top-Level Domain* (ccTLD) including <.it>, <.eu> etc., or *Generic Top-Level Domain* (gTLD) including <.com>, <.net>, <.org> etc.

  It is managed by the registry operators ("**Registries**"), as organisations delegated by IANA, to which one or more TLDs are assigned (*e.g.*, <.it> is managed by *Registro.it* within the *Istituto di Informatica e Telematica* by the CNR) to administer their assignment policies and the central registry database of registered domain names.

[1] The DNS is the universal server system, hierarchical and distributed, that guarantees the registration and operation of domain names, so that they are associated with web services (*e.g.*, websites and e-mail) and able to operate user access through the so-called 'resolution' of the relevant IP address. Domain names (*e.g.*, <chiomenti.net>) can therefore be conceived as the names of the "nodal points" of the Internet, attributed to a subject offering services on the web in a broad sense – be they companies, bodies or private individuals – and therefore visible and usable by users so that they can access the relevant web resources.

[2] ICANN - click here to visit the website - is a non-profit, multistakeholder organisation founded in 1998 and based in Los Angeles, USA. ICANN's function is to safeguard the operational stability of the Internet, to promote competition, to broaden the representation of the global Internet community and to develop policy appropriate to its intent through participatory and consensus-based processes. Within this framework, it is responsible for assigning Internet Protocol (IP) addresses, protocol identifiers, managing the Top-Level Domain (TLD) system as well as the root server systems.

- **Second Level Domain** ("**SLD**") – it is the alphanumeric abbreviation selected 'at will' – but not for this reason always selectable in practice or, in any case, legitimately selected (see below) – at the time of registration of the domain name by the subject offering services on the web. This is, therefore, the most "distinctive" and identifying portion of the domain name (*e.g.,* < chiomenti>).

  It is managed by special service providers ("**Registrars**"), such as organisations that generally operate on the basis of contractual agreements with the Registries, carrying out a "retail" activity to subjects requesting the registration of domain names such as companies, bodies, individuals ("**Registrants**"), sometimes also offering hosting services for the relevant websites. They are therefore the market interlocutors for the registration, modification or cancellation of information on domain names in the database registers held by the Registries.

Therefore, for what matters here, the main crux of the matter lies in the assignment of domain names to the relevant Registrants by the Registrars.

II. THE SO-CALLED. «*CYBERSQUATTING*»

Cybersquatting is an unlawful practice (see below) consisting in the speculative hoarding, in bad faith, more or less systematically, of certain signs or names by third party Registrants – compared to those who can legitimately boast intellectual property rights or other rights (*e.g.*, name rights) – by registering them as domain names, with the aim of monetizing and/or otherwise exploiting the 'exclusivity' obtained at a technical level from the Registries' database.

It should be noted, in fact, that registration is carried out by Registrars on the basis of a criterion of chronological priority of the request (the so-called "first come first served" principle)[3]. At the same time, the Registrars are required to verify exclusively that the domain name applied for is available in the database: they do not generally carry out wide-ranging prior art checks, in areas-portions of the TLD managed by other Registries than the reference Registries (nor is such checking comparable to that carried out at intellectual property offices).

Obtaining registration of a formally 'free' domain name – even if it is a well-known sign and/or name – or of a domain name that has already been registered as a second level but under a different TLD, or with small variations or even typos in the already registered domain name (so-called "typesquatting"), is in principle not at all difficult for cybersquatters. Over time, moreover, new cybersquatting strategies flourish, such as that of "punycode"[4]. Once obtained, as long as the cybersquatter remains formally a registrant, the corresponding domain name may not be registered by the legitimate rights holder, nor may it be used to build his own website or be used specifically as the @"domain" in an e-mail address.

Among the various consequences generated by cybersquatting, including those of an economic and social nature – not least, in this respect, phishing attempts rather than the posting of fake news or inappropriate content on the web, even credibly, given the use of usurped famous names – is the violation of intellectual property rights. Below is the legal framework of reference, the relevant remedies currently available, as well as some new legislation that is emerging at EU level.

III. LEGAL FRAMEWORK, REMEDIES & PRECAUTIONARY MEASURES

Even before the advent of Legislative Decree no. 30 of 10 February 2005, Industrial Property Code ("**IPC**") – which in art. 22 explicitly included domain names among the typical distinctive signs, providing for *inter alia* the prohibition to adopt as a "*company domain name a sign equal or similar to another person's trademark*" – already in the well-known "Amadeus case" of 1997[5], the national case law had expressed itself on the innovative issue, holding that the domain name constituted a real distinctive sign, able to enter into conflict with other signs typified by the legislator, therefore capable of assuming a legally relevant role in the confusing phenomena of the market.

At a national level, there have been numerous rulings on cybersquatting, in which the latter has been considered an unlawful confusing practice "*capable of precluding trademark owners from using the Internet as a further distinctive sign*"[6] and which "*allows the owner of the site to more easily gain commercial contacts that, in the absence of the use of the domain name, it*

[3] In this regard, it is worth noting section 4. of *Regolamento di assegnazione e gestione dei nomi a dominio nel ccTLD.it* enacted by *Registro.it* with reference to granting registration of <.it> TLD domain names.

[4] Inspired by the unicode coding system of the same name, it is a technique aimed at "circumventing" the (already existing) registration of a domain name by using symbols (instead of alphabetical characters) to graphically obtain a reference to the letters of the alphabet, with the effect of registering a domain name that is visually identical but technically different from the existing one.

[5] See Order issued by Milan Court on 10 June 1997.

[6] See judgement issued by the Milan Court on 20 February 2009.

would not have been able to obtain if not at the price of massive advertising investments and after years of appreciated activity in the reference sector"[7].

Owners of industrial property rights on domain names, therefore, may first seek protection against cybersquatters by availing themselves of the judicial remedies offered by the IPC. In particular, it is possible to submit a request for the issuing of an injunction which prohibits further use of the illegally registered domain name, along with its provisional transfer to the complainant albeit subject to the provision of a suitable security deposit if it is found appropriate by the judge (art. 133 IPC). It is also possible to bring a judicial action for a claim of the domain name either registered in violation of art. 22 CPI or in bad faith, so that it is revoked or transferred to the entitled person by the registration authority (art. 118 CPI). The foregoing goes without prejudice to bring an action for compensation for damages, suffered as a result of the violation of industrial property rights on the domain name (art. 125 CPI), as well as for seeking protection under unfair competition laws (art. 2598 of the Italian Civil Code). Lastly, cybersquatters may also be punishable under criminal law, as they may be guilty of counterfeiting, altering or using the trademarks or distinctive signs of others (Article 473 of the Italian Criminal Code).

* * *

Without prejudice to judicial protection, here is a review of the main alternative means potentially available to brand owners affected by cybersquatting.

1) Sending **cease & desist letters** to the cybersquatters as well as to any registrant service providers and/or other Internet service providers (ISPs) such as, for instance, the site's hosting providers, in particular where the victim of the offence is also affected by the content of the site (bearing in mind that Italian Legislative Decree No. 70/2003 provides for cases in which the ISP may also be prosecuted for the purposes of compensation for damages).

2) Initiation of an **arbitration procedure under the *Uniform Domain-Name Dispute Resolution Policy*** ("**UDRP**") established by ICANN in 1999[8] – without the need for an agreement with the other party – administered by ICANN-accredited dispute resolution service providers, such as the *Arbitration and Mediation Center* at the *World Intellectual Property Organization* ("**WIPO**")[9].

If the arbitration panel decides in favour of the complainant, it will order the competent Registrar to transfer the domain name to the rightful owner or to cancel it, as the case may be. This remedy offers the advantage of an agile and less costly procedure compared to the judicial one – at the same time not prejudicing the appeal, before or after the UDRP procedure, since the latter could be suspended – regardless of the location of the Registrant-cybersquatter, rather than the complainant or the Registrar, as well as making the decisions public (which can be a great deterrent for cybersquatters).

One of the proofs of the spread of the phenomenon in the cyberworld is precisely the number of decisions issued at WIPO in the UDRP field from 1999 to 2020 (more than 48,000 cases) as well as the protagonists. Among others, there are a number of decisions in the fashion sector in which a number of *haute couture* fashion houses[10] were victorious, in which WIPO, having taken note of the reputation acquired on the market by the respective trademarks and of the damage caused to them, ordered in all cases the transfer of the disputed domain name to the claimants.

3) Initiation of an arbitration procedure under the ***Uniform Rapid Suspension System*** ("**URS**") established by ICANN in 2015[11], as a rights protection mechanism that complements the UDRP, offering a faster and lower-cost route for rights holders experiencing the most egregious instances of infringement. Unlike the UDRP, however, the arbitration panel's decision may order the Registrar to suspend and/or redirect the disputed domain name, without being able to reach the relevant reassignment.

4) Initiation of an **opposition procedure before the competent Registry**. With regard to domain names with the TLD <.it>, for example, it is possible to initiate opposition proceedings before the *Registry.it* by any person who considers that its rights have been infringed by the disputed domain name, including cases where the latter is

[7] See judgement issued by the Turin Court on 26 October 2007.

[8] Here is the link to the ICANN info page.

[9] Most notably, the UDRP administrative procedure is only available for disputes concerning an alleged abusive registration of a domain name; that occurs when the following criteria are met: *(i)* the domain name registered by the domain name registrant is identical or confusingly similar to a trademark or service mark in which the complainant (the person or entity bringing the complaint) has rights; and *(ii)* the domain name registrant has no rights or legitimate interests in respect of the domain name in question; and *(iii)* the domain name has been registered and is being used in bad faith.

[10] Amongst other decisions, please refer to *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] Here is the link to the ICANN info page.

identical or likely to lead to confusion with a trademark or other distinctive sign of the opponent, as well as identical to his/her own name and surname. In the presence of a valid opposition request, the Registry adds the status of "*challenged*" to the domain name – which prevents it from being transferred to another Registrant – and, in the event that the request exceeds all the validation steps provided for by the specific regulation[12], the Registry immediately deletes the domain name and transitions it into the status of "*inactive/toBeReassigned*" (therein starting a phase for the relative registration by the victorious opponent).

5) Initiation of **equitable arbitration before the competent Registry**. Also in this case, with reference to domain names with the TLD <.it>, pursuant to the above-mentioned regulation[13] it is possible to initiate arbitration before the competent Registry (on the UDRP model, but in this case the consent of both parties is required) managed by *Dispute Resolution Service Providers* (PSRD), the purpose of which is to transfer the assignment of the domain name to the person who has the right to it if the complainant proves that the Registrant is not entitled to the use or to legally dispose of the domain and that the domain name was registered and maintained in bad faith. Also, in this case, if the PSRD decides in favour of the complainant, the outcome is similar to that set out in paragraph **4)**, but this will not have been anticipated by an indication of the domain name as "challenged" in the database: this is why, where the arbitration procedure mentioned above is opted for, it is advisable to start an opposition procedure at the same time.

* * *

Finally, the following initiatives can be evaluated as precautionary measures (potentially reducing the economic and organisational effort when cybersquatting occurs):

1) Registration in the ***Trademark ClearingHouse*** database set up by ICANN[14] in 2013 in view of the programme to launch the new generic top-level domain names (gTLDs) which would create, as for each new TLD, new "universes" of registrability. The defence mechanism is based on the 'registration' of one's trademark with the *Trademark Clearinghouse* in order to obtain certain services from the latter, consisting of the reservation of one's domain name for the new gTLDs (*'Sunrise'* service) or the provision of alert notifications in the event of cybersquatting attempts by third parties (*'Trademark Claims'* service).

2) Enrolment in ***Blocking Services offered by some Registries*** in addition to those offered by the *Trademark ClearingHouse*, generally on the assumption that the applicant is already enrolled with the latter;

3) **Brand monitoring** actions to intercept threats proactively (even before a reactive approach), with a view to anticipating future risks – as far as possible – and mitigating the related risks.

IV. NEW REGULATIONS IN SIGHT?

One of the main obstacles that may be experienced (*inter alia*) in attempting to take action against cybersquatters is the difficulty of accessing the identification data of Registrants. This is because the policies in force before Registries and Registrars apply confidentiality criteria that do not appear to be legally workable – at least they do not in a generalised and uniform manner with respect to natural or legal persons – insofar as they are based on Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation - "**GDPR**") often referred to in such policies[15].

[12] Here is the link to the *Linee Guida sulla Risoluzione delle dispute nel ccTLD.it*.

[13] Here is the link to the *Linee Guida sulla Risoluzione delle dispute nel ccTLD.it*.

[14] Here is the link to the official page and here is the link to the ICANN info page.

[15] In this regard please refer to the F.A.Q. published by ICANN (here is the link) pointing out those criteria, then implemented by the policies of Registries and Registrars downstream: «[…] *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*** […]» (emphasis added).

On the one hand, in fact, with reference to Registrants-legal persons and the publication of information concerning them, as is well known, the relevant processing does not fall within the scope of the GDPR[16]. On the other hand, with reference to Registrants-natural persons and the possibility of third parties requesting access to information concerning them, it would be the GDPR itself to provide for the conditions for the processing of personal data based on (*inter alia*) the legitimate interests of third-party access seekers – such as the defence of a right infringed by cybersquatting activities – as obvious in the framework of a balance with the interests and fundamental rights of the natural persons concerned[17].

In this regard, the intention of the European legislator arising out of the proposal for the revision of the so-called "NIS Directive"[18], as part of the *Cybersecurity Strategy for the Digital Decade* published by the European Commission on December 16, 2020 is to be welcomed. This proposal, in fact, seems to be aimed at requiring Member States to impose *ad hoc* obligations on DNS actors, on top of those generally provided under their qualification of "essential operators" in the NIS framework (also excluding DNS actors from the application of the size-thresholds provided for essential operators). Most notably, Member States should ensure *inter alia* that Registries and Registrars:

- collect and maintain **accurate and complete** domain name registration data to identify and contact Registrants;
- make **publicly available** – without undue delay after registration of a domain name – data that does not fall within the scope of EU data protection rules (*e.g.*, data concerning legal persons);
- provide to the legitimate access seekers an **efficient access**, **without undue delay**, to domain name registration data;
- put in place **policies and procedures** ensuring the above, thereby making them publicly available.

This holds even more true since the pandemic situation seems to have fueled a growth of cybercrime and, in this sense, WIPO itself has shown a steady increase in cybersquatting cases filed under UDRP in 2020 compared to 2019 and, in the first two months of 2021, there were already more than 600 cases[19].

Contacts

Gilberto Nava
Partner – Chiomenti
IP, TMT, Data Protection Department
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
IP, TMT, Data Protection Department
T. +39.02.72157.758
anna.gardini@chiomenti.net

[16] Reference is made to *Recital* n. 14 of the GDPR: «*The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.* ***This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person***» (emphasis added).

[17] Reference is made to art. 6, par. 1, let. f). of the GDPR: «*Processing shall be lawful only if and to the extent that at least one of the following applies:* […] ***f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject*** *which require protection of personal data, in particular where the data subject is a child* […]» (emphasis added).

[18] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[19] Here is the link to the WIPO statistics portal.