Revista Famecos
mídia, cultura e tecnologia

ISSN: 1415-0549
e-ISSN: 1980-3729

DOI: http://dx.doi.org/10.15448/1980-3729.2018.3.29210

JORNALISMO

Jornalistas expostos e vulneráveis: ataques digitais como modalidade de risco profissional[1]

Journalists exposed and vulnerable: digital attacks as a form of professional risk

Rogério Christofoletti
Professor do Programa de Pós-Graduação em Jornalismo da Universidade Federal de Santa Catarina, Florianópolis, SC, Brasil
Orcid: 0000-0003-1065-4764
<rogerio.christofoletti@uol.com.br>

Ricardo José Torres
Doutorando no Programa de Pós-Graduação em Jornalismo da Universidade Federal de Santa Catarina, Florianópolis, SC, Brasil
Orcid: 0000-0001-5288-6550
<rickjtorres@hotmail.com>

Como citar este artigo (How to cite this article):

CHRISTOFOLETTI, Rogério; TORRES, Ricardo T. Jornalistas expostos e vulneráveis: ataques digitais como modalidade de risco profissional. **Revista Famecos**, Porto Alegre, v. 25, n. 3, p. x-xx, setembro, outubro, novembro e dezembro de 2018: ID29210. DOI: http://dx.doi.org/10.15448/1980-3729.2018.3.29210.

RESUMO

O jornalismo é uma atividade de risco, e seu exercício pode afetar a integridade física, a saúde mental e a convivência social e profissional. Outros recentes perigos do ecossistema digital se somam às agressões físicas, mortes e perseguições. É preciso, no entanto, observar o avanço de casos de invasão de privacidade, vigilância e outras violações. Pode-se dizer que existem riscos digitais para a atividade jornalística? De que tipos e como se caracterizam? Para responder, recorremos às pesquisas bibliográfica e documental. Analisamos 80 relatórios sobre agressões a jornalistas e ataques à liberdade de imprensa de nove organizações não-governamentais. São documentos reconhecidos pela categoria e indústria, e que permitem a formulação de políticas para o setor e o aperfeiçoamento do mercado. O corpus cobre o período 2001-2016, e sua análise é feita a partir de categorias de ataques que elaboramos a partir da bibliografia na área. Ao final, com a definição de risco digital que sugerimos e a descrição desses ataques, objetivamos contribuir para a sensibilização a essas novas ameaças.

Palavras-chave: Riscos Digitais. Vigilância comunicacional. Privacidade de jornalistas.

ABSTRACT

Journalism is a risky activity, and its exercise can affect physical integrity, mental health and social and professional coexistence. Other recent dangers of the digital ecosystem add to physical aggression, death and persecution. However, it is necessary to watch cases of invasion of privacy, surveillance and other violations. Can we say that there are digital risks to the journalistic activity? What types? How are they works? To answer, we resorted to bibliographical and documentary research. We have analyzed 80 reports of attacks on journalists and attacks on press freedom from nine NGO. They are reports recognized by journalists and media, and that allow the formulation of policies for the sector and the improvement of the market. The corpus covers the period 2001-2016, and its analysis is made from categories of attacks that we elaborate from the bibliography in the area. In the end, with the definition of digital risk that we suggest and the description of these attacks, we aim to contribute to raising awareness of these new threats.

Keywords: Digital Risks. Surveillance of communications. Privacy of journalists.

1 Este artigo é produto da pesquisa "Privacidade e Jornalismo: atualizações de conceitos, dilemas e entornos", com financiamento do CNPq, desenvolvida pelo primeiro autor, e é também parte das reflexões da tese de doutoramento do segundo autor. Resultados parciais foram apresentados sob a

Introdução

As revelações de Edward Snowden sobre os programas e as ações de vigilância massiva global da National Security Agency (NSA) e seus parceiros governamentais e corporativos são paradigmáticas não apenas pelo seu alcance, mas também pela ousadia. Após julho de 2013, vieram à tona as informações de que os Estados Unidos não só bisbilhotavam cidadãos comuns dentro e fora de suas fronteiras, mas espionavam grandes empresas, como a Petrobras, e seguiam os passos de chefes de Estado, como a chanceler alemã Angela Merkel e presidentes da república, como Dilma Rousseff (Brasil) e Enrique Peña Nieto (México).

O esquema denunciado escandalizou o planeta dadas as condições assimétricas que tornavam essa máquina de espionagem tão poderosa quanto descontrolada. As evidências mostraram que a NSA extrapolava suas funções de origem e transgredia os limites constitucionais. Conforme mostrado, sua atuação levava a vantagens comerciais inéditas em algumas disputas e o monitoramento de governantes violava tratados e a própria soberania digital de outros países (Greenwald, 2014; Harding, 2014). Sob a ordem de "coletar tudo de todos", a estratégia dava a seus comandantes poderes inéditos, quase preditivos nas arenas econômica, política, militar e social.

Apesar de assustador, o episódio causou turbulências internacionais momentâneas, protocolares apenas. Nenhuma atitude prática foi tomada para reduzir o ímpeto intrusivo de seus operadores, nenhuma mudança de postura foi efetivada diante da comunidade internacional. A espionagem não terminou e nem os esforços de coleta massiva de dados foi descontinuado. Após as revelações de Snowden, a sensação generalizada de insegurança tecnológica só aumentou, e as noções de privacidade e intimidade encolheram ainda mais no imaginário coletivo.

Para alguns grupos sociais, como os jornalistas, é mais aguda e perigosa a violação dos direitos de reserva e autopreservação. Se repórteres se sentirem espionados, vigiados ou monitorados, muito possivelmente recuarão em suas investigações, e muito provavelmente o público não terá acesso a informações de seu interesse. As revelações de Snowden não tratam especificamente 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 críticos acusou o governo mexicano de usar um

forma de resumo expandido no 5º Simpósio Internacional da Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade (Lavits), no Chile, em novembro de 2017.

software para espionar seus celulares. Peña Nieto negou a ação, e o episódio – ainda sem desfecho – passou a ser conhecido como *Gobierno Espía*[2].

Um relatório intitulado GOBIERNO ESPÍA - Vigilancia sistemática a periodistas y defensores de derechos humanos en México (2017), divulgado por três organizações não-governamentais mexicanas (Red en Defensa de los Derechos Digitales, SocialTIC e Article 19 México y Centroamérica), em junho de 2017, detalhou as tentativas de infecção por meio do *malware* Pegasus, afetando seis jornalistas mexicanos. Evidências contundentes de especialistas demonstraram que o *hacking* ratifica o envolvimento do governo nas ações de vigilância comunicacional. Segundo *The New York Times (2017)*, 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 fabricante assegura que seus produtos são vendidos exclusivamente para governos e operacionalizados por agências governamentais autorizadas.

O programa Pegasus possibilita o acesso remoto a telefones celulares a partir de links que expõem o sistema operacional dos dispositivos tendo uma capacidade invasiva praticamente irrestrita, em tempo real, a dados como contatos, mensagens, microfones e câmeras. Os ataques que ocorreram entre janeiro de 2015 e julho de 2016 demonstraram vulnerabilidades que afetam, particularmente, a capacidade investigativa da atividade jornalística.

O caso é mais uma gota que transborda o copo da violência contra jornalistas no México, apontado como um dos países mais perigosos para se exercer a profissão no mundo. No continente americano, o segundo país que mais oferece riscos a repórteres e comunicadores é o Brasil, mas outras nações também preocupam e têm situação pior quando o assunto é liberdade de imprensa/condições de exercício pleno do jornalismo (Mioli, 2017)[3]. Em novembro de 2017, o "Barômetro" dos Repórteres Sem Fronteiras indicava que Coreia do Norte, Eritreia, Turcomenistão, Síria e China eram os piores países para jornalistas em 180 pesquisados. Pelo que se percebe geograficamente, Ásia, África e América Latina são regiões explosivas, mas há que se ressaltar que os monitoramentos das atividades priorizam agressões físicas, mortes, prisões e perseguições. Outros perigos afetam o cotidiano dos jornalistas?

2 Ver mais em: https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/; https://www.projectpoder.org/es/2017/06/gobierno-espia-la-vigilancia-sistematica-en-contra-de-periodistas-y-defensores-de-derechos-humanos-en-mexico/ e http://aristeguinoticias.com/tag/gobiernoespia/

3 No 10º Índice Anual de Impunidade Global, do Comitê de Proteção aos Jornalistas, Brasil e México estão também entre os países que menos solucionam e punem crimes contra esses profissionais no mundo.

Alta exposição e riscos invisíveis

O jornalismo é uma atividade de alta exposição. Para obter informações necessárias para seus relatos cotidianos, jornalistas transitam por zonas e situações de confronto, lidam com personagens perigosos e ficam sujeitos a condições insalubres, exaustivas e estressantes. Jornalistas exploram a lógica adversarial de pessoas e grupos poderosos e, muitas vezes, ficam na linha tiro que as separa. A exposição pública e o contato com ameaças diversas tornam a profissão tão fascinante quanto arriscada.

Por essa razão também, diversas organizações não-governamentais classistas e humanitárias monitoram violações a direitos e casos de violência contra jornalistas em suas atividades profissionais. Registro e relatório dessas agressões auxiliam na composição de uma paisagem dos constrangimentos, cerceamentos e impedimentos que ameaçam o livre e pleno exercício jornalístico, e que se desdobram ainda em danos para a cidadania e a democracia. Inventariar os atentados à vida e à integridade física desses profissionais é fundamental para aferir aspectos voláteis como liberdade de expressão e de imprensa, autonomia e independência editorial, solidez e consistência democrática.

Desde o final do século passado, as mudanças tecnológicas e culturais tornaram ainda mais complexa a tarefa de caracterizar segurança e liberdade dos jornalistas. Digitalização da informação e descentralização de bancos de dados consagraram a internet como plataforma de comunicação e informação. A popularização de equipamentos que ampliam o tempo e a experiência de conexão contribuiu para a hiperconectividade (Jenkins, Ford e Green, 2014), a multimidialidade (Salaverría, 2014) a ubiquidade (Pavlik, 2014) e a ampliação da vida digital. Todos os quadrantes da experiência humana sofreram modificações, inclusive o jornalismo. Ameaças antes presentes apenas na vida tangível tiveram seus derivados no espelho on-line, 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 (novos) perigos atualizam ações que violentam a prática jornalística, e à medida que impactam na qualidade, diversidade, pluralidade e integridade das informações, por que não os identificar, os caracterizar e os quantificar?

Há que se lembrar ainda que os riscos digitais são perigos mais extensivos que os demais, já acompanhados pelas ONGs que militam na área. Isto é: nem todo repórter atua em zona de conflito ou arrisca a vida, mas não há jornalista que não utilize computadores, *smartphones*, internet ou sistemas de informação em seu cotidiano. Nem todo repórter é perseguido politicamente, mas todo jornalista está potencialmente exposto a ser monitorado, espionado ou *hackeado*, seja dentro ou fora das redações. Em resumo: jornalistas estão mais

suscetíveis a riscos digitais que a físicos, independentemente de sua geografia, influência social, posição na hierarquia empresarial ou área a que se dedicam.

Riscos digitais envolvem perigo real ou imediato, e sinalizam condições de vulnerabilidade. A exemplo de outros tipos de risco, são condições mais ou menos previsíveis de perda ou dano, e podem, por isso, ser detectadas, evitadas ou combatidas. Na nossa concepção, esses riscos podem ser originados em três planos: ambiental, de manejo e de interação. Quando a redação, o local de trabalho ou o domicílio dos jornalistas sofrem espionagem, monitoramento indevido ou outras ameaças à privacidade e à segurança desses profissionais, pode-se dizer que os riscos digitais estão concentrados no ambiente. Quando *devices* ou *gadgets* usados pelos jornalistas servem de porta de entrada para ameaças à sua privacidade e à segurança profissional, pode-se afirmar que os riscos são derivados do manejo desses equipamentos. Quando rotinas, costumes, relacionamentos e trocas simbólicas com sujeitos, sistemas e organizações permitem ameaças e danos, pode-se dizer que os riscos digitais são produtos da interação. Essa nossa caracterização mostra a multiplicidade dos pontos potencialmente vulneráveis.

Vale notar que o risco não é quantificável, já que ele é mais circunstância e contexto, e não ocorrência. Mas riscos digitais podem resultar em ataques digitais, esses, sim, passíveis de identificação, registro, tipificação e contabilidade. Entendemos ataques digitais 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. Esses 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.

Em situações práticas que potencialmente afetam rotinas jornalísticas, esses ataques são percebidos conforme a Tabela 1:

Tabela 1 - Tipos de Ataques Digitais

Escutas telefônicas sem autorização na redação ou local de trabalho
Escutas telefônicas sem autorização na casa do jornalista ou em seu telefone celular/smartphone
Instalação não autorizada de câmeras ou microfones na redação/local de trabalho
Instalação não autorizada de câmeras ou microfones na casa do jornalista
meaças por telefone
Ameaças por SMS (*Short Message Service*: Serviço de Mensagens Curtas, em português)
iolação ou interceptação de e-mail funcional ou pessoal do jornalista
· Violação ou interceptação de mensagens instantâneas (WhatsApp, Signal ou Telegram)
Coleta de dados e histórico de navegação
Instalação e ativação de vírus, *malware* ou código malicioso para coleta ou destruição de arquivos
Furto de senhas por meio de *phishing* ou *pharming*
- Monitoramento de navegação em tempo real
· Violação e invasão de sistemas nas redações
Furto ou extravio de arquivos ou informações
Quebra de criptografia de mensagens ou arquivos
· Ameaças em redes sociais
· Violação de contas pessoais na internet
Ameaças por e-mail
- Descuidos de manutenção e/ou não atualização de antivírus ou sistemas de segurança digital.

Fonte: Categorias elaboradas a partir de Artículo 19 (2013), Carlo e Kamphuis (2014), Sierra (2013).

A bibliografia sobre cibersegurança é vasta na informática e tem se espalhado também na forma de referências para usuários não-especializados. Moore (2016) e Taylor e outros (2017) são alguns exemplos mais recentes. Estudos sobre as implicações da vigilância na sociedade e na atividade jornalística também vêm sendo realizados por diferentes autores em diversas perspectivas como: Bauman e Lyon (2014), Bauman e outros (2015), Marx (2016), Lyon (2017), Bell e Owen (2017). Cabe destacar, que quando tratamos do conceito de vigilância nesse estudo, nos reportamos à possibilidade de intrusão das comunicações, interceptação e armazenamento de dados pessoais e ao monitoramento de ações jornalísticas.

As obras sobre quebra de privacidade e necessidade de aumento da segurança digital dirigidas a jornalistas também têm surgido no mercado editorial com mais vigor nos últimos anos. Elas tratam do fenômeno dos *whistleblowers* e dos grandes vazamentos de informação (Greenberg, 2012; Brevini e outros, 2013; Goldfarb, 2015; Ruby e outros, 2017) e passam ainda pelo desenvolvimento de habilidades digitais específicas para incremento da segurança pessoal dos profissionais e das próprias fontes de informação (Büchi e outros, 2016; Bradshaw, 2017; Wasserman, 2017). Para efeitos deste artigo, seguimos as perspectivas de Nissebaum (2010), Martins (2013), Richards (2015) e McStay (2017) nos estudos sobre privacidade, já sinalizados em Christofoletti (2015; 2017) e Christofoletti e Torres (2017).

Há também um grande volume de referências na forma de cartilhas ou manuais que seguem o "modelo de ameaça", reforçando a necessidade de modificar condutas, adotar práticas preventivas, reduzir vulnerabilidades e aumentar medidas protetivas.

Peña Ochoa (2013) explica a jornalistas como funciona a internet sob a perspectiva de direitos digitais. Carlo e Kamphuis (2014) advertem que as ameaças se modificam com a evolução tecnológica, o que exige de jornalistas entenderem os conceitos de segurança de informação na teoria e nunca deixar de aprender sobre proteção na prática. A Fundación para la Libertad de Prensa, junto com a Organização das Nações Unidas, a Fundação Karisma e os Repórteres Sem Fronteiras elaboraram um manual prático para jornalistas (FLIP, 2015). Outras organizações do mesmo tipo formularam seus documentos: Committee for Journalist Protection (2012), Artículo 19 (2013), International Center For Journalists e Freedom House (Sierra, 2013), Repórteres Sem Fronteiras (2017). Fernandez e Mancini (s/d) enfatizaram a urgência de repórteres praticarem um "criptojornalismo", fundamentado na criptografia como medida de autoproteção e segurança de informações e fontes. Dagan (2017) vai além e enaltece anonimato, mecanismos de buscas mais seguros, etc.

Organizações de mídia decidiram capacitar seus profissionais diante das muitas ameaças enfrentadas diariamente. Na Alemanha, a Deutsche Welle promoveu um workshop em 2013 em sua *Akademia* (Survey Digital, 2017). No Reino Unido, a BBC editou *Editorial Guidelines* (2017) específicas para orientar seus profissionais em aspectos editoriais, de relacionamento com o público e fontes, e prático-operacionais. Ainda na Inglaterra, *The Guardian* – junto com Institute of Advanced Legal Studies da University of London – editaram um documento para instruir seus jornalistas a como proteger fontes e vazadores em contextos digitais (Guardian, 2017).

Amplos, variados, intensos e invisíveis, os riscos digitais permitem ataques digitais que podem comprometer controle e integridade das informações, a proteção pessoal de jornalistas e a de suas fontes. Desta forma, afetam a liberdade de imprensa e a segurança de repórteres, redatores e editores. Esses ataques são inventariados nos *reports* das ONGs que fazem esse monitoramento? Qual a taxa de ocorrência? Como são caracterizados?

Aspectos metodológicos e resultados

Para mapear e avaliar os ataques digitais a jornalistas, vamos recorrer a relatórios produzidos por organizações não-governamentais nacionais e internacionais datados entre 2001 e 2016. A janela de observação compreende 15 anos e cobre as duas primeiras décadas do século, o que nos dá margem para detectar eventuais padrões.

A amostra teve como critérios de escolha: a) A organização responsável pelo documento deve ter reconhecimento público, nacional ou internacional; b) Os *reports* devem oferecer relatos ou estatísticas sobre liberdade de expressão/imprensa e sobre riscos aos jornalistas, sendo considerados perigos físicos, psíquico-emocionais, morais, jurídicos, políticos ou digitais; c) Os documentos devem ter prioritariamente produção e circulação seriada; d) Os relatórios podem abranger as realidades específicas ou contextos globais. Tais critérios permitiram alcançar o volume de 80 documentos de nove organizações, conforme relatado a seguir:

■ Tabela 2 – Amostra da pesquisa

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 :La Sombra de la Impunidad y la Violencia	Artigo 19 – México	01	2008
Agresiones contra la libertad de expression.	Artigo 19 – México	01	2009
Liberdade de Imprensa no Brasil	Associação Brasileira de 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

Fonte: Elaborada pelos autores a partir do corpus de análise

Para analisar a amostra e desenvolver o estudo, utilizamos como método parâmetros da pesquisa documental e da pesquisa bibliográfica, associados à coleta e análise de dados. Para realizar a análise documental, desenvolvemos um protocolo específico (Tabela 3).

Tabela 3 – Protocolo de Pesquisa

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.
Ações: Análise dos casos com avaliação isolada. Tipificação.	**Ações:** Avaliação e sistematização.	**Ações:** Avaliação e compilação dos dados.

Fonte: Elaborada pelos autores

A primeira leitura dos relatórios aponta para variedade nos formatos e na 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, o enquadramento dos riscos não está alinhado ao ecossistema digital. Percebe-se, porém, a ocorrência de situações regulatórias e contextos com alto risco de ameaça e violação das comunicações privadas de jornalistas em diferentes partes.

Para facilitar a identificação de episódios de ataques digitais nos 80 relatórios, recorremos a uma lista de 40 palavras-chave relacionadas ao uso de tecnologias de comunicação e informação e à interação digital. A partir dessa nuvem de palavras, varremos a amostra alcançando resultados não visíveis de imediato. O processo de localização dos termos foi feito pelo sistema de busca interna do aplicativo leitor de arquivos em formato PDF, o que gerou 18.010 registros, que foram depurados com a leitura manual de cada ocorrência.

■ **Figura 1 – Nuvem de palavras-chave**

Fonte: Elaborada pelos autores

Nesta fase, percebemos que os ataques digitais aparecem de diferentes maneiras, sem padrão de apresentação e na maior parte das vezes associados à ameaça física dos jornalistas. Essa condição permite enxergar um panorama situacional das questões propostas e seus entornos. Percebeu-se ainda que os relatórios dos últimos cinco anos (2012-2016) problematizaram com mais nitidez e empenho aspectos como vigilância comunicacional, violações à privacidade e emergências do ecossistema digital, o que sinaliza que tais ameaças vêm se tornando mais agudas ultimamente.

A amostra permitiu a identificação de 452 ataques nos 15 anos de período observado, taxa que pode ser considerada baixa, se levados em conta o alcance geográfico, a janela temporal e a larga disseminação dos usos e apropriações tecnológicas entre os jornalistas. Com base nos dados, podemos afirmar que em média um ataque digital contra jornalistas aconteceu a cada 12 dias no planeta! A baixa ocorrência permite inferir que as ameaças não foram graves o suficiente para serem registradas; que não são habitualmente notificadas ou, o que é pior: elas sequer foram notadas!

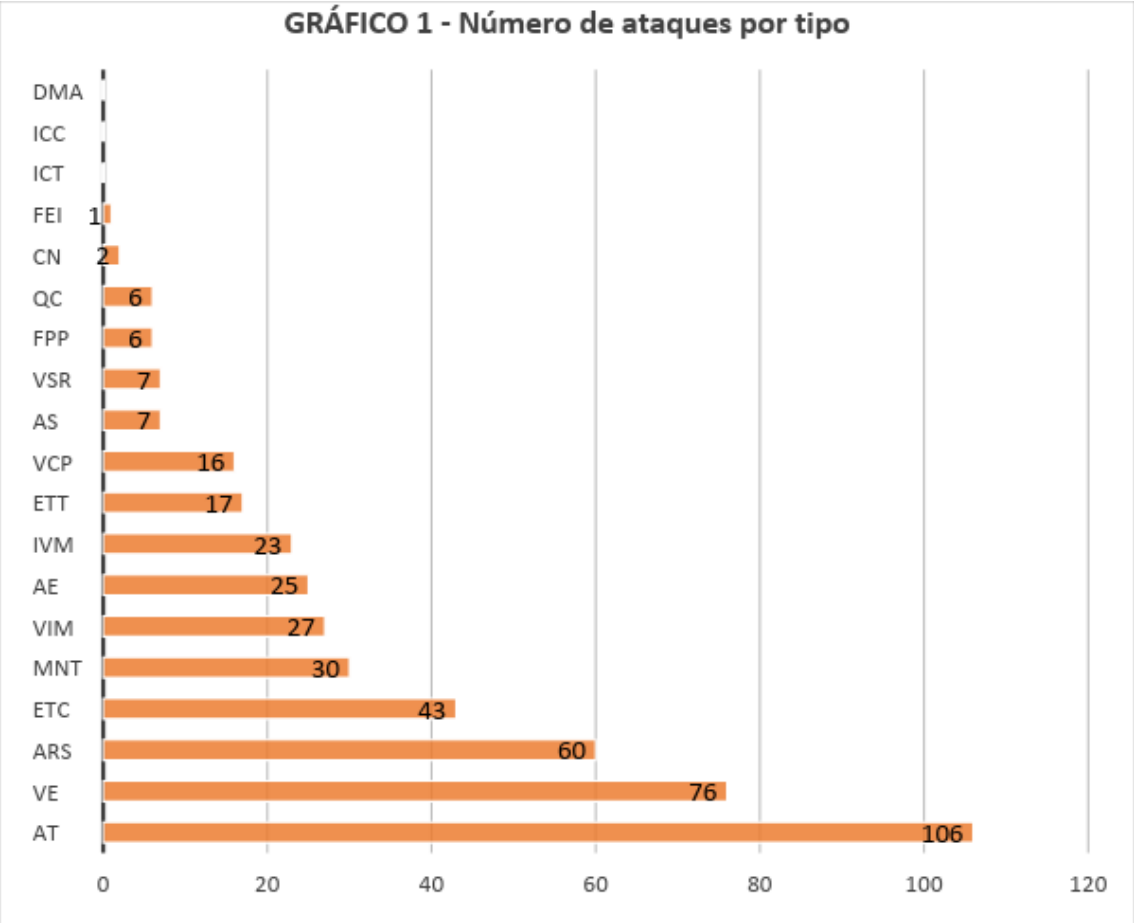
Chama a atenção, no entanto, a diversidade das ocorrências. Dos 19 tipos investigados neste estudo, apenas três não foram reportados nos documentos da amostra: instalação não-autorizada de câmeras ou microfones na redação/local de trabalho (ICT), na casa do jornalista (ICC) e descuidos de manutenção e/ou não-atualização de antivírus ou sistemas de segurança digital (DMA). Os dois primeiros tipos requerem ações mais intrusivas que podem resultar, inclusive, na invasão física de territórios e propriedades. Já a última implica em reconhecer desatenção e até negligência na garantia de segurança digital.

O tipo de ataque mais frequente detectado neste estudo foi a ameaça por telefone a jornalista (AT) com 106 registros, quase um quarto dos episódios. Violação e interceptação de e-mail foi relatada 76 vezes, e ameaças em redes sociais, 60. Somados, os três tipos de ataques mais comuns ultrapassam 53% dos casos, e apontam para maiores riscos de manejo de equipamentos e de interação. Nesses casos, *devices* possibilitam as ameaças digitais, vulnerabilidade que fica maior ainda diante da natureza dos relacionamentos entre jornalistas, fontes e outros sujeitos por meio desses equipamentos e tecnologias.

Os riscos de manejo e de interação não ficam restritos apenas aos ataques digitais mais contabilizados. Eles são os mais frequentes no geral, e incluem ainda monitoramento de navegação em tempo real (MNT=30 registros); violação ou interceptação de mensagem instantânea (VIM=27); ameaças por e-mail (AE=25); instalação e ativação de vírus, *malware* ou código malicioso para coleta ou destruição de arquivos (IVM=23); violação de contas pessoais na internet (VCP=16); ameaças por SMS (AS) e violação e invasão de sistemas nas redações (VSR), com sete relatos cada; furto de senhas por meio de *phishing* ou *pharming* (FPP) e quebra de criptografia (QC), com seis casos cada; coleta de dados de histórico na navegação (CN=2); furto ou extravio de informações (FEI=1).

Embora não tenham sido mencionadas situações de instalação não autorizada de câmeras ou microfones na redação/local de trabalho (ICT) e na casa do jornalista (ICC), os riscos ambientais existem, conforme se percebe pelos 43 casos de escutas telefônicas sem autorização na casa de jornalista ou em seu telefone celular/smartphone (ETC) e nos 17 de escutas na redação ou local de trabalho (ETT), que podem se dar tanto mediante invasão física, infiltração ou de forma remota.

■ **Gráfico 1: Número de ataques digitais por tipo no período 2001-2016**



Fonte: Elaborado pelos autores a partir de suas categorias.

Analisando os dados por autores dos relatórios, observa-se que a Freedom House é a organização que mais relatou ocorrências – 212 (47%) –, o que pode estar associado a uma sensibilidade ou compreensão maior em relação aos riscos digitais como ameaça ao jornalismo. O extrato referente à Freedom House abrange 15 dos 19 tipos de ataques listados. Os relatórios dos Repórteres Sem Fronteiras totalizaram 62 casos em 13 modalidades distintas. Na sequência, destacam-se os observadores brasileiros que identificaram 52, 29 e 25 episódios no período, respectivamente, nos *reports* da Fenaj, ANJ e Abert. O Comitê de Proteção aos Jornalistas listou 24 ataques de 9 tipos, e a Federação Internacional de Jornalistas, 20 registros de quatro tipos.

Os documentos da Artigo 19 e da Relatoria Especial de Liberdade de Expressão da Comissão Interamericana de Direitos Humanos (CIDH) da Organização dos Estados Americanos (OEA) são os que menos registram ataques na amostra pesquisada.

Considerações finais

Neste artigo buscamos apresentar elementos objetivos para a urgente discussão sobre riscos e ameaças do ecossistema digital à prática do jornalismo. O ponto de partida é o de que as práticas conectadas e em rede trazem potencialidades à reportagem, à edição e à difusão de conteúdos jornalísticos, mas elas também contribuem para a exposição desses profissionais aos riscos digitais e aumentam a vulnerabilidade de fontes e informações.

Definimos risco digital e tipificamos quase duas dezenas de ataques digitais, perseguindo suas ocorrências em 15 anos de relatórios de nove organizações que monitoram a violência contra os jornalistas e os ambientes de liberdade de expressão e de imprensa. A baixa incidência dos ataques pode levar a crer que as ameaças digitais compõem um cenário pouco ameaçador. Entretanto, sua variedade de modos e ampla difusão – em todas as partes do mundo – chamam a atenção pelos diferentes graus de sofisticação nas ações invasivas, intrusivas, de interceptação, extravio e até destruição de dados. Os poucos registros – 452 em uma década e meia – evidenciam a necessidade de que as organizações de monitoramento revejam suas metodologias para reunir mais informações sobre essas violências profissionais, de maneira a permitir leituras mais complexas e profundas das reais ameaças que rondam as redações.

Por meio da análise e reflexão sobre os relatórios apresentamos um panorama da abordagem de riscos digitais nos últimos 15 anos e reiteramos noções, ações e inércias que envolvem os entornos do monitoramento comunicacional em ambientes digitais.

Os resultados deste estudo permitem apontarmos que o monitoramento comunicacional e a privacidade dos jornalistas são temas que precisam ser abordados de forma mais específica nos relatórios que buscam mapear riscos e ameaças ligadas à atividade jornalística. Esses temas já aparecem em diversos *reports*, particularmente nos últimos cinco anos, mas os desafios do ecossistema digital estão fragmentados em noções genéricas que dificultam o entendimento e o fortalecimento de uma consciência jornalística dos riscos digitais envolvidos na sua atividade.

Diversos indícios apontam para o fato de que órgãos de Estado e grandes corporações de tecnologia estão monitorando as comunicações eletrônicas de jornalistas em diferentes partes do mundo sem supervisão ou conhecimento judicial.

Em 2016, a divisão de liberdade de expressão e desenvolvimento dos meios de comunicação da Unesco lançou o informe *Cómo desarollar la seguridad digital para el periodismo*. Na publicação (Henrichsen, 2016), as autoras mapeiam desafios tecnológicos, institucionais, psicossociais e econômicos para enfrentar

os riscos que afetam jornalistas e organizações de mídia. Mas elas ressaltam que existem ainda desafios político-legais que envolvem governos, ONGs, corporações e outras entidades, o que torna a problemática multifacetada, complexa e dinâmica.

A criação e manutenção de um ambiente favorável à prática livre do jornalismo são uma responsabilidade de governos, jornalistas, sociedade e companhias que ajudam a desenvolver o ambiente digital. Esse entendimento ficou parcialmente claro durante a 73ª Assembleia Geral da Associação Interamericana de Imprensa, realizada no final de outubro de 2017 nos Estados Unidos. Na ocasião, o Google anunciou medidas de proteção avançada que podem aumentar a segurança digital de jornalistas no continente. Tais cuidados vão de defesa mais forte contra o *phishing*, passando pela proteção adicional de dados sensíveis contra o compartilhamento acidental e bloqueios contra acessos fraudulentos.

Ao mesmo tempo em que oferece recursos complementares para aumentar a segurança de jornalistas, o Google também disponibiliza outro atraente conjunto de ferramentas para facilitar o trabalho de repórteres que lidam com muitos dados. O Google News Lab é sedutor, mas não há garantia alguma de que as informações ali manipuladas on-line estejam a salvo da observação, monitoramento, processamento, guarda ou compartilhamento com terceiros pelo próprio Google.

Um relatório divulgado em 2017 pelos Repórteres Sem Fronteiras (RSF) denunciou a submissão de grandes corporações da internet frente a governos autoritários e para atender interesses econômicos. A ONG manifestou preocupação com os crescentes episódios de vigilância online de jornalistas e defendeu a criação de instrumentos globais para regular tais situações (RSF, 2017).

Díaz (2017) enfatiza que a adoção de ferramentas e práticas de segurança digital requer investimentos financeiros, de tempo e de capacitação dos profissionais, e que mesmo assim são menos custosos que os danos que a falta de segurança pode gerar. "Apesar dos inumeráveis e louváveis esforços da comunidade tecnológica para desenvolver ferramentas e guias que facilitem o acesso do público geral aos temas da segurança digital, esses assuntos permanecem obscuros e complexos para muita gente". Mesmo para jornalistas. Por essa razão surgem iniciativas para a difusão de uma cultura de segurança para repórteres e editores, a exemplo do site Privacidade para Jornalistas (PPJ, 2017), originado a partir de um projeto australiano.

Parte da solução está nas redações e na própria disposição dos jornalistas a adotar recursos para sua segurança digital. Numa pesquisa com 154 jornalistas do mundo todo, 60% responderam que não usam nenhum tipo de ferramenta

para sua segurança física ou digital. Na América Latina, esse índice chega a 73%, afirmou Ramos (citado por Mioli, 2016), para quem "as diferenças regionais no uso refletem o nível de assimilação da tecnologia no jornalismo" (Mioli, 2016).

Estudo global sobre o nível tecnológico das redações mostrou que mais da metade dos jornalistas falha ao proteger suas informações ou fontes. A pesquisa de 2017 do International Center For Journalists (ICFJ, 2017) abrangeu mais de 2700 redações de 130 países em 12 línguas. Entre as conclusões, um espesso muro de vulnerabilidades digitais (ICFJ, 2017).

Embora cada vez mais sejam usados recursos digitais para pesquisar, relatar histórias, envolver públicos e disseminar dados, 53% dos jornalistas e 54% das redações não recorrem a nenhuma ferramenta de segurança digital. E quando o fazem, mais frequentemente usam encriptação de e-mails. Novamente, as assimetrias regionais saltam aos olhos. Se 61% das redações europeias adotam medidas de segurança, na América Latina, elas são apenas 38%.

Indisposição política em diversos países, dificuldades econômicas das organizações de mídia, desinteresses corporativos e resistências culturais dos próprios jornalistas ampliam a paisagem de riscos digitais. Somar esforços para enfrentar cada uma dessas forças nos parece ser urgente, pois elas não colocam apenas o jornalismo em risco. Também expõem a liberdade e a privacidade por meio das quais tracejamos os contornos do que chamamos de democracia.

Referências Bibliográficas

ARTÍCULO 19. **Guía de Seguridad digital y de la información para periodistas**, 2013. Disponível em: http://coberturaderiesgo.articulo19.org/wp-content/uploads/2013/07/guia_seguridad_digital.pdf. Acesso em: 17 nov. 2017.

BAUMAN, Zygmunt. **Vigilância Líquida: Diálogos com David Lyon**. Rio Janeiro: Zahar, 2014.

BAUMAN, Zygmunt e outros. Após Snowden: Repensando o Impacto da Vigilância. **Revista ECO PÓS**, Rio de Janeiro, v. 18, n. 3, p. 8-35, 2015. Disponível em: https://goo.gl/TTkVUA. Acesso em: 12 mar. 2018.

BELL, Emily. OWEN, Taylor (org.). **Journalism After Snowden: The Future of Free Press in the Surveillance State.** New York: Columbia University Press, 2017.

BRADSHAW, P. Chilling Effect: Regional journalists' source protection and information security. **Digital Journalism**, London, Vol. 5, Issue 3, 2017.

BREVINI, B.; HINTZ, A.; MCCURDY, P. **Beyond WikiLeaks:** implications for the future of communications, journalism and society. New York: Palgrave Macmillan, 2013.

BÜCHI, M.; JUST, N.; LATZER, M. Caring is not enough: the importance of Internet skills for online privacy protection. **Information, Communication and Society**, London, Vol. 20, n. 8, 2016.

CARLO, S.; KAMPHUIS, A. **Information Security for Journalists**. The Centre for Investigative Journalism: London, 2014.

CHRISTOFOLETTI, R.; TORRES, R. J. Orientações e inflexões sobre privacidade em manuais internacionais de ética jornalística. In: COSTA, Cristina. (Org.). **Privacidade, Sigilo e Compartilhamento**. 1. ed. São Paulo: ECA/USP, v. 1, p. 104-111, 2017.

CHRISTOFOLETTI, Rogério. **Privacidade como dimensão problemática da alteridade: análise de dez dicionários de jornalismo**. **Brazilian Journalism Research**, v. 13, n. 2, p. 96-119, agosto de 2017.

_____. Privacidade: o que podemos esperar quando não podemos mais esperar? In: CHRISTOFOLETTI, Rogério (org.) **Questões para um jornalismo em crise**. Florianópolis: Insular, p. 233-248, 2015.

DAGAN, M. **Online privacy for journalists: a must-have guide for journalism in 2017**. Disponível em: https://www.vpnmentor.com/journalist-privacy-guide.pdf. Acesso em: 12 dez. 2017

DÍAZ, M. **Agressiones a periodistas: periodismo, libertad de expresión y seguridad digital**. Disponível em: https://www.derechosdigitales.org/11196/periodismo-libertad-de-expresion-y-seguridad-digital/. Acesso em: 16 nov. 2017.

EDITORIAL Guidelines. **BBC**, Londres, (s/d). Disponível em: http://www.bbc.co.uk/editorialguidelines. Acesso em: 17 set. 2017.

FERNANDEZ, N.; MANCINI, P. **CryptoPeriodismo**. Manual Ilustrado Para Periodistas. Disponível em: http://cryptoperiodismo.org. Acesso em: 20 jan. 2018

FUNDACIÓN PARA LA LIBERTAD DE PRENSA. **Manual Antiespías: herramientas para la protección digital de periodistas,** 2015.

GOBIERNO ESPÍA. Vigilancia sistemática a periodistas y defensores de derechos humanos en México, junio de 2017. Disponível em: https://r3d.mx/gobiernoespia. Acesso em: 17 set. 2017. PDF.

GOLDFARB, R. (ed.). **After Snowden: privacy, secrecy, and security in the information age**. New York: St. Martin's Press, 2015.

GREENBERG, A. **This machine kills secrets**. London: Virgin Books, 2012.

GREENWALD, G. **Sem lugar para se esconder**. Rio de Janeiro: Sextante, 2014.

GUARDIAN NEWS AND MEDIA; INFORMATION LAW AND POLICY CENTRE. **Protecting sources and whistleblowers in a digital era**. London, 2017.

Disponível em:. https://clip.blogs.sas.ac.uk/files/2017/02/Sources-Report_webversion_22_2_17.pdf. Acesso em: 8 dez. 2017

HARDING, L. **Os arquivos Snowden**. Rio de Janeiro: Leya, 2014.

HENRICHSEN, Jennifer R.; BETZ, Michelle; LISOSKY, Joanne M. **Cómo desarrollar la seguridad digital para el periodismo**. Unesco, México, 2016. Disponível em: http://almeria.fape.es/wp-content/uploads/2016/08/INFORME_UNESCO.pdf. Acesso em: 17 nov. 2017

INTERNATIONAL CENTER FOR JOURNALISTS (ICFJ). **The State of Technology in Global Newsrooms**. 2017. Disponível em: http://www.icfj.org/sites/default/files/ICFJTechSurveyFINAL.pdf. Acesso em: 17 nov. 2017.

JENKINS, Henry; FORD, Sam; GREEN, Joshua. **Cultura da Conexão: Criando valor e significado por meio da mídia propagável**. São Paulo: Aleph, 2014.

LYON, David. Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity. **International Journal of Communication**, Vol. 11, 2017, p. 824-842. Disponível em: https://goo.gl/ARwPTG. Acesso em: 20 fev. 2018

MARTINS, Paulo. **O público em privado**: direito à informação e direitos de personalidade. Coimbra: Almedina, 2013.

MARX. Gary T. **Windows into the Soul: Surveillance and Society in an Age of High Technology**. Chicago: Chicago Press, 2016.

MCSTAY, Andrew. **Privacy and the media**. Los Angeles/London: Sage, 2017.

MIOLI, Teresa. CPJ: México e Brasil estão entre os países com maior aumento da impunidade em crimes contra jornalistas nos últimos dez anos**. Blog Jornalismo nas Américas**, Austin, 31 out. 2017. Disponível em: https://knightcenter.utexas.edu/pt-br/blog/00-18953-cpj-mexico-e-brasil-estao-entre-os-paises-com-maior-aumento-da-impunidade-em-crimes-co. Acesso em: 16 nov. 2017

MIOLI, Teresa. Jornalistas precisam aprender a usar ferramentas de segurança digital para enfrentar situações de risco, aponta relatório. **Blog Jornalismo nas Américas**, Austin, 16 maio 2016. Disponível em: https://knightcenter.utexas.edu/pt-br/blog/00-17111-jornalistas-precisam-aprender-usar-ferramentas-de-seguranca-digital-para-enfrentar-sit. Acesso em: 17 nov. 2017.

MOORE, A.A. (ed.) **Privacy, Security and accountability: ethics, law and policy**. London-New York: Rowman & Littlefield, 2016.

NISSENBAUM, Helen. **Privacy in context**: technology, policy and integrity of social life. Stanford: Stanford Law Book, 2010.

PAVLIK, John V. Ubiquidade: O 7.º princípio do jornalismo na era digital. In: CANAVILHAS, João (org.) **Webjornalismo:** 7 caraterísticas que marcam a diferença. Covilhã: LabCom, 2014. p. 159-184.

PEÑA OCHOA, P. ¿Cómo funciona Internet? Nodos críticos desde una perspectiva de los derechos. Guía para periodistas. Santiago de Chile: ONG Derechos Digitales, 2013. Disponível em: https://www.derechosdigitales.org/wp-content/uploads/Comofunciona-internet-ebook.pdf. Acesso em: 7 dez. 2017

PRIVACIDADE PARA JORNALISTAS (PPJ). **Proteja suas fontes**, 2017. Disponível em: https://privacidadeparajornalistas.org. Acesso em: 17 nov. 2017.

RAMOS, J.G. **Journalist Security in the Digital World: a Survey. Are We using the right tools?** Center for International Media Assistance, 2016. Disponível em: https://www.cima.ned.org/resource/journalist-security-in-the-digital-world/. Acesso em: 19 dez. 2017

REPÓRTERES SEM FRONTEIRAS (RSF). **Censura e vigilância de jornalistas: um negócio sem escrúpulos**, 2017. Disponível em: https://rsf.org/sites/default/files/rapport_cs_pt_v2-2.pdf. Acesso em: 17 nov. 2017.

RICHARDS, Neil M. Four privacy miths. IN: SARAT, A. **A world without privacy: what law can and should do?** NY: Cambridge University Press, 2015.

RUBY, F.; GOGGIN, G.; KEANE, J. Comparative Silence still? Journalism, academia, and the Five Eyes of Edward Snowden (2017). **Digital Journalism**, London, Vol. 5, Issue 3, 2017.

SALAVERRÍA, Ramón. Multimedialidade: Informar para cinco sentidos. In: CANAVILHAS, João (org.) **Webjornalismo: 7 caraterísticas que marcam a diferença**. Covilhã: LabCom, 2014. p. 25-52.

SEGURIDAD de la información. **Manual de Seguridad para Periodistas**. Committee for Journalist Protection, 2012. Disponível em: https://www.cpj.org/es/2012/04/seguridad-de-la-informacin.php. Acesso em: 14 jan. 2018

SIERRA, J. L. Manual de seguridad digital y móvil para periodistas y blogueros. International Center For Journalists & Freedom House, 2013. Disponível em: https://freedomhouse.org/sites/default/files/Manual%20de%20seguridad%20web%20Imprenta%20Final.pdf. Acesso em: 22 fev. 2018

SURVEY DIGITAL Safety for Journalists. DW AKADEMIE, 2013. Disponível em: http://akademie.dw.de/digitalsafety/. Acesso em: 17 set. 2017.

TAYLOR, L.; FLORIDI, L.; SLOOT, B. (eds.) **Group Privacy: new challenges of data technology**. Oxford: Springer, 2017.

AHMED, Zam y PERLROTH, Nicole. 'Somos los nuevos enemigos del Estado': el espionaje a activistas y periodistas en México. The New York Times. Nova Iorque, 19 jun. 2017, América Latina: México. Disponível em: https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/?mcubz=1. Acesso em: 19 set. 2017.

WASSERMAN, E. Safeguarding the News in the Era of Disruptive Sources. **Journal of Media Ethics**, v. 32, n. 2, p. 72-85, 2017.

Recebido em: 20/11/2017
Aceito em: 14/03/2018

Dados dos autores:

Rogério Christofoletti | rogerio.christofoletti@uol.com.br
Professor do Programa de Pós-Graduação em Jornalismo da Universidade Federal de Santa Catarina. Jornalista, mestre em Linguística e doutor em Ciências da Comunicação. Pesquisador do CNPq (PQ2). Líder do Observatório da Ética Jornalística (objETHOS).

Endereço do autor:
Universidade Federal de Santa Catarina
Campus Universitário, Trindade
88040-970 – Florianópolis/SC

Ricardo José Torres | rickjtorres@hotmail.com
Doutorando no Programa de Pós-Graduação em Jornalismo da Universidade Federal de Santa Catarina. (POSJOR/UFSC).

Endereço do autor:
Universidade Federal de Santa Catarina
Campus Universitário, Trindade
88040-970 – Florianópolis/SC

Justificativa do artigo: Em "Jornalistas expostos e vulneráveis: ataques digitais como modalidade de risco profissional", os autores empreendem uma discussão sobre ameaças e vulnerabilidades de repórteres, editores e redatores no atual contexto de comunicação digital, cujos riscos são amplificados por vigilância, espionagem e métodos intrusivos de coleta e uso de dados pessoais. O artigo é derivado de pesquisa que investiga transformações na privacidade e no jornalismo, e em pesquisa de doutorado em andamento sobre a capacidades de jornalistas investigativos de manterem a função de contravigilância nas sociedades. O artigo avança numa tipologia de ataques digitais e contribui com a formulação de conceitos de risco digital e ataque digital contra jornalistas.

Contribuições dos autores: Ambos os autores fizeram contribuições substanciais para concepção, desenvolvimento, redação e revisão crítica do trabalho; e aprovação final da versão para publicação.