

Contribuições à CPICIBER

Pedro N. Mizukami

Centro de Tecnologia e Sociedade

FGV Direito Rio

Introdução



Latest Unease on Right:
Ryan Is Too Far Left



Ben Carson Finds
Momentum in Provocative
Remarks



CNN Sees Smaller Field,
With Greater Focus, as
Lure for Democratic
Debate

In Choreographed Campaigns,
Candidates Stumble Over Choice of
Music

POLITICS

Obama Won't Seek Access to Encrypted User Data

By NICOLE PERLROTH and DAVID E. SANGER OCT. 10, 2015

✉️ Email

📘 Share

🐦 Tweet

📁 Save

➦ More

CUPERTINO, Calif. — The Obama administration has backed down in its bitter dispute with Silicon Valley over the encryption of data on iPhones and other digital devices, concluding that it is not possible to give American law enforcement and intelligence agencies access to that information without also creating an opening that China, Russia, cybercriminals and terrorists could exploit.

With its decision, which angered the [F.B.I.](#) and other law enforcement agencies, the administration essentially agreed with [Apple](#), [Google](#), [Microsoft](#) and a group of the nation's top cryptographers and computer scientists that millions of Americans would be vulnerable to hacking if technology firms and smartphone manufacturers [were required](#) to provide the government with “back doors,” or access to their source code and encryption keys.



President Obama hosted a state dinner at the White House for President Xi Jinping of China in September. Timothy D. Cook, the chief executive of Apple, sat at the head table with Mr. Obama and Mr. Xi. Zach Gibson/The New York Times

Publicidade

Luxemburgo

Justiça europeia invalida acordo UE-EUA sobre transferência de dados



06/10/2015 - 06h33min

Compartilhar



O Tribunal de Justiça da União Europeia invalidou nesta terça-feira o acordo entre a UE e os Estados Unidos para a transferência de dados pessoais, pelas revelações de espionagem em massa das agências americanas, uma decisão que afeta empresas como o Facebook.

"O Tribunal de Justiça declara inválido o acordo estabelecido entre Bruxelas e Washington, conhecido como 'Safe harbour'", anunciou a corte ao pronunciar-se sobre uma ação do austríaco Max Schrems.

Em sua denúncia, Schrems solicitava às autoridades irlandesas que suspendessem a transferência de seus dados pessoais aos Estados Unidos por parte do Facebook, empresa que tem sede na Irlanda para suas atividades europeias.

Publicidade

ZH RECOMENDA

Receba em seu e-mail nossa **newsletter** semanal com conteúdo selecionado por editores de ZH.

Seu e-mail

Enviar >

Siga ZH nas redes sociais



Publicidade

O MELHOR DA ZH

Um cenário de diversidade e complexidade:

- Contexto internacional e transjurisdicional;
- Compreensão e domínio de problemas bastante técnicos;
- Múltiplas interfaces com outros ramos do direito, com atividades econômicas, sociais, e com discussões em andamento;
 - Privacidade;
 - Liberdade de expressão;
 - Inovação.
- Dificuldade em se atingir o meio termo/equilíbrio entre os diversos interesses e direitos em jogo;
- Pluralidade de temas.

Pluralidade de temas:

- Crimes digitais em espécie e bens jurídicos tutelados (honra, patrimônio, liberdade sexual, dentre outros);
- Proteção a dados pessoais;
- Criptografia e seus usos;
- Anonimato e navegação anônima;
- Retenção de dados;
- Bloqueio de sites e neutralidade de rede;
- Cooperação internacional.

Processos em andamento:

- Regulamentação do Marco Civil da Internet;
- Debate público sobre o Anteprojeto de Lei para Proteção de Dados Pessoais;
- Continuidade do processo de modernização da Lei de Direitos Autorais;
- Outros projetos de lei em discussão no momento:
 - PL 215/2015 (crimes contra a honra);
 - PL 2390/2015 (Cadastro Nacional de Acesso à Internet);
 - PL 3237/2015 (altera definição de “administrador de sistema autônomo”);
 - PL 1879/2015 (guarda de dados adicionais para provedores de aplicações);
 - PLS 180/2015 (altera dispositivos do Marco Civil da Internet);
 - PL 4060/2012 e PLS 181/2014 (proteção a dados pessoais).

Dois temas:

1. Retenção de dados;
2. Bloqueio de sites em razão de violações a direitos autorais.

1. Retenção de dados

Contexto:

- Marco Civil da Internet;
 - Guarda de registros de conexão (1 ano – art. 13, *caput*) e de acesso a aplicações de internet (6 meses – art. 15, *caput*), acesso mediante ordem judicial;
 - Guarda cautelar por períodos maiores (art. 13, § 2º e 15, § 2º);
 - Dados cadastrais (art. 10, § 3º)
- Debates em andamento no âmbito do PL 215/2015;
 - Acesso sem ordem judicial (não prosperou na CCJC);
 - Ampliação das obrigações de coleta de dados (cadastrais) – *“Art. 10, § 3º – O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação, endereço completo, telefone, CPF, conta de e-mail, na forma da lei, pelas autoridades que detenham competência legal para sua requisição, cabendo aos provedores, obrigatoriamente, a adoção de providências de coleta, obtenção, organização e disponibilização dos referidos dados cadastrais de modo a atender o aqui disposto, se e quando por elas requisitados.”*

[Acervo](#)[Análises](#)[Opinião](#)[Eventos](#)[News](#)[Cadastre-se](#)[Anuncie](#)[Downloads](#)[Quem Somos](#)

+ OUTROS DESTAQUES

PRIVACIDADE

CGI edita resolução criticando a aprovação do PL Espião

sexta-feira, 09 de outubro de 2015 , 18h49

INFRAESTRUTURA

Embratel instala infraestrutura de telecom para Olimpíada

sexta-feira, 09 de outubro de 2015 , 18h48

INTERNET DAS COISAS

Soluções de automação residencial da Insteon serão lançadas no Brasil

sexta-feira, 09 de outubro de 2015 , 18h42

TRIBUTAÇÃO

Banda larga cresce 31% em agosto, mas alta do ICMS pode comprometer futuro

sexta-feira, 09 de outubro de 2015 , 18h13

INFRAESTRUTURA

PRIVACIDADE

União Europeia invalida diretiva de retenção de dados

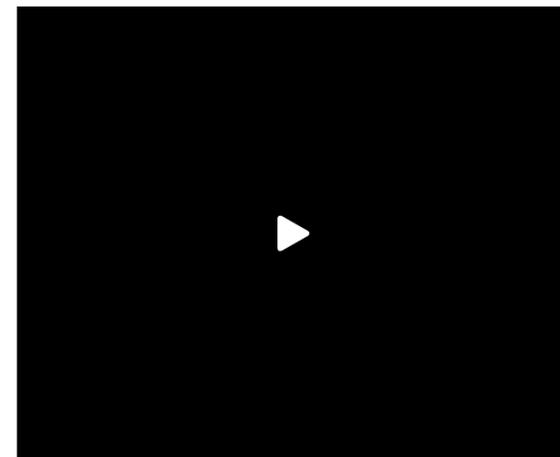
terça-feira, 08 de abril de 2014 , 15h13 | POR REDAÇÃO

O Tribunal de Justiça Europeu decidiu nesta terça, 8, invalidar a Diretiva de Retenção de Dados de 2006, que obrigava operadoras de telecomunicações de países da União Europeia a armazenar dados por seis meses (com prazo máximo de até dois anos). A entidade julgou o pedido da High Court (Tribunal Supremo da Irlanda) e o Verfassungsgesichtshof (Tribunal Constitucional da Áustria), que argumentaram que a diretiva feria os direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais.

Isso porque o Tribunal europeu constatou que essa guarda de dados permitia brechas jurídicas de segurança e privacidade, como saber "com que pessoa e através de que meio um assinante ou um usuário registrado se comunicou". Além disso, a brecha permitiria determinar o tempo dessa chamada o local onde ela foi feita, bem como conhecer a frequência das comunicações entre usuários por um determinado período. "Estes dados, considerados no seu todo, são suscetíveis de fornecer indicações muito precisas sobre a vida privada das pessoas cujos dados são conservados, como os hábitos da vida cotidiana, locais de residência permanentes ou temporários, as deslocamentos diários, atividades exercidas, relações sociais e meios sociais frequentados", declarou a entidade em comunicado. "A diretiva imiscui-se de forma especialmente grave nos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais".

O Tribunal considera que a diretiva abrange de forma generalizada todos os indivíduos, meios de comunicação eletrônica e dados de tráfego, não fazendo uma diferenciação para

RECEBA NOSSA
NEWSLETTER
DIARIAMENTE



EVENTOS

Congresso
Latino-Americano
2015
Satélites

O evento dos que decidem. Grandes definições do mercado e novidades



Decisão do Tribunal de Justiça da União Europeia, casos C-293/12 e C-594/12

- Entendeu que o art. 6.º da Diretiva 2006/24 (prazo de retenção de dados deve ser não inferior a 6 meses e não superior a 2 anos) é incompatível com os arts. 7º, 8º, I e 52, I da Carta de Direitos Fundamentais da União Europeia;
- **Art. 7º – respeito pela vida privada e familiar;**
- **Art. 8º, I – proteção a dados pessoais;**
- **Art. 52, I – princípio da proporcionalidade:** “Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efectivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros”.

Decisão do Tribunal de Justiça da União Europeia, casos C-293/12 e C-594/12

- “abrange de maneira geral todas as pessoas, todos os meios de comunicação eletrónica e todos os dados relativos ao tráfego, não sendo efetuada nenhuma diferenciação, limitação ou exceção em função do objetivo de luta contra as infrações grave”
- “não estabelece critérios objetivos que permitam delimitar o acesso das autoridades nacionais competentes aos dados e a sua utilização posterior para prevenir, detetar ou agir penalmente contra infrações suscetíveis de ser consideradas suficientemente graves, à luz da amplitude e da gravidade da ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta”

Decisão do Tribunal de Justiça da União Europeia, casos C-293/12 e C-594/12

- “impõe que os dados sejam conservados por períodos não inferiores a seis meses, não procedendo a uma distinção entre as categorias de dados em função da sua eventual utilidade relativamente ao objetivo prosseguido ou em função das pessoas em causa”
- “não se especifica que a determinação do período de conservação se deve basear em critérios objetivos a fim de garantir que se limita ao estritamente necessário”.



SECTIONS ▾

NEWS

SPECIAL REPORTS

LINKSDOSSIERS

INTERVIEWS

OPINIONS

INFOGRAPHICS

BLOGS

VIDEOS

Search



HOME > DIGITAL > NEWS

Germany toughens up on data retention

📅 19 May 2015 - 07:25 updated: 19 May 2015 - 12:47

EurActiv.com by Catherine Stupp

Languages: Français

Comments



German Minister of Justice Heiko Maas [SPD Schleswig-Holstein /Flickr]

German policymakers have moved to strengthen data retention laws, insisting that information will only be stored in Germany, and for much shorter periods, after the

POPULAR CONTENT



Brussels makes overture on 'data flow' agreement in TTIP



INFOGRAPHIC: How Digital is the EU in 2015?



Brussels tackles territorial copyright in digital strategy



Cyber security directive held up in face of 'Wild West' Internet



French surveillance legislation is off to a bad start



No Digital Europe without a strong Telecom Single Market



Oettinger calls for 'Europeanisation' of digital policy



Princípios Internacionais sobre a Aplicação Dos Direitos Humanos na Vigilância Das Comunicações

VERSÃO FINAL MAIO DE 2014*

Enquanto as tecnologias que facilitam a vigilância estatal das comunicações têm avançado, os Estados não têm cumprido seu dever de assegurar que leis, regulamentos, atividades, poderes e autoridades relacionados à Vigilância das Comunicações cumpram os padrões e leis de direitos humanos internacionais. Este documento tenta esclarecer como a lei internacional dos direitos humanos se aplica no atual ambiente digital, especialmente tendo em conta o aumento e as alterações técnicas e tecnológicas da Vigilância das Comunicações. Estes princípios podem oferecer a grupos da sociedade civil, empresas, Estados e a outros atores um instrumento para avaliar se as leis e práticas atuais ou propostas sobre monitoramento são consistentes ou não com os direitos humanos.

Estes princípios são o resultado de uma consulta global com grupos da sociedade civil, da indústria e especialistas internacionais em questões jurídicas, políticas e tecnológicas relacionadas à Vigilância das Comunicações.

PREÂMBULO

A privacidade é um direito humano fundamental para a manutenção de sociedades abertas e democráticas. É essencial à dignidade humana e reforça outros direitos, tais como a liberdade de expressão e de informação e a liberdade de associação, sendo reconhecida pela lei internacional dos direitos humanos.¹ A Vigilância das Comunicações interfere no direito à privacidade, dentre vários outros direitos humanos. Como resultado, pode ser justificada apenas quando determinada pela lei, necessária para atingir um fim legítimo e proporcional ao fim almejado.²

Antes da adoção pública da internet, princípios jurídicos bem estabelecidos e encargos logísticos inerentes ao monitoramento das comunicações limitavam a Vigilância das Comunicações por parte dos Estados. Nas últimas décadas, porém, essas barreiras logísticas para vigilância diminuíram e a aplicação dos princípios jurídicos em novos contextos tecnológicos tornou-se nebulosa. A explosão de

Princípios Internacionais sobre a Aplicação Dos Direitos Humanos na Vigilância Das Comunicações (Necessary and Proportionate)

- existe uma alta probabilidade de que um crime grave ou ameaça específica a um Fim Específico foi ou será cometido, e;
- existe alta probabilidade de que evidências ou materiais relevantes para tal crime grave ou ameaça específica a um Fim Legítimo seriam obtidos acessando as Informações Protegidas procuradas, e;
- outras técnicas menos invasivas foram esgotadas ou seriam inúteis, de forma que as técnicas utilizadas sejam a opção menos invasiva, e;
- as informações acessadas serão limitadas ao que é relevante e essencial ao crime grave ou ameaça específica ao Fim Legítimo alegado; e

Princípios Internacionais sobre a Aplicação Dos Direitos Humanos na Vigilância Das Comunicações (Necessary and Proportionate)

- quaisquer informações coletadas a mais não serão mantidas, mas, pelo contrário, serão prontamente destruídas ou devolvidas; e
- as informações serão acessadas somente pela autoridade especificada e usadas apenas para a finalidade e pela duração para as quais foi concedida a autorização;
- as atividades de vigilância solicitadas e técnicas propostas não comprometem a essência do direito à privacidade ou as liberdades fundamentais.

2. Bloqueio de sites

Contexto:

- Marco Civil da Internet:
 - Art. 9, § 3º – *“Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo”.*
- Proposta da Motion Picture Association:
 - Exceção ao princípio da neutralidade de rede para o bloqueio técnico de sites que contenham conteúdo em violação de direitos autorais.

Problemas:

- Necessidade e proporcionalidade;
- Danos colaterais a outros direitos;
- Questões de ordem técnica;
- Efetividade da medida.

Relatório Frank La Rue (2011) – *rapporteur* especial para a proteção do direito à liberdade de opinião e expressão

- Preocupação com uso de tecnologias de bloqueio e filtragem pelos Estados, por potenciais danos à liberdade de expressão”;
- Entende que as condições que levam ao bloqueio geralmente não se encontram previstas em lei, ou quando estão, são vagas e amplas a ponto de ensejar bloqueio arbitrário e excessivo;
- Viola o art. 19 (3) do Pacto Internacional sobre os Direitos Civis e Políticos;
- Ainda quando justificadas, as medidas são desnecessárias e desproporcionais em relação aos fins almejados;

ICANN SSAC – Security and Stability Advisory Committee

- Documentos SAC 050 (14 de junho de 2011) e SAC 056 (09 de outubro de 2012);
- “Todas as abordagens técnicas para bloqueio de DNS e, ainda mais, tentativas de contornar o bloqueio, terão impacto na segurança e/ou estabilidade de usuários e aplicações” (SAC 050);
- Bloqueio de acesso a conteúdo via DNS tem sérias implicações técnicas, inclusive relacionadas à segurança e estabilidade da internet. O SSAC recomenda a qualquer governo compreender a fundo os potenciais problemas desse tipo de medida antes de partir para implementação (SAC 056).

ISOC (Internet Society) – “Internet Society Perspectives on Domain Name System (DNS) Filtering”

- “A Internet Society acredita que políticas e regulações que requerem a interrupção da infraestrutura de DNS, seja por filtragem de resultados ou por apreensão de nomes de domínio, têm sérias deficiências”:
 - São facilmente contornáveis;
 - Não resolvem o problema;
 - Incompatíveis com DNSSEC;
 - Causa danos colaterais;
 - Coloca usuários em risco;
 - Encoraja a fragmentação da internet;
 - Incentiva o uso de serviços “underground”;
 - Preocupação quanto a direitos humanos e devido processo legal.



News

[UvA News](#) [Professorial appointments](#) [UvA in the spotlight](#)

[← List](#)

Blocking The Pirate Bay has virtually no effect

28 October 2012

The recent blocking of The Pirate Bay file-sharing website has hardly made a dent in downloading from illegal sources, according to a report co-authored by researchers Joost Poort of the Institute for Information Law (IViR) at the University of Amsterdam (UvA) and Jorna Leenheer of Tilburg University's Centerdata institute.

In their report (titled *Filesharing 2012, Downloaden in Nederland*), the researchers set out findings of a survey conducted among several thousand Dutch residents regarding the downloading and streaming of music, films, TV programmes, games and books. More than three-quarters of all respondents who subscribe to the Dutch ISPs Xs4ALL and Ziggo indicated they never download from illegal sources at all. Of the remaining Ziggo and Xs4ALL subscribers,

"L'Agcom non ferma la pirateria digitale che anzi aumenta". Colpa dell'Effetto Streisand



Uno studio universitario italiano si aggiunge agli altri che hanno messo in discussione l'efficacia della repressione pura nella lotta al copyright. Ecco cosa dice

di ARTURO DI CORINTO

MEDIA PIRACY IN EMERGING ECONOMIES



Edited by Joe Karaganis

<http://piracy.americanassembly.org/the-report/>

Conclusões:

- Necessidade de se avaliar meios mais hábeis para lidar com a questão;
- Filtragem/bloqueio de conteúdo deve ser sopesado com esses outros meios em uma análise de necessidade e proporcionalidade;
- Danos colaterais devem ser levados em consideração tanto em relação à violação a outros direitos (liberdade de expressão, livre iniciativa) quanto em relação a potenciais problemas técnicos;
- Contextualizar a discussão sobre filtragem/bloqueio no âmbito maior dos direitos autorais, especialmente em relação a regimes em discussão como o de notice-and-takedown (EUA) e, preferencialmente, notice-and-notice (Canadá).



■ [Home](#) » [Aprofunde](#) - Debates Públicos

Aprofunde - Debates Públicos

Baixe as contribuições do Centro de Tecnologia e Sociedade da FGV DIREITO RIO para a Consulta Pública do CGI.br sobre o Marco Civil:

-  [Sobre a definição de termos relativos à proteção de dados presentes no Marco Civil](#)
-  [Sobre Neutralidade de Rede](#)
-  [Sobre a proteção aos registros, aos dados pessoais e às comunicações privadas, sobre a guarda de registros de conexão e sobre a Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações](#)

Baixe as contribuições do Centro de Tecnologia e Sociedade da FGV DIREITO RIO para a Consulta Pública do Ministério da Justiça sobre o Marco Civil:

-  [Contribuições do CTS sobre o Marco Civil](#)

Baixe as contribuições do Centro de Tecnologia e Sociedade da FGV DIREITO RIO para a Consulta Pública do Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de Dados Pessoais:

-  [Sobre proteção de dados pessoais](#)

Outras leituras:

-  [Sobre Neutralidade de Rede e o Futuro das Comunicações no Brasil](#)
-  [Nota técnica dos pesquisadores do CTS, InternetLab e GPOPAI sobre o PL 215/2015](#)



Exceto onde indicado em contrário, todos os conteúdos desta página estão licenciados com uma Licença Creative Commons - Atribuição-Compartilhável 4.0 Internacional.

<http://direitorio.fgv.br/cts/marcocivil-dadospessoais/aprofunde>

pedro.mizukami@fgv.br