

Projeto de Lei n.º 706/XIV

Contributo da Google para a discussão do Projeto de Lei n.º 706/XIV, que delimita as circunstâncias em que deve ser removido ou impossibilitado o acesso em ambiente digital a conteúdos protegidos, bem como os procedimentos e meios para alcançar tal resultado

A Google agradece a oportunidade de apresentar observações ao Projeto de Lei n.º 706/XIV.

Esta iniciativa legislativa está em linha com os Memorandos de Entendimento para defesa dos direitos de autor e direitos conexos já existentes e em vigor, conferindo-lhes força de lei. Porém, ao contrário dos Memorandos de Entendimento – que produzem efeitos *inter partes* –, um ato legislativo relativo a este tema terá inevitavelmente um impacto mais amplo e pode, por conseguinte, ter consequências inadvertidas para entidades terceiras, que não os signatários dos Memorandos.

As presentes observações prendem-se com dois tipos de consequências: as de natureza jurídica (1.) e as de ordem técnica (2.). Com o intuito de contribuir para a minimização das consequências negativas que exploramos de seguida, propomos também alterações à letra do atual projeto de lei (3.).

1. Consequências jurídicas

1.1. Os tipos de "intermediários" abrangidos pelo projeto de lei são excessivamente amplos, gerando riscos significativos de regulação excessiva e sobreinclusiva, e repercussões negativas para a liberdade de expressão, acesso à informação e outros direitos fundamentais

- a.** Os intermediários sujeitos à aplicação do projeto de lei que ora se discute são definidos por referência ao Decreto-Lei n.º 7/2004, que os define como prestadores intermediários que prestam serviços técnicos para o acesso, disponibilização e utilização de informação ou serviços em linha independentes da geração da própria informação ou serviço. O artigo 5.º do projeto de lei, relativo aos deveres dos prestadores intermediários de serviços em rede, faz ainda referência a “serviços de simples transporte”, “instrumentos de busca” ou qualquer outro serviço que preveja a associação de conteúdos em rede, bem como “serviços de armazenagem a título principal, intermediária ou outro”.
- b.** Esta ampla definição engloba todos os tipos de serviços na Internet, até mesmo um serviço de DNS público¹. Ao contrário das remoções efetuadas por um prestador de serviços de armazenagem, as quais podem visar um ou mais conteúdos específicos, as remoções por DNS só podem ser efetuadas a nível do domínio. Esta funcionalidade

¹ O DNS público consiste num serviço que traduz nomes de domínio em endereços IP numéricos que indicam onde esses domínios podem ser encontrados na Internet. Um servidor DNS indica a um dispositivo o endereço do servidor de que está à procura, da mesma forma que é possível encontrar um número de telefone numa lista telefónica. O dispositivo, por sua vez, utiliza este endereço para se conectar a um website, utilizar uma aplicação ou enviar um email. O DNS depende de dois tipos de servidores para possibilitar estas pesquisas: servidores de referência (*authoritative servers*), que armazenam a entrada DNS principal para um domínio que indica onde este pode ser encontrado na Internet, e resolvedores recursivos (*recursive resolvers*), que pesquisam endereços a partir de servidores de referência. Os resolvedores recursivos também procedem ao armazenamento temporário (*caching*) – um processo em que são armazenadas as entradas DNS para websites populares, resultando numa resolução mais rápida. O DNS público do Google é uma rede de resolvedores recursivos. Os utilizadores contam com os serviços DNS enquanto ferramenta de navegação para os fazer chegar a websites na Internet, selecionando prestadores com base numa variedade de fatores, tais como velocidade, fiabilidade, ou controlos opcionais disponibilizados pelo prestador.

suscita sérias preocupações relacionadas com bloqueios excessivos, assim como consequências negativas para a liberdade de expressão, uma vez que todo um domínio poderá ficar inacessível devido ao conteúdo de *uma única* página ou subdomínio. Em 2011, por exemplo, o bloqueio DNS de um único domínio mooo.com levou a que mais de 84.000 subdomínios se tornassem inacessíveis através do DNS, muitos dos quais não alojavam qualquer conteúdo ilícito².

- c. Em virtude do escopo alargado da noção de “intermediários” do projeto de lei, não é claro se os titulares de direitos têm primeiro de requerer providências contra os fornecedores de acesso à Internet antes de se dirigirem a outros intermediários, ou se podem à partida requerer a mais ampla providência (i.e., requerendo-a contra todos os tipos de intermediários). A primeira opção seria evidentemente preferível – caso contrário, uma providência poderia ser decretada contra intermediários que são meramente secundários ou mesmo irrelevantes relativamente a uma alegada ou potencial violação. Em qualquer caso, tal possibilidade poderia ter um efeito inibidor das atividades dos intermediários em Portugal, afigurando-se também como atentatória da liberdade de empresa – uma liberdade fundamental consagrada na Carta dos Direitos Fundamentais da UE (artigo 16.º).
- d. O projeto de lei em apreço deve ser dirigido apenas a prestadores intermediários de serviços de simples transporte que prestem serviços de acesso à Internet, uma vez que são estes, afinal, os destinatários dos mecanismos de autorregulação em que o projeto de lei assumidamente se baseia.

1.2. A lei proposta arrisca-se a entrar em conflito com a Diretiva relativa aos direitos de autor e direitos conexos no mercado único digital (“Diretiva MUD”) e com a futura Lei dos Serviços Digitais (“Digital Services Act” ou “DSA”).

Qualquer nova obrigação imposta às plataformas online, incluindo os prestadores de serviços de armazenagem, entra inevitavelmente em conflito com a iminente transposição da Diretiva MUD e com o futuro *Digital Services Act*. Como é sabido, os Estados-Membros não podem interferir com os processos de transposição das diretivas da UE. Qualquer ação legislativa estritamente nacional arriscar-se-ia, no momento atual, a violar o princípio da cooperação leal enquanto princípio constitucional da União.

- a. No que concerne à Diretiva MUD, o artigo 17.º institui um regime de responsabilidade para os prestadores de serviços de partilha de conteúdos em linha (OCSSP), com certas salvaguardas (ligadas à noção de “melhores esforços”). O artigo 17.º impõe também a criação de mecanismos de reclamação e recurso nas próprias plataformas, para lidar com casos de litígio acerca da remoção e/ou bloqueio do acesso a conteúdos ilícitos. Devido à amplitude dos “intermediários” abrangidos pelo regime previsto no Projeto de Lei n.º 706/XIV, os OCSSP acabariam também por ser afetados pelo mesmo. Contudo, as especificidades do regime de responsabilidade e do mecanismo de reclamação e recurso da Diretiva MUD não são compatíveis com o Projeto de Lei n.º 706/XIV, que estabelece um regime fundamentalmente diferente – sobretudo porque contempla a intervenção de uma entidade terceira (a IGAC) no processo de remoção. Existem, no entanto, muitos outros exemplos de incompatibilidade entre ambos os regimes: por exemplo, o Projeto de Lei n.º 706/XIV prevê um prazo fixo (48 horas) para remover ou bloquear o acesso ao conteúdo, enquanto que o compromisso atingido a nível europeu foi no sentido de se utilizar o conceito de “diligência”, exatamente por ser mais flexível e suscetível de se adaptar a diferentes cenários, capacidades tecnológicas e agentes.

² Cf. <https://cdt.org/insights/an-object-lesson-in-overblocking/>.

- b. Em relação ao Digital Services Act, o regime de procedimentos de notificação e retirada (*notice and takedown*) funciona com base na localização do conteúdo a ser removido, em particular os URLs. O Projeto de Lei n.º 706/XIV iria muito além disso, podendo assim acarretar problemas no futuro, dado que os Estados-Membros não estão autorizados a aplicar regras nacionais mais rigorosas até que a Comissão assim o confirme. O não cumprimento desta obrigação tem como consequência que as regras nacionais em questão se considerem inoponíveis (cf. Processos C-41/93 e C-194/94 do TJUE).

2. Consequências técnicas

2.1. Falta de eficiência e consequências não pretendidas do bloqueio de websites

O bloqueio de websites não é a forma mais eficaz de combater a pirataria. Os piratas podem facilmente escapar a estes bloqueios, alterando domínios e endereços IP. É importante notar que o bloqueio de websites comporta um elevado risco de bloqueio de conteúdos lícitos que estejam armazenados no mesmo nome de domínio ou endereço IP que o conteúdo ilícito³.

2.2. Falta de eficiência e consequências não pretendidas de impedir o acesso ao DNS

O DNS é um alvo ineficaz para o bloqueio/filtragem de conteúdos, devido às muitas alternativas disponíveis. A maioria dos utilizadores da web recorre ao resolvidor DNS padrão disponibilizado pelo seu fornecedor de acesso à Internet. Na maioria dos casos, serviços de DNS alternativos não são a opção padrão para os utilizadores, o que significa que aqueles que o utilizam fazem-no por opção. Estes utilizadores estão geralmente conscientes da multiplicidade de serviços DNS disponíveis e aptos a fazer alterações ao seu serviço DNS com base na qualidade e natureza dos serviços prestados (optando, por exemplo, por um serviço mais rápido ou mais fiável, ou com filtragem opcional). Estes utilizadores têm um leque de alternativas à sua escolha. Para além dos serviços disponibilizados a nível local pelos fornecedores de acesso à Internet, várias empresas tecnológicas globais competem no âmbito do fornecimento dos seus próprios serviços DNS, nomeadamente a Microsoft Azure, a Oracle, a Cisco, a Cloudflare e muitas outras.

As propostas de remoção/bloqueio do DNS não “removem” efetivamente o conteúdo: o conteúdo permanece alojado no servidor anfitrião (“*host server*”) e a menção do nome de domínio permanece registada, impedindo-se apenas os resolvidores recursivos de responder a consultas de nomes de domínio bloqueados. Uma vez que o conteúdo continua a existir e permanece acessível – quer através de outro serviço DNS, quer através da introdução direta de um endereço IP anfitrião –, a remoção/bloqueio do DNS não constitui uma via eficaz para efetuar verdadeiras remoções de conteúdo. Utilizadores determinados e tecnologicamente proficientes conseguirão facilmente encontrar outra via para aceder ao website pretendido.

É por esta razão que o Comité Consultivo para a Segurança e Estabilidade da ICANN afirmou que “devido à arquitetura da Internet, o bloqueio por nome de domínio pode ser facilmente contornado pelos utilizadores finais e é, portanto, suscetível de ser largamente ineficaz a longo prazo e repleto de repercussões imprevistas a curto prazo”. Os riscos técnicos de curto prazo citados incluem a procura de vias alternativas pelos utilizadores, diagnósticos incorretos de bloqueios pelas equipas de segurança e IT, bloqueios excessivos, e potenciais conflitos com as Extensões de Segurança do DNS⁴.

³ Veja-se o seguinte exemplo: <https://www.techdirt.com/articles/20170221/07045336754/cogent-accidentally-blocks-websites-global-ham-fisted-piracy-filtering-effort.shtml>.

⁴ <https://www.icann.org/en/system/files/files/sac-056-en.pdf>.

2.3. O alargamento do âmbito de aplicação da lei de modo a incluir eventos em direto depara-se com impossibilidades técnicas

Se o projeto de lei for modificado de modo a abranger também o bloqueio de eventos transmitidos em direto, não poderão ser ignoradas as falhas subjacentes às soluções técnicas necessárias a atingir tal resultado. É muitas vezes impossível para um intermediário bloquear apenas o *stream* ou *streams* de um evento em direto. Dependendo do tipo de intermediário e das suas capacidades instaladas, a exigência de que seja bloqueado um *stream* pode resultar num bloqueio sobreinclusivo (*overblocking*) extremo, ou mesmo em obstáculos à capacidade de operar de modo seguro em Portugal. As alterações necessárias à infraestrutura e aos mecanismos de funcionamento dos intermediários implicariam, em alguns casos, mudanças fundamentais na forma como estes intermediários operam. E, entretanto, os piratas terão encontrado outra forma de fazer chegar às suas audiências o conteúdo pirateado - os piratas são sobejamente conhecidos por mudar para novos *streams*, novos endereços de IP, novos nomes de domínio ou até novos intermediários a meio de eventos.

3. Alterações propostas

Artigo 1.º Objeto	Artigo 1.º Objeto	Comentários
<p>1. (...)</p> <p>2. A presente lei estabelece, ainda, o procedimento administrativo a adotar em caso de disponibilização ilícita de conteúdos protegidos pelo direito de autor e pelos direitos conexos, incluindo as obrigações dos prestadores intermediários de serviços em rede previstos no n.º 5 do artigo 4.º do Decreto-Lei n.º 7/2004, de 7 de janeiro, na sua redação atual, no âmbito desse procedimento.</p>	<p>1. (...)</p> <p>2. A presente lei estabelece, ainda, o procedimento administrativo a adotar em caso de disponibilização ilícita de conteúdos protegidos pelo direito de autor e pelos direitos conexos, incluindo as obrigações dos prestadores intermediários de serviços de simples transporte previstos no n.º 1 do artigo 14.º do Decreto-Lei n.º 7/2004, de 7 de janeiro, na sua redação atual, no âmbito desse procedimento.</p>	<p>A lei é inspirada pelos Memorandos de Entendimento antipirataria e estes aplicam-se apenas aos fornecedores de acesso à Internet.</p> <p>É certo que nos Memorandos se utiliza o conceito geral de "prestadores intermediários de serviços em rede", mas, na prática, os únicos alvos dos pedidos de bloqueio/remoção têm sido operadores de telecomunicações que fornecem acesso à Internet.</p>
<p>Artigo 3.º Poderes específicos de fiscalização e controlo</p> <p>1. (...)</p> <p>2. Para efeitos da presente lei, considera-se que disponibiliza ilicitamente conteúdos protegidos pelo direito de autor e pelos direitos conexos, quem:</p>	<p>Artigo 3.º Poderes específicos de fiscalização e controlo</p> <p>1. (...)</p> <p>2. Para efeitos da presente lei, considera-se que disponibiliza ilicitamente conteúdos protegidos pelo direito de autor e pelos direitos conexos, quem:</p>	

<p>a) Por qualquer forma comunique, coloque à disposição do público ou armazene conteúdos protegidos, sem autorização dos respetivos titulares do direito de autor e dos direitos conexos;</p> <p>b) Disponibilize serviços ou meios destinados a serem utilizados por terceiros para a violação do direito de autor e dos direitos conexos ou que se destinem a interferir com o normal e regular funcionamento do mercado de obras e prestações;</p> <p>c) Disponibilize serviços que visem neutralizar medidas eficazes de carácter tecnológico para a proteção do direito de autor e dos direitos conexos ou dispositivos de informação para a gestão eletrónica de direitos.</p> <p>3. (...)</p> <p>4. (...)</p> <p>5. (...)</p> <p style="text-align: center;">Artigo 5.º Deveres dos prestadores intermediários de serviços em rede</p> <p>1. Sem prejuízo do cumprimento dos demais deveres legais e regulamentares relativos ao exercício da sua atividade, os prestadores intermediários de serviços em rede estão obrigados, no prazo máximo de 48 horas, a contar da respetiva</p>	<p>a) Por qualquer forma comunique, coloque à disposição do público ou armazene conteúdos protegidos, sem autorização dos respetivos titulares do direito de autor e dos direitos conexos;</p> <p>b) Disponibilize serviços ou meios destinados a serem utilizados por terceiros para a violação do direito de autor e dos direitos conexos ou que se destinem a interferir com o normal e regular funcionamento do mercado de obras e prestações;</p> <p>b) Disponibilize principalmente serviços que têm como único ou principal objetivo visem neutralizar medidas eficazes de carácter tecnológico para a proteção do direito de autor e dos direitos conexos ou dispositivos de informação para a gestão eletrónica de direitos.</p> <p>3. (...)</p> <p>4. (...)</p> <p>5. (...)</p> <p style="text-align: center;">Artigo 5.º Deveres dos prestadores intermediários de serviços em rede</p> <p>1. Sem prejuízo do cumprimento dos demais deveres legais e regulamentares relativos ao exercício da sua atividade, os prestadores intermediários de serviços de simples transporte estão obrigados, dentro de um período de tempo razoável, a</p>	
--	--	--

<p>notificação, a cumprir as determinações do inspetor-geral das atividades culturais, no sentido de remover ou impossibilitar o acesso, a disponibilização e a utilização de conteúdo protegido pelo direito de autor e pelos direitos conexos.</p> <p>2. Para efeitos do disposto no número anterior, os prestadores intermediários de serviços em rede estão obrigados:</p> <p>a) A cumprir as determinações da IGAC para remover ou impossibilitar o acesso a obras ou conteúdos protegidos, designadamente, através do impedimento de acesso a determinado ou determinados URLs ou DNS associado ou de acesso a conteúdos disponibilizados por determinado ou determinados IPs, quando se trate de prestadores intermediários de serviços de simples transporte, e prestem o serviço de acesso à Internet;</p> <p>b) A cumprir as determinações da IGAC para remover ou impossibilitar o acesso ao conteúdo protegido, designadamente, através do impedimento de acesso a determinado ou determinados URLs ou DNS associado ou de acesso a conteúdos disponibilizados por determinado ou determinados IPs, quando prestem o serviço de associação de conteúdos em rede,</p>	<p>contar da respetiva notificação, a cumprir as determinações do inspetor-geral das atividades culturais, no sentido de remover ou impossibilitar o acesso, a disponibilização e a utilização de conteúdo protegido pelo direito de autor e pelos direitos conexos.</p> <p>2. Para efeitos do disposto no número anterior, os prestadores intermediários de serviços de simples transporte que prestem o serviço de acesso à Internet estão obrigados a cumprir as determinações da IGAC para remover ou impossibilitar o acesso a obras ou conteúdos protegidos, designadamente, através do impedimento de acesso a determinado ou determinados URLs ou DNS ou de acesso a conteúdos disponibilizados por determinado ou determinados IPs.</p> <p>3.1.1.— A cumprir as determinações da IGAC para remover ou impossibilitar o acesso a obras ou conteúdos protegidos, designadamente, através do impedimento de acesso a determinado ou determinados URLs ou DNS associado ou de acesso a conteúdos disponibilizados por determinado ou determinados IPs, quando se trate de prestadores intermediários de serviços de simples transporte, e prestem o serviço de acesso à Internet;</p> <p>3.1.2.— A cumprir as determinações da IGAC para remover ou impossibilitar o acesso ao conteúdo protegido, designadamente,</p>	
--	--	--

<p>por meio de instrumentos de busca, hiperligações ou processos análogos;</p> <p>c) A cumprir as determinações da IGAC para remover ou impossibilitar o acesso ao conteúdo protegido, designadamente, através do impedimento de acesso a determinado ou determinados URLs ou de acesso a conteúdos disponibilizados por determinado ou determinados IPs, quando prestem serviços de armazenagem a título principal, intermediária ou outro e o conteúdo protegido se encontre armazenado nos seus servidores.</p> <p>3. (...)</p> <p>4. (...)</p> <p>5. Nos casos previstos na alínea a) do n.º 4 do artigo 3.º, os prestadores intermediários de serviços devem adotar as medidas referidas no número anterior, no mais curto prazo possível, após a notificação da determinação da IGAC.</p>	<p>através do impedimento de acesso a determinado ou determinados URLs ou de acesso a conteúdos disponibilizados por determinado ou determinados IPs, quando prestem o serviço de associação de conteúdos em rede, por meio de instrumentos de busca, hiperligações ou processos análogos;</p> <p>e) — A cumprir as determinações da IGAC para remover ou impossibilitar o acesso ao conteúdo protegido, designadamente, através do impedimento de acesso a determinado ou determinados URLs ou de acesso a conteúdos disponibilizados por determinado ou determinados IPs, quando prestem serviços de armazenagem a título principal, intermediária ou outro e o conteúdo protegido se encontre armazenado nos seus servidores.</p> <p>3. (...)</p> <p>4. (...)</p> <p>5. Nos casos previstos na alínea a) do n.º 4 do artigo 3.º, os prestadores intermediários de serviços de simples transporte devem adotar as medidas referidas no número anterior, no mais curto prazo possível, após a notificação da determinação da IGAC.</p>	
---	---	--

<p>6. Incumbe ainda aos prestadores de serviços em rede:</p> <p>a) Sempre que exista ilicitude manifesta, informar a IGAC, de imediato, quando tiverem conhecimento de atividades ilícitas, que se desenvolvam por via dos serviços que prestam;</p> <p>b) Satisfazer os pedidos de identificação dos destinatários dos serviços com quem tenham acordos de armazenagem.</p> <p>7. Nenhuma responsabilidade recai sobre o prestador intermediário de serviços pelas medidas adotadas em cumprimento de uma determinação da IGAC.</p>	<p>6. Incumbe ainda aos prestadores intermediários de serviços de simples transporte:</p> <p>a) Sempre que exista ilicitude manifesta, informar a IGAC, de imediato, quando tiverem conhecimento de atividades ilícitas, que se desenvolvam por via dos serviços que prestam;</p> <p>b) Satisfazer os pedidos legítimos de identificação dos destinatários dos serviços com quem tenham acordos de armazenagem.</p> <p>7. Nenhuma responsabilidade recai sobre o prestador intermediário de serviços de simples transporte pelas medidas adotadas em cumprimento de uma determinação da IGAC.</p>	
--	---	--