Novos tempos, novas regras

O tratamento dos conteúdos ilegais e DNS Abuse

A proliferação de conteúdos ilegais na Internet belisca, ainda que muitas vezes inconscientemente, a confiança que temos nesta gigante e atualizada enciclopédia que está ao nosso dispor de forma imediata e, na maioria das vezes, sem qualquer custo (pelo menos direto). É sabido, e quanto a isso não tenhamos ilusões, que nem tudo o que cai na nossa rede é fidedigno ou tem chancela científica. Longe disso. Porém, é também sabido que as manobras e expedientes de desinformação e, muito para além do desejável, a rápida disseminação de discursos de ódio, racismo, xenofobia são teias virtuais em que até os mais atentos incautamente caiem. E porquê? Porque estamos expostos, somos presas fáceis.

No passado dia 15 de dezembro, a Comissão Europeia (CE) publicou a tão aguardada proposta de Regulamento para reger os serviços digitais no espaço europeu – o Digital Services Act (DSA). Este diploma visa contribuir para a consolidação de um quadro jurídico mais robusto em matéria de proteção do consumidor e respeito pelos direitos fundamentais online, criando, por exemplo, mecanismos de maior escolha e, lá está, menor exposição aos conteúdos ilegais. Trata-se, em suma, de instituir um quadro regulamentar claro e eficaz em matéria de transparência e responsabilidade dos prestadores de serviços digitais e promover a inovação, o crescimento e a competitividade no seio do mercado único europeu. O documento que está neste momento a ser debatido no Parlamento Europeu antecipa-nos uma definição de conteúdos ilegais que, em tradução livre, se resume a uma atividade, incluindo a compra e venda de bens e a prestação de serviços, não conforme com a lei comunitária ou de um Estado membro.

Se futuramente queremos ver os consumidores unicamente como atores e não vítimas da transição digital temos de identificar quem, na cadeia de valor, deve ter a responsabilidade de, digamos, "olhar" (proativamente ou não) para os conteúdos que, rápida e muitas vezes descontroladamente, circulam na rede. Primeira nota: o DSA será aplicável aos prestadores intermediários de serviços em rede ("providers of intermediary services"), isto é, àqueles que prestam serviços técnicos para o acesso, disponibilização e utilização de informações ou serviços em linha independentes da geração da própria informação ou serviço. Registries (como o .PT) e registrars são aqui chamados à colação e, a coberto nomeadamente dos considerandos 27 e 83, são qualificados de prestadores intermediários de serviços em rede,

podendo vir, por esta razão, a estar sujeitos às novas obrigações previstas neste Regulamento que, em todo o caso, variam de acordo com o papel, dimensão e impacto do prestador intermediário no ecossistema digital. Assim, é alargada a qualificação legal de "prestador de serviço da sociedade da informação" para "prestador intermediário de serviços". Desta análise muito preliminar resulta ainda que a esta tipologia de prestadores cumpre cooperar com as autoridades nacionais competentes, executando pontualmente as suas indicações, designadamente no sentido de bloquear/remover conteúdos ilegais. Note-se que esta mesma obrigação é aplicável ainda que o prestador intermediário de serviços em rede goze de alguma das isenções de responsabilidade sobre a gestão de conteúdos ilegais previstas no Capítulo II do DSA, isto é, quando presta o serviço com total neutralidade, limitando-se a processar as informações fornecidas por um determinado utilizador do serviço, de forma automática e tecnicamente isenta, não desempenhando, por isso, um papel ativo sobre a edição desses conteúdos, nem exercendo sobre estes qualquer tipo de controlo.

Dito isto, e ressalvado que está o facto dos comentários acima se reportarem a um diploma cuja redação final ainda está no horizonte, parece-nos importante referir não se vislumbrar qualquer obrigação de monitorização proactiva ao nível dos conteúdos ilegais online, nem uma responsabilidade efetiva e direta de ação que não se reduza ao âmbito que está limitado pela natureza tipicamente técnica que caracteriza a função de um registriy. O que nos parece já sedimentado é que fazer parte desta cadeia, neste caso, significará fazer pontes, colaborar, e apoiar as autoridades que sejam identificadas com competências legais nesta matéria.

Neste ponto concreto, a linha que nos parece estar a ser traçada no DSA não é integralmente inovadora. Se olharmos para a letra do Regulamento (EU) 2017/2394 do Parlamento Europeu e do Conselho, de 12 de dezembro de 2017, relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de proteção dos consumidores, somos surpreendidos com uma previsão, nos termos da qual, as autoridades competentes poderem solicitar diretamente aos registos (Registry) – em Portugal, a Associação DNS.PT - e entidades gestoras de nomes de domínio (Registrars) a prestação de todas as informações que considerem pertinentes à investigação, atribuindo-lhes em última instância a competência para, nomeadamente, e reproduzindo com as devidas adaptações, a letra do ora identificado articulado "(...) *apagar um nome de domínio plenamente qualificado e autorizar a autoridade competente em causa a registá-lo*", Do nosso ponto de vista, a solução aqui preconizada pelo legislador vai ainda mais longe que a

mera colaboração, podendo, in extremis, impor uma acção, tenha ela eficácia prática ou não: apagar um nome de domínio!

Nota ainda para a Estratégia Europeia para um mais efetivo combate ao abuso sexual de menores, tornada pública no passado mês de julho, onde parece claro ir replicar-se a mira orientada a players como os registries. Neste momento estão a ser ponderadas pela Comissão várias soluções legislativas que passam pela criação de um quadro regulatório capaz de fixar medidas de deteção, comunicação às autoridades competentes e, eventualmente, remoção de conteúdos online com esta natureza. Espera-se novidades ao longo deste primeiro semestre do ano.

Parece óbvio que remover conteúdos ilegais da Internet é a única forma de evitar o acesso aos mesmos, o problema está em saber como fazê-lo de forma eficaz. Grande parte dos caminhos possíveis que podem ser trilhados – incluindo o bloqueio ou a remoção do respectivo nome de domínio – têm em comum o facto de os conteúdos continuarem disponíveis e acessíveis, só se alterando a via e o tempo que demoramos para lá chegar. Não vamos aqui replicar a análise[1] feita pelo CENTR[2], onde tivemos oportunidade de participar, sobre o papel dos ccTLD's na gestão dos conteúdos ilegais; ficamos só pelas conclusões mais relevantes que derivam de um pressuposto: os ccTLD não têm acesso a conteúdos nem alojam ou transferem conteúdos através da sua infraestrutura. No imedidato e para além do cumprimento estrito das obrigações que emergem, ou venham a emergir, do edifício legislativo europeu no que a esta matéria diz respeito, cumpre chamar a si um dever de consciencialização e educação da sua comunidade sobre os perigos da Internet; facilitar e potenciar a colaboração com forças policiais e restantes autoridades competentes; e disponibilizar de forma célere e dentro dos limites da lei, identificação dos contactos associados a nomes de domínio utilizados para possibilitar o acesso a conteúdos ilegais.

As escolas de direito ensinam logo nos primeiros anos, que o necessário rejuvenescimento dos sistemas jurídicos vem muitas vezes de dentro. O alcance desta afirmação podia levar-nos longe, mas vamos aqui ser lineares: pode o juíz abster-se de julgar quando há uma omissão na lei, quando esta não é suficientemente clara, ou nos deixa espaços de discricionariedade? Se sim, estaremos nós a por em causa princípios chave como a

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

estabilidade e a segurança jurídica? Aqui entra o fundamental papel da jurisprudência na eventual formação dos sistemas jurídicos. Dito isto, e não obstante os primeiros passos do legislador comunitário que identificámos acima, não podíamos omitir aqui uma decisão (I ZR 13/19) inédita do Tribunal de Justiça Federal Alemão (TJFA) relativamente à responsabilidade dos registrars pelos conteúdos publicados online, associados a nomes de domínio pelos quais sejam responsáveis na qualidade de entidade gestora/técnica. No longo texto do Acórdão pode surpreendentemente ler-se que o registrar que, por conta do registrant, proceda ao registo de um nome de domínio junto do respetivo registry, fornecendo os dados técnicos e administrativos necessários para o efeito, participando, assim, no seu processo de ativação, é subsidiariamente responsável pelos conteúdos publicados online que violem direitos de propriedade intelectual e que estejam associados a esse nome de domínio. Se neste caso concreto não olhamos diretamente para a questão do bloqueio ou remoção de um domínio, a matéria está fortemente intrincada e prende-se com o âmbito da responsabilidade dos diferentes elos desta cadeia.

Perdoem-nos esta longa introdução, onde até podíamos ter alargado a nossa análise, mas pareceu-nos útil para enquadrar as opções que procurámos plasmar nas regras de Registo de .PT em matéria de bloqueio ou remoção de domínios que alogem conteúdos ilegais ou ações configuráveis como de DNS Abuse.

O conceito de DNS Abuse é pela primeira vez definido na al. g) do Glossário das Regras, e circunscreve-se aos casos em que o nome de domínio é usado, intencionalmente ou não, para atividades de disseminação de malware, phishing, pharming, botnets e/ou spam. Contrariamente, e reportando agora a vossa atenção para o conceito de conteúdos ilegais, a sua natureza ampla e multifacetada, acima já aflorada, levou-nos a optar por não apresentar nenhuma definição formal, sob pena de incorrermos em rigor duvidoso. Porém, também aqui, não se trata de matéria omissa, e no n.º 4 do artigo 25.º clarifica-se: *"(...) o .PT não é, em caso algum, responsável pela utilização que é dada ao nome de domínio, designada mas não exclusivamente, pelos conteúdos que lhe estão associados"*. A responsabilidade pela utilização que é dada ao nome do domínio, e por inerência, aos conteúdos que lhe sejam associados, é exclusiva do registrant. Assim dita o n.º 2 do artigo 23.º.

Quanto às situações de DNS Abuse, caso identifiquemos que um nome de domínio é utilizado para atividades aqui subsumiveis, os responsáveis do domínio serão notificados para assegurarem as medidas necessárias à sua correção. Caso a atividade maliciosa

identificada persista, e sempre que aplicável, o .PT reportará a situação à autoridade competente (n.º 3 do artigo 25.º). Este mecanismo agora formalmente plasmado no texto das Regras de Registo, para além de formalizar aquilo que são as preocupações do .PT em matéria de segurança[3], cristaliza o que era o trabalho já desenvolvido pelo seu Serviço de Operação de Segurança, o PTSoc[4]. O PTSoc tem hoje já mecanismos que permitem identificar ativamente domínios que estejam a ser usados para atividades enquadráveis no conceito de DNS Abuse[5]. Cabe, por exemplo, ao PTSoc comunicar aos responsáveis pelo domínio e/ou autoridade competente, as situações de DNS Abuse que, direta ou indiretamente identifique no âmbito da sua atividade de monitorização.

Resta-nos uma última questão – talvez mesmo a mais importante -, que é a de saber se afinal o .PT pode remover um domínio ao qual estejam associados conteúdos ilegais. A resposta é sim. Ao abrigo do disposto na al. a) do artigo 22.º, o nome de domínio é removido de imediato quando o .PT seja informado da perda do direito de uso do mesmo pelo seu titular, e desde que tal resulte de uma notificação nesse mesmo sentido por entidade com competência legal para o efeito. Como dissemos, e essa questão já foi aflorada acima, não vamos discorrer aqui sobre a eficácia prática de uma notificação neste mesmo sentido. O propósito aqui é outro. O propósito é o de demonstrar que foram criados mecanismos céleres que nos permitirão agir de forma colaborativa e em conformidade com a lei aplicável.

Em suma, procurámos nestas Regras espelhar não só aquilo que são os nossos compromissos institucionais6, mas também aqueles que hoje já decorrem da lei - recordamos aqui as obrigações que decorrem do nosso estatuto de Operador de Serviços Essenciais, à luz da Lei n.º 46/2018, de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço – assim como os que se prerspetivam para breve, e que acima tentámos elencar. Em paralelo, e porque nesse campo as dúvidas não existem, baseámos a nossa intervenção em princípios de neutralidade, transparência e de estrita colaboração com as entidades que a lei identifique como competentes no que a esta matéria diz respeito.

[3] Todas as iniciativas do .PT na área da segurança estão devidamente descritas em: https://www.dns.pt/pt/seguranca/

[4] https://www.dns.pt/pt/seguranca/centro-de-operacoes-de-seguranca-soc/

[5] Em 2020 foram detetados pelo PTSoc, 186 casos de DNS Abuse. Relatório completo em: https://www.dns.pt/fotos/editor2/relatorios/relatorio2020_ptsoc.pdf

[6] O .PT e o Centro Nacional de Cibersegurança assinaram em 2019 um Protocolo de Colaboração, que tem servido de base para uma colaboração estreita, e particularmente frutífera, em várias frentes e iniciativas.

Um contorno final que nos parece merecer aqui referência. Neste âmbito em análise, o .PT chama a si uma responsabilidade remanescente, mas fundamental: manter a sua base de dados de contactos associados aos nomes de domínios atualizada, completa e com informação precisa. Trata-se de tarefa difícil e onde é bem de ver, a informação que seja tratada pelos registrars, enquanto agentes de registo, enquanto intermediários no processo, é uma peça fundamental. De novo caímos na importância da colaboração, feita de diálogo e proximidade. Fechamos com nova promessa, a do empenho para que o nosso elo nunca seja o mais fraco.