lavits ****** 2017
5to Simposio Internacional LAVITS
Vigilancia, Democracia y Privacidad
en América Latina: Vulnerabilidades y resistencias

ISSN 2175-9596

PRIVACIDADE E MONITORAMENTO DE JORNALISTAS: RISCOS DIGITAIS PROFISSIONAIS NO BRASIL E MÉXICO ENTRE 2001 E 2006

Privacidad y monitoreo de periodistas: riesgos digitales profesionales en Brasil y México entre 2001 y 2016

Privacy and monitoring of journalists: professional digital risks in Brazil and Mexico between 2001 and 2016

Rogério Christofoletti[a]
Ricardo José Torres[b]

[(a)] Universidade Federal de Santa Catarina (UFSC). E-mail: rogerio.christofoletti@ufsc.br.
[(b)] Universidade Federal de Santa Catarina (UFSC). E-mail: rickjtorres@hotmail.com.

Resumo

Os dois países mais ricos e populosos da América Latina são também os que oferecem maior risco para os jornalistas na região. Relatórios de monitoramento de organizações não-governamentais mostram mortes, prisões e outras ameaças no Brasil e México, e muitos desses crimes têm ficado impunes. O contexto de hiperconectividade, vigilância massiva e disseminação de técnicas de controle cada vez mais intrusivas alertam para outros riscos para os jornalistas, que violam seus direitos digitais. O recente episódio "Gobierno Espía", no México, é um exemplo. Para discutir o tema, analisamos 80 relatórios sobre agressões a jornalistas e ataques à liberdade de imprensa de nove organizações. A análise compreende o período 2001-2016, e tenta responder se constam da amostra riscos como vigilância, espionagem e violação à privacidade e como essas ameaças podem ser caracterizadas na região. A pouca visibilidade desses riscos e a insuficiência no enfrentamento do problema estão entre os resultados encontrados.
Palavras-chave: Vigilância; Jornalistas; Riscos Digitais; Brasil; México.

Resumen

Los dos países más ricos y populosos de América Latina son también los que ofrecen mayor riesgo para los periodistas en la región. Los informes de monitoreo de organizaciones no gubernamentales muestran muertes, arrestos y otras amenazas en Brasil y México, y muchos de

estos crímenes han quedado impunes. El contexto de hiperconectividad, vigilancia masiva y diseminación de técnicas de control cada vez más intrusivas advierte a otros riesgos para los periodistas. El reciente episodio "Gobierno Espía", en México, es un ejemplo. Para discutir el tema, analizamos 80 informes sobre agresiones a periodistas y ataques a la libertad de prensa de nueve organizaciones. El análisis abarca el período 2001-2016, e intenta responder si se incluyen en la muestra riesgos como vigilancia, espionaje y violación a la privacidad y cómo estas amenazas pueden ser caracterizadas en la región. La poca visibilidad de estos riesgos y la insuficiencia en el enfrentamiento del problema están entre los resultados encontrados.
Palabras clave: *Vigilancia; Periodistas; Riesgos Digitales; Brasil; México.*

Abstract

The two richest and most populous countries in Latin America are also the ones that pose the greatest risk to journalists in the region. Monitoring reports from nongovernmental organizations show deaths, arrests and other threats in Brazil and Mexico, and many of these crimes have gone unpunished. The context of hyper-connectivity, mass surveillance and the spread of increasingly intrusive control techniques warn of other risks to journalists who violate their digital rights. The recent episode "Gobierno Espía", in Mexico, is an example. To discuss the issue, we have analyzed 80 reports of assaults on journalists and attacks on press freedom in nine organizations. The analysis covers the period 2001-2016, and attempts to respond if risks, such as surveillance, espionage, and privacy breaches are included in the sample, and how these threats can be characterized in the region. The low visibility of these risks and the insufficiency in facing the problem are among the results found.
Keywords: *Surveillance; Journalists; Digital Risks; Brazil; Mexico.*

INTRODUÇÃO

As denúncias de espionagem massiva e monitoramento global de Edward Snowden em 2013 chamaram a atenção para o gigantesco aparato técnico da National Agency of Security (NSA) e seus parceiros estrangeiros e corporativos. A nova situação alarmou autoridades, sistemas de regulação, ativistas e usuários em geral.

Para alguns grupos, como os jornalistas, é mais aguda e perigosa a violação da privacidade e segurança digital. Se repórteres se sentirem vigiados, muito possivelmente recuarão em suas investigações, e muito provavelmente o público não terá informações de seu interesse. É verdade que as revelações de Snowden não tratam de ações para controlar jornalistas, mas chega a ser irônico que um dos países cujo chefe foi monitorado pela NSA seja alvo de denúncias desse tipo. Em junho de 2017, um grupo de jornalistas acusou o governo mexicano de usar um *software* para espionar seus celulares. Enrique Peña Nieto negou a ação, e o episódio – ainda sem desfecho – passou a ser

conhecido como Gobierno Espía[1].

Relatório[2] divulgado pela Red en Defensa de los Derechos Digitales, SocialTIC e Article 19 México y Centroamérica detalhou as tentativas de infecção por meio do *malware* Pegasus e que afetaram seis jornalistas. Especialistas demonstraram que o *hacking* vincula o governo nas ações de vigilância comunicacional. Segundo The New York Times[3], pelo menos três agências federais mexicanas investiram 80 milhões de dólares em *softwares* de espionagem da empresa israelense NSO Group que produz o Pegasus. A própria empresa assegura que seus produtos são vendidos exclusivamente para

governos e operacionalizados por agências governamentais autorizadas.

Pegasus possibilita acesso remoto a telefones celulares a partir de links que expõem o sistema operacional dos dispositivos tendo grande capacidade invasiva, praticamente irrestrita, e em tempo real. Os ataques ocorreram entre janeiro de 2015 e julho de 2016 e as vulnerabilidades afetam, particularmente, a capacidade investigativa do jornalismo.

O caso é mais um na escalada da violência contra jornalistas no México, apontado como um dos locais mais perigosos para se exercer a profissão. No continente americano, o segundo país a oferecer mais riscos é o Brasil. Até o momento, não há evidências de que estejam em curso programas de espionagem nas redações, mas além de características econômicas ou demográficas, o histórico de impunidade em crimes contra esses profissionais aproximam os dois países. A observação sistemática dessas agressões se concentra, sobretudo, no registro de mortes, agressões e prisões. Ameaças à privacidade e à segurança informacional são ainda pouco conhecidas e discutidas.

Brasil e México têm os maiores PIBs da América Latina e também são os mais populosos. Nona maior do planeta, a economia brasileira movimentou mais de 1,7 trilhão de dólares em 2015, e a mexicana, quase 1,2 trilhão, conforme dados do Fundo Monetário Internacional. Órgãos oficiais

[1] Ver mais em: https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje; em: https://www.projectpoder.org/es/2017/06/gobierno-espia-la-vigilancia-sistematica-en-contra-de-periodistas-y-defensores-de-derechos-humanos-en-mexico; e em: http://aristeguinoticias.com/tag/gobiernoespia. Todos recuperados em 12 de setembro de 2017.
[2] Disponível em: https://r3d.mx/gobiernoespia. Recuperado em 17 de setembro de 2017.
[3] Disponível em: https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/?mcubz=1. Recuperado em 17 de setembro de 2017.

estimam populações nas casas dos 207 milhões e 121 milhões, respectivamente, que – somadas – equivalem a mais da metade dos habitantes da América Latina. Apesar disso, a dupla não tem o que celebrar quando se trata de indicadores de liberdade de imprensa. De acordo com os Repórteres Sem Fronteiras, em 2016, o México ocupou a 149ª posição entre 180 países em termos de segurança para jornalistas. No mesmo ano, o Brasil ficou em 104º lugar. Nos últimos anos, têm sido os locais mais perigosos do subcontinente para se atuar[4], onde há mortes, agressões, perseguições e impunidade nos crimes contra jornalistas.

ATAQUES DIGITAIS CONTRA JORNALISTAS

Diversas organizações monitoram violações a direitos e casos de violência contra jornalistas. O registro e o relatório dessas agressões auxiliam na composição de uma paisagem dos constrangimentos, cerceamentos e impedimentos ao livre exercício jornalístico, e que se desdobram ainda em danos para a cidadania e a democracia. Desde o final do século passado, mudanças tecnológicas e culturais tornaram ainda mais complexa a tarefa de caracterizar segurança e liberdade dos jornalistas. Digitalização da informação e explosão na difusão dos dados consagraram a internet como plataforma de comunicação e informação. Ameaças antes presentes apenas na vida tangível tiveram seus derivados no espelho online, o que nos leva a defender que riscos digitais deveriam ser considerados também como formas de violência contra jornalistas em relatórios sobre liberdade de imprensa. À medida que esses perigos atualizam ações contra o jornalismo, e à medida que impactam na qualidade, diversidade, pluralidade e integridade das informações, por que não identificá-los e quantificá-los?

Afirmamos que riscos digitais são perigos mais extensivos que os demais. Nem todo repórter atua em zona de conflito ou arrisca a vida, mas não há jornalista que não use computadores, smartphones, internet ou sistemas de informação em seu cotidiano. Jornalistas estão mais suscetíveis a riscos digitais que a físicos, independentemente de sua geografia, influência social, posição ou área a que se dedicam. Riscos digitais envolvem perigo real ou imediato, ameaça ou vulnerabilidade. A exemplo de outros tipos, são condições mais ou menos previsíveis de perda ou dano, e podem, por isso, ser detectadas, evitadas ou combatidas.

[4] Cuba e Venezuela também têm sido acompanhadas de perto por esses monitoramentos.

Esses riscos podem ser originados em três planos: ambiental, de manejo e de interação. Quando a redação, local de trabalho ou domicílio podem sofrer espionagem, monitoramento indevido ou ameaças à privacidade e à segurança desses profissionais, pode-se dizer que os riscos digitais estão concentrados no ambiente. Quando *devices* ou *gadgets* dos jornalistas servem de porta de entrada para ameaças à privacidade e à segurança profissional, pode-se afirmar que os riscos são derivados do manejo desses equipamentos. Quando rotinas, costumes, relacionamentos e trocas simbólicas podem permitir ameaças e danos, pode-se dizer que os riscos digitais são produtos da interação. Essa caracterização mostra a multiplicidade das potenciais vulnerabilidades.

Riscos digitais podem levar a ataques digitais, entendidos aqui como agressões ou violações no ciberespaço ou em situação de interação digital que coloquem em perigo o acesso, a integridade e a privacidade de informações, fontes e autores de produtos jornalísticos. Tais ataques objetivam interceptar, monitorar, extraviar, degradar, deteriorar, inutilizar, destruir ou divulgar sem autorização trechos de informação, identidades, localidades e outros dados sensíveis que podem contribuir para riscos físicos ou danos morais e materiais. Listamos 19 tipos.

Tabela 1

Tipos de Ataques Digitais
ETT - Escutas telefônicas sem autorização na redação ou local de trabalho; ETC - Escutas telefônicas sem autorização na casa do jornalista ou em seu telefone celular/smartphone; ICT - Instalação não autorizada de câmeras ou microfones na redação/local de trabalho;
ICC - Instalação não autorizada de câmeras ou microfones na casa do jornalista;
AT- Ameaças por telefone;
AS - Ameaças por SMS (*Short Message Service*: Serviço de Mensagens Curtas, em português);
VE- Violação ou interceptação de e-mail funcional ou pessoal do jornalista;
VIM - Violação ou interceptação de mensagens instantâneas (WhatsApp, Signal ou Telegram);
CN - Coleta de dados e histórico de navegação;
IVM - Instalação e ativação de vírus, *malware* ou código malicioso para coleta ou destruição de arquivos;
FPP - Furto de senhas por meio de *phishing* ou *pharming:* formas de fraude online para pescar dados do usuário.
MNT - Monitoramento de navegação em tempo real; VSR - Violação e invasão de sistemas nas redações;
FEI - Furto ou extravio de arquivos ou informações;
QC - Quebra de criptografia de mensagens ou arquivos; ARS - Ameaças em redes sociais; VCP - Violação de contas pessoais na internet; AE - Ameaças por e-mail; DMA - Descuidos de manutenção e/ou não atualização de antivírus ou sistemas de segurança digital.

Rogério Christofoletti e Ricardo José Torres: Tipos de Ataques Digitais. 2017.

A bibliografia sobre cibersegurança é vasta na computação e a dirigida a jornalistas cresce em proporção geométrica. São cartilhas ou manuais que recomendam modificar condutas, adotar práticas preventivas, reduzir vulnerabilidades e aumentar medidas protetivas [Ochoa (2013), Carlo & Kamphuis (2014), Dagan (2017)]. Organizações também formulam seus guias, a exemplo de Flip (2015), Committee for Journalist Protection (2012), Artículo 19 (2013), International Center For Journalists e Freedom House (SIERRA, 2013), Repórteres Sem Fronteiras (2017).

Para identificar e avaliar os ataques digitais a jornalistas no Brasil e México, recorremos a uma amostra de 80 relatórios de nove organizações entre 2001 e 2016. Na amostra, a organização-autora deve ter reconhecido público, nacional ou internacional; os *reports* devem oferecer dados sobre liberdade de expressão/imprensa e sobre riscos à segurança; os documentos devem ter produção e circulação seriada prioritariamente; e podem abranger as realidades específicas de Brasil e/ou México, ou contextos globais.

Tabela 2

Documento	**Origem**	**Quant.**	**Período**
Relatório sobre Liberdade de Imprensa no Brasil	Associação Nacional dos Jornais (ANJ)	08	2004-2016
Relatório Violência e Liberdade de Imprensa	Federação Nacional dos Jornalistas (Fenaj)	12	2001; 2005-2016
Report Freedom of the Press	Freedom House	15	2002-2016
La Libertad de Información en el mundo	Repórteres Sem Fronteiras (RSF)	06	2009-2014
Report on Journalists Killed	International Federation of Journalists	12	2001-2013
Annual Report	Comite de Proteção aos Jornalistas (CPJ)	06	2011-2016
Relatório Violações à Liberdade de Expressão	Artigo 19 – Brasil	04	2013-2016
Graves violações à liberdade de expressão de jornalistas e defensores dos direitos humanos	Artigo 19 – Brasil	01	2012
Libertad de Prensa en México	Artigo 19 – México	01	2008
Agresiones contra la libertad de expression	Artigo 19 – México	01	2009
Liberdade de Imprensa no Brasil	As. Bras. Emissoras de Rádio e TV (Abert)	10	2007-2016
Informe Especial sobre La Liberdad de Prensa en Mexico	Relatoria Especial de Liberdade de Expressão da Comissão Interamericana de Direitos Humanos (CIDH) da Organização dos Estados Americanos (OEA)	01	2010
Liberdade de imprensa nas Américas	Idem	02	2008;2013
Liberdade de Expressão no Brasil	Idem	01	2005-2015

Rogério Christofoletti e Ricardo José Torres: Amostra da pesquisa. 2017.

Para analisar a amostra, desenvolvemos um protocolo de pesquisa específico.

Tabela 3

Questões centrais analisadas a) Os ataques digitais da Tabela 10 são inventariados nos reports das ONGs mencionados acima? b) Qual a sua taxa de ocorrência? c) Como eles são caracterizados?		
Etapa 1: Extrato de cada relatório.	**Etapa 2:** Extrato por organização.	**Etapa 3:** Consolidação dos dados.
Como fizemos: Análise dos casos. Relato e tipificação.	**Como fizemos:** Avaliação e sistematização.	**Como fizemos:** Avaliação e compilação dos dados.

Rogério Christofoletti e Ricardo José Torres: Protocolo de pesquisa. 2017.

A primeira leitura aponta para variação de formatos e estrutura dos documentos, fatores que dificultam a identificação imediata de ataques digitais e que – com isso – reduzem seu peso e importância no contexto de ameaça aos jornalistas. De forma predominante, riscos não estão alinhados ao ecossistema digital. No mundo todo, foram identificados 452 ataques, de 19 tipos, nos 15 anos de período observado.

Apenas três modalidades não foram reportadas: instalação não-autorizada de câmeras ou microfones na redação/local de trabalho (ICT), na casa do jornalista (ICC) e descuidos de manutenção e/ou não-atualização de antivírus ou sistemas de segurança digital.

Brasil e México tiveram 137 casos. No primeiro, foram 119, frequentemente de riscos à integridade física e ofensas. As ameaças e constrangimentos em mídias sociais (ARS) apareceram 49 vezes. Emerge em alguns documentos uma preocupação com a formatação de grupos que empregam o que podemos chamar de "vigilância digital odiosa". Esses grupos realizam campanhas que questionam o trabalho e ameaçam a integridade física e a vida dos jornalistas. No México, os episódios mais visíveis ratificaram a importância de medidas de prevenção, detecção e impedimento de ações abusivas de vigilância comunicacional. Como no Brasil, os ataques mais comuns eram ameaças à integridade física. Violência, muitas mortes e alto risco são destacados nos relatórios. A recorrência tem contribuído para uma atmosfera de intimidação.

Nos 39 relatórios globais, Brasil e México são tratados como locais com riscos significativos para a prática jornalística. Mapeamos poucos registros de ataques digitais nas publicações gerais: no Brasil, ETC (1), ETT (1), AT (3); no México, ARS (2), AT (4), AE (1), AS (1). Para a Freedom House, o México deixou de ser classificado como "parcialmente livre" em 2011 para ser "não livre". De modo geral, os relatórios globais ressaltam que o México apresenta violência endêmica, riscos nítidos para a atuação jornalística e redução na liberdade de expressão por meio de dispositivos regulatórios intrusivos. No Brasil, observa-se aumento exponencial de formas de repressão da atividade jornalística e cresce o número de mortes. O Marco Civil da Internet (2014) aparece como importante instrumento regulatório alinhado à privacidade e à liberdade de expressão, mas parcialmente regulamentado.

Esta pesquisa atendeu a dois objetivos, sendo o primeiro permitir uma aproximação da problemática dos riscos digitais para jornalistas, assunto ainda tratado de forma superficial pelas organizações de notícia, jornalistas e autoridades que devem enfrentar e coibir crime e violência. O segundo objetivo foi o de propor definições de riscos e ataques digitais.

Indícios concretos apontam que órgãos do Estado e corporações monitoram as comunicações eletrônicas de jornalistas em diferentes partes do mundo sem supervisão judicial. Propomos a identificação do problema e implicações relacionadas à vigilância e sugerimos o monitoramento de

situações que denotem abusos e ataques, e medidas de visibilidade dos riscos que envolvem a privacidade dos jornalistas. Queremos apontar a necessidade urgente de manter "zonas de atuação seguras" para o exercício do jornalismo na internet e a importância de condutas de precaução para preservação de liberdades ligadas a privacidade comunicacional dos jornalistas.

REFERÊNCIAS

Artículo 19 (2013). *Guía de Seguridad digital y de la información para periodistas* [documento online]. Recuperado em 17 de setembro de 2017 de http://coberturaderiesgo.articulo19.org/wp-content/uploads/2013/07/guia_seguridad_digital.pdf.

Carlo, S., & Kamphuis, A. (2014). *Information Security for Journalists*. London: The Centre for Investigative Journalism.

Committee for Journalist Protection (2012). Seguridad de la información. *Manual de Seguridad para Periodistas* [documento online]. Recuperado em 17 de setembro de 2017 de https://www.cpj.org/es/2012/04/seguridad-de-la-informacin.php.

Dagan, M. (2017). Online privacy for journalists: a must-have guide for journalism in 2017. *vpnMentor*. Recuperado em 17 de setembro de 2017 de https://www.vpnmentor.com/journalist-privacy-guide.pdf.

Fundación para la Libertad de Prensa (2015, abril 21). *Manual Antiespías:* herramientas para la protección digital de periodistas. Recuperado em 17 de setembro de 2017 de https://flip.org.co/index.php/es/publicaciones/manuales/item/1767-manual-antiespias-herramientas-para-la-proteccion-digital-de-periodistas.

Ochoa, P. P. (2013). ¿Cómo funciona Internet? Nodos críticos desde una perspectiva de los derechos. *Guía para periodistas*. Santiago de Chile: ONG Derechos Digitales. Recuperado em 12 de setembro de 2017 de https://www.derechosdigitales.org/wp-content/uploads/Comofunciona-internet-ebook.pdf.

Repórteres sem Fronteiras (2017). *Censura e vigilância de jornalistas: um negócio sem escrúpulos* [documento online]. Recuperado em 17 de setembro de 2017 de https://rsf.org/sites/default/files/rapport_cs_pt_v2-2.pdf.

Sierra, J. L. (2013). Manual de seguridad digital y móvil para periodistas y blogueros. *International Center for Journalists & Freedom House*. Recuperado em 12 de setembro de 2017 de https://goo.gl/cNfstC.