

CRIPTOGRAFIA, HACKING E BLOQUEIOS DE APLICATIVOS À LUZ DE DIREITOS HUMANOS

Entrevista com Amie Stepanovich

ENCRYPTION, HACKING AND APP BLOCKING FROM A HUMAN RIGHTS PERSPECTIVE

Interview with Amie Stepanovich

Também disponível em / also available at

www.internetlab.org.br

São Paulo, Maio de 2017

INTERNETLAB
pesquisa em direito e tecnologia

CRIPTOGRAFIA, HACKING E BLOQUEIOS DE APLICATIVOS À LUZ DE DIREITOS HUMANOS

ENCRYPTION, HACKING AND APP BLOCKING FROM A HUMAN RIGHTS PERSPECTIVE

Entrevistada

Interviewee

Amie Stepanovich

Entrevistadores

Interviewers

Dennys Antonialli

Beatriz Kira



Este trabalho está licenciado sob uma licença Creative Commons CC BY 3.0 BR. Essa licença permite que outros remixem, adaptem e criem obras derivadas sobre a obra original, inclusive para fins comerciais, contanto que atribuam crédito ao autor corretamente.

Texto da licença:

<https://creativecommons.org/licenses/by/3.0/br/legalcode>

This work is licensed under a Creative Commons CC BY 3.0 BR license.

EQUIPE INSTITUCIONAL | INSTITUTIONAL TEAM:

Diretor/Director: Dennys Antonialli; *Diretor/Director:* Francisco Brito Cruz; *Diretora/Director:* Mariana Giorgetti Valente

EQUIPE DO PROJETO | PROJECT TEAM:

Coordenadoras de pesquisa /Research Leaders: Beatriz Kira e Jacqueline de Souza Abreu

Estagiária de pesquisa/Research Interns: Paula Pécora de Barros e Ana Luiza Araujo

ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA, 2017.

INTERNETLAB / Avenida Ipiranga, 344, Edifício Itália, Conjunto 11 B / www.internetlab.org.br

0.	INTRODUÇÃO	9
	<i>INTRODUCTION</i>	
1.	O QUE É CRIPTOGRAFIA E POR QUE ELA EXISTE?	12
	<i>WHAT IS ENCRYPTION AND WHAT ARE ITS PURPOSES?</i>	
2.	É POSSÍVEL CONTORNAR OU QUEBRAR A CRIPTOGRAFIA?	16
	<i>IS IT POSSIBLE TO CIRCUMVENT ENCRYPTION?</i>	
3.	COMO SABER SE A CRIPTOGRAFIA É REALMENTE FORTE?	20
	<i>HOW TO ENSURE ENCRYPTION IS TRULY STRONG?</i>	
4.	COMO DEVE SER O ACESSO DE AUTORIDADES A METADADOS?	24
	<i>IN WHICH CIRCUMSTANCES LAW ENFORCEMENT COULD HAVE ACCESS TO METADATA?</i>	
5.	E QUANDO O ESTADO VIRA “HACKER”?	27
	<i>WHAT ABOUT HACKING BY GOVERNMENTS?</i>	
6.	REFORMA DOS ACORDOS DE COOPERAÇÃO JUDICIÁRIA INTERNACIONAL (MLATS)	32
	<i>MUTUAL LEGAL ASSISTANCE TREATIES (MLATS) REFORM</i>	
7.	O FUTURO DO DEBATE NO BRASIL E POSSÍVEIS DESDOBRAMENTOS NA AMÉRICA LATINA	36
	<i>THE FUTURE OF THE DEBATE IN BRAZIL AND POSSIBLE IMPACTS IN LATIN AMERICA</i>	

ENTREVISTADA INTERVIEWEE

Amie Stepanovich

Amie Stepanovich trabalha para garantir que as leis e políticas de vigilância e cibersegurança reconheçam e respeitem os direitos humanos. Na organização *Access Now*, Amie é responsável pela área de políticas públicas em tecnologia dos Estados Unidos e lidera projetos globais na interseção de direitos humanos e vigilância do Estado. Amie atuou como Diretora do Projeto de Vigilância Doméstica na *Electronic Privacy Information Center*, onde participou de audiências públicas tanto no Senado como na Câmara dos Deputados, bem como em assembleias legislativas estaduais. Amie é membro do conselho consultivo da Internet Education Foundation e foi nomeada Embaixadora da Privacidade pelo *Privacy Commissioner* de Ontário, Canadá. Em 2014, foi reconhecida pela revista *Forbes* como uma das 30 líderes com menos de 30 anos na área de Direito e Políticas Públicas. Amie obteve seu J.D. na New York Law School, e seu B.S. na Universidade Estadual da Flórida.

Amie Stepanovich works to ensure that laws and policies on surveillance and cybersecurity recognize and respect human rights. At Access Now, Amie manages and develops the organization's U.S. policy and leads global projects at the intersection of human rights and government surveillance. Previously, Amie was the Director of the Domestic Surveillance Project at the Electronic Privacy Information Center, where she testified in hearings in both the Senate and the House of Representatives, as well as in State legislatures. Amie is a board member of the Internet Education Foundation. Amie was named as a Privacy Ambassador by the Information and Privacy Commissioner of Ontario, Canada and was recognized in 2014 as one of Forbes magazine's 30 under 30 leaders in Law and Policy. She has a J.D. from New York Law School, and a B.S. from the Florida State University.

ENTREVISTADORES

INTERVIEWERS

Dennys Antonialli

Doutorando em direito constitucional pela Universidade de São Paulo, com graduação em direito pela mesma universidade (2008), mestrado em direito pela Universidade de Stanford (JSM, 2011) e mestrado profissional em “Law and Business”, conjuntamente oferecido pela Bucerius Law School e pela WHU Otto Beisheim School of Management (MLB, 2010). Atuou junto à equipe de políticas públicas em tecnologia e direitos civis na American Civil Liberties Union of Northern California (ACLU/NC) e como consultor jurídico do “Timor Leste Legal Education Project”, da Stanford Law School/Asia Foundation. Foi ganhador do 1º lugar do Steven M. Block Civil Liberties Award da Stanford Law School (2011) e do 1º lugar do Prêmio Marco Civil da Internet e Desenvolvimento da Escola de Direito da Fundação Getúlio Vargas (SP). Foi pesquisador do Alexander von Humboldt Institute for Internet and Society (Berlim), participou do Summer Doctoral Program do Oxford Internet Institute e foi Visiting Scholar na Stanford Law School. Fundador do Núcleo de Direito, Internet e Sociedade da FDUSP (NDIS) e diretor presidente do InternetLab.

PhD candidate in Constitutional Law at the University of São Paulo (Brazil), where he also earned his bachelor of laws degree (LL.B., 2008). He holds a “Master of the Science of Law” degree from Stanford Law School (J.S.M., 2011) and a “Master of Law and Business” from Bucerius Law School/WHU Otto Beisheim School of Management in Germany (MLB, 2010). Dennys has worked in the technology and civil liberties team of the Policy Department of the American Civil Liberties Union of Northern California (ACLU/NC) and acted as a legal consultant for the “Timor-Leste Legal Education Project” (Stanford Law School/Asia Foundation). He has been awarded the first place prize of the “2011 Steven M. Block Civil Liberties award” for best written work on civil liberties at Stanford Law School and won the first place prize of the “Brazil’s Internet Framework Bill & Development Award” (Google/FGV-SP). In 2013, he was a research fellow at the Alexander von Humboldt Institute for Internet and Society (Berlin). In July 2014, Dennys attended the Summer Doctoral Program at the Oxford Internet Institute. In 2016, was a visiting scholar at the Stanford Law School. Founder of the “Law, Internet and Society Nucleus” of the University of São Paulo (NDIS-USP), he is currently executive director of the InternetLab.

Beatriz Kira

Mestranda em direito econômico pela Universidade de São Paulo, com graduação em direito pela mesma universidade. Em 2013, realizou intercâmbio acadêmico na Ludwig-Maximilians-Universität München, período em que foi bolsista do Departamento de Intercâmbio Acadêmico da Alemanha (DAAD). Em 2015, participou do programa de intercâmbio da Secretaria de Assuntos Legislativos (SAL) do Ministério da Justiça e da Secretaria para Assuntos Jurídicos (SAJ) da Casa Civil. Em 2016, participou do Annenberg-Oxford Media Policy Summer Institute, realizado na Universidade de Oxford. Foi bolsista do Programa de Educação Tutorial (PET) – Sociologia Jurídica, do Ministério da Educação, e trabalhou como assistente de pesquisa da Rede de Pesquisa Empírica em Direito. Atualmente, é integrante do Grupo Direito e Políticas Públicas da Faculdade de Direito da Universidade de São Paulo e líder da área de conjuntura do InternetLab, onde também integrou a pesquisa “Economia do compartilhamento e seus desafios regulatórios”.

Master of Laws student at the University of São Paulo, where she also earned her Bachelor of Laws degree (LL.B., 2015). In 2013, Beatriz was an exchange student at the Ludwig-Maximilians-Universität München (LMU), on a scholarship from the German Academic Exchange Service (DAAD). In 2015, she participated in a training course in drawing up legislation and public policy development organized by the Brazilian Ministry of Justice. In 2016 she attended the Annenberg-Oxford Media Policy Summer Institute, held at the University of Oxford. She is a former scholarship holder from Programa de Educação Tutorial

(PET), of the Brazilian Ministry of Education, and worked as junior researcher with the Brazilian Network of Empirical Legal Studies. Currently, Beatriz is a researcher fellow with the Law and Public Policy Research Group at the University of São Paulo and coordinator of the Policy Watch area of InternetLab, where she was also part of the project “Sharing economy and its regulatory challenges”.

EQUIPE ENVOLVIDA NO PROJETO **PROJECT TEAM**

Francisco Carvalho de Brito Cruz

Mestre e doutorando em Filosofia e Teoria Geral do Direito na Faculdade de Direito da Universidade de São Paulo (FDUSP). Graduado em Direito pela Faculdade de Direito da Universidade de São Paulo (FDUSP) e, durante o curso, bolsista do Programa de Educação Tutorial (PET) – Sociologia Jurídica. Foi pesquisador visitante (2013) no Center for Study of Law and Society da Universidade da Califórnia – Berkeley, por meio de programa de intercâmbio da Rede de Pesquisa Empírica em Direito (REED). Foi ganhador do 1º lugar do Prêmio Marco Civil da Internet e Desenvolvimento da Escola de Direito da Fundação Getúlio Vargas (SP). É advogado com atuação nas áreas de direito digital, propriedade intelectual, imprensa e direito do consumidor. Fundador e coordenador do Núcleo de Direito, Internet e Sociedade (NDIS FDUSP). Atualmente é diretor do InternetLab.

Master and PhD candidate in Philosophy and Jurisprudence by the School of Law of Universidade de São Paulo (FDUSP). Graduated in Law by School of Law of Universidade de São Paulo (FDUSP) and, in the course of that program, received a scholarship from Programa de Educação Tutorial (PET) –Sociology of Law. Visiting Researcher (2013) at the Center for Study of Law and Society of the University of California – Berkeley, through Rede de Pesquisa Empírica em Direito (REED) exchange program. Mr. Brito Cruz received the Marco Civil da Internet e Desenvolvimento Award of the School of Law of Fundação Getúlio Vargas (SP). Attorney-at-law, practices in areas such as CyberLaw, Intellectual Property, Consumer Law and Press. He was founder and coordinator of FDUSP Group of Law, Internet and Society (NDIS) between 2012 and 2014 and is currently a director of InternetLab.

Jacqueline de Souza Abreu

Doutoranda em Direito na Universidade de São Paulo (USP). Mestre em direito pela University of California, Berkeley (EUA), com foco em direito e tecnologia, e pela Ludwig-Maximilians-Universität München (Alemanha), com foco em direitos fundamentais. Graduada em direito pela USP. Durante a graduação, foi bolsista de iniciação científica da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) e do Programa de Estímulo ao Ensino de Graduação (PEEG) nas áreas de Filosofia e Teoria Geral do Direito e membro do Núcleo de Direito, Internet e Sociedade da USP. Realizou intercâmbio acadêmico de graduação também na LMU, período em que foi bolsista do Serviço Alemão de Intercâmbio Acadêmico (DAAD). Foi pesquisadora-júnior na FGV DIREITO SP e assistente de pesquisa visitante do Berkman Klein Center for Internet and Society da Harvard University. Atualmente é líder do projeto “Vigilância e Privacidade”; no InternetLab, centro independente de pesquisa em direito e tecnologia.

PhD student in Law at the University of São Paulo (USP). Master of Laws from the University of California, Berkeley, School of Law, with a Certificate of Specialization in Law and Technology, and Master of Laws from the Ludwig-Maximilians University of Munich, with focus in Fundamental Rights. Holds a Bachelor’s Degree in Law from USP (LL.B., 2014). Former scholarship holder from Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) and Programa de Estímulo ao Ensino de

Graduação (PEEG) and member of USP's Law, Internet and Society Group. Participated in an academic exchange program with LMU, on a scholarship from the German Academic Exchange Service (DAAD). Worked as junior researcher at FGV DIREITO SP and as summer intern at the Berkman Klein Center for Internet and Society at Harvard University. Currently, Jacqueline leads the project "Privacy and Surveillance" at InternetLab, a law and technology research center.

Paula Pécora de Barros

Graduanda em Direito na Universidade de São Paulo (USP), onde participa do programa de duplo-diploma em Direito pela Université de Lyon. Foi bolsista de Iniciação Científica pelo Programa Unificado de Bolsas da USP (2015-2016) e faz parte do Serviço de Assessoria Jurídica Universitária – SAJU (2014-2016), vinculada à FDUSP, e da ONG TETO (2016). Participa do Grupo de Estudos Avançados de Escolas Penais do Instituto Brasileiro de Ciências Criminais (IBCCRIM). Realizou intercâmbio acadêmico para pesquisa na Universidade do Porto (2016). Atualmente é estagiária de pesquisa no InternetLab.

Bachelor student of laws at the University of São Paulo (USP), where she attends courses of the double degree program in Law offered by the Université de Lyon. She was a recipient of a research scholarship by the Unified Program of Scholarships by USP (2015-2016) and she also participates in the Service of Juridical Aid – SAJU (2014-2016) from USP and the ONG TETO (2016). She is a member of the Group of Advanced Studies on Penal Schools at the Brazilian Institute for Criminal Sciences – IBCCRIM. She was a research exchange student at the University of Porto (July/2016). Currently, she is a research intern at InternetLab.

Ana Luiza Araujo

Graduanda em Letras na Faculdade de Filosofia, Letras e Ciências Humanas da Universidade de São Paulo (FFLCH/USP), com habilitação em Inglês. Passou pelos cursos de Ciências Sociais e Jornalismo e atualmente é a estagiária responsável pelas traduções do InternetLab.

Ana is a Bachelor student of Languages with emphasis in English at the Faculty of Philosophy, Languages and Literature, and Human Sciences of the University of São Paulo (FFLCH/USP). She also passed through the courses of Journalism and Social Sciences and currently is the intern responsible for InternetLab's translations.

0. INTRODUÇÃO

0. *INTRODUCTION*

Por Jacqueline de Souza Abreu

Amie Stepanovich, diretora de políticas públicas dos Estados Unidos na ONG dedicada a direitos digitais *Access Now*, esteve no Brasil em março para uma conferência na Faculdade de Direito da Universidade de São Paulo, e o InternetLab, como já fez com outros três especialistas, aproveitou sua visita para entrevistá-la.¹

Especialista na área de vigilância e privacidade, levamos à Amie diversas questões que foram provocadas ou avançadas pelos três casos de bloqueios do WhatsApp no Brasil. Em todos os casos, os bloqueios foram determinados como medida de constrangimento para que a empresa Facebook Brasil cooperasse com a Justiça brasileira entregando dados de comunicações de usuários do WhatsApp, aplicativo de mensagens imensamente popular no Brasil, do qual a empresa Facebook Inc. é proprietária.² À base da disputa estão questões complexas como os limites da jurisdição brasileira sobre uma empresa sediada no exterior, os obstáculos colocados pela criptografia de ponta-a-ponta ao acesso a informações de usuários,³ a legalidade dos bloqueios perante o Marco Civil da Internet,⁴ e a constitucionalidade dos bloqueios diante do direito à liberdade de comunicação.⁵

Todas essas questões, e outras delas decorrentes, são abordadas pela Amie nesta entrevista. A pesquisadora e ativista explica as complexidades da criptografia e defende sua importância para a segurança no ambiente digital, sem deixar de levar em consideração que nenhuma tecnologia é perfeita e que falhas podem se esconder por trás de códigos fechados. Sobre a crescente dificuldade alegada por autoridades de segurança pública no acesso a dados de usuários no âmbito de investigações, Amie esclarece como isso tem ampliado atuações controversas e perigosas para direitos humanos, em que o próprio Estado atua como hacker. Ao lado disso, chama atenção para como reformas em mecanismos de cooperação internacional para acesso a dados podem ajudar a resgatar tais autoridades do sentimento de frustração e ceticismo em que se encontram, e que alimentam pressões contra criptografia e levam a ameaças de bloqueios.

Nesse sentido, essa entrevista com a Amie aborda temas que estão na ordem do dia das pautas de Direito e Justiça no cenário brasileiro e internacional.

¹ InternetLab entrevista Julia Powles, disponível em http://www.internetlab.org.br/wp-content/uploads/2017/01/ENTREVISTA_JULIA_POWLES_v04.pdf. InternetLab entrevista Hans-Jörg Albrecht, disponível em http://www.internetlab.org.br/wp-content/uploads/2016/06/Entrevista_ProfHans_final.pdf. InternetLab entrevista Barbara Van Schewick, disponível em <http://www.internetlab.org.br/wp-content/uploads/2015/12/bvs-entrevista.pdf>.

² Ver bloqueios.info.

³ Ver ABREU, Jacqueline de Souza, “From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp”, *Columbia Journal of Transnational Law Online Edition*, 17 de outubro de 2016, disponível em <http://jtl.columbia.edu/from-jurisdictional-battles-to-crypto-wars-brazilian-courts-v-whatsapp/>.

⁴ Ver ABREU, Jacqueline de Souza, “Bloqueios do WhatsApp têm base legal? As disputas interpretativas e seus defensores”, in: bloqueios.info, InternetLab, 06 de março de 2017, disponível em <http://bloqueios.info/pt/bloqueios-do-whatsapp-tem-base-legal-as-disputas-interpretativas-e-seus-defensores/>; MANSUR, Felipe, “ADI 5527 e bloqueios: um problema na redação da lei ou na sua interpretação?”, in: bloqueios.info, InternetLab, 18 de novembro de 2016, disponível em <http://bloqueios.info/pt/adi-5527-e-bloqueios-um-problema-na-redacao-da-lei-ou-na-sua-interpretacao/>

⁵ Ver BARROS, Paula Pécora, “ADPF 403 no STF: Bloqueios do WhatsApp são constitucionais?” in: bloqueios.info, InternetLab, 18.11.2016, disponível em: <http://bloqueios.info/pt/adpf-403-no-stf-bloqueios-do-whatsapp-sao-constitucionais/>.

By Jacqueline de Souza Abreu

Amie Stepanovich, U.S. Policy Manager at *Access Now*, a non-profit organization dedicated to digital rights, was in Brazil in March for a conference at the University of São Paulo, School of Law, and InternetLab, took the opportunity to interview her, similarly to what it has done before with three other experts.⁶

Amie, an expert in privacy and surveillance law and policy, addressed several issues that were provoked or advanced by the three WhatsApp blocking cases in Brazil. In all cases, the blockages were determined to constrain Facebook Brasil's cooperation with Brazilian courts, handing over communications data from WhatsApp users, an immensely popular messaging application in Brazil, which Facebook Inc. owns.⁷ At the root of the dispute are complex issues such as the limits of Brazilian jurisdiction over a company based abroad, the obstacles imposed by end-to-end encryption for accessing user information,⁸ the legality of blocking orders before the Marco Civil da Internet (*Brazilian Internet Civil Rights Framework*),⁹ and the compatibility of these decisions with the constitutional right to freedom of communication.¹⁰

These and other related issues are addressed by Amie in this interview. The researcher and activist explains the complexities of encryption and defends its importance for security in the digital environment, while taking into account that no technology is perfect and that failures can hide behind closed source software. Regarding the growing difficulty alleged by law enforcement authorities in accessing user data during the course of investigations, Amie clarifies how this raised actions that are not only controversial per se, but also dangerous to human rights, such as when governments engage in hacking. She also draws attention to how reform can help alleviate the sense of frustration and skepticism around MLATs,¹¹ which now fuel the pressure against encryption and lead to threats of blockages.

In this sense, this interview with Amie addresses topics that are on the Law and Justice agenda in the Brazilian and the international scenarios.

⁶ InternetLab interviews Julia Powles, available at http://www.internetlab.org.br/wp-content/uploads/2017/01/ENTREVISTA_JULIA_POWLES_v04.pdf. InternetLab interviews Han-Jörg Albrecht, available at http://www.internetlab.org.br/wp-content/uploads/2016/06/Entrevista_ProfHans_final.pdf. InternetLab interviews Barbara Van Schewick, available at <http://www.internetlab.org.br/wp-content/uploads/2015/12/bvs-entrevista.pdf>.

⁷ See <http://appblocking.info/>.

⁸ See ABREU, Jacqueline de Souza, "From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp", *Columbia Journal of Transnational Law Online Edition*, 17 October 2016, available at <http://jtl.columbia.edu/from-jurisdictional-battles-to-crypto-wars-brazilian-courts-v-whatsapp/>.

⁹ See Abreu, Jacqueline de Souza. "Is there legal support for WhatsApp blocks? Interpretative disputes and their advocates", in: bloqueios.info, InternetLab, March 7th 2017, available at <http://bloqueios.info/en/is-there-legal-support-for-whatsapp-blocks-interpretative-disputes-and-their-advocates/>; Mansur, Felipe. "ADI 5527 and appblocks: a problem in the wording of the law or in its interpretation?", in: bloqueios.info, InternetLab, November 18 2016, available at <http://bloqueios.info/en/adi-5527-and-appblocks-a-problem-in-the-wording-of-the-law-or-in-its-interpretation/>.

¹⁰ See Barros, Paula Pécora de. "ADPF 403 in STF: Are WhatsApp blockings constitutional?", in: bloqueios.info, InternetLab, November 18 2016, available at <http://bloqueios.info/en/adpf-403-in-stf-are-whatsapp-blockings-constitutional/>.

¹¹ Mutual Legal Assistance Treaties.



**1. O QUE É CRIPTOGRAFIA E
POR QUE ELA EXISTE?**

***1. WHAT IS ENCRYPTION AND
WHAT ARE ITS PURPOSES?***

InternetLab: Eu gostaria de começar essa conversa falando sobre criptografia. Como eu acredito que você esteja acompanhando, esse tópico está bastante quente no Brasil atualmente. Recentemente, algumas decisões judiciais determinaram a suspensão do aplicativo WhatsApp, utilizado por milhões de brasileiros e brasileiras, em todo o país. A questão envolvia o acesso a dados de usuários, incluindo o conteúdo das comunicações e, em alguns casos, possibilidades de interceptação de futuras comunicações feitas pelo aplicativo. Autoridades brasileiras têm argumentado que a criptografia pode ser um obstáculo para a investigação de crimes graves. Como a criptografia funciona e por que é importante para usuários, especialmente a criptografia de ponta-a-ponta?

Amie Stepanovich: A criptografia está de fato no coração da segurança no mundo digital. À medida que as pessoas cada vez mais movem suas informações online, a criptografia oferece muitas das proteções às quais nós estamos acostumados no mundo analógico, real. Coisas como manter documentos privados, ter a certeza de que pessoas que você não quer que vejam as suas comunicações não estão abrindo as suas cartas, por exemplo (o equivalente sendo os seus e-mails). A criptografia é aquela proteção a qual nos referimos quando falamos sobre espaço digital.

Então é muito importante fornecer incentivos para as companhias desenvolverem e implementarem uma criptografia realmente forte, porque o problema é que há muitas vulnerabilidades em produtos e serviços digitais, e quando as pessoas usam esses serviços, elas têm inseguranças naturais inerentes a elas. Eu ainda hei de ver algum produto que seja 100% seguro. Por isso é importante falar com as empresas e realmente fazê-las perceber as vantagens de se usar a criptografia, e o fato de que é bom para seus usuários.

A criptografia também está intrinsecamente conectada aos direitos humanos. Os usuários só

InternetLab: I want to start this conversation talking about encryption. As I am sure you have been following, this is a very hot topic in Brazil right now. We have had a few court orders demanding the suspension of WhatsApp, used by millions of Brazilians, in the entire country. The issue there was access to users' data, including the content of communications and even, in some cases, possibly a way of intercepting future communications in the app. Law enforcement has been claiming that encryption may be an obstacle to investigations of serious crimes. I wanted to ask you first how does encryption work and why is it important for users, particularly end-to-end encryption?

Amie Stepanovich: Encryption is really at the heart of security in the digital world. As people move more and more of their information online, encryption provides a lot of the protections that we are used to in the analog, in the real world. Things like keeping documents private, making sure that people who you don't want to see your communications aren't opening your letters, for example (your emails being the equivalent). Encryption is that protection, when you start talking about digital space.

So it's really important to provide companies with a lot of incentives to develop and implement really strong encryption, because the problem is that there are a lot of vulnerabilities in digital products and services, and people just have natural insecurities built in, when they use those services. I am yet to see any product that's 100% secure. Thus it's important to talk to companies and really make them see the benefit of using encryption, the fact that it's good for their users.

Encryption is also inherently connected to human rights. Users really can only exercise their right to freedom of expression, right to freedom of the press, or right to privacy, for example, if they have access to encryption. The problem is that actions like what we saw in Brazil with the court shutting down WhatsApp provides the wrong incentives to companies.



A criptografia está de fato no coração da segurança no mundo digital

podem exercer o direito à liberdade de expressão, à liberdade de imprensa, à privacidade, por exemplo, se tiverem acesso à criptografia. O problema é que ações como essas que nós vimos no Brasil, com juízes determinando o bloqueio do WhatsApp, fornecem os incentivos errados para as empresas.

A criptografia pode ser cara para desenvolver e difícil de ser implementada, especialmente uma criptografia realmente forte. As empresas estão tentando implementar modelos totalmente novos e repensar a segurança, e isso é realmente um ótimo processo e nós queremos que elas façam isso. Mas se as empresas acharem que serão submetidas a bloqueios, ou multas, ou à prisão por causa da implementação da criptografia, elas pensarão duas vezes antes de investir nisso. Isso prejudica os direitos humanos, prejudica a segurança digital e torna muitas pessoas mais vulneráveis a crimes - o que é exatamente o oposto do objetivo que o governo busca. O governo quer ajudar a solucionar crimes, mas a falta de criptografia torna as pessoas

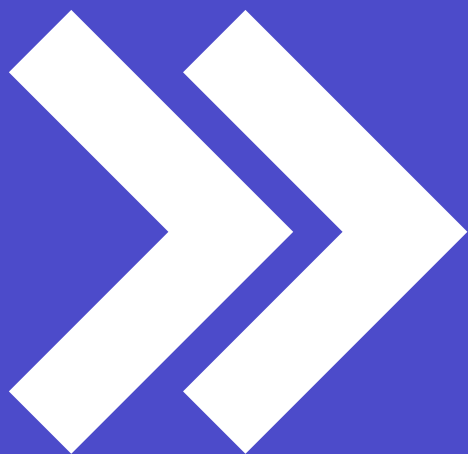
Encryption can be expensive to develop and it can be difficult to implement, especially really strong encryption. Companies are trying to put in place whole new models and rethink security, and that's a really great process and we want them to do that. But if they think that they are going to be subject to shutdowns, or fines, or imprisonment for doing that, it's going to make them think twice about it. It thus harms human rights, harms digital security and makes a lot of people more vulnerable to crime - which is exactly the opposite goal of what the government wants to accomplish. The government wants to help solve crimes, but lack of encryption makes people more likely to have their data vulnerable, to have their data compromised. And that could be done by people trying to take advantage of them financially, and steal their credit card information, for instance, or to blackmail them to steal further personal data. And that is what we're trying to prevent, that increase in crime.

Encryption also makes people more protected against street crime, because the numbers show

mais vulneráveis a terem seus dados comprometidos. E isso pode ser o caso de pessoas tentando tirar vantagens financeiras e roubar informações de cartão de crédito, por exemplo, ou buscando chantagear para roubar outros dados pessoais. Então é isso que nós estamos tentando evitar, esse aumento nos crimes.

A criptografia também faz com que as pessoas fiquem mais protegidas contra crimes comuns, porque os números mostram que criminosos têm menor interesse em roubar dispositivos digitais móveis se eles estiverem criptografados. iPhones são alvos comuns, porque esses aparelhos têm um alto valor de revenda. Mas se o dispositivo estiver criptografado, ele terá um uso mais limitado, então os roubos serão menos frequentes. E esse é apenas mais um benefício da implementação de uma criptografia forte.

that burglars are less likely to steal digital devices if they are encrypted. iPhones, for instance, are a huge target for criminals, because they have a high resale value. But if those devices are encrypted, they are of less use, so they are not stolen as often. And this is just another benefit of deploying the strong encryption.



2. É POSSÍVEL CONTORNAR OU QUEBRAR A CRIPTOGRAFIA?

2. *IS IT POSSIBLE TO CIRCUMVENT ENCRYPTION?*

InternetLab: Desenvolvendo um pouco mais o que você acaba de dizer sobre como essa tecnologia funciona, algumas autoridades de segurança pública têm alegado que há formas de obter acesso ao conteúdo das comunicações, apesar do uso da criptografia. Uma possível estratégia a qual essas autoridades estariam se referindo é o uso do chamado ataque “*man-in-the-middle*”. Você poderia explicar o que é isso e se há outras formas de contornar ou quebrar a criptografia, para esses fins? E, nesses casos, quais seriam as consequências para os usuários?

Amie Stepanovich: Há muito o que explicar aqui. Eu acho que a primeira coisa que vocês precisam saber é que a criptografia não é uma panaceia, ela não resolve todos os problemas. Mesmo no caso da criptografia mais forte disponível, sempre haverá meios de quebrá-la. Isso dito, a criptografia ainda é a melhor defesa contra vigilância em massa. Ela deixa a vigilância muito mais cara, você não pode

InternetLab: Elaborating a little bit on what you have just said about how the technology works, some law enforcement experts have been claiming that there are actual ways of having access to the content of communications in spite of the use of encryption. One possible strategy that they are referring to is the use of the so called “*man-in-the-middle* attack”. Could you explain to us what that is and if there would be other ways of circumventing encryption for those purposes? And in those cases what would be the consequences of these solutions for users?

Amie Stepanovich: There’s a lot to unpack there. I think the first thing that you need to know is that encryption is not a panacea, it does not solve all problems. Even if you use the strongest encryption available, there are always ways to break into it. Now, that said, encryption is the best defense against mass surveillance. It makes surveillance a lot more expensive, because you can’t collect a lot



coletar muitas informações diretamente dos cabos se essa informação está toda criptografada, o que significa que os Estados são forçados a utilizar uma vigilância mais específica, individualizada, o que é algo bom.

Nesses cenários específicos, há ainda muitas maneiras de os Estados terem acesso a dados criptografados, o que exige que usuários e empresas não apenas implementem criptografia, mas também implementem outras práticas e boa “higiene de segurança digital”, como nós chamamos, para continuar a proteger esses dados, para adicionar camadas adicionais de proteção.

Ataques do tipo *man-in-the-middle*, de forma simplificada, ocorrem quando pessoas te fazem sentir como se você estivesse conversando com outra pessoa (e você pode realmente estar se comunicando com aquela pessoa), mas alguém está entrando e pode ver aquela comunicação enquanto ela acontece, ou pode estar falsificando a pessoa na outra ponta, então na verdade você está se comunicando com essa outra pessoa, que não é quem você pensa que é.

Empresas como a *Signal*, desenhadas pela *Open Whisper Systems*, tentaram resolver isso ao indicar aos usuários quando seus amigos mudam suas chaves. O aplicativo diz “a pessoa na outra ponta tem uma chave nova”, e te encoraja a verificar se aquela ainda é a mesma pessoa, ligando para ela para perguntar “sua chave mudou?”, ou mandando uma mensagem por um canal diferente. Isso é feito para tentar verificar a identidade da pessoa na outra ponta, para cortar esses ataques do tipo *man-in-the-middle*. Mas nem todo mundo faz isso, o que significa que essas pessoas podem estar suscetíveis, e essas são práticas às quais as pessoas precisam se acostumar, se elas realmente querem estar seguras e protegidas.

Outra coisa é não clicar em links aleatórios nem e-mails, ou baixar softwares estranhos, porque isso também compromete as pontas finais, os aparelhos com os quais você se comunica, o que é outra vulnerabilidade na criptografia. Uma criptografia fraca também pode ser comprometida, ou facilmente aberta à força. E criptografia

of information of the wire if all that information is encrypted, which means it pushes governments toward more targeted individualized surveillance - which is a good thing.

In those targeted scenarios there are still a lot of ways governments have to get access to encrypted data, which means it requires users and companies not only to implement encryption, but also to implement other practices and good “digital security hygiene”, as we call it, to continue to protect that data, to add those extra levels of security.

Man-in-the-middle attacks, in a very simplified explanation, are when people can make you feel like you are communicating with another person (and you might actually be communicating with that person), but somebody is coming in and is able to see that communication as it happens, or spoofing the party on the other end, so you are actually communicating with this other person, who is not who you think you are talking to.

Companies like *Signal*, designed by *Open Whisper Systems*, have tried to solve that by indicating to users when their friends’ keys change. They will say “the person on the other end has a new key” and they encourage you to verify that is still that person, to reach out, call them and say “has your key changed?”, or send them a message on a different channel. And that is to try to verify the identity of the person on the other end, to cut off these *man-in-the-middle* attacks. But not everybody does that, which means they could be susceptible, and those are the practices that people need to get accustomed to, if they do want to be secure and protect themselves.

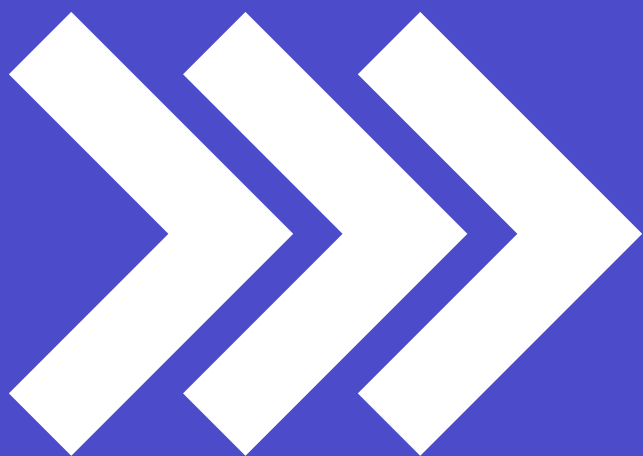
Other things are not clicking on random links and emails or downloading strange software, because these can also compromise the endpoints, the devices that you are communicating on, which is another vulnerability in encryption. Weak encryption can also be compromised or brute forced often. And improperly implemented encryption, which we see often, can have vulnerabilities that people can push through. There are a lot of different ways, which is why we say that companies should be encouraged,

implementada impropriamente, o que nós vemos com muita frequência, pode ter vulnerabilidades das quais as pessoas podem se aproveitar. Existem muitos caminhos, e é por isso que nós dizemos que as empresas deveriam ser incentivadas, novamente, a empregarem todos os recursos disponíveis para tornarem seus dispositivos seguros. Porque mesmo nesse cenário, há muitos pontos fracos, que deixam as pessoas inseguras, e não só inseguras em relação aos Estados, mas também inseguras em relação a maus atores.

Então se começarmos a falar sobre exigir que as companhias tirem recursos da segurança e passem a desenhar produtos com “criptografia que funciona às vezes mas é projetada para falhar”, e você não pode decidir quando essas falhas irão acontecer, então trata-se de um modelo ruim de uma forma geral.

again, to put all the resources they can into making their devices secure. Because even in that scenario, there are a lot of weaknesses that make people insecure, and not only insecure to governments but also insecure to bad actors.

So if we start talking about requiring companies to take resources away from security to design a product with “encryption that works sometimes but is designed to fail”, and you can’t decide when those failures are going to happen, then that’s just a bad model overall.



3. COMO SABER SE A CRIPTOGRAFIA
É REALMENTE FORTE?

3. *HOW TO ENSURE ENCRYPTION IS
TRULY STRONG?*

InternetLab: Recentemente, foram publicadas notícias sobre uma vulnerabilidade na criptografia de ponta-a-ponta instalada no WhatsApp. Essas alegações foram feitas por um especialista em Berkeley (cidade da Califórnia, nos Estados Unidos) e realmente levaram as pessoas a se questionarem acerca da segurança do uso aplicativo. O WhatsApp respondeu oficialmente a essas alegações, afirmando que sua criptografia é segura e que essa era, na verdade, uma característica do aplicativo. Eu gostaria de usar esse caso para perguntar sobre a importância de códigos abertos para o debate em torno da criptografia. Isso é algo que deveria ser encorajado? Isso poderia beneficiar hackers e autoridades de segurança pública, no sentido de possibilitar manipulações do código ou descobertas de furos com maior facilidade?

Amie Stepanovich: O uso de tecnologia de código aberto é algo que a *Access Now* apoia, porque é possível ver como o software é construído. Então se existe uma vulnerabilidade, sim, autoridades de segurança pública poderão ser capazes de enxergá-la e tirar vantagens disso, mas o resto do mundo também será capaz de vê-la. Assim, há uma probabilidade significativamente maior de uma falha ser descoberta e ser corrigida se o código for aberto, simplesmente por conta do número de olhos observando.

Quando se trata de uma tecnologia de código fechado, por natureza, há um número muito limitado de pessoas revisando esse software. Empresas de software que têm códigos fechados, como a Apple, frequentemente realizam auditorias, com muitos engenheiros de segurança de alto-nível, mas, no fim do dia, há menos olhos olhando para esse código, e esse é realmente um dos grandes benefícios dos softwares de código aberto.

Eu também quero comentar a matéria que você mencionou sobre o WhatsApp, e sobre “os recursos embutidos” em oposição aos “bugs do sistema”, porque eu acho isso muito interessante. Nós encorajamos as empresas, novamente, a desenvolverem a criptografia mais forte possível,

InternetLab: Recently we have seen stories in the news about a vulnerability in the end-to-end encryption built into WhatsApp. These were claims made from a security expert in Berkeley that really made some people question their security when using the app. WhatsApp has officially responded to those claims stating that its encryption is secure and that this was actually a feature of the app. I wanted to use this story to ask you about the importance of open-sourced code to the encryption debate. Is that something we need to encourage? Could that benefit hackers and law enforcement authorities in the sense that they could manipulate the code or find security holes more easily?

Amie Stepanovich: Open source technology is something that *Access Now* promotes, because you can see what the software is built upon. So if there is a vulnerability, yes law enforcement might be able to see that and to take advantage of it, but the rest of the world will also be able to see it. Thus, there is a significantly higher likelihood that it will be discovered and able to be patched if the software is open source, just because of the number of eyes on it.

When you have a piece of closed source technology, it means, by nature, that there is a very limited number of people reviewing that software. Software companies that are closed sourced, like Apple, often have lots of audits, lots of high-level security engineers, but at the end of the day they have fewer eyes looking over their code, and that’s really one of the big benefits of open source software.

I do want to touch on a piece that you said about WhatsApp, and about “the features” versus “the bugs”, because I think this is really interesting. We encourage companies, again, to develop as strong encryption as possible, but there are reasons not to have the strongest encryption in every single service. Encryption is tied to keys, so if you have a service that you, by nature, want to be able to access from lots of different devices, it doesn’t make sense to have a single device with the key on it – because it makes it a lot harder to access that data, if you



Há uma probabilidade significativamente maior de uma falha ser descoberta e corrigida se o código for aberto, simplesmente por conta do número maior de olhos revisando o software.

mas há razões para não usar a criptografia mais forte em todos os serviços. Isso porque a criptografia está ligada a chaves, de modo que, se você tem um serviço que, por natureza, você queira acessar de vários dispositivos diferentes, não faz sentido a chave estar em um único dispositivo – porque isso torna muito mais difícil o acesso aos dados, se você quiser recuperá-los, ou fazer cópias de segurança. E é por isso que muitas pessoas que têm um iPhone, embora o disco rígido do iPhone seja criptografado, fazem cópias de segurança de seus dados na nuvem (iCloud), o que dá de volta para a Apple o acesso a esses dados. Isso é porque essas pessoas querem a garantia de que, se os seus telefones caírem no mar, por exemplo, elas terão seus dados de volta.

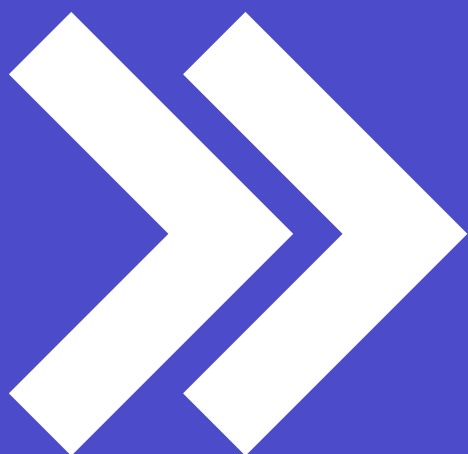
Então há razões legítimas para usuários não usarem a criptografia mais forte em alguns produtos e em alguns serviços, ou adotarem práticas que enfraquecem a proteção que eles têm. É realmente muito importante, mesmo nesses casos, que ainda haja alguma forma de criptografia, que os dados

want to be able to retrieve data, or if you want it backed up. And this is why a lot of people who own an iPhone, even though the iPhone hard drive is encrypted, backup their data to the iCloud, which gives that access back to Apple. It's because those people want to know that, if their phone falls into an ocean, for instance, they can get their data back.

So there are legitimate reasons for users not having the strongest encryption in some products and in some services, or having practices that weaken the protection that they have. It's really important in those cases that you still have some form of encryption, that you are still protecting the data, and that you are very honest with users. We think it is actually much worse to provide users with a false sense that they have more security than they actually have, than to just not provide them the security to begin with. Because you are going to give those users this idea that they can do things and that they are protected. So they might take risks that they would not otherwise take, which puts them

ainda sejam protegidos, e que as empresas sejam muito honestas com os usuários. Nós achamos que na verdade é muito pior dar aos usuários uma falsa sensação de maior segurança do que eles realmente têm, em vez de simplesmente não oferecer segurança a eles. Porque os usuários vão pensar que podem fazer coisas e que eles estão protegidos. Então eles poderão tomar atitudes de risco que eles não tomariam em outras circunstâncias, e isso os coloca em uma posição pior do que a que eles estavam antes. Então é realmente muito importante que as empresas escutem essa mensagem de que elas precisam ser honestas e abertas com seus usuários sobre o que elas estão fazendo.

in a worse off position than they were before. And it is really important for companies to hear that message, that they need to be honest and open with their users about what they are doing.



**4. COMO DEVE SER O ACESSO DE
AUTORIDADES A METADADOS?**

***4. IN WHICH CIRCUMSTANCES
LAW ENFORCEMENT COULD HAVE
ACCESS TO METADATA?***



InternetLab: Outra questão que tem sido debatida é o acesso a metadados. Na legislação brasileira, não há um tratamento específico dado a metadados, o que significa que não há requisitos legais ou circunstâncias estabelecidas em lei nas quais tais dados podem ser acessados. Isso de alguma forma tornou mais fácil o acesso por autoridades de segurança pública a dados de geolocalização e outros tipos de dados. Em quais circunstâncias você acha que metadados podem ser obtidos pelas autoridades e quais devem ser os requisitos para tanto? Se você puder também explicar como essa questão funciona nos Estados Unidos, seria ótimo.

Amie Stepanovich: Nós achamos que metadados devem ter exatamente a mesma proteção dada ao conteúdo, porque metadados são muitas vezes tão reveladores quanto o conteúdo, quando não mais reveladores. O que é interessante sobre metadados é que eles não podem mentir. Eu posso escrever um email e o conteúdo dele pode ser todo inverídico, todas as palavras dele, mas as informações como de onde eu mandei aquele email, para quem eu o mandei, a hora em que eu mandei, isso tudo são informações factuais, que podem revelar muito sobre aquela comunicação. Então nós achamos que as proteções precisam ser as mesmas.

Mas há muitos problemas. Primeiramente, nos EUA, nós temos uma doutrina chamada “doutrina dos terceiros”, que existe desde antes da Internet moderna, e determina que quando uma pessoa dá suas informações voluntariamente para um terceiro, ela perde seu interesse de privacidade em relação àquelas informações. E metadados, por sua natureza, são sempre dados a um terceiro. Sua companhia telefônica precisa ser capaz de rotear as suas ligações, então ela precisa saber para quem você está ligando, e o seu celular precisa saber onde você está, porque ele precisa ser capaz de fornecer o serviço e de conectá-lo a uma torre, e isso oferece ainda mais baixos níveis de proteção para os usuários.

Nos EUA, nós tentamos superar esses obstáculos com a aprovação de leis específicas que oferecem

InternetLab: Another issue that has been debated is access to metadata. Under Brazilian law, there is no specific treatment granted to metadata, meaning there are no specific requirements or circumstances under which these data can be accessed. This has made it somehow easier for law enforcement to have access to geolocation data and other sorts of data. In which circumstances do you think metadata could be obtained by law enforcement and which should be the requirements for doing so? If you could also explain us briefly how does that work in the US, that would be great.

Amie Stepanovich: We think that metadata should have the exact same protections as content, because metadata is often as revealing, if not more revealing than content. What is interesting about metadata is that it can't lie. I can write an email and it can be all not true, every single word of it, but the information about where I sent that email, who I sent it to, what time I sent it, that is factual information that can reveal a whole lot about that communication. So we think that the protections need to be the same.

But there are many problems. First of all, in the United States we have a doctrine called “the third party doctrine”, which dates back to before the modern Internet and talks about how, when you give your information voluntarily to a third party, you lose your privacy interest in that information. And metadata by the nature of what it is, is always given to a third party. Your phone company needs to be able to route your calls, so they need to know who you are calling, and your cell phone needs to know where you are, to be able to send you service and to connect you to a tower, which provides additional lower levels of protection for users.

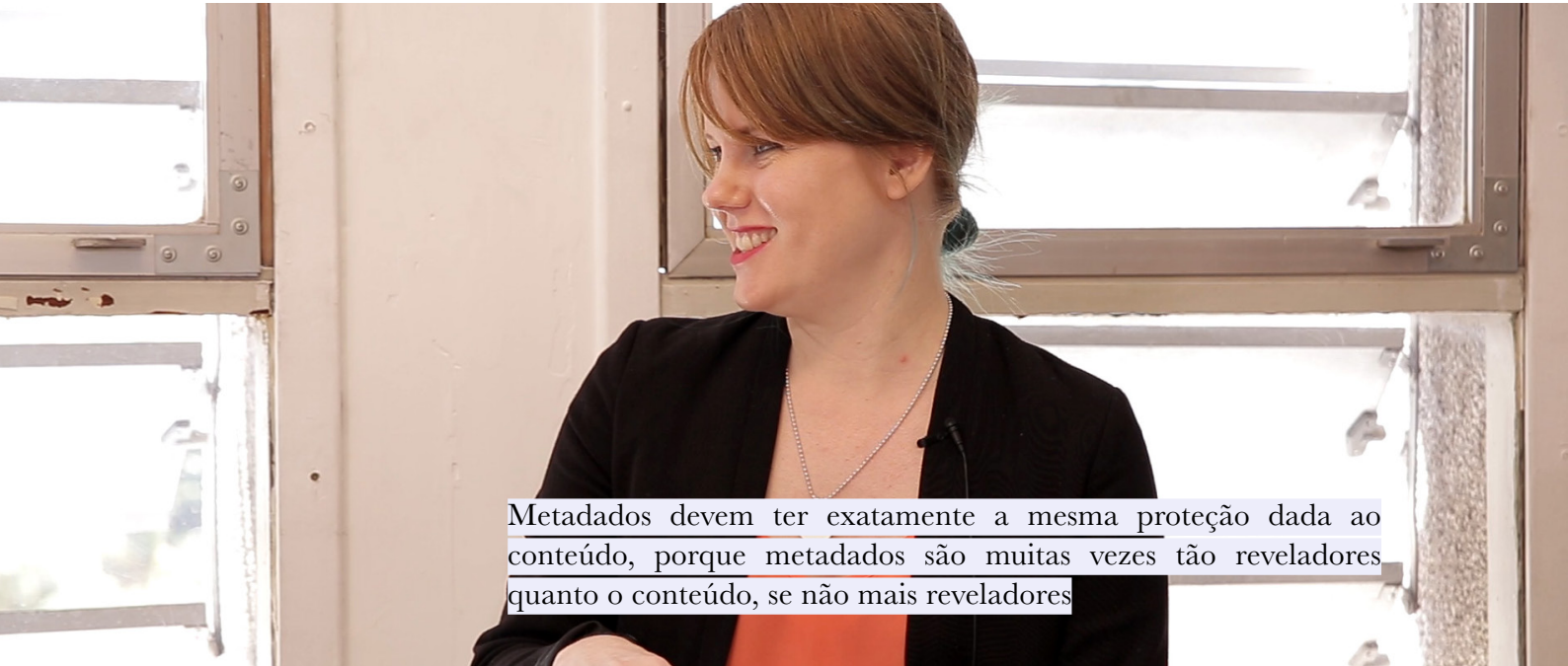
In the US we have tried to overcome those hurdles by passing specific laws that provide higher levels of protection, that run around the third party doctrine. For example, there's a law in Congress right now that has been proposed to protect location information and to ensure that you have to show some suspicion, and that you have to go to a court

níveis mais altos de proteção e que contornam a doutrina dos terceiros. Por exemplo, há uma lei em trâmite agora no Congresso que foi proposta para proteger informações de localização e para garantir que seja necessário mostrar alguma suspeita, ir a um tribunal e conseguir um mandado para acessar dados de localização, por conta de quão sensíveis esses dados são. Nós achamos que essa é a abordagem correta e nós também achamos que a doutrina de terceiros é bastante ultrapassada, por conta da quantidade de dados que nós entregamos a terceiros. Nós achamos que isso não é mais viável no mundo digital, da maneira que deve ter sido muitos anos atrás, décadas atrás.

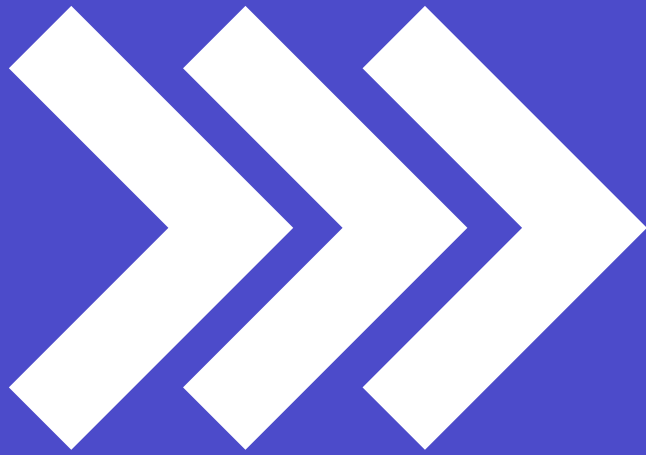
Também é importante notar que os metadados não podem ser criptografados, ou nós ainda não descobrimos uma maneira de fazê-lo. E existem razões para isso, mas no fim do dia as pessoas precisam perceber que, ainda que suas comunicações sejam criptografadas, seus dados estão por aí mundo afora, e que eles não estão assim tão protegidos por proteções digitais. Então eles são de mais fácil acesso também para autoridades de segurança pública.

and get a warrant to access location data, because of how sensitive location data is. We think that is the right approach and we also think that the third-party doctrine is far outdated, because of how much data we turn over to third parties. We think that it is no longer tenable in the digital world, in the way that it might have been many many years ago, decades ago.

It is also important to note that metadata can't be encrypted, or we haven't figured out a way to do it yet. And there are reasons for that, but at the end of the day people need to realize that, even if their communications are encrypted, that data is out there in the world and it is not as protected through digital protections. So it's more easily accessible also to law enforcement.

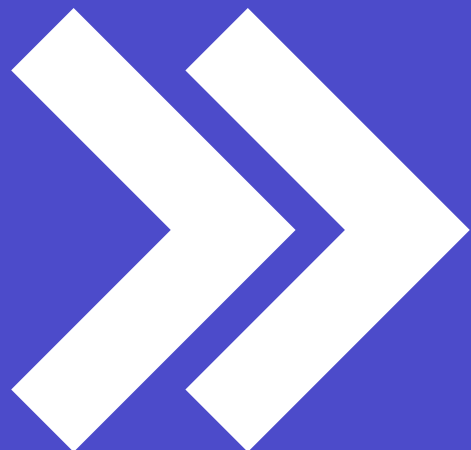


Metadados devem ter exatamente a mesma proteção dada ao conteúdo, porque metadados são muitas vezes tão reveladores quanto o conteúdo, se não mais reveladores



**5. E QUANDO O ESTADO
VIRA "HACKER"?**

**5. *WHAT ABOUT HACKING BY
GOVERNMENTS?***



InternetLab: Nós falamos sobre a moldura jurídica que regula o acesso a dados de usuários, mas algo que eu gostaria de adicionar a essa conversa é a possibilidade de o próprio Estado hackear dispositivos de usuários. Notícias recentes reportaram que autoridades brasileiras estiveram em contato com empresas que fornecem “soluções de vigilância” para governos, como a empresa italiana *Hacking Team*. Outras histórias sugerem que as autoridades brasileiras têm pressionado empresas de telefonia a adotar e usar infiltração de malwares para obter informações armazenadas em telefones celulares. Quais os riscos para direitos humanos associados quando o Estado vira hacker? Em quais casos, se houver algum, essa medida será legítima? Você poderia também comentar sobre a recente implementação da Regra 41 do Código de Processo Penal dos Estados Unidos? Como ela se relaciona com esse debate?

Amie Stepanovich: A *Access Now*, no ano passado, publicou um relatório chamado *A Human Rights Response to Government Hacking* (disponível apenas em inglês).¹² Nós tentamos olhar especificamente para quais impactos o hackeamento tem na proteção dos direitos humanos dos usuários. Então nós olhamos para os diferentes tipos de hackeamento pelo Estado e para as diferentes motivações que governos podem ter, por exemplo, para conduzir vigilância – que é uma das maiores razões, para ter acesso a dados de usuários. Estados também têm hackeado dispositivos para ditar uma mensagem e para garantir que ela ou seja promovida ou de alguma forma diminuída, o que nós chamamos de “controle de mensagens”. E uma terceira razão seria causar algum tipo de dano. É possível hackear dispositivos, por exemplo, para fazê-los explodir ou fazê-los superaquecer, para causar danos no mundo físico. Escutamos com frequência nos EUA membros do Congresso falando sobre ciberguerra, e dizendo

InternetLab: We’ve been talking about the legal frameworks for access to users data but one thing I wanted to add to this conversation is the possibility of governments hacking users’ devices. Recent news stories reported that Brazilian authorities have had contact with companies that provide “surveillance solutions” for governments, such as the Italian *Hacking Team*. Other stories suggest that Brazilian authorities have pushed telecom companies to adopt and use malware infiltration to obtain information stored in cell phones. What are the risks for human rights associated with government hacking? In what cases, if any, can this measure be legitimate? And also, could you comment on the recent implementation of Rule 41 of the Federal Rules of Criminal Procedure in the US? How does that relate to this whole debate?

Amie Stepanovich: *Access Now*, last year, published a report called *A Human Rights Response to Government Hacking*.¹³ We tried to look at specifically what impact hacking has on human rights protections for users. So we looked at the different types of government hacking and the different motivations that governments may have, for example, to conduct surveillance – which is a big one, to get access to user data. Governments have also hacked into devices in order to dictate a certain message and to ensure that either a message is promoted or kind of tampered down, which we call “messaging control”. And then a third one is to do some sort of damage. You can hack into devices, for example, to make them explode or to make them overheat in a way, to cause a physical world damage. You often hear in the US these members of Congress talking about cyber war, and saying “they [criminals] are going to hack into the electric grid and shut it down”. That is this “causing damage” scenario.

What we have determined is that the second motivation, the messaging control, and the third

¹² *Access Now*, “A Human Rights Approach to Government Hacking”, disponível em: <https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf>.

¹³ *Access Now*, “A Human Rights Approach to Government Hacking”, available in: <https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf>.

que “eles [criminosos] vão invadir a rede elétrica e desligar toda a rede”. Isso é esse cenário de “causar danos”.

O que nós estabelecemos é que a segunda motivação, o controle de mensagens, e a terceira, causar danos, são absolutamente inconsistentes com a proteção de direitos humanos, considerando o que elas são atualmente capazes de fazer. O hackeamento por motivos de vigilância, entretanto, pode ser consistente com direitos humanos. Nós não condenamos o hackeamento pelo Estado. Nós realmente achamos que ele é ruim para os usuários, por uma série de razões, porque é um tipo muito diferente de outros tipos de vigilância e nós temos muita certeza de que isso não é algo deveria ser louvado. Mas nós também temos clareza de que os Estados estão fazendo isso, nós sabemos que isso não vai parar tão cedo, e que nós estamos nesse mundo muito real em que Estados em todo o mundo estão tentando hackear dispositivos.

Então o que nós estamos tentando dizer na prática é que se isso for usado para vigilância, é

one, causing damage, are just absolutely inconsistent with human rights protections, considering what they are currently capable of doing. The surveillance motivated hacking though might be consistent with human rights. We do not condone government hacking. We actually think that government hacking is bad for users for a whole range of reasons, because it is very different from other types of surveillance and we are very clear that this is not something that we think should be blessed. But we are also clear that we know governments are doing it, we know it is not going to stop anytime soon, and that we are in this very real-world of governments all over the world trying to hack into devices.

So what we try to say practically is, if you are going to do that for surveillance, you need to have a legal framework in place. You cannot simply contract with a company like *Hacking Team*, or use existing surveillance authority that was designed for less invasive activity than hacking, to cram in the use of these very invasive tools. We set out 10 safeguards and we say these are what you need to have in law. Things like greater transparency and assurance that



preciso ter uma moldura jurídica em vigor. Não é possível simplesmente contratar uma empresa como a *Hacking Team*, ou utilizar uma autoridade de vigilância existente, que foi estabelecida para uma atividade menos invasiva do que hackear, para inserir o uso dessas ferramentas muito mais invasivas. Nós estabelecemos 10 garantias que nós acreditamos que precisam estar na lei. Coisas como maior transparência e a segurança de que não será causado nenhum dano, e que o Estado vai tentar remover o malware do dispositivo depois da operação de hackeamento. Nós achamos que isso é necessário.

Isso dito, a Regra 41 do Código de Processo Penal dos Estados Unidos é a regra que determina onde juízes podem autorizar buscas. Ela basicamente diz que, com algumas exceções, um juiz pode apenas autorizar uma busca na jurisdição na qual o dispositivo será investigado. E isso era um limite prático para o hackeamento pelo Estado, porque muitas vezes as autoridades estavam hackeando dispositivos porque elas não sabiam onde esses dispositivos estavam localizados. E o que diversos tribunais disseram é que você não pode autorizar um mandado para algo que você não sabe onde está, por causa da Regra 41 e desse requisito de que o objeto esteja presente na sua jurisdição.

As recentes emendas foram aprovadas por um Comitê Federal, aprovadas pela Suprema Corte e então elas foram para o Congresso. Tudo o que o Congresso tinha que fazer era não fazer nada e então elas entrariam em vigor. Normalmente, o Congresso aprova a lei e só então a lei muda. Nesse caso, a mudança na regra entraria em vigor simplesmente por inatividade. E a mudança na regra dizia que, em alguns cenários, basicamente cenários de hackeamento pelo Estado, um juiz poderia emitir um mandado para o hackeamento pelo Estado, adicionando uma nova exceção.

Nossa opinião sobre essa mudança foi de que ela estava colocando o carro na frente dos bois, porque nós não temos uma moldura jurídica que estabeleça o que é necessário para o hackeamento pelo Estado. Então nós estamos removendo essas

you are not going to cause damage, and that you are going to try to remove the malware from the device after the hacking operation. We think that this is necessary.

Now that said, Rule 41 in the Federal Rules of Criminal Procedure in the United States is the rule that governs where magistrate judges can authorize searches. It essentially says, with a few exceptions, that a magistrate judge can only authorize a search in the jurisdiction where the device is to be searched. It was a practical limit on government hacking, because a lot of times they were hacking into devices because they didn't know where they were located. And what several courts have said is that you cannot authorize a warrant for something you don't know where it is, because of Rule 41 and this requirement that the object be present in your jurisdiction.

The recent amendments were passed by a Federal Committee, approved by the Supreme Court and then they went to Congress. All Congress had to do was nothing and then the law went into effect. Normally, the Congress passes the law and then the law changes, but here it was just by inaction that the rule change went into effect. And the rule change said that, in certain scenarios (basically government hacking scenarios) the judge can issue a warrant for government hacking – it added this new exception.

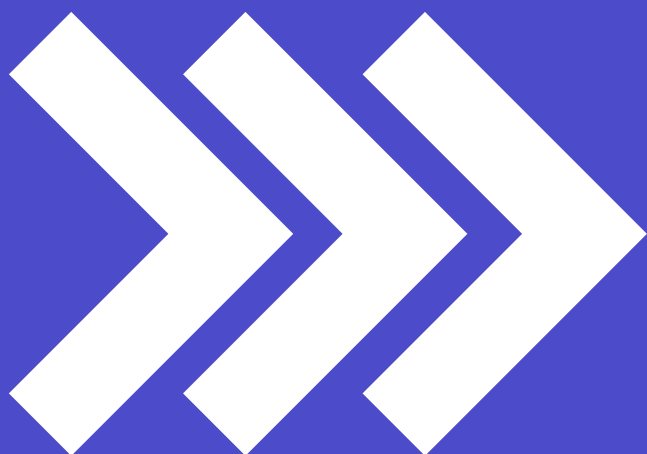
Our opinion on that change was that it was putting the cart before the horse, because we don't have the legal framework which is necessary for government hacking. So we were removing these procedural barriers to make it easier to hack into objects, into devices, without having thought through the substantive rules that need to be in place as well. So we think that that is a very negative thing. We are now in a scenario where we are not sure how government is using these authorities, but we know they are, after that rule change went into effect. And we still don't have the proper substantive rules in place for it.

We think that all countries should really be considering a legal framework. We are seeing it, Netherlands has a law on government hacking, Italy

barreiras processuais para tornar o hacker objetos e dispositivos mais fácil, sem ter pensado com calma nas regras substantivas que precisam estar em vigor também. Então nós achamos que isso é uma coisa muito negativa. Nós estamos hoje em um cenário no qual nós não temos certeza de como o Estado está usando essas capacidades, mas nós sabemos que eles estão, após essa mudança da regra ter entrado em vigor. E nós ainda não temos as regras substantivas adequadas em vigor.

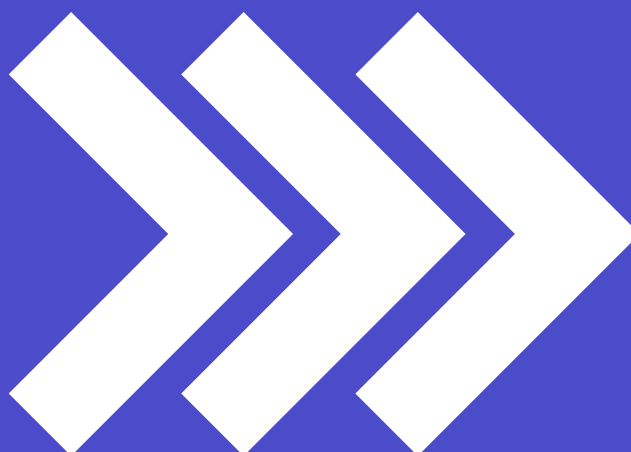
Nós achamos que todos os países deveriam realmente considerar uma moldura jurídica. E nós estamos vendo isso. A Holanda tem uma lei sobre hackeamento pelo Estado, a Itália acabou de propor uma lei sobre isso que, considerando que nós achamos que o Estado não deveria estar hackeando, é uma lei bastante boa e bastante protetiva. A Austrália também tem uma moldura jurídica, e nós gostaríamos de ver mais países entrando nesse mundo de possuírem um enquadramento legal.

just proposed a law on that, which, noting that we don't think they should be hacking at all, is actually quite good and quite protective. Australia has also a framework and we would like to see more countries move into that world of having a legal framework.



6. REFORMA DOS ACORDOS
DE COOPERAÇÃO JUDICIÁRIA
INTERNACIONAL (MLATS)

6. *MUTUAL LEGAL ASSISTANCE
TREATIES (MLATS) REFORM*



InternetLab: Com frequência, temos visto que estes pedidos de acesso a dados de usuários envolvem empresas cujos servidores estão baseados fora do Brasil, e em alguns casos não tem representação no país. Isso adiciona uma camada extra de complexidade aos casos, no sentido de que eles dependem de cooperação internacional para se tornarem mais operacionalizáveis. Os acordos de cooperação judiciária internacional (MLATs, na sigla em inglês) estão no coração dessas molduras. Autoridades de segurança pública, no entanto, têm sido muito críticas a respeito das suas fraquezas. Esses mecanismos seriam lentos, burocráticos e ineficientes para exigir o acesso a dados de usuários. Quais reformas você acredita serem necessárias para fazê-los funcionar melhor?

Amie Stepanovich: Eu acho que há dois passos para isso. Na *Access Now*, meu colega Drew Mitnick está prestes a apresentar a nossa proposta, sobre como e o que nós achamos que deveria mudar. E a primeira coisa a ser mudada são os próprios MLATs. Nós achamos que o sistema de MLATs, em geral, é um sistema de proteção dos direitos humanos. Ele funciona para proteger usuários, especialmente usuários em países nos quais há menos salvaguardas aos direitos humanos.

O problema é que ele é devagar e burocrático, especialmente no caso de crimes hiperlocais. Por exemplo, um crime que acontece no Brasil, com um criminoso brasileiro e uma vítima brasileira e está tudo aqui, e de repente há um pedaço de informação vital para a investigação que está localizado em um servidor nos Estados Unidos. Então é preciso passar por um processo de um ano para ter acesso a esses dados. Isso é realmente infeliz, é bastante frustrante. Eu sei que é frustrante no Brasil e em outros países também.

Eu acho que nós precisamos olhar para a jurisdição e problemas jurisdicionais e ter certeza de que nós estamos exercendo a jurisdição nos lugares corretos. Nós precisamos investir mais nos MLATs, precisamos dar mais treinamento para as pessoas utilizarem o processo de MLAT. Essas são apenas

InternetLab: Very often, we have seen that these requests for users data involve companies whose servers are based outside of Brazil and sometimes which do not even have offices in Brazil. This adds another layer of complexity to these cases in the sense that they depend on international cooperation frameworks to become more operable. The Mutual Legal Assistance Treaties (MLATs) are at the heart of these frameworks. Law enforcement authorities have been very vocal about their weaknesses though. These are slow, bureaucratic and inefficient mechanisms to demand access to users data. In your views, what kind of reforms should be made to make them work better?

Amie Stepanovich: I think there are two steps to this. In *Access Now*, my colleague Drew Mitnick is about to put forward our proposal on how we think and what we think should change. And the first thing is to change the MLATs themselves. We think the MLAT system by and large is a human rights protective system. It works to protect users, specially users in countries where there are fewer human rights protections.

The problem is that it is slow and bureaucratic, specially for hyperlocal crimes. For instance, a crime that happens in Brazil, with a Brazilian criminal and a Brazilian victim, and everything is here, and all of a sudden there's a vital piece of data for the investigation which is located on a server in the United States. So you have to go through this year's long process to get access to that data. That is really unfortunate, it's very frustrating. It's frustrating in Brazil and in other countries, as well.

I think we need to be looking at jurisdiction and jurisdictional issues and make sure that we are exerting jurisdiction in the right places. We need to be providing more funding for MLATs, we need to be providing more training for people to go through the MLAT process. These are just a few of the things that you need to fix in the basic MLAT model, while still protecting human rights. You can't sacrifice human rights at the altar of efficiency.

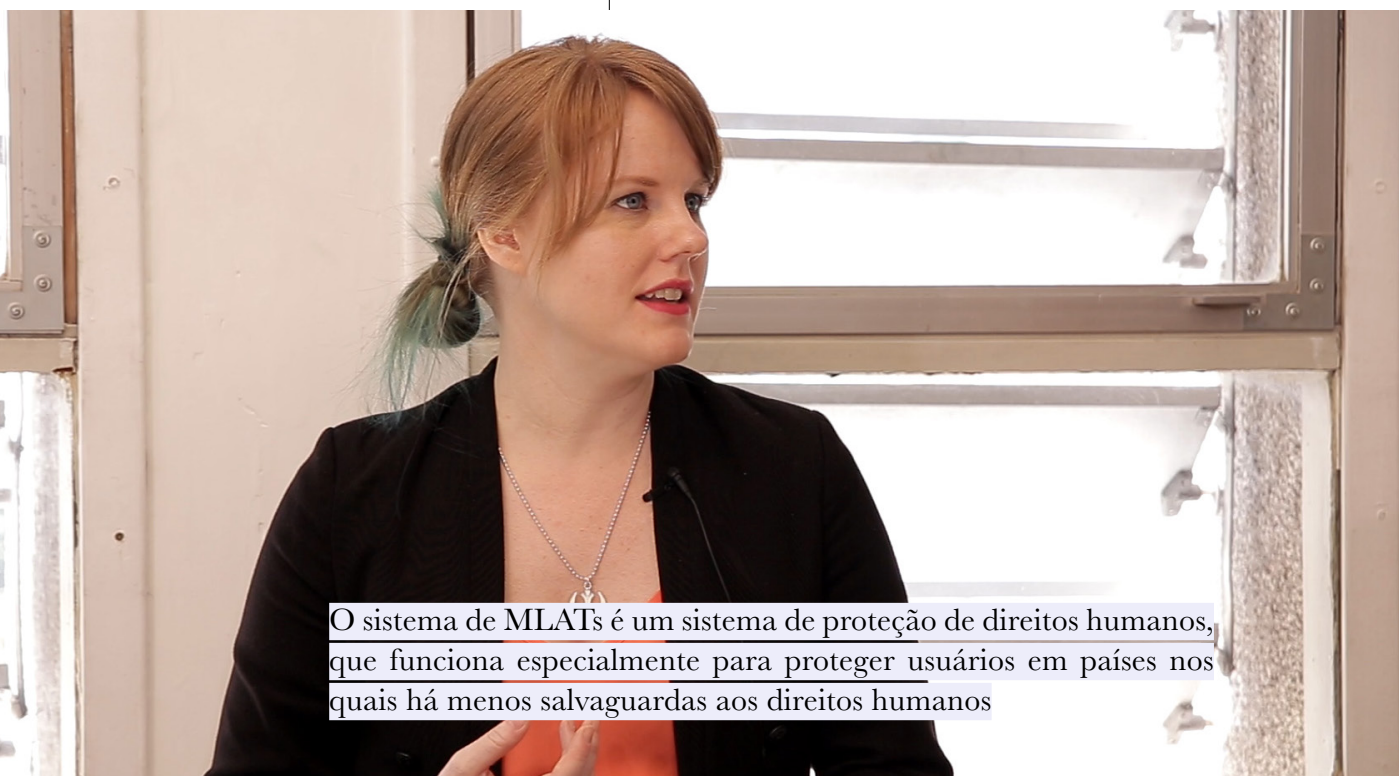
algumas das coisas que precisam ser melhoradas no modelo básico de MLAT, ao mesmo tempo protegendo os direitos humanos. Você não pode sacrificar os direitos humanos no altar da eficiência.

Isso dito, uma das coisas que também está sendo proposta é a possibilidade de países entrarem em acordos, nos quais seria possível contornar o sistema de MLAT, para pedir informações diretamente para as empresas, em algumas jurisdições. Há agora um projeto para mudar a lei nos Estados Unidos, para permitir esses tipos de acordos, porque eles não poderiam acontecer de com a lei em vigor. Nós achamos que a ideia pode ser muito positiva, que ela pode aliviar um pouco da pressão no sistema. De modo que alguns países, que protegem os direitos humanos, poderiam ter um acesso mais direto, o que significa que eles poderiam ter um processo mais eficiente, porque um pouco desse atraso seria deixado para trás.

Mas há muitos problemas com a atual proposta. Primeiro, ela não evita de fato que países implementem leis ruins para os direitos humanos, como leis de retenção de dados localização. A proposta para contornar o sistema de MLAT não

That said, one of the things that are also being proposed is the ability for countries to enter into agreements, where they could bypass the MLAT system and go directly to the companies, in certain jurisdictions. There is right now a legal proposal to change the law in the United States, to allow for these type of agreements, because they couldn't happen under current law. We think that the idea of this might be very positive, it might alleviate some of the pressure on the system. So that some countries that protect human rights can get more direct access, which means that other countries would have a more efficient process, because some of that backlog would be led up.

But there are many problems with the current proposal. First, it does not actually prevent countries from implementing bad laws for human rights, like mandatory data localization. The proposal to bypass the MLAT system doesn't prevent that from being in place, which means it's not solving some of the underlying problems. Second, it doesn't include MLAT reform, so you're not solving this underlying problem by providing for the greater efficiency of



O sistema de MLATs é um sistema de proteção de direitos humanos, que funciona especialmente para proteger usuários em países nos quais há menos salvaguardas aos direitos humanos

evita que esse tipo de lei seja aprovado, o que significa que ela não está resolvendo alguns dos problemas inerentes. Segundo, ela não inclui uma reforma do MLAT, então, novamente, não está resolvendo esse problema inerente nem conferindo mais eficiência para o processo. E então não protege adequadamente os direitos humanos.

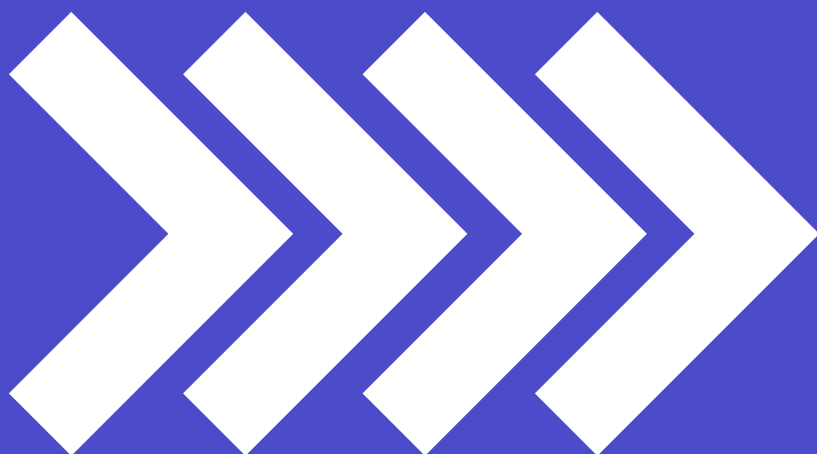
Um dos países sendo considerados para um acordo inicial é o Reino Unido. O Reino Unido acabou de aprovar uma das leis de vigilância mais invasivas do mundo, no ano passado, a Lei de Poderes Investigatórios (*Investigatory Powers Bill*), que permite uma quantidade enorme de atividades de vigilância. E com essa proposta, se ela permitir que o Reino Unido tenha acesso a empresas dos EUA, você pode imaginar que ela não estará protegendo adequadamente direitos humanos. Então nós achamos que é preciso elevar os padrões, que se um governo quer ter um acesso mais fácil, se ele quer contornar isso, ele precisaria mostrar que oferece mais proteções para os indivíduos.

E a outra coisa que eu considero estar no coração disso, e que não está sendo discutida, é que a proposta permitiria proteções apenas para cidadãos dos Estados Unidos, e a lei britânica, em geral, tem algumas proteções para cidadãos do Reino Unido. Mas essa não é uma proposta limitada apenas aos dois países no acordo. Então se o Reino Unido quisesse pedir diretamente para uma companhia estadunidense informações sobre brasileiros, há pouquíssimas proteções em vigor, o que significa que isso iria comprometer os direitos humanos de usuários em quase todos os países do mundo. Brasil, Alemanha, Austrália, Tunísia. Todos os usuários do mundo teriam menos direitos porque o Reino Unido poderia acessar mais facilmente os seus dados. E eu acho que isso é uma enorme falha no sistema que precisa ser corrigida também.

the process. And then it doesn't adequately protect human rights.

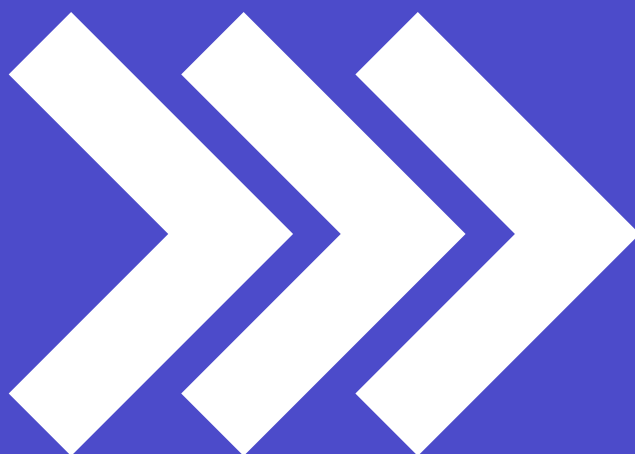
One of the countries being looked at for an initial agreement is the United Kingdom. The UK just passed one of the most invasive surveillance laws in the world last year, the *Investigatory Powers Bill*, that allows for huge amounts of surveillance. And this proposal, if it would allow the UK to get access to the US companies, you can imagine that it really is not adequately protecting rights. So we think that we need to increase the standards. If governments want easier access, if they want to bypass this, they actually should show that they have greater protections for individuals.

And the other thing that I think is at the heart of this, but that isn't being discussed, is that the proposal would allow for protections for American citizens, and UK law, by and large, has some protections for UK citizens. But this is not a proposal limited to just the two countries in the agreement. So if the UK wanted to go directly to a US company and get information about Brazilian citizens, there are very few protections in place, which means it would undermine the human rights of users in every other country around the world. Brazil, Germany, Australia, Tunisia. Every user would have fewer rights because the UK would then be able to get greater access to their data. And I think that that is a huge hole in the system that needs to be plugged well.



7. O FUTURO DO DEBATE NO BRASIL E POSSÍVEIS DESDOBRAMENTOS NA AMÉRICA LATINA

7. THE FUTURE OF THE DEBATE IN BRAZIL AND POSSIBLE IMPACTS IN LATIN AMERICA



InternetLab: Nós gostaríamos de terminar nossa conversa de hoje com suas perspectivas para o futuro, especialmente sua opinião sobre o cenário brasileiro. As disputas jurídicas sobre a legalidade dos bloqueios de sites e aplicativos se tornaram uma questão constitucional no Brasil: duas ações constitucionais que desafiam a constitucionalidade de tais medidas foram apresentadas ao Supremo Tribunal Federal brasileiro. No âmbito do Poder Legislativo, onze projetos de lei sobre bloqueios de sites e aplicações foram recentemente apresentados ao Congresso Nacional, alguns visando proibir bloqueios em qualquer hipótese e outros regulando a medida em situações específicas.¹⁵ Em comum entre todos esses projetos está o pressuposto de que a aprovação de uma só lei seria capaz de lidar com toda a complexidade que envolve a polêmica dos bloqueios - apesar das diferenças nas circunstâncias de cada caso, seus motivos e as fundamentações utilizadas. Considerando o papel de liderança desempenhado pelo Brasil ao tratar dessas questões, qual você acredita que serão os impactos do desdobramento dessas questões em outros países da América Latina? Como você vê o futuro dessas tensões? Como avançar no debate?

Amie Stepanovich: Eu acho que a primeira coisa a ser considerada é que bloqueios de sites e serviços viola direitos humanos. E uma das coisas nas quais nós precisamos pensar é que talvez esses bloqueios não sejam a forma de lidar com alguns desses problemas que precisam ser resolvidos, que há outros caminhos para isso. Bloqueios tendem a ser consideravelmente fáceis, mas eles também tendem a ser muito amplos, e afetam muitos usuários e muitos discursos legítimos. Então se você aprovar uma lei sobre essa questão, que não seja uma proibição, mesmo que essa lei forneça alguns parâmetros, você estará recepcionando essa prática de maneira global. E isso pode ser

InternetLab: We wanted to end our conversation with your perspectives to the future, specially your views on the Brazilian scenario. The legal disagreements about the legality of blockages have become a constitutional issue in Brazil: two constitutional complaints challenging the constitutionality of such measures were brought before the Brazilian Federal Supreme Court. Within the Legislative Power eleven draft bills were presented in the National Congress about website and application blockings that deal with the question in different manners, either by prohibiting blockages in any circumstance or by regulating it in specific situations.¹⁶ All of them share the presumption that the approval of only one law will be able to deal with all the complexity that involves the issue of blocking, even though the circumstances of each case, their motives and legal grounds are quite different. Considering Brazil's pioneering role in addressing these issues, what are the impacts that the unfolding of these discussions might have in other Latin American countries? How do you see the future of these tensions? Are there any ways we can move forward?

Amie Stepanovich: I think the first thing to consider is that shutdowns of websites and services violate human rights. And one of the things that we need to think about is that maybe shutdowns aren't the way to deal with some of the issues that need to be dealt with, that there are other paths to do this. Shutdowns tend to be fairly easy, but they also tend to be very broad, and affect a lot of users and a lot of legitimate speech. So if you pass a law on this issue, other than a prohibition, even if it provides some standards, you are blessing the practice across the board. And that can really be a slippery slope toward undermining human rights and allowing for a lot of legitimate content to be shut down.

¹⁵ Ver KIRA, Beatriz. "Em busca de uma bala de prata: Congresso analisa projetos sobre bloqueios de sites e aplicativos", in: bloqueios.info, 02 de dezembro de 2016, disponível em: <http://bloqueios.info/pt/em-busca-de-uma-bala-de-prata/>.

¹⁶ See KIRA, Beatriz. "Finding a 'silver bullet': Brazilian Congress analyses draft bills about website and application blockings", in: apblocking.info, December 2nd, 2016, available in: <http://bloqueios.info/en/finding-a-silver-bullet/>.

um caminho realmente perigoso em direção ao comprometimento dos direitos humanos e permitirá que muitos conteúdos legítimos sejam tirados do ar.

Eu acho que o Brasil tem mostrado muita liderança no mundo dos direitos digitais. O Marco Civil da Internet [Lei 12965/2014] foi mundialmente revolucionário ao aplicar os direitos humanos tradicionais no mundo digital. E então eu acho que há muito espaço aqui para o Brasil seguir com essa liderança e proibir esse tipo de bloqueio.

Um dos países mais notórios por seus bloqueios é a Turquia, que já tirou o Twitter do ar em diversas ocasiões e proibiu alguns discursos. Eu diria que o Brasil é um forte concorrente, com os seus bloqueios do WhatsApp, e está tentando ganhar a competição em termos do número total de vezes que um único serviço pode ser bloqueado. Eu acho que isso é ruim para os usuários de uma maneira geral.

Então talvez isso não seja algo que nós devemos recepcionar com uma lei, mas sim deixar mais claro que isso é proibido sob a lei em vigor. Há um argumento de que o Marco Civil não permite bloqueios de serviços como um todo, apenas partes deles, de acordo com o dispositivo do artigo 12, e eu acho que esse é um argumento com mérito legal. Eu acho que seguir nessa direção pode ser um caminho positivo

I do think Brazil has shown a lot of leadership in the world of digital rights. Globally the Marco Civil [Brazilian Internet Civil Rights Framework] was revolutionary in applying traditional human rights in the digital world. And so I think there's a lot of space here for Brazil to continue that lead and to prohibit this type of blocking.

One of the countries that is most notorious for blocking is Turkey, which has shut down Twitter on several occasions and prevented that speech from taking place. I would argue that Brazil is competing with its shutdowns of WhatsApp and trying to elbow in on the sheer number of times a single service can be shut down. I think that that is bad for users across the board as well.

So maybe it is not something that we should be blessing with a law, as much as clarifying that it is prohibited under current law. There is an argument that the Marco Civil does not allow for full services to be shut down, only pieces of them, under the article 12 provision, and I think that is a legally merited argument. I think moving in that direction might be a positive way to go.

