

Bloqueios de Aplicações

Considerações sobre o PLS 169/2017

Carlos Affonso Souza

@caffsouza



Seção V

**Da Suspensão do Funcionamento ou do Bloqueio de Acesso
a Aplicações de Internet**

Art. 23-A. O Juiz poderá determinar a suspensão do funcionamento de aplicação de internet hospedada no Brasil ou o bloqueio do acesso de aplicação de internet hospedada no exterior que incentive ou promova a prática de crime.

§ 1º A ordem de suspensão de funcionamento ou o bloqueio de acesso deverá ter o alcance e a duração necessários para a cessação da atividade criminosa.

§ 2º É vedada a suspensão do funcionamento de aplicação de internet destinada ao envio e recebimento de mensagens instantâneas, sendo possível apenas o bloqueio de terminais específicos de acesso.

§ 3º Se a aplicação de internet se destinar precipuamente à prática de crime, poderá ser determinada a interrupção de seu funcionamento, caso esteja hospedada no Brasil, ou o bloqueio definitivo de seu acesso, se estiver hospedada no exterior. ”

JUSTIFICAÇÃO

Recentemente foi divulgado pela mídia o caso do jogo chamado “baleia azul”, supostamente surgido na Rússia, em que crianças e adolescentes, por meio de redes sociais, são incentivados a cumprirem desafios macabros. No total, são 50 desafios, iniciando por alguns considerados mais “simples” – como automutilação para desenhar baleias no corpo, assistir filmes de terror ou ficar doente – até o desafio final, no qual é proposto o suicídio.

Jogos como esse têm se espalhado pela *internet*. Segundo especialistas, o mundo *online* em que as crianças e adolescentes estão inseridos, onde é crescente o número de instrumentos eletrônicos como celulares e *tablets*, pode estar contribuindo para esse cenário. Nesse ambiente, os jovens se sentem pressionados pelas redes sociais a seguir certo estilo de vida, como uma necessidade de reafirmação e de inserção entre outros jovens.

Se o objetivo é bloquear aplicações nas quais ocorram crimes, o projeto vai bloquear as principais redes sociais, sites de vídeos e aplicações do País.

É importante diferenciar o ato ilícito cometido pelo usuário da plataforma da ilicitude da plataforma em si.

O Marco Civil da Internet possui regime de responsabilidade e remoção de conteúdo que vem sendo aplicado pelos tribunais, com destaque para o Superior Tribunal de Justiça.

MCI :: Art. 19. Com o intuito de assegurar a **liberdade de expressão** e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

Art. 19. (...) § 2º A aplicação do disposto neste artigo para infrações a **direitos de autor** ou a direitos conexos depende de previsão legal específica, que deverá respeitar a **liberdade de expressão** e demais garantias previstas no art. 5º da Constituição Federal.

Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo **cenas de nudez ou de atos sexuais de caráter privado** quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

STJ, 3º T., REsp 1.642.997 - RJ, Rel. Min. Nancy Andri ghi, julg. 12.09.17, publ. 15.09.2017.

“a regra a ser utilizada para a resolução de uma dada controvérsia deve levar em consideração o momento de ocorrência do ato ou, em outras palavras, quando foram publicados os conteúdos infringentes. Para fatos ocorridos antes da entrada em vigor do Marco Civil da Internet, deve ser obedecida a jurisprudência desta corte. No entanto, após a entrada em vigor da Lei 12.965/2014, o termo inicial da responsabilidade da responsabilidade solidária do provedor de aplicação, por força do art. 19 do Marco Civil da Internet, é o momento da notificação judicial que ordena a retirada de determinado conteúdo da internet.”

O debate nacional sobre bloqueios está pendente de decisão no STF.

Projeto de Lei no Senado (PLS200/2016) vai em sentido diametralmente contrário.

PLS 200/2016

Autoria Sen. José Medeiros

Parecer pela aprovação (CCT) Sen. Aloysio Nunes

"Seção V

Da intervenção no provimento de conexão à internet

Art. 23-A. Não será cabível medida administrativa ou judicial contra pessoa responsável pela provisão de conexão à internet, bem como pela transmissão, comutação ou roteamento, que tenha por objeto interferir, dificultar, suspender ou interromper o acesso de usuários a aplicações da internet ou seu funcionamento."(NR)

Debate internacional: várias formas de bloqueio são questionadas por especialistas (DNS, IP)

Na Europa, diferentes condições para o bloqueio demandam uniformização. Resistências à decisão do Tribunal de Justiça Europeu.

Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill

May 2011

Authors:

Steve Crocker, Shinkuro, Inc.
David Dagon, Georgia Tech
Dan Kaminsky, DKH
Danny McPherson, Verisign, Inc.
Paul Vixie, Internet Systems Consortium

*Affiliations provided for identification only
Brief biographies of authors available below*

- The U.S. Government and private industry have identified Internet security and stability as a key part of a wider cyber security strategy, and if implemented, the DNS related provisions of PROTECT IP would weaken this important commitment.
- DNS filters would be evaded easily, and would likely prove ineffective at reducing online infringement. Further, widespread circumvention would threaten the security and stability of the global DNS.
- The DNS provisions would undermine the universality of domain names, which has been one of the key enablers of the innovation, economic growth, and improvements in communications and information access unleashed by the global Internet.
- Migration away from ISP-provided DNS servers would harm efforts that rely on DNS data to detect and mitigate security threats and improve network performance.
- Dependencies within the DNS would pose significant risk of collateral damage, with filtering of one domain potentially affecting users' ability to reach non-infringing Internet content.
- The site redirection envisioned in Section 3(d)(II)(A)(ii) is inconsistent with security extensions to the DNS that are known as DNSSEC. The U.S. Government and private industry have identified DNSSEC as a key part of a wider cyber security strategy, and many private, military, and governmental networks have invested in DNSSEC technologies.
- If implemented, this section of the PROTECT IP Act would weaken this important effort to improve Internet security. It would enshrine and institutionalize the very network manipulation that DNSSEC must fight in order to prevent cyberattacks and other malevolent behavior on the global Internet, thereby exposing networks and users to increased security and privacy risks.



An internet service provider may be ordered to block its customers' access to a copyright-infringing website

Such an injunction and its enforcement must, however, ensure a fair balance between the fundamental rights concerned

Constantin Film Verleih, a German company which holds, inter alia, the rights to the films 'Vicky the Viking'¹ and 'Pandorum', and Wega Filmproduktionsgesellschaft, an Austrian company which holds the rights to the film 'The White Ribbon'², became aware that their films could be viewed or even downloaded from the website 'kino.to'³ without their consent. At the request of those two companies, the Austrian courts prohibited UPC Telekabel Wien, an internet service provider ('ISP') established in Austria, from providing its customers with access to that site. UPC Telekabel considers that such an injunction cannot be addressed to it, because, at the material time, it did not have any business relationship with the operators of kino.to and it was never established that its own customers acted unlawfully. UPC Telekabel also claims that the various blocking measures which may be introduced could, in any event, be technically circumvented. Finally, some of those measures are excessively costly.

Hearing the case at last instance, the Oberster Gerichtshof (Supreme Court, Austria) asked the Court of Justice to interpret the EU Copyright Directive⁴ and the fundamental rights recognised by EU law. The directive provides for the possibility for rightsholders to apply for an injunction against intermediaries whose services are used by a third party to infringe their rights⁵. UPC Telekabel submits that it cannot be considered to be an intermediary in that sense.



Institut suisse de droit comparé
Schweizerisches Institut für Rechtsvergleichung
Istituto svizzero di diritto comparato
Swiss Institute of Comparative Law

COMPARATIVE STUDY

ON

BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT

Após uma decisão do Tribunal de Justiça Europeu que, em 2014, permitiu o bloqueio de sites como forma de lutar contra as violações dos direitos autorais, "houve grandes objeções a este desenvolvimento introduzido pelo TJCE; especialmente os tribunais alemães inferiores se recusaram a seguir a liderança do TJCE devido à limitada eficácia das medidas de bloqueio, que podem representar um problema no nível dos direitos humanos, em termos de proporcionalidade e transferência de poder judicial para provedores".



JUDICIARY OF
ENGLAND AND WALES

Current UK practice on website-blocking injunctions
and the need for further harmonisation

Online Platforms and Intermediaries in Copyright Law
Ludwig Maximilian University of Munich

24 March 2017

(Mr Justice) Richard Arnold

In order for an injunction to be granted it must be (i) necessary, (ii) effective, (iii) dissuasive, (iv) not unduly costly or complicated, (v) avoid barriers to legitimate trade, (vi) fair and equitable and strike a fair balance between the fundamental rights engaged, (vii) proportionate and (viii) safeguarded against abuse. Of these factors, proportionality is the key one, since consideration of the other factors feeds into the proportionality analysis.

4. The need for a more harmonised legal framework

- If greater consistency is to be achieved, a more harmonised legal framework is required.
- A first step would be a more harmonised legislative basis for injunctions against intermediaries whose services are used to infringe IPRs, such as specifying more clearly who is an intermediary, the threshold conditions to be satisfied and the essential procedural requirements (e.g. bringing a claim against the infringer or not).
- A second step would be a more harmonised basis for the underlying claims for infringement. Since most claims to date concern copyright infringement, this would mainly relate to the copyright *acquis* and in particular communication to the public.



"Site Blocking" to reduce online copyright infringement

A review of sections 17 and 18 of the Digital Economy Act

"Das técnicas que consideramos mais efetivas, apenas o bloqueio baseado na Inspeção profunda de pacotes (DPI) parece oferecer um nível de granularidade em que o bloqueio não seria uma grande preocupação. O uso do DPI não é, no entanto, sem risco, pois levanta questões de privacidade e é extremamente complicado de implementar com base em tecnologias atuais. O bloqueio de DNS talvez ofereça uma opção mais simples e menos dispendiosa, mas é provável que seja totalmente efetivo somente até DNSSEC ser implementado, portanto, talvez não seja uma solução de longo prazo. O bloqueio do endereço IP simplesmente não é suficientemente granular e a facilidade com a qual pode ser contornada sugeriria que não é um candidato técnico adequado. O bloqueio de URL é atualmente usado, mas seu alcance limitado e facilidade de evasão sugerem que, na melhor das hipóteses, é um papel complementar ao lado do bloqueio de DNS ".

Bloqueio no Brasil tira WhatsApp do ar na Argentina e Chile

Decisão da Justiça de São Paulo afetou usuários de outros países da América Latina

São Paulo – O bloqueio do **WhatsApp** no Brasil está afetando também outros países. Veículos de imprensa da América do Sul relatam que usuários de países vizinhos, principalmente Argentina e Chile, estão sem acesso ao **aplicativo** de mensagens.

O **Diario Financiero**, do Chile, explica que isso acontece por conta de uma empresa que presta serviços a operadoras, a Level 3. Ela usa cabos submarinos e terrestres para levar a conexão até o Chile.

A Level 3 é responsável pela conexão internacional para operadoras chilenas como Entel, GTD e VTR. A solução foi recorrer a outras prestadoras de serviço que não apresentavam problemas.

Usuários da Argentina e Uruguai também foram afetados. Alguns sites relatam reclamações por parte de diversos usuários desses países. As causas, aqui, são as mesmas relacionadas à interrupção do serviço no Chile.

É importante distinguir entre o ilícito cometido pelo usuário da plataforma e a ilicitude da plataforma em si.

Para os casos de ilícitos cometidos por usuários, o Marco Civil já dispõe de mecanismos para responsabilização e remoção de conteúdos.

O debate sobre bloqueio de aplicações se encontra pendente de decisão no STF. Projetos contraditórios no Senado.

Juízes podem determinar o bloqueio de sites, como medida extrema, se valendo do poder de cautela, que deve ser proporcional.

Debate internacional revela visões distintas (mesmo dentro da Europa).

www.itsrio.org

www.facebook.com/ITSriodejaneiro

CAFF@ITSRIO.ORG

