Registries e conteúdos *online*

Council of European National Top-Level Domain Registries

Índice

Sumário Executivo

Os membros do CENTR, que são *registries* de ccTLD, gerem os domínios de topo (*top-level domains* - TLDs) correspondentes ao país (*country code Top-Level Domains*, ccTLDs) na Internet. As suas responsabilidades vão desde disponibilizar e operar a infraestrutura técnica do sistema de nomes de domínio (*domain name system*, DNS) do seu TLD, organizando o processo de registo de nomes de domínio, até à manutenção proativa da base de dados do *registry*, por forma a que os nomes de domínio possam ser usados para navegar na Internet.

Os conteúdos abusivos e ilegais minam a confiança na Internet enquanto plataforma de inovação, criatividade e oportunidades económicas. Os *registries* de ccTLD estão empenhados em contribuir para uma abordagem abrangente e eficaz contra conteúdos ilegais *online*.

A Internet é um conjunto global de redes de computadores interligadas que permitem a comunicação recorrendo a endereços IP numéricos únicos. O Sistema de Nomes de Domínio (DNS) funciona como um estrato por cima da infraestrutura de IP. Os nomes de domínio tornam a navegação na Internet mais fácil para o utilizador. Por exemplo, quando um utilizador escreve o nome de domínio de um *site*, o DNS comunica ao dispositivo do utilizador qual é o endereço IP correspondente no qual os conteúdos do *site* podem ser encontrados.

Para que seja possível encontrar conteúdos *online*, os mesmos têm de estar guardados pelo menos num computador ou num servidor que esteja ligado à Internet. Para remover eficazmente conteúdos da Internet, estes têm de ser apagados no dispositivo em que estão alojados ou então esse dispositivo tem de ser desligado da Internet.

A qualificação dos conteúdos como “ilegais” depende do quadro jurídico nacional e pode variar dependendo do contexto. A autoridade à qual compete esta avaliação é definida la nível nacional.

Remover conteúdos ilegais da Internet é a única forma eficaz de evitar o acesso aos mesmos. O editor de conteúdos e o fornecedor de alojamento têm acesso direto aos conteúdos ou ao dispositivo que os guarda e devem ser os primeiros a serem contactados.

Quando um nome de domínio é usado para possibilitar o acesso ao conteúdo, o titular do nome de domínio pode ser o fornecedor dos conteúdos e do alojamento, ou ser capaz de o identifica. A base de dados oficial do *registry* com informação sobre todos os nomes de domínio registados sob o seu TLD pode ajudar a identificar e a contactar o titular do nome de domínio.

Quando não for possível remover conteúdos ilegais da Internet, que é a única solução eficaz, pode tentar fazer-se com que seja mais difícil os utilizadores os encontrarem ou a eles acederem. Existem vários métodos de "bloquear" conteúdos na Internet, a vários níveis e envolvendo vários intervenientes. No entanto, todos têm em comum o facto de os conteúdos continuarem disponíveis e de as medidas tomadas poderem causar danos colaterais não intencionais. Por conseguinte, devem ser tidos como uma medida intercalar, a ser adotada em caso de urgência ou quando todas as outras alternativas tenham falhado. Bloquear ou apagar um nome de domínio é uma dessas medidas.

Os quadros jurídicos de cada país definem que conteúdos são ilegais, quem tem poderes para lidar com os mesmos e que processos são admissíveis dentro da lei. Podem existir diferenças de país para país. Os *registries* dos ccTLD têm requisitos diferentes quanto a quem pode registar nomes de domínio e quais são os seus deveres. A combinação destes requisitos e do quadro jurídico nacional influencia as políticas e iniciativas que o *registry* desenvolve para abordar a questão dos conteúdos ilegais *online*.

Tipicamente, estas políticas estão enraizadas na comunidade local, são compatíveis com as leis locais, respondem a necessidades locais e, muitas vezes, foram desenvolvidas em colaboração com outras partes interessadas locais. Políticas e práticas bem sucedidas para um ccTLD podem inspirar outros. No entanto, devido às raízes e particularidades locais, não há garantias que replicar um projeto ou uma política conduza ao mesmo resultado positivo ou lícito no quadro legal de um outro ccTLD.

Como abordagem possível ao tema dos conteúdos ilegais, os *registries* de ccTLD, focam-se, entre outros, no seguinte:

- Formação e consciencialização abrangente da comunidade.
- Formação e colaboração estreita com as autoridades e as forças policiais.
- A manutenção de uma base de dados de um *registry* para melhorar a qualidade dos dados do registo WHOIS pode ter um impacto indiretamente positivo, dado que é pouco provável que pessoas mal intencionadas registem um nome de domínio usando informação pessoal correta.
- Definir procedimentos para partilhar dados do *registry* com terceiros dentro dos limites da regulamentação nacional sobre reserva da intimidade da vida privada (privacidade).
- Desenvolver processos e procedimentos para responder à identificação de conteúdos suspeitos. Estes procedimentos normalmente têm em comum o facto de se aplicarem a casos limitados e bem definidos, e de estar envolvida uma entidade externa especializada na avaliação desse tipo de conteúdos.

Introdução

Os membros do CENTR gerem o registo de um ou mais domínios de topo correspondentes ao país (ccTLDs) na Internet. As suas responsabilidades vão desde disponibilizar e operar a infraestrutura técnica do sistema de nomes de domínio do seu TLD, organizando o processo de registo de nomes de domínio, até à manutenção proactiva da base de dados de registos, de forma que os nomes de domínio possam ser usados para navegar na Internet.

Os membros do CENTR acreditam que a confiança e a segurança *online* são essenciais para que a Internet continue a ser uma plataforma de inovação, criatividade e oportunidades económicas. Os conteúdos abusivos e ilegais minam a confiança na Internet. Os *registries* estão empenhados em contribuir, juntamente com outros intervenientes, para uma abordagem abrangente e eficaz aos conteúdos ilegais na Internet.

Objetivo deste documento

O esforço conjunto e a colaboração bem sucedida exigem que as partes interessadas compreendam e respeitem as funções, os papéis e as limitações de cada uma. O objetivo deste documento é clarificar o papel de um *registry* de ccTLD explicar a sua relação com conteúdos *online*, explorar as possibilidades e limitações das ações e gerir as expetativas quanto ao que um *registry* pode e não pode fazer em matéria de conteúdos ilegais *online*.

Visão geral do documento

A primeira parte do documento explica o funcionamento da Internet, onde é que os conteúdos online estão localizados e como é que podem ser acedidos, e o papel de facilitação do sistema de nomes de domínio (DNS).

A segunda parte do documento analisa a questão dos conteúdos ilegais na Internet e como é que os registries de ccTLD podem contribuir para ações que levem à remoção dos mesmos.

A terceira parte é dedicada às atuais políticas e práticas de um *registry*, dando exemplos de como vários *registries* de ccTLD desenvolvem políticas e tomam medidas que servem da melhor forma as necessidades das suas comunidades locais e contribuem, dessa forma, para a batalha conjunta contra conteúdos ilegais *online*.

A Internet, o Sistema de Nomes de Domínio e Conteúdos *Online*

O DNS como parte da infraestrutura da Internet

A Internet e a sua infraestrutura

A Internet é um conjunto de redes de computadores que estão interligadas e que formam um sistema de comunicação global. O Protocolo Internet (*Internet Protocol*, IP) é o método ou conjunto de regras segundo as quais são enviados dados pela Internet de um dispositivo para outro. Para que a transferência seja bem sucedida, é importante que o remetente e o destinatário possam ser identificados e localizados entre milhões de computadores, smartphones, servidores, IoT e outros dispositivos que estão ligados à Internet. Por conseguinte, todos os dispositivos ligados têm pelo menos um endereço IP que os identifica entre todos os outros dispositivos. Um endereço IP pode ser representado como uma etiqueta numérica[1]: por exemplo, o endereço IP 2001:db8:85a3::8a2e:370:7334[2] poderia identificar o interface de um servidor no qual os conteúdos de um *site* estão guardados.

O Sistema de Nomes de Domínio

Para o utilizador, ler e recordar endereços IP numéricos é difícil. Para resolver esta questão, o sistema de nomes de domínio (DNS) permite a utilização de nomes de domínio para designar endereços IP. O DNS funciona como um estrato por cima da infraestrutura de IP. Quando, por exemplo, um utilizador escreve um nome de domínio num motor de busca, ou clica numa ligação com um nome de domínio, o dispositivo vai procurar o endereço IP correspondente no DNS. Quando o DNS devolve um endereço IP, o dispositivo do utilizador sabe onde é que os conteúdos de um *site* ou a caixa de correio associada a um endereço de correio eletrónico (*e-mail*) podem ser encontrados na Internet.

[1] Os endereços IPv6 têm 128 bits e são representados usando uma cadeia hexadecimal. A versão mais antiga, a IPv4, tem 32 bits e é representada em grupos de números decimais separados por pontos.

[2] Este endereço IP destina-se exclusivamente a efeitos de documentação e não está encaminhado para a internet pública (RFC 3849, IPv6 Documentation prefix).

[3] Para saber mais sobre o funcionamento do DNS visite: https://www.centr.org/edution/the-dns.html.

Um *registry* de nomes de domínio é responsável pela gestão de um ou mais TLDs. Todos os *registries* têm de respeitar as regras e os requisitos técnicos do DNS, mas, relativamente a políticas, cada TLD continua a ser responsável por definir as suas próprias regras. Os TLDs genéricos (gTLDs) têm de cumprir as políticas e processos gerais desenvolvidos pela comunidade ICANN, ao passo que os TLDs correspondentes aos países (ccTLDs) definem a sua própria política de acordo com as necessidades da sua comunidades Internet nacional.

Conteúdos *online*

Os conteúdos têm de ser criados, guardados e disponibilizados antes de poderem ser encontrados na Internet. A forma como isto acontece é descrita neste capítulo, ao identificar os diferentes papéis e responsabilidades[4].

Disponibilizar conteúdos *online*

Fornecedor de conteúdos

O editor de conteúdos fornece à Internet texto, som, imagens, vídeos, animações e outras formas de conteúdos que são carregadas num *site*, publicadas num blogue, disponibilizadas em plataformas sociais, etc. O editor de conteúdos pode ser, mas não é necessariamente, o criador original dos conteúdos.

Para poderem estar acessíveis através da Internet, os conteúdos têm de estar guardados pelo menos num computador ou num servidor que esteja ligado à mesma. Um editor de conteúdos pode usar o seu próprio computador ou servidor ou, o mais habitual, usar os serviços e infraestrutura de um fornecedor de alojamento.

Fornecedor de alojamento

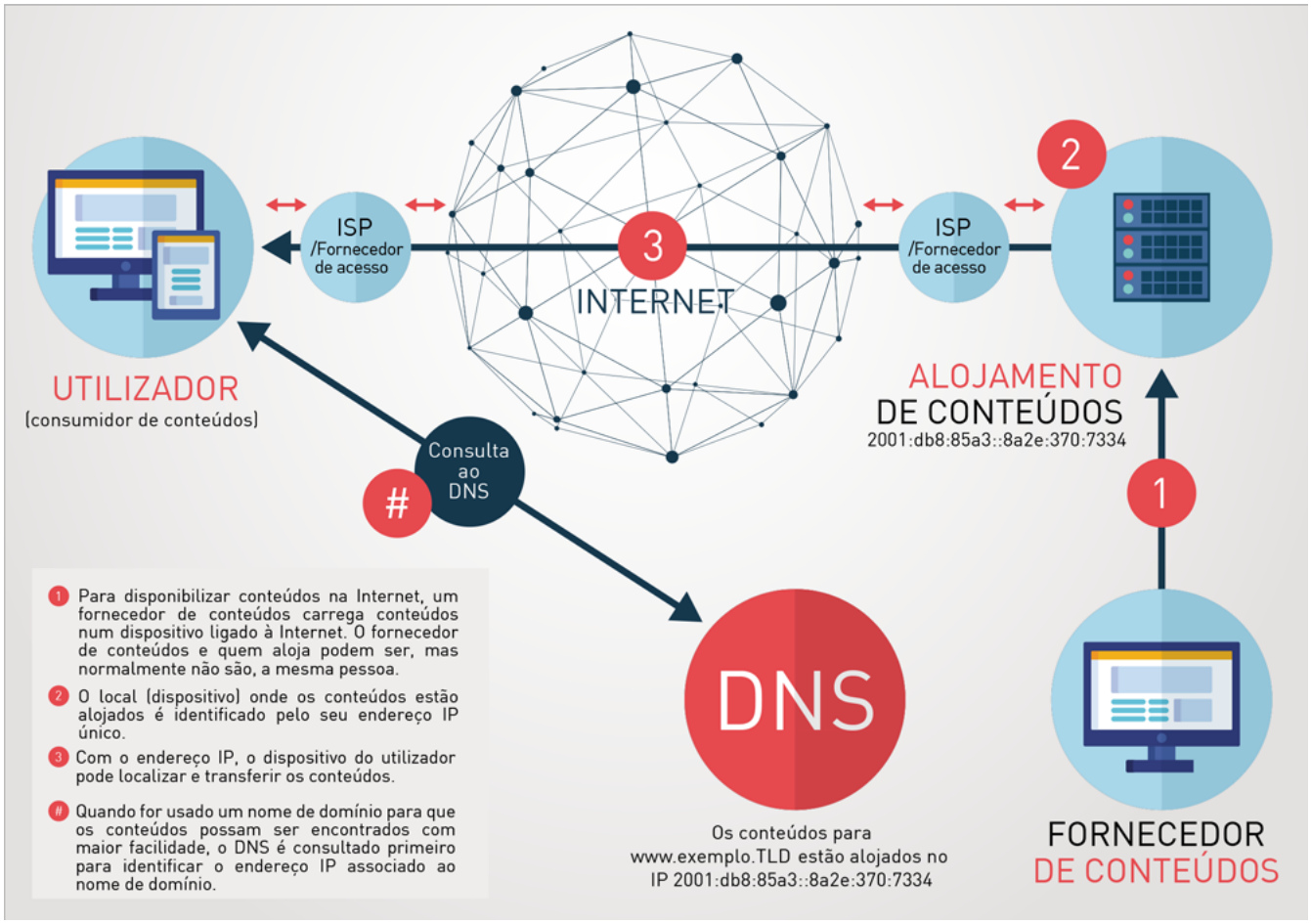
Um fornecedor de alojamento fornece armazenamento e conectividade, possui os conhecimentos técnicos e, mais importante ainda, as necessárias infraestrutura, capacidade e largura de banda para poder lidar com o tráfego que pode vir de qualquer local na Internet, a qualquer hora do dia. Os fornecedores de alojamento facultam a plataforma para os conteúdos serem alojados, mas não decidem o que é ou não é publicado - os seus clientes (os editores de conteúdos) é que o fazem. Com poucas exceções, geralmente correspondentes a grandes organizações com a sua própria infraestrutura e redes, um fornecedor de conteúdos recorre geralmente aos serviços de um fornecedor de alojamento. Os fornecedores de alojamento têm grandes centros de dados com servidores que contêm os conteúdos dos seus clientes. Estes servidores estão ligados à Internet e podem ser identificados pelo seu endereço IP exclusivo. Existem vários tipos de alojamento; os mais comuns são o alojamento de *sites* e o alojamento de correio eletrónico. O alojamento de redes sociais (por exemplo, vídeos gerados pelo utilizador) pode ser um caso especial entre a edição e o alojamento.

[4] Os intervenientes podem combinar um ou mais papéis descritos neste capítulo, por exemplo um ISP também pode prestar serviços de alojamento.

Fornecedor de Serviço Internet / Fornecedor de Acesso à Internet

O fornecedor de serviço Internet (*Internet Service Provide*r, ISP) fornece acesso à Internet. Através da sua rede e da sua infraestrutura, os seus clientes podem aceder à Internet. O ISP vai atribuir endereços IP aos dispositivos ligados à sua rede, por exemplo, os servidores do fornecedor de alojamento, o modem do utilizador da Internet, etc. O ISP é um fornecedor de acesso e, como tal, não armazena conteúdos, mas os conteúdos movimentam-se na sua infraestrutura.

Existem outros intervenientes que asseguram o transporte e troca de dados entre redes, como pontos de partilha de Internet (*Internet Exchange Points*, IXPs) e operadores de redes de transporte (de curta ou longa distância) ou redes de entrega de conteúdos (*Content Delivery Networks*, CDN)[5] que alojam cópias dos conteúdos dos seus clientes em servidores em várias localizações geográficas para otimizar a experiência do utilizador final (por exemplo, Cloudflare). A sua relação com os conteúdos não é aqui abordada em profundidade.



[5] https://en.wikipedia.org/wiki/Content_delivery_network

Usar o DNS enquanto ferramenta para ajudar a encontrar conteúdos

O Sistema de Nomes de Domínio (DNS) faculta uma função que ajuda a navegar na Internet. Permite que o endereço IP associado a um nome de domínio seja encontrado. Por conseguinte, algumas pessoas comparam o DNS a uma lista telefónica ou a um registo de imóveis ou de empresas[6].

Titular de um nome de domínio/*Registrant*

Um editor de conteúdos pode registar um nome de domínio para tornar mais fácil para os utilizadores encontrarem conteúdos que tenha disponibilizado *online*. O nome de domínio funciona como uma etiqueta por cima do endereço IP, é mais fácil de memorizar que o endereço IP e pode conter informações únicas, como o nome da empresa num endereço de *e-mail* ou a referência ao conteúdo num nome de domínio de um *site*.

O titular do nome de domínio não é necessariamente o fornecedor (ou o único fornecedor) dos conteúdos publicados sob o nome de domínio. Por exemplo, *sites* de universidades, de blogues ou de redes sociais permitem que vários utilizadores publiquem conteúdos num *site* identificado por um único nome de domínio.

O titular/*registrant* de um nome de domínio tem o direito de usar um nome de domínio específico. Para obter este direito, uma pessoa ou uma entidade regista o nome no *registry* do TLD, diretamente ou através de um *registrar*. O titular do nome de domínio é responsável pela forma como o nome é usado.

Registrar

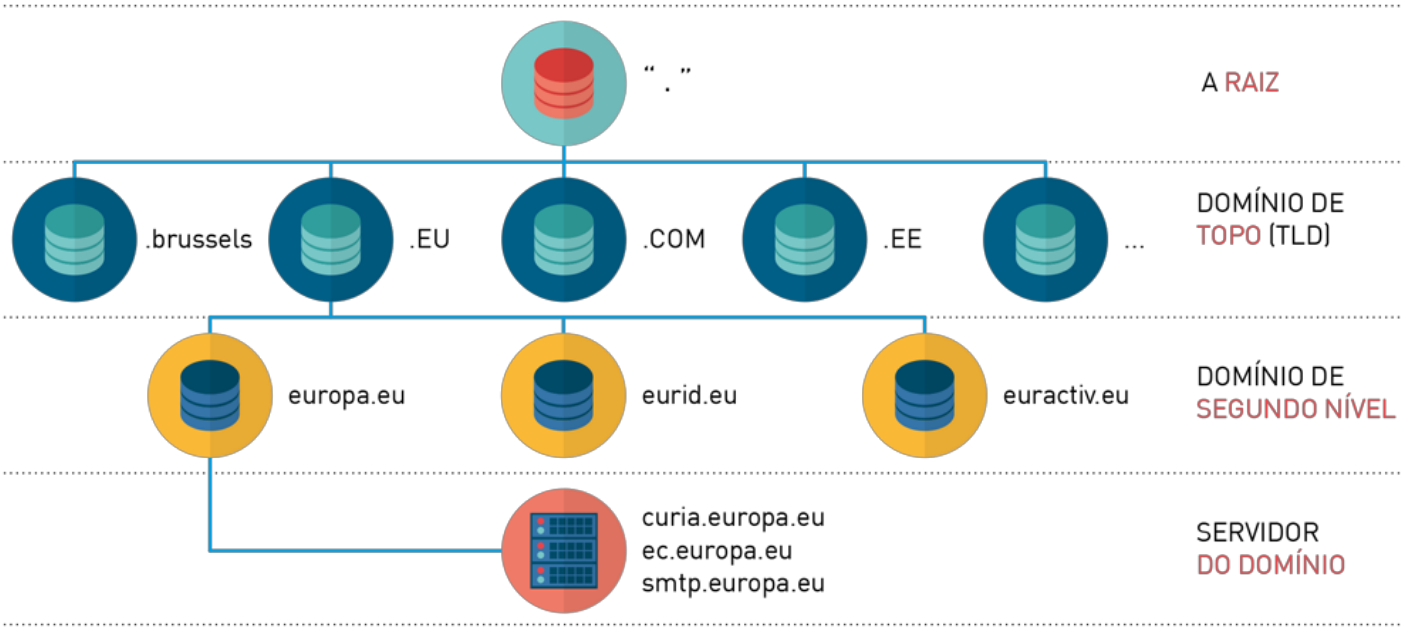
O *registrar* é uma empresa que presta serviços de registo de domínios a empresas e particulares, diretamente ou através de uma rede de revendedores. O *registrar* é acreditado por um ou mais *registries* para fornecer nomes de domínio sob os TLDs. O *registrar* vai verificar a disponibilidade do nome de domínio e tratar do processo de registo, ao passo que o *registry* gere o TLD do nome pedido. Como parte integrante do processo de registo, o *registrar* vai submeter a informação de contacto do titular do nome de domínio e a informação técnica relacionada com o nome de domínio (por exemplo, que servidores de nomes contêm os registos DNS que vão comunicar aos programas de navegação na *web* e aos clientes de *e-mail* onde podem encontrar o servidor *web* com os conteúdos do *site* ou o servidor de correio que processa o *e-mail*). Um *registrar* não aloja conteúdos e estes não passam pela sua infraestrutura. Na prática, no entanto, muitos *registrars* também fornecem serviços de alojamento e outros serviços aos seus clientes.

Registry de TLD

O *registry* gere a única base de dados oficial de nomes de domínio registados sob o seu TLD e publica esta informação no DNS. Os servidores de um *registry* de domínios contêm informações sobre o titular do nome de domínio, o registo do domínio (por exemplo, a data de validade), os endereços IP associados ao nome de domínio e outros elementos técnicos. Um *registry* publica um ficheiro de zona atualizado várias vezes por dia, que é um ficheiro de texto que contém mapeamentos entre o nome de domínio e os seus servidores de nomes para cada nome registado, bem como outros recursos. Este ficheiro contém as informações sobre a forma de localizar endereços IP e outras informações necessárias para navegar na Internet. Os *registries* não armazenam nem melhoram conteúdos.

[6] https://en.wikipedia.org/wiki/Domain_Name_System

Nota: A maioriar dos ISPs põe em *cache* informações do DNS sobre nomes de domínio recentemente consultados de TLDs diferentes, nos chamados servidores de nomes não oficiais, para agilizar a experiência de pesquisa dos seus clientes. É só quando uma resposta recente não está disponível no servidor do ISP que o DNS é consultado. Em consequência, as alterações feitas ao DNS (como por exemplo a remoção de um nome de domínio no DNS por parte do *registry*) podem demorar a ficar ativas em toda a Internet.



A estrutura ramificada do DNS

Tomar medidas contra conteúdos ilegais na net

O que são conteúdos ilegais?

Definição pelos quadros jurídicos nacionais

O termo "ilegal" é usado para descrever conteúdos que são proibidos num contexto nacional, independentemente do motivo. A Comissão Europeia, por exemplo, define conteúdos ilegais como "qualquer informação que não cumpra o direito da União ou o direito do Estado Membro em causa".[7] Para além de questões relacionadas com o abuso sexual de menores, não há muito consenso a nível internacional sobre o que são conteúdos apropriados de uma perspetiva de política pública. O que é permitido numa jurisdição pode ser proibido noutra. A admissibilidade dos conteúdos também pode estar relacionada com o contexto: conteúdos considerados ilegais num contexto (como filmes obscenos vistos por menores) pode ser aceitável noutro (como quando são vistos por adultos), mesmo dentro da mesma jurisdição.[8]

Alguns países definiram um quadro jurídico direcionado aos conteúdos *online*, ao passo que noutras jurisdições as questões relacionadas com conteúdos *online* são tratadas com base nos quadros jurídicos gerais existentes, que não são específicos da Internet. Um estudo comparativo em 47 Estados Membros do Conselho da Europa relevou quatro grandes categorias de fundamentos jurídicos para apreciar a legalidade dos conteúdos *online*:

- a proteção da saúde e da moral (incluindo pornografia infantil ou jogo ilegal);
- a proteção da segurança nacional, da integridade territorial ou da segurança pública (incluindo contraterrorismo);
- a proteção de direitos de propriedade intelectual; e
- a proteção contra difamação e tratamento ilícito de dados pessoais.[9]

Quem pode apreciar a legalidade dos conteúdos?

A classificação dos conteúdos como "ilegais" depende do quadro jurídico nacional e pode mesmo variar dependendo do contexto. Saber se os conteúdos são ilegais ou não é decisão que pertence aos tribunais de cada país ou às autoridades competentes. Além disso, o processo seguido pode variar mesmo dentro da mesma jurisdição. Se umas entidades podem ter o poder de apreciar a legalidade dos conteúdos e agir diretamente com fundamento nessa apreciação, outras podem estar dependentes de decisão judicial prévia para poder agir.

---

[7] *Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online* (Recomendação da Comissão de 1.3.2018 sobre medidas para resolver a questão dos conteúdos ilegais *online*), C(2018)1177, Comissão Europeia, Março de 2018, https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-ilegal- content-online

[8] *Internet Society Perspectives on Internet Content Blocking: An Overview,* Internet Society, Março de 2017, https://www.internetsociety. org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf

[9] *Comparative study on blocking, filtering and take-down of illegal Internet content,* COE, Dezembro de 2015, https://www.coe.int/en/ web/freedom-expression/study-filtering-bloquear-and-take-down-of-illegal-content-on-the-Internet (acedido em 7 de junho de 2018).

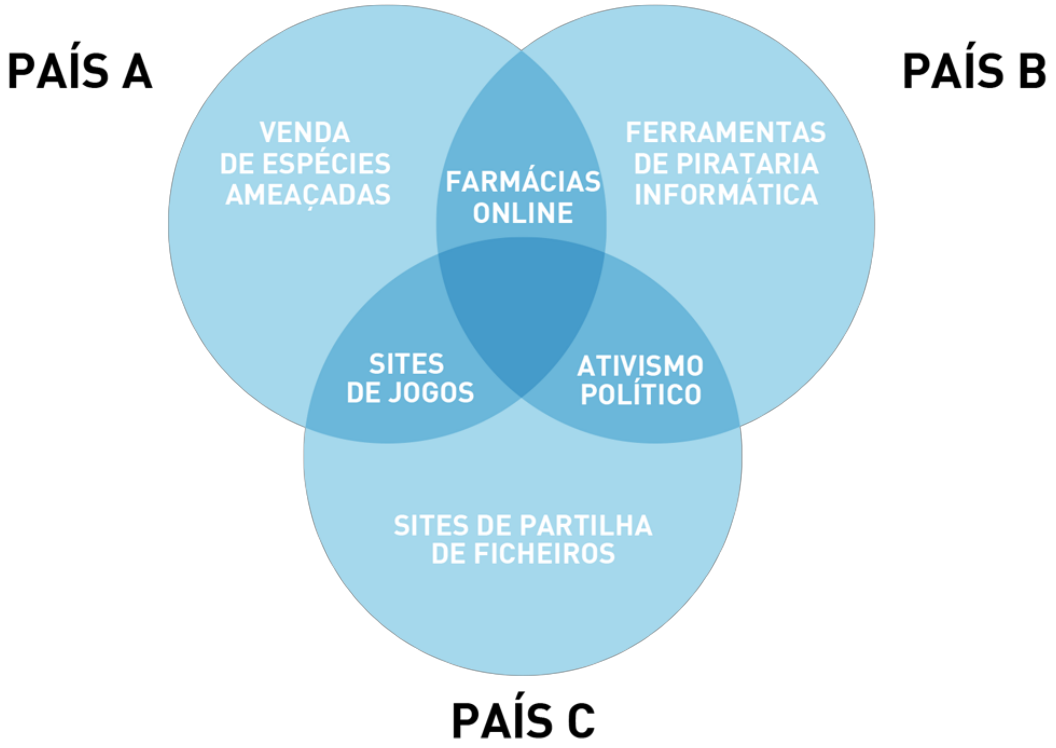


Diagrama de Venn que mostra que o que é legal em alguns países não é em outros.

O editor de conteúdos é responsável pelos conteúdos que disponibiliza a outros utilizadores da Internet. É da responsabilidade do titular do nome de domínio assegurar que o seu nome de domínio não é utilizado para possibilitar que conteúdos ilegais estejam acessíveis na Internet. Para aditar mais um nível de complexidade, o fornecedor e o utilizador que consome os conteúdos podem não estar na mesma jurisdição. Além disso, os próprios conteúdos podem estar alojados ainda noutra região geográfica com as suas próprias leis, moral e definição do que é legal ou não.

Um *registry* de um ccTLD está na mesma posição que qualquer organização ou mesmo pessoa singular no que diz respeito a conteúdos *online*. Pode proceder a uma avaliação e formar uma opinião sobre o que pensa estar dentro e fora de enquadramento legal, mas não tem nenhuma autoridade especial para apreciar efetivamente a legalidade do conteúdo que é colocado *online*. Quando um *registry* acede a conteúdos *online*, fá-lo da mesma forma que qualquer pessoa que navegue num *site* na Internet e transfira os conteúdos para o seu computador. Não existe qualquer atalho que permita a um *registry* obter informações particulares sobre quais são os conteúdos publicados pelos titulares de domínios. Os *registries* de ccTLD não alojam conteúdos e estes não passam através da sua infraestrutura.

Alguns *registries* têm prevista, nos seus termos e condições, a possibilidade de tomarem medidas em casos óbvios de conteúdos ilegais, em que não existam muitas dúvidas e riscos de responsabilidade mínimos. Em geral, os *registries* não estão equipados, não têm pessoal nem estão bem posicionados para procurar ativamente conteúdos ilegais na Internet.

Onde é que os conteúdos *online* estão localizados?

Localização na Internet

Para poderem estar acessíveis através da Internet, os conteúdos têm de estar guardados pelo menos num computador ou num servidor que esteja ligado à Internet. A localização dos conteúdos é especificada pelo(s) endereço(s) IP único(s) do(s) dispositivo(s)[10] onde estão armazenados.

Localização física

Geograficamente, o(s) dispositivo(s) que contém (contêm) os conteúdos pode (podem) estar em qualquer lugar do mundo onde exista energia e uma ligação à internet. Não existem regras ou requisitos estritos sobre o local onde os conteúdos devem ser alojados tecnicamente, muito embora a localização física possa ter influência na velocidade e na qualidade da ligação.

Os conteúdos podem ser armazenados apenas num servidor ou em vários servidores (por exemplo, alojamento na nuvem, alojamento agrupado (*clustered hosting*)). Podem estar num ou mais servidores, no mesmo país do fornecedor de conteúdos, ou do utilizador dos mesmos. E podem também estar em qualquer lugar do mundo e ser-lhes aplicadas regras de diferentes jurisdições.

Remover conteúdos ilegais

Remover conteúdos ilegais da Internet é a única solução eficaz para evitar o acesso aos mesmos. Esta remoção pode ser concretizada apagando os conteúdos no dispositivo onde estão guardados ou desligando esse dispositivo da Internet.

Contactar o editor de conteúdos ou o fornecedor de alojamento

O editor de conteúdos e o fornecedor de alojamento têm acesso direto aos conteúdos ou ao dispositivo que guarda os mesmos. O editor de conteúdos tem as ferramentas e os códigos de acesso para alterar ou remover os conteúdos que disponibilizou num *site,* rede social ou noutros locais. O fornecedor de alojamento pode remover os conteúdos dos seus servidores ou, efetivamente, impedir que os conteúdos sejam acedidos através da sua infraestrutura.

De notar que os fornecedores de alojamento normalmente guardam conteúdos de clientes diferentes na mesma máquina física. Por conseguinte, desligar ou confiscar um servidor pode afetar diferentes fornecedores de conteúdos e fazer com que conteúdos legítimos fiquem inacessíveis. Os editores de redes sociais e *sites* de blogues podem ter a possibilidade de remover publicações questionáveis ou conteúdos ilegais que sejam publicados nas suas plataformas.

[10] Em termos técnicos, o endereço IP identifica o interface através do qual o dispositivo troca informações, não o próprio dispositivo.

Contactar o titular do nome de domínio

O titular do nome de domínio é a primeira pessoa a contactar se um nome de domínio for usado para possibilitar o acesso a conteúdos ilegais. Pode acontecer que o titular do nome de domínio seja o mesmo ou que esteja próximo do editor de conteúdos. O titular do nome de domínio pode não ser a fonte dos conteúdos ilegais ou pode não ter conhecimento de que o seu nome de domínio está a ser usado para possibilitar o acesso a conteúdos ilegais[11]. No entanto, na maioria dos casos, o titular do nome de domínio deverá estar em condições de ajudar a identificar a fonte dos conteúdos ilegais e tomar medidas para os remover.

O *registry* mantém a base de dados oficial com informações sobre todos os nomes de domínio registados sob o seu TLD e pode ajudar a identificar e contactar o *registrant*. A base de dados do *registry* contém, entre outras informações sobre o titular do nome de domínio, informações sobre o registo do domínio (por exemplo, a data de validade) e os endereços do servidor de nomes relacionados com o nome de domínio.

Os *registries* de ccTLD fazem um grande esforço em termos de manutenção das suas bases de dados e aceitam pedidos de informações legítimos. Contactar o *registry* para pedir informações sobre o titular do nome de domínio pode ser o primeiro passo do processo para remover efetivamente conteúdos ilegais da Internet. O capítulo III, que versa sobre as atuais práticas de *registry*, contém mais informações sobre esta matéria.

Nota: para efeitos de aplicação da lei e para as autoridades policiais em especial, pode valer a pena contactar os *registrars*, dado que podem estar em condições de fornecer informações suplementares úteis, tais como elementos sobre faturação ou cartões de crédito e informações sobre outros domínios registados pelo mesmo cliente, etc.

Tornar mais difícil encontrar conteúdos

Outras medidas a tomar quando a eliminação de conteúdos ilegais falhar

Quando não for possível encontrar ou entrar em contacto com o editor de conteúdos ou o fornecedor de alojamento para remover os conteúdos ilegais da Internet, pode-se tentar dificultar o acesso aos conteúdos por parte dos utilizadores. Existem vários métodos para bloquear conteúdos na Internet, a vários níveis e envolvendo vários intervenientes. Um relatório de 2017 da Internet Society[12] descreve os métodos mais correntes e avalia a sua eficácia. O documento analisa métodos de bloqueio baseados no IP e em protocolos, na inspeção de pacotes, no URL, na plataforma e no DNS ao nível da rede ou do ISP. O relatório conclui que, independentemente do nível e do método, "o recurso a bloqueio na internet para responder a conteúdos é geralmente ineficiente, muitas vezes ineficaz e passível de causar danos colaterais não intencionais a utilizadores da Internet." Bloquear conteúdos não resolve o problema: os conteúdos continuam disponíveis e, por conseguinte, o bloqueio deve ser encarado como uma medida intercalar em caso de emergência ou quando todas as outras alternativas tenham falhado.

Este documento foca-se nas ações tomadas pelo *registry*, como por exemplo quando um *registry* impede um nome de domínio de resolver um endereço IP válido, bloqueando temporariamente o nome de domínio ou apagando-o da zona.

[11] É o caso, por exemplo, de grandes redes de universidades ou plataformas de redes sociais, em que muitos utilizadores publicam conteúdos, etc., ou de quando um servidor fica comprometido e é usado por criminosos para alojar conteúdos.

[12] *Internet Society Perspectives on Internet Content Blocking: An Overview*, Internet Society, março de 2017, https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf

Riscos e inconvenientes quando o registry elimina um nome de domínio

Bloquear ou apagar um nome de domínio e, como tal, removê-lo do DNS significa que um utilizador deixa de obter um endereço IP válido quando procura o nome de domínio. O utilizador recebe uma mensagem de erro a informá-lo de que o nome de domínio não existe e o *site* esperado não aparece[13].

Apagar ou bloquear um nome de domínio é uma operação técnica relativamente simples, mas corresponde a uma intervenção drástica no DNS, com a consequência de que o nome de domínio deixa de poder ser usado para visualizar os conteúdos (tanto ilegais como legais) publicados sob o nome de domínio e os seus vários subdomínios e que todos os serviços associados ao nome de domínio, como o correio eletrónico, deixam de funcionar. Isto normalmente acontece em poucas horas, mas também pode levar alguns dias devido aos dados que estão em *cache*. Qualquer decisão de eliminar ou bloquear deve tomar em consideração todas as consequências e conseguir um equilíbrio entre a prudência e a proporcionalidade. O Regulamento da UE relativo à cooperação em matéria de proteção dos consumidores (que entra em vigor em janeiro de 2020), por exemplo, diz claramente que ordenar aos *registries* que apaguem nomes de domínio só deve ser considerado "caso não estejam disponíveis outros meios eficazes para fazer cessar ou proibir a infração abrangida pelo presente regulamento e a fim de evitar o risco de causar um prejuízo grave aos interesses coletivos dos consumidores."[14]

Alguns ccTLDs, com base na sua lei e na sua jurisdição nacional, estabeleceram relações com as respetivas forças policiais e/ou empresas de segurança devidamente credenciadas ou centros nacionais de resposta a incidentes de segurança informática (CERTs) para melhorar a confiança no seu ccTLD, apagando ou desativando de forma expedita nomes de domínio usados para fins criminosos. Essas relações caraterizam-se geralmente por uma compreensão mútua do processamento e dos mecanismos de controlo para garantir que as decisões são justas e responsáveis. As medidas que podem ser tomadas dependem do quadro de políticas do ccTLD e das questões jurídicas associadas.

Nos parágrafos seguintes descrevem-se alguns dos riscos e questões associados à ação de bloquear ou apagar nomes de domínio.

Bloquear ou apagar um nome de domínio pode fazer com que seja mais difícil encontrar conteúdos ilegais na Internet, mas não resolve a questão ou o crime, dado que os conteúdos continuam disponíveis para quem os quiser encontrar. A isso acrescem alguns riscos e constrangimentos, que serão analisados de seguida.

Eficácia duvidosa e falso sentimento de segurança, dado que os conteúdos continuam disponíveis.

Bloquear ou apagar um nome de domínio não remove conteúdos ilegais da internet. Os conteúdos continuam disponíveis e podem ser acedidos diretamente usando o endereço IP em vez do nome de domínio. A forma de o fazer não exige grandes conhecimentos científicos e uma simples pesquisa no Google permite encontrar explicações e vídeos sobre como é que se acede a um *site* através do seu endereço IP. Apagar o nome de domínio reduz as hipóteses de os utilizadores serem confrontados acidentalmente com conteúdos ilegais, mas não impede as pessoas que procuram ativamente esse tipo de conteúdos de o fazerem. "Devido à arquitetura da Internet, o bloqueio através do nome de domínio pode ser facilmente contornado pelos utilizadores finais, sendo, por conseguinte, provavelmente totalmente ineficaz a longo prazo e tendo consequências imprevistas a curto prazo."[15]

[13] *Domain Conflicts in the Legal System*, Norid, setembro de 2017, https://www.norid.no/en/domenekonflikter/rettslig-behandling/ veileder/

[14] Regulamento (UE) 2017/2394 de 12 de dezembro de 2017, que entra em vigor em 17 de janeiro de 2020. Artigo 9.º, n.º 4, alínea g), https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32017R2394&qid=1553166286569&from=EN

[15] *SAC 056 - SSAC Advisory on Impacts of Content Blocking via the Domain Name System*, SSAC, 9 de outubro de 2012.

Além disso, os fornecedores de conteúdos ilegais podem antecipar-se ao bloqueio e tomar medidas preventivas para reduzir ainda mais o seu efeito. Um fornecedor de conteúdos pode, por exemplo, registar múltiplos nomes de domínio sob o mesmo TLD ou sob vários TLDs em jurisdições diferentes, e deixá-los todos resolver o mesmo endereço IP e, portanto, aceder aos mesmos conteúdos. As hiperligações utilizadas em *e-mails* ou colocadas em plataformas ou *sites* podem ligar diretamente ao endereço IP, sem usar o DNS.

Risco de bloqueio massivo excessivo e da existência de danos colaterais

Quando um nome de domínio é apagado ou bloqueado afeta todos os conteúdos que podem ser acedidos através do mesmo e dos subdomínios, incluindo os conteúdos ilegais, mas também todos os outros conteúdos. Apagar o nome de domínio de uma rede social ou de um blogue onde os utilizadores individuais podem publicar os seus próprios conteúdos ou criar o seu blogue pessoal vai afetar todos os utilizadores, não apenas os que publicaram conteúdos ilegais, mas também os que publicaram as suas fotografias de família ou expressaram uma opinião política ou empresas que usam o *site* para efeitos de promoção e comércio eletrónico, etc. Quando se bloqueia um nome de domínio, todos os serviços associados ao mesmo, por exemplo, o correio eletrónico, deixam imediatamente de funcionar.

Num caso de estudo fictício referido na publicação *Domain Conflicts in the Legal System*, o *registry* norueguês descreve o impacto e as consequências de bloquear o nome de domínio da Universidade de Oslo, na sequência de um estudante ter publicado conteúdos ilegais numa página sob o domínio da universidade.[16]

Risco de excesso de fiscalização e facilidade de cometer erros

A facilidade técnica com que os nomes de domínio podem ser bloqueados cria um risco de excesso de fiscalização.[17] Os custos do erro são baixos do lado de quem aplica a medida, mas, pelo contrário, podem ter um impacto dramático do lado do titular do nome de domínio cujo domínio for indevidamente bloqueado[18], por exemplo, uma empresa cujo *site* é de comércio eletrónico ou uma instituição que deixou de estar acessível por *e-mail*.

Nota: há outras formas de bloquear ou intervir no DNS, por exemplo, ao nível do ISP ou do *registrar*. A maioria destas formas acarreta riscos semelhantes e pode ser contornada. Nenhuma solução de bloqueio é eficaz, já que não remove os conteúdos.

[16] Ver caixa na pág. 10, *Domain Conflicts in the Legal System,* Norid, setembro de 2017, https://www.norid.no/en/domenekonflikter/ rettslig-behandling/veileder/

[17] *Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation:* (páginas 1379 - 1383).

[18] Um exemplo está descrito na seguinte publicação de um blogue: *Main French Internet Provider Orange blocks traffic to Google*, Alix Guillard, 27.10.2016, https://en.blog.nic.cz/2016/10/27/french-orange-blocks-traffic-to-google/

Atuais práticas de um ccTLD

Conforme já foi referido, os quadros jurídicos nacionais definem que conteúdos são ilegais, quem tem poderes para lidar com os mesmos e que processos são admissíveis dentro da lei. Estes aspetos podem variar de um país para outro. Acresce que os *registries* de ccTLD têm requisitos diferentes relativamente a quem pode registar nomes de domínio e quais são os seus deveres. A combinação destes requisitos e do quadro jurídico nacional influencia as políticas e iniciativas que o *registry* desenvolve para abordar a questão dos conteúdos ilegais *online*.

Tipicamente, estas políticas estão enraizadas na comunidade local, são compatíveis com as leis nacionais, respondem a necessidades locais e, muitas vezes, foram desenvolvidas em colaboração com outras partes interessadas. Políticas e práticas bem sucedidas num ccTLD podem inspirar outros. No entanto, devido às raízes e particularidades nacionais, não há garantias que replicar uma medida ou política conduza ao mesmo resultado, positivo ou lícito, num outro ccTLD.

Formação e consciencialização, com especial atenção a um diálogo aberto e à colaboração com as autoridades e as forças policiais

Existem vários tipos de riscos e perigos que os utilizadores enfrentam quando estão *online* (técnicos, de privacidade, etc.),Reconhecer e tratar conteúdos ilegais é um deles. Diferentes *registries* de ccTLD consideram que têm o dever de alertar a sua comunidade para os perigos da Internet. Nesse sentido formam e dão orientações sobre a forma como os utilizadores se podem proteger, mitigar esses riscos ou resolver problemas.

Formação e consciencialização abrangente da comunidade

Os *registries* de ccTLD estão envolvidos na consciencialização e educação das suas comunidades Internet nacionais, por forma a tornar a Internet um local mais seguro. Os *registries* levam a cabo iniciativas para alertar e educar os titulares de nomes de domínio e a comunidade nacional de utilizadores sobre os conteúdos potencialmente ilegais e dão orientações quanto à forma de reagir. Os *registries* informam as suas comunidades de várias formas, por exemplo, organizando reuniões ou participando em sessões de trabalho, fazendo apresentações, referindo a matéria dos conteúdos ilegais nas suas publicações, etc.

Muitos *sites* de *registries* integram uma página ou uma secção sobre conteúdos ilegais. Descrevem as potenciais questões e perigos, explicam a política do *registry*, esclarecem o seu papel neste âmbito e o que pode ou não (tecnicamente) ser feito no caso de conteúdos ilegais.

O *registry* orienta qualquer utilizador que pretenda reclamar de conteúdos potencialmente ilegais *online*, indicando organizações e organismos governamentais especializados na avaliação e tratamento de determinados tipos de conteúdos *online* (por exemplo, jogo ilegal, pornografia infantil, contrafação de bens, etc.).

Exemplos

Nic.at (.at): o *site* do *registry* austríaco informa sobre um gabinete nacional para sinalizar casos de pornografia infantil e nacional-socialismo na Internet. Ver aqui e aqui.

Nominet (.uk): o *registry* do .uk explica aos utilizadores que pretendem reclamar sobre conteúdos de *sites* que podem contactar o *registrar* ou o titular do *site* e fornece ligações para várias autoridades sediadas no Reino Unido que podem estar em condições de ajudar. Ver aqui

AFNIC (.fr): o *registry* francês disponibiliza uma ligação à plataforma própria do Ministério do Interior onde os "conteúdos de *sites* ou condutas ilícitas ou contrárias à lei e à ordem pública" podem ser denunciados.

Norid (.no): o *site* do *registry* norueguês disponibiliza uma ligação ao *site* da polícia, com orientações sobre a forma de comunicar à polícia atividades ilícitas *online*, e ao serviço de aconselhamento slettmeg.no, que disponibiliza conselhos sobre a forma de remover informação da Internet.

.PT (.pt): o *registry* português, em colaboração com outras organizações que lidam com a disseminação não autorizada de conteúdos protegidos por direitos de autor, desenvolveu e aloja um portal que faculta um acesso fácil e rápido a *sites* que oferecem conteúdos digitais que respeitam os direitos de propriedade intelectual dos autores e criadores.

Os *registries* por vezes usam os seus canais de comunicação para alertar para criminosos que usam *sites* falsos, por exemplo para obter as credenciais de acesso dos utilizadores a serviços bancários ou de comércio eletrónico, e para mostrar como é que os utilizadores podem verificar a legitimidade dos *sites*. Normalmente, os *sites* falsos estão registados sob um TLD mais exótico de um país estrangeiro e o próprio *registry* não tem acesso nem influência sobre a forma como o nome de domínio é usado.

Exemplo

Aviso recente do SIDN (.nl) contra fraude bancária *online*.

Formação e colaboração estreita com as autoridades e as forças policiais

Muitos *registries* dedicam particular atenção à consciencialização e ao estabelecimento de boas relações com as forças policiais e outras autoridades (como organismos de proteção dos consumidores ou serviços de regulação e inspeção de jogos). É importante que estes organismos e autoridades, que, em muitos casos, têm poderes para apreciar a legalidade dos conteúdos, compreendam o que um *registry* faz e o que pode fazer para os ajudar no caso de conteúdos ilegais, assim como para criar bons canais de comunicação. Essa compreensão evita que se perca um tempo precioso quando pedem ao *registry* que tome medidas que este não tem capacidade para tomar ou que não enderecem os seus pedidos às pessoas ou serviços que podem reagir de forma adequada. As forças policiais desempenham um papel importante no combate contra conteúdos ilegais *online* e devem, na maioria dos casos, ser consideradas o primeiro ponto de contacto para reclamações.

É importante que aqueles que trabalham nas forças policiais e nas autoridades que atuam neste âmbito entendam como a Internet e o DNS funcionam, incluindo o papel do *registry* e as possibilidades e limitações de ação ao nível do *registry*. Alguns *registries* também desenvolvem orientações ou procedimentos para uma comunicação fluida e expedita entre determinados organismos ou autoridades e o *registry*.

Exemplos

A NORID (.no) produziu um guia informativo destinado às forças policiais e àqueles que trabalham no sistema judicial - *Domain conflicts in the legal system.* O *registry*, em colaboração com os serviços do Ministério Público, desenvolveu também orientações específicas sobre a forma como as forças policiais devem proceder quando confiscam o registo de um nome de domínio.

A SWITCH (.ch): no caso de processos penais ou administrativos, as autoridades podem abordar o *registry* com pedidos para revogar ou bloquear nomes de domínio. Em colaboração com o regulador, o *registry* desenvolveu orientações sobre a forma como as autoridades devem proceder nesses casos e qual é o âmbito das ações a que o SWITCH pode recorrer em resposta a instruções das autoridades.

A Nominet (.uk), ao consultar a sua comunidade Internet nacional, desenvolveu um processo de colaboração com as forças policiais do Reino Unido. No âmbito deste processo, as forças policiais do Reino Unido podem apresentar à Nominet certificados formais de uso criminoso ou conteúdos criminosos em relação a nomes de domínio sob .uk que levam à sua suspensão em 48 horas após a notificação do *registrant* e do *registrar* do domínio. Anualmente, é publicado um relatório de atividades suspeitas.

O *registry* como fornecedor de dados oficiais sobre nomes de domínio

Conforme já foi referido, a única solução eficaz para combater os conteúdos ilegais é removê-los da Internet. Se um utilizador ou uma organização detetar conteúdos ilegais num *site*, um dos primeiros passos a dar é contactar o titular do nome de domínio, que pode remover ou adaptar os conteúdos.

O *registry* recolhe dados porque precisa de identificar quem é o titular do nome de domínio (o seu cliente) e de contactar o mesmo em caso de litígio, problemas técnicos, alteração dos Termos e Condições, pagamentos em falta, etc. Os Termos e Condições dos *registries* normalmente exigem expressamente que o titular do nome de domínio forneça dados e elementos para contacto válidos no momento do registo e que mantenha essas informações atualizadas. Fornecer dados falsos ou incorretos constitui uma violação dos Termos e Condições e pode levar à eliminação de um nome de domínio.

Os *registries* dedicam muito tempo à manutenção da base de dados. Isto não só melhora a qualidade dos dados de registo WHOIS, mas pode também ter um impacto indiretamente positivo, dado que é pouco provável que pessoas mal intencionadas registem um nome de domínio usando a sua informação pessoal correta. As ações e práticas para manter uma base de dados de elevada qualidade dependem de fatores específicos do *registry*, como a legislação nacional, a dimensão do registry, a quantidade de registos processados etc., e pode consistir em:[19]

- avaliação rigorosa dos dados fornecidos no momento do registo, para excluir elementos obviamente falsos (por exemplo, *registrant*s chamados “Rato Mickey”);
- verificações de formato automático dos dados fornecidos (por exemplo, endereço de *e-mail*, número de telefone);

[19] Estes exemplos baseiam-se num inquérito feito pelo CENTR aos seus membros em 2017.

- verificação da documentação jurídica fornecida pelo *registrant*, nos países onde esse tipo de documentação tem de ser apresentada;
- verificação aleatória dos dados do registo de nomes de domínio já registados (por exemplo, o *registry* seleciona e verifica aleatoriamente um determinado número de domínios por dia, por mês ou por ano);
- verificação dos dados em caso de queixa;
- verificação dos dados fornecidos por confronto com bases de dados oficiais (por exemplo, código postal válido, número de telefone existente, número de sociedade/pessoa coletiva ou número de identificação nacional, se essa informação for exigida no momento do registo).

Deve notar-se que muitos *registries* de ccTLD não têm nenhum contacto direto com o *registrant* de um nome de domínio. Nesse caso, todos os contactos, incluindo o fornecimento e a atualização dos dados, processam-se através do *registrar*.

> **Exemplos de esforços dos *registries* para obterem e manterem dados do registo corretos:**
>
> A Norid (.no) exige que todos os titulares de domínios estejam registados no Registo Central de Coordenação de Entidades Jurídicas ou no Registo Nacional Norueguês. A entidade gestora do .no verifica regularmente se os titulares dos domínios ainda existem, de acordo com o Registo Central de Coordenação de Entidades Jurídicas. Os domínios detidos por entidades jurídicas que deixaram de existir são automaticamente selecionados para remoção.
>
> A DK Hostmaster (.dk) exige que os *registrants* dinamarqueses se identifiquem através do NemID, uma solução de *login* usada por bancos, *sites* governamentais e outras empresas privadas dinamarquesas. Os *registrants* estrangeiros são sujeitos a uma avaliação de risco, que vai determinar se vão receber um pedido para fornecerem prova da sua identidade antes do registo - risco alto - ou num prazo de 30 dias após o registo - risco baixo (os clientes considerados sem risco não têm de fornecer prova). Se o titular do nome de domínio não puder ou não fornecer prova da sua identidade, o nome de domínio é apagado.
>
> A SIDN (.nl) considera as lojas *online* falsas prejudiciais para a reputação do .nl, enquanto domínio de topo forte e seguro. Por isso, está a trabalhar em sistemas de deteção precoce de domínios usados para lojas *online* falsas e a analisar comunicações de vítimas de burla e informações recebidas do Gabinete Nacional para Comunicação de Fraudes na Internet. Se os dados do registo dos nomes de domínio envolvidos forem falsos, o registry pode desativá-los.

Alguns *registries* colocaram em prática procedimentos especiais para comunicar ou reclamar dados de registo falsos:

- Nominet (.uk) - Reclamação de dados WHOIS incorretos
- AFNIC (.fr) –Pedido de verificação das informações do *registrant*
- DNSBelgium (.be) - Revogar/Revogar+

Partilhar dados do *registry* com terceiros

Os *registries* têm de respeitar a regulamentação nacional em matéria de reserva da intimidade da vida privada quando partilham informações sobre titulares de domínios com terceiros. A política e o procedimento para obter as informações para contacto podem ser encontradas no respetivo *site*. As práticas diferem de acordo com o *registry*, alguns *registries* exigem que as informações sejam pedidas manualmente através de um formulário *online*, outros fornecem acesso (limitado depois do RGPD) à sua base de dados (através do protocolo WHOIS) e outros, ainda, criaram uma ferramenta que permite enviar uma mensagem diretamente ao *registrant*.

> **Exemplos**
>
> AFNIC (.fr) Pedido de divulgação de dados pessoais
>
> AFNIC (.fr) Pesquisar o contacto administrativo de um nome de domínio
>
> DomReg.lt (.lt) Contactar o *registrant* do domínio

Responder à identificação de conteúdos suspeitos

Alguns *registries* criaram procedimentos para responder à sinalização de conteúdos suspeitos, bloqueando ou suspendendo nomes de domínio em certos casos. Estes procedimentos normalmente têm em comum o facto de se aplicarem a casos limitados e bem definidos e de uma entidade externa especializada na avaliação desse tipo de conteúdos estar envolvida.

Este tipo de procedimentos pode ser útil quando uma decisão judicial para remover um nome de domínio demore um tempo considerável. Um dos riscos é que as pessoas que procedem à sinalização não se apercebam do impacto limitado da medida tomada pelo *registry* e deixem de prosseguir outras medidas para remover os conteúdos da Internet.

> **Exemplos**
>
> A SIDN (.nl) definiu um procedimento voluntário de identificação e eliminação baseado no código de conduta de Sinalização e Eliminação nacional holandês. O Procedimento de identificação e eliminação só pode ser invocado se a pessoa que o aciona puder provar que tomou as medidas suficientes para abordar o fornecedor de conteúdos, o gestor do *site*, o *registrant* e o *registrar* do nome de domínio, pelo motivo óbvio de que está dentro do âmbito dos mesmos agir conformemente. Só em casos inquestionavelmente ilegais é que a SIDN pode decidir (temporariamente) remover os servidores de nomes de um domínio.
>
> Switch (.ch) - o artigo 15.º da Portaria sobre Domínios Internet prevê um fundamento jurídico para bloquear nomes de domínio no caso de “suspeitas fundadas de que o nome de domínio em causa está a ser usado para 1) aceder a dados críticos por meios ilegais; ou 2) distribuir *software* mal intencionado”; e se um pedido de bloqueio for apresentado por um serviço de combate ao crime cibernético reconhecido pelo regulador suíço. Ver aqui

Finlândia (.fi) - o artigo 172.º da Lei sobre Serviços de Comunicações Eletrónicas dá à TRAFICOM o direito de tomar as medidas necessárias para detetar, impedir, investigar e remeter para investigação judicial violações significativas de segurança da informação direcionadas a redes ou serviços de comunicações públicos que usem nomes de domínio com o código .fi ou aos seus titulares. As medidas necessárias podem ser ações direcionadas ao servidor de dados do nome de raiz do .fi e podem incluir o seguinte: 1) impedir e restringir tráfego para o nome de domínio; 2) reencaminhar o tráfego para o nome de domínio para o endereço de outro nome de domínio; e 3) outras medidas técnicas comparáveis na aceção dos números 1 e 2.

A EURid (.eu) anunciou recentemente uma colaboração com a Coligação Internacional Anti-Contrafação (*International Anti-Counterfeiting Coalitio*n, IACC) para ajudar a limpar a base de dados de registo do espaço de nomes de domínio sob .eu e .ею, de nomes de domínio fraudulentos e criar um espaço de domínio mais seguro para os utilizadores da Internet.

Conclusão

Os conteúdos abusivos e ilegais minam a confiança na Internet. Os quadros jurídicos nacionais definem que conteúdos são ilegais e quem tem poderes para lidar com os mesmos dentro da lei. Estes aspetos podem variar de um país para outro.

Remover conteúdos ilegais da Internet é a única solução eficaz que evita o acesso aos mesmos. O editor de conteúdos e o fornecedor de alojamento têm acesso direto aos conteúdos ou ao dispositivo que os guarda. Os *registries* de ccTLD não têm acesso a conteúdos nem alojam ou transferem conteúdos através da sua infraestrutura.

Os *registries* de ccTLD estão empenhados em contribuir para uma abordagem abrangente e eficaz aos conteúdos ilegais *online* e vão desenvolver políticas e iniciativas, por exemplo:

- consciencializar e educar as suas comunidades sobre os perigos da Internet;
- facilitar a colaboração com forças policiais e autoridades;
- fornecer dados do registo sobre nomes de domínio suspeitos;
- ou responder à identificação de nomes de domínio utilizados para possibilitar o acesso a conteúdos suspeitos, no quadro da jurisdição nacional.

As políticas e práticas de sucesso ilustradas no documento podem inspirar outros ccTLDs. No entanto, devido às raízes e particularidades nacionais, não há garantias de que replicar uma medida ou uma política leve ao mesmo resultado positivo ou, de facto, considerado lícito para outro ccTLD.

O CENTR é a associação de *registries* europeus de domínios de topo correspondentes a países (ccTLD), tais como .de para a Alemanha ou .si para a Eslovénia. O CENTR tem atualmente 55 membros de pleno direito e 9 membros associados – em conjunto, são responsáveis por mais de 80% de todos os nomes de domínio registados em todo o mundo. Os objetivos do CENTR são promover e participar no desenvolvimento de padrões elevados e de melhores práticas entre *registries* de ccTLD.

Classifique este Documento do CENTR

(Obrigada pelo seu contributo!)

CENTR vzw/asbl
Belliardstraat 20 (6.º andar) 1040 Bruxelas, Bélgica
Tel: +32 2 627 5550
Fax: +32 2 627 5559
secretariat@centr.org
www.centr.org

Para se manter a par das atividades e dos relatórios do CENTR, siga-nos no Twitter, no Facebook ou no LinkedIn