New times, new registration rules

Handling of illegal content and DNS Abuse

The proliferation of illegal online content undermines, albeit often unconsciously, our trust in this giant and updated encyclopaedia that is available to us immediately and, most of the time, at no cost (at least, no direct cost). We are aware, and in this regard we have no illusions, that not everything that falls into our network is true or scientifically accurate. Far from it. However, we also know that the manoeuvres and expedients of disinformation and, far beyond the desirable, the rapid dissemination of hate speech, racism and xenophobia, are virtual webs in which even the most attentive ones fall into. Why does this happen? Because we are exposed, because we are easy preys.

On 15 December, the European Commission (EC) published the long-awaited Regulation proposal to govern digital services in the European Union - the Digital Services Act (DSA). This act aims to contribute to the consolidation of a more robust legal framework on consumer protection and respect for fundamental online rights, for example by creating mechanisms of greater choice, thus reducing exposure to illegal content. In short, it is about establishing a clear and effective regulatory framework of transparency and accountability for providers of digital services and promoting innovation, growth and competitiveness within the European single market. The document currently being debated by the European Parliament anticipates a definition of illegal content which, freely translated, refers to any activity, including the purchase and sale of goods and the provision of services, that are illegal according to European Union or national law.

If, in the future, we want to look at consumers solely as stakeholders and not victims of the digital transition, we need to identify who, in the value chain, should have the responsibility of 'looking' (proactively or not) at the content that, quickly and many times uncontrollably, is available online. First: the DSA will apply to providers of intermediary services, that is to say those providing technical services for access, availability and use of information or online services independent of the creation of the information or service itself. Registries (such as .PT) and registrars are called upon here to collate and, namely under recitals 27 and 83, are qualified as providers of intermediary services, and may therefore be subject to the new obligations under this Regulation which, in any case, vary according to the role, size and impact of the provider of intermediary services on the digital ecosystem. Thus, the legal qualification of 'provider of information society services' is extended to 'provider of

intermediary services'. It is also clear, from this very preliminary analysis, that this type of provider must cooperate with the competent national authorities, occasionally following their indications, namely to block/remove illegal content. It should be noted that this very same obligation applies even if the provider of intermediary services enjoys some liability exemptions on the management of illegal content provided for in Chapter II of the DSA, that is, when it provides the service with complete neutrality, by merely processing the information provided by a particular service user, automatically and technicallyexempt, thus not playing an active role in the editing of such content, nor exercising any control over it.

Having said that, and bearing in mind that the above comments refer to a piece of legislation whose final wording is still on the horizon, it seems important to mention that there is no glimpse of any obligation for proactive monitoring of illegal online content, nor an effective and direct responsibility for action that is not reduced to the scope limited by the typically technical nature that characterizes a registry's function. To us, what seems final is that, to be part of this chain, in this case, it will mean building bridges, collaborating and supporting the authorities identified with legal powers in this matter.

Regarding this particular point, the line we believe is being drawn in the DSA is not entirely innovative. If we look at the wording of Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017, on cooperation between national authorities responsible for the enforcement of consumer protection laws, we are surprised by a forecast, pursuant to which competent authorities may request directly to registries - in Portugal, Associação DNS.PT - and domain name managing bodies (registrars) the provision of all information they deem relevant to the investigation, conferring on them the ultimate competence to, *inter alia*, reproduce, *mutatis mutandis*, the wording of the previously identified pleading *'(...) to delete a fully qualified domain name and to allow the competent authority concerned to register it'.* In our view, the solution herein advocated by the legislator goes even further than a mere collaboration and it may, *in extremis*, impose an action, practically effective or not: to delete a domain name!

Also noteworthy is the European Strategy for a more effective fight against sexual abuse of minors, made public last July, where it seems clear that it will replicate the target pointed at players as the registries. The European Commission is currently considering a number of legislative solutions, including the creation of a regulatory framework capable of establishing measures of detection, communication to competent authorities and, possibly, removal of online content of this nature. News is expected during this first half of the year.

It seems obvious that removing illegal content from the Internet is the only way to prevent access to it, but the problem lies in how to do it effectively. Much of the possible paths that can be followed - including blocking or removing the corresponding domain name - have in common the fact that content is still available and accessible,. just changing the route and the time it takes us to access it. We are not going to replicate here the analysis[1] made by CENTR[2], where we had the opportunity to participate, on the role of ccTLDs in the management of illegal content, we will share only the most relevant conclusions that derive from one assumption: ccTLDs do not have access to content, nor do they host or transfer content through its infrastructure. Now, and in addition to the strict fulfilment of the obligations which emerge, or will emerge, from the European Parliament in this regard, it is necessary to call upon ourselves to raise awareness and education of the dangers of the Internet in our community; to facilitate and increase collaboration with police forces and other competent authorities; and to make available, promptly and within the limits of the law, identification of contacts associated with domain names used to enable access to illegal content.

Law schools teach, in the first years, that the necessary rejuvenation of legal systems often comes from within. Analysing this statement could take us a long way, but let us be straightforward: can a judge refrain from judging when there is an omission in the law, when it is not clear enough, or leaves room for discretion? If so, are we calling into question key principles such as stability and legal certainty? This is where the fundamental role of jurisprudence lies in the possible creation of legal systems. Having said that, and notwithstanding the first steps of the above identified community legislator, we could not omit here an unprecedented ruling (I ZR 13/19) by the German Federal Court of Justice (TJFA) regarding registrars' liability for content published online, associated with domain names for which they are responsible as the managing/technical body. In the long text of the Judgment, it can be surprisingly read that a registrar that, on behalf of the registrant, registers a domain name with the corresponding registry, providing the necessary technical and administrative data for this purpose, thus participating in its activation process, is subsidiary responsible for online content that violates intellectual property rights and those associated with that domain name. If, in this particular case, we do not look directly at the

[1] https://centr.org/library/library/policy-document/domain-name-registries-and-online-content.html
[2] https://centr.org/

issue of blocking or removing a domain, the matter is heavily intricate and relates to the scope of responsibility of the different links in this chain.

Excuse us for this long introduction, where we could even have extended our analysis, but it seemed useful to us to frame the options we sought to embody in .PT's Terms & Condiions (Registration Rules) on the block or removal of domains with illegal content or configurable actions such as DNS Abuse.

The concept of DNS Abuse is first defined in paragraph g) of the Rules Glossary, and is limited to cases where the domain name is used, intentionally or unintentionally, for malware, phishing, pharming, botnets, and/or spam dissemination activities. On the contrary, and now referring to the concept of illegal content, its broad and multifaceted nature, which has already been mentioned, has led us to choose not to present any formal definition, under the risk of incurring dubious rigour. However, this is also not a matter of omission, and Article 25(4) clarifies: *'(...) .PT is not, under any circumstances, liable for the use given to the domain name, designated but not exclusively, for the contents associated with it.'* The registrant is the sole responsible for the use given to the domain name, and by default, to the contents associated with it. Thus states Article 23(2).

As for DNS Abuse situations, in case we identify that a domain name is being used for subsumable activities, those responsible for the domain name will be notified to ensure implementation of the necessary measures to correct it. If the identified malicious activity persists, and where applicable, .PT will report the situation to the competent authority (Article 25.3). This mechanism now formally embodied in the Registration Rules text, in addition to formalising .PT's concerns on security[3], also crystallises the work already developed by its Security Operation Service, the PTSoc[4]. The PTSoc currently has mechanisms to actively identify domains that are being used for activities that fit the concept of DNS Abuse[5]. For example, it is up to the PTSoc to communicate to those responsible for a domain and/or to competent authority situations of DNS Abuse that, directly or indirectly, it identifies during its monitoring activity.

[3] All .PT initiatives in the area of security are duly described at: https://www.dns.pt/pt/seguranca/
[4] https://www.dns.pt/pt/seguranca/centro-de-operacoes-de-seguranca-soc/
[5] In 2020, PTSoc detected 186 cases of DNS Abuse. Full report available here: https://www.dns.pt/fotos/editor2/relatorios/relatorio2020_ptsoc.pdf

One last question remains - perhaps even the most important one - which is whether or not .PT can remove a domain to which illegal content is associated. The answer is 'yes'. Under Article 22(a), the domain name is immediately removed when .PT is informed of the loss of the right to use it by its owner,and as long as this results from a notification to that effect by an entity with legal competence for that purpose. . As we have said before, and above, we will not digress on the practical effectiveness of a notification in this regard. We have a different intent. Our purpose is to show that rapid mechanisms have been put into place that will enable us to act collaboratively and in compliance with the applicable law.

In short, we sought, with these Rules, to mirror not only our institutional commitments6, but also those that already are a result of the law - we recall here the obligations arising from our status as Operator of Essential Services under Law No. 46/2018, of 13 August, which establishes the Cyberspace Security Legal Framework - as well as those coming soon, and which we have tried to list above. At the same time, because this field leaves no doubts, we have based our intervention on principles of neutrality, transparency and close cooperation with the bodies identified by the law as competent in this area.

A final note worth mentioning. In this context of analysis, .PT calls upon itself an additional, yet key, responsibility: to keep its contact database associated with domain names updated, complete and with accurate information. This is a difficult task and the information handled by registrars, as registration agents, as intermediaries in the process, is a fundamental part. Once again, we fall into the importance of collaboration, made up of dialogue and closeness. We close with a new promise, that of commitment, so that our link is never the weakest.

[6] In 2019, .PT and the Portuguese National Cybersecurity Center signed a Protocol of Collaboration, which has served as a basis for a close and particularly fruitful collaboration on various fronts and initiatives.