UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE COMUNICAÇÃO E EXPRESSÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM JORNALISMO

Ricardo José Torres

Jornalismo vigilante sob vigilância:
vulnerabilidades e potencialidades do jornalismo investigativo brasileiro

Florianópolis
2020

Ricardo José Torres

Jornalismo vigilante sob vigilância:
vulnerabilidades e potencialidades do jornalismo investigativo brasileiro

Tese submetida ao Programa de Pós-Graduação em Jornalismo da Universidade Federal de Santa Catarina para a obtenção do Título de Doutor em Jornalismo.
Orientador: Prof. Dr. Rogério Christofoletti.
Coorientador: Prof. Dr. Samuel Pantoja Lima.

Florianópolis
2020

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Torres, Ricardo José
Jornalismo vigilante sob vigilância vulnerabilidades e potencialidades do jornalismo investigativo brasileiro : vulnerabilidades e potencialidades do jornalismo investigativo brasileiro / Ricardo José Torres ; orientador, Rogério Christofoletti, coorientador, Samuel Pantoja Lima, 2020.
285 p.

Tese (doutorado) - Universidade Federal de Santa Catarina, Centro de Comunicação e Expressão, Programa de Pós Graduação em Jornalismo, Florianópolis, 2020.

Inclui referências.

1. Jornalismo. 2. Jornalismo investigativo. 3. Privacidade. 4. Segurança digital para jornalistas. 5. Vigilância digital. I. Christofoletti, Rogério . II. Pantoja Lima, Samuel . III. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Jornalismo. IV. Título.

Ricardo José Torres

Jornalismo vigilante sob vigilância:

vulnerabilidades e potencialidades do jornalismo investigativo brasileiro

O presente trabalho em nível de doutorado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Prof. Dr. Rafael de Almeida Evangelista
Universidade Estadual de Campinas (Unicamp)

Prof.ª Dr.ª Daiane Bertasso
Universidade Federal de Santa Catarina (UFSC)

Prof.ª Dr.ª Stefanie Carlan da Silveira
Universidade Federal de Santa Catarina (UFSC)

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de doutor em Jornalismo.

Documento assinado digitalmente
Rogerio Christofoletti
Data: 07/06/2020 11:01:06-0300
CPF: 154.860.838-66

Coordenação do Programa de Pós-Graduação
Prof. Dr. Rogério Christofoletti

Documento assinado digitalmente
Rogerio Christofoletti
Data: 07/06/2020 11:03:33-0300
CPF: 154.860.838-66

Prof. Dr. Rogério Christofoletti
Orientador

Florianópolis, 2020.

Gus disse aos jornalistas que a agência poderia rastrear seus smartphones mesmo quando desligados; que a agência poderia monitorar cada uma das suas comunicações. Lembre-se: era uma multidão de jornalistas domésticos. Jornalistas estadunidenses. E Gus disse poderia de um jeito que significava pôde, pode e poderá. Ele falava de uma maneira claramente perturbada e perturbadora, pelo menos para um sumo sacerdote da CIA:

"A tecnologia está se movendo mais rápido do que o governo ou a lei podem acompanhar. Vocês deveriam perguntar quais são seus direitos e quem é o dono de seus dados".

Eu estava chocado; se uma pessoa do nível hierárquico menor que Gus fizesse uma apresentação como essa, estaria vestindo laranja antes do fim do dia.

A cobertura da confissão foi publicada só no The Huffington Post. Mas a apresentação ainda se encontrava no YouTube pelo menos seis anos depois. A última vez que vi tinha 313 visualizações – uma dúzia delas era minha.

O que aprendi com isso foi que para que minha revelação fosse eficaz, eu teria de fazer mais que apenas entregar alguns documentos aos jornalistas – mais, até, que os ajudar a interpretar os documentos. Eu teria de me tornar parceiro deles, fornecer-lhes o treinamento tecnológico e as ferramentas para ajudá-los a fazer suas reportagens com precisão e segurança. Seguir esse caminho significaria entrar de cabeça em um dos crimes capitais do trabalho na inteligência: outros espiões teriam cometido espionagem, sedição e traição, mas eu estaria ajudando e instigando um ato de jornalismo. O perverso disso é que, legalmente, esses crimes são praticamente sinônimos. A lei estadunidense não faz distinção entre fornecer informações sigilosas à imprensa em nome do interesse público e fornecê-las, ou até vendê-las, ao inimigo. A única opinião que eu já havia encontrado que contradizia isso provinha de minha primeira doutrinação na CI; lá, haviam dito que, de fato, era um pouco melhor oferecer a venda de segredos ao inimigo que oferecê-los gratuitamente a um repórter. Um repórter contaria ao público, ao passo que seria improvável que um inimigo compartilhasse seu prêmio, inclusive com seus aliados.

Considerando os riscos que eu estava correndo, precisava identificar pessoas em quem pudesse confiar e que também fossem confiáveis para o público. Eu precisava de repórteres diligentes, mas discretos, independentes e confiáveis. Teriam que ser fortes para me desafiar acerca das distinções entre o que eu suspeitava e o que as evidências provavam, e para desafiar o governo quando ele os acusasse falsamente de pôr vidas em risco com seu trabalho. Acima de tudo, eu precisava ter certeza de que quem eu escolhesse não acabaria cedendo ao poder quando posto sob pressão – o que, certamente, não seria como nada que eles, ou eu, já houvessem experimentado antes.

Edward Snowden[1]

[1] Trecho do livro de Edward Snowden "Eterna vigilância", tradução: Sandra Martha Dolinsky. São Paulo: Planeta do Brasil, 2019, p. 261-262.

À memória do meu pai, Antonio Torres, um exemplo de trabalho, dedicação, honestidade e resiliência, a minha mãe, Sirlei Teresinha Torres, pelo amor incomensurável e a minha esposa, Fabíola Markendorf, por ser a luz que ilumina o meu caminho e todos os meus dias.

AGRADECIMENTOS

Como é bom poder agradecer. Ao longo dos últimos anos, me dediquei à produção de conhecimento por meio das possibilidades que a pesquisa oferece. Desde então, busquei compreender as inter-relações e experiências da forma mais proveitosa possível, desfrutando das oportunidades. Apostei na dedicação e no trabalho. Além disso, contei com o apoio e com a confiança de pessoas especiais.

Primeiramente, agradeço a Deus por guiar os meus passos e me conduzir todos os dias. A Fabíola, um ser iluminado a quem guardo sentimentos indescritíveis de amor, afeto, carinho. Trilhamos juntos, há mais de uma década, um caminho repleto de momentos, bons e ruins, e construímos dia após dia uma relação de companheirismo e aprendizado.

Ao nosso mascote Ted que há seis anos é o repositório de amor e carinho da nossa casa.

Aos meus pais, Antonio e Sirlei, que em todos os momentos depositaram os melhores sentimentos e me motivaram a continuar acreditando no meu potencial. Pelas lições de vida e persistência constantes, pela fé e pela luta que marcam as suas trajetórias e me inspiram a trabalhar todos os dias.

Ao professor Rogério Christofoletti, meu orientador, a quem não tenho palavras para agradecer. Uma das pessoas mais inteligentes e afetuosas que já conheci, alguém que me ofereceu oportunidades, confiança, numerosos ensinamentos e foi um grande parceiro ao longo de toda a jornada acadêmica.

Meu agradecimento ao professor Samuel Pantoja Lima, por todas as dicas, inúmeras conversas e pelo coração amazônico.

Aos professores Rafael de Almeida Evangelista, Daiane Bertasso, Stefanie Carlan da Silveira, Luciana Kraemer da Silva e Jacques Mick por terem aceito o convite para integrar a banca de avaliação, por dedicarem tempo e atenção durante a leitura da tese, pelas contribuições e melhorias apontadas.

Sou grato a todos os jornalistas que participaram das distintas etapas desta pesquisa, especialmente aos nove profissionais que dedicaram o seu tempo e dividiram as suas experiências durante as entrevistas em profundidade e aos 78 participantes que compartilharam as suas percepções na *survey*.

Concluir uma tese de doutorado na Universidade Federal de Santa Catarina parecia algo inconcebível e inacreditável. Hoje, como servidor da UFSC, me orgulho ainda mais disso

e agradeço todos os dias pela possibilidade de estar nesse ambiente pujante e dinâmico que é público, gratuito e de excelência.

A todos os professores e servidores do Programa de Pós-Graduação em Jornalismo da UFSC (PPGJOR/UFSC) pelo suporte e pela generosidade;

A Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo auxílio financeiro, que me ajudou a desenvolver o estudo.

Aos colegas do Observatório da Ética Jornalística (objETHOS) pelas trocas ao longo de nossos encontros e reuniões;

Por fim, dedico a minha gratidão a todos os colegas do PPGJOR, amigos e familiares que de alguma forma contribuíram para concretização deste objetivo.

RESUMO

O contexto atual de vigilância comunicacional em meios digitais exige dos jornalistas investigativos um senso permanente de sua vulnerabilidade e a adoção de uma cultura de segurança digital. Jornalistas que desenvolvem investigações jornalísticas sobre temas sensíveis enfrentam as possibilidades de intervenção relacionadas à vigilância das comunicações, interceptação e armazenamento de dados pessoais e o monitoramento de ações jornalísticas no ecossistema digital. A partir desse panorama, o presente estudo é orientado pelo seguinte problema de pesquisa: diante da vigilância digital massiva realizada por governos e corporações, quais são as principais vulnerabilidades e potencialidades do jornalismo investigativo brasileiro? Parte-se dos seguintes pressupostos: a investigação jornalística transpassada pelas possibilidades tecnológicas pode ser limitada por ferramentas de vigilância comunicacional; as ferramentas de comunicação digital facilitam a projeção de ações ligadas ao jornalismo, ao ativismo e de hacktivistas e, ao mesmo tempo, fazem emergir a urgência da proteção das comunicações e fontes dos jornalistas; a desproporção entre a capacidade de vigilância do Estado e de grandes corporações transnacionais em relação ao jornalismo gera consequências nocivas à democracia. Nosso principal objetivo é examinar ações que envolvem o jornalismo investigativo, apontando potencialidades e vulnerabilidades no ecossistema digital. Os objetivos específicos são observar a emergência de tensionamentos impostos pela vigilância relacionados ao jornalismo investigativo, verificar implicações resultantes da possibilidade de intrusão comunicacional na atividade jornalística contemporânea e defender a necessidade de estímulos e convenções relacionadas com a formatação de uma cultura de riscos digitais para jornalistas. O percurso metodológico adotado está organizado em quatro etapas distintas. Inicialmente, desenvolvemos uma pesquisa exploratória e revisão bibliográfica que discute questões teóricas e delimita os caminhos metodológicos mais adequados aos objetivos. Na sequência, realizamos o mapeamento de casos concretos e ações jornalísticas relacionadas às diferentes formas de vigilância digital realizadas em contextos distintos a partir de apontamentos e condutas indicadas em relatórios de agressões à jornalistas e ataques à liberdade de imprensa. Na terceira etapa, selecionamos jornalistas investigativos para realização de entrevistas em profundidade, três para validação do roteiro de perguntas e seis para a efetivação da técnica de pesquisa. Em seguida, avaliamos as entrevistas por meio de protocolos e ferramentas de análise, elencando os aspectos percebidos, adequados e negligenciados nas investigações jornalísticas realizadas em espaços digitais potencialmente vigiados. Na quarta etapa, utilizamos a técnica de pesquisa *survey,* baseada na amostragem bola de neve (GOODMAN, 1961), para aplicação de 78 questionários a jornalistas investigativos ligados à abordagem de assuntos sensíveis, sendo que 60 foram validados. Os resultados apontam as ações que estão sendo desenvolvidas, assim como as lacunas e problemáticas que envolvem a vigilância digital, o vazamento de dados e o acesso às novas fontes de informação no ambiente digital. Também apresentam práticas jornalísticas relevantes em matéria de vigilância das comunicações, aspectos negligenciados pelos profissionais, identificação de ferramentas e condutas para minimização da intrusão comunicacional, vulnerabilidades e possibilidades presentes nas investigações jornalísticas contemporâneas.

Palavras-chave: Jornalismo investigativo. Jornalismo brasileiro. Privacidade. Segurança digital para jornalistas. Vigilância digital.

ABSTRACT

The current context of communicational surveillance in digital media requires investigative journalists to have a permanent sense of their vulnerability and to adopt a culture of digital security. Journalists who develop journalistic investigations on sensitive topics face the possibilities of intervention related to the surveillance of communications, interception and storage of personal data and the monitoring of journalistic actions in the digital ecosystem. Based on this panorama, the present study is guided by the following research problem: before the massive digital surveillance carried out by governments and corporations, what are the main vulnerabilities and potential of Brazilian investigative journalism? It starts from the following assumptions: journalistic investigation permeated by technological possibilities can be limited by communicational surveillance tools; digital communication tools facilitate the projection of actions related to journalism, activism and hacktivists and, at the same time, bring out the urgency of protecting journalists' communications and sources; the disproportion between the surveillance capacity of the state and that of large transnational corporations in relation to journalism has harmful consequences for democracy. Our main objective is to examine actions that involve investigative journalism, pointing out potentials and vulnerabilities in the digital ecosystem. The specific objectives are to observe the emergence of tension imposed by surveillance related to investigative journalism, to verify implications resulting from the possibility of communicational intrusion in contemporary journalistic activity and to defend the need for stimuli and conventions related to the formatting of a culture of digital risks for journalists. The methodological path adopted is organized in four distinct stages. Initially, we developed an exploratory research and bibliographic review that discusses theoretical issues and delimits the most appropriate methodological paths to the objectives. Then, we mapped concrete cases and journalistic actions related to the different forms of digital surveillance carried out in different contexts based on notes and conduct indicated in reports of attacks on journalists and attacks on press freedom. In the third stage, we selected investigative journalists to conduct in-depth interviews, three to validate the questionnaire and six to carry out the research technique. Then, we evaluated the interviews using protocols and analysis tools, listing the aspects perceived, adequate and neglected in the journalistic investigations carried out in potentially monitored digital spaces. In the fourth stage, we used the survey research technique, based on snowball sampling (GOODMAN, 1961), for the application of 78 questionnaires to investigative journalists linked to the approach of sensitive subjects, 60 of which were validated. The results point to the actions that are being developed, as well as the gaps and problems that involve digital surveillance, data leakage and access to new sources of information in the digital environment. They also present relevant journalistic practices in terms of surveillance of communications, aspects neglected by professionals, identification of tools and conducts to minimize communicational intrusion, vulnerabilities and possibilities present in contemporary journalistic investigations.

Keywords: Investigative journalism. Brazilian journalism. Privacy. Digital security for journalists. Digital surveillance.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE GRÁFICOS

SUMÁRIO

INTRODUÇÃO

> *Por muito tempo, a ideia de um mundo "totalmente vigiado" parecia um delírio utópico ou paranoico, fruto da imaginação mais ou menos alucinada daqueles obcecados por complôs. No entanto, devemos nos render à evidência: aqui e agora vivemos sob o controle de uma espécie de Império da Vigilância. Sem nos apercebermos, somos cada vez mais observados, espionados, vigiados, controlados, fichados. Novas tecnologias estão sendo aperfeiçoadas todos os dias para rastrear nossas trilhas. Empresas comerciais e agências de publicidade armazenam nossas vidas. Sob o pretexto de lutar contra o terrorismo e outras pragas, os governos, mesmo os mais democráticos, permanecem como o Big Brother, e não hesitam em quebrar suas próprias leis para nos espionar melhor. Em segredo, os novos Estados orwellianos tentam, muitas vezes com a ajuda dos gigantes da Rede, elaborar arquivos exaustivos de nossos dados pessoais e nossos contatos, extraídos dos diferentes suportes eletrônicos*[2] *(RAMONET, 2017, online, tradução livre).*

A partir de amplos avanços e variadas formas de apropriação e uso das tecnologias de comunicação vivenciamos o redimensionamento das configurações de articulação e de intersecções entre o jornalismo e a vigilância. Essa relação está conectada com a essência do jornalismo investigativo, delineando-se na perspectiva de monitorar o poder, revelar atos ilícitos, tornar os cidadãos informados e fomentar o debate público por meio de atos de vigilância (WAISBORD, 2000). Aspectos contextuais e históricos intervêm nas práticas jornalísticas orientadas por tradições e princípios que formatam as ações vigilantes em diferentes partes do mundo. Apesar da influência inequívoca do modelo de jornalismo investigativo estadunidense, particularmente na América Latina e na Europa, ele não pode ser considerado o único paradigma possível para ações jornalísticas de investigação.

> Em resumo, a noção de jornalismo investigativo é equívoca. Mais do que métodos particulares de coleta de notícias ou reação pública específica, o que caracteriza o jornalismo investigativo é que os repórteres descobrem informações sobre abusos de poder[3]. (WAISBORD, 2000, p. 19, tradução livre).

[2] No original: Durante mucho tiempo, la idea de un mundo “totalmente vigilado” há parecido un delirio utópico o paranoico, fruto de la imaginación más o menos alucinada de los obsesionados por los complots. Sin embargo, hay que rendirse a la evidencia: aquí y ahora vivimos bajo el control de una especie de Imperio de la Vigilancia. Sin que nos demos cuenta, estamos, cada vez más, siendo observados, espiados, vigilados, controlados, fichados. Cada día se perfeccionan nuevas tecnologías para el rastreo de nuestras huellas. Empresas comerciales y agencias publicitarias cachean nuestras vidas. Con el pretexto de luchar contra el terrorismo y otras plagas, los gobiernos, incluso los más democráticos, se erigen en Big Brother, y no dudan en quebrantar sus propias leyes para poder espiarnos mejor. En secreto, los nuevos Estados orwelianos intentan, muchas veces con la ayuda de los gigantes de la Red, elaborar exhaustivos ficheros de nuestros datos personales y de nuestros contactos, extraídos de los diferentes soportes electrónicos.

[3] No original: In summary, the notion of investigative journalism is equivocal. More than particular news-gathering methods or specific public reaction, what characterizes investigative journalism is that reporters dig out information about power abuses.

Definições como jornalismo investigativo, jornalismo de investigação, *watchdog journalism*[4], jornalismo *muckraking* refletem experiências e práticas muito influenciadas pela perspectiva estadunidense. Diante de inúmeras formas de tratamento e nomenclatura, optamos pela utilização de uma noção mais ampla que chamamos de "jornalismo vigilante" e, alternadamente, jornalismo investigativo. Defendemos essa definição para tratar de questões que consideramos cruciais para a investigação jornalística contemporânea. Não se trata da busca de novas palavras para velhos dilemas que transpassam as ações atreladas ao jornalismo investigativo ou de investigação. A utilização de uma definição específica (jornalismo vigilante) está associada com desafios que não são necessariamente novos, mas dinâmicos e progressivos. Estamos nos reportando às características ambientais ligadas com as tecnologias comunicacionais de onde emergem vulnerabilidades (capacidade sem precedentes de vigilância comunicacional, monitoramento, modulação e intrusão nas investigações jornalísticas) e possibilidades (unidades de informação, plataformas de vazamento, acesso facilitado às fontes, maneiras distintas de investigar, divulgar e receber informações).

Diante desse cenário, o jornalismo investigativo passa por transformações inescapáveis e latentes que precisam de uma compreensão que vá além da percepção que acompanha e se molda à realidade da atividade jornalística nas últimas seis décadas. No contexto atual, para vigiar a sociedade, o jornalista precisa proteger a sua liberdade de comunicação em meios digitais e lutar pela liberdade individual no ambiente digital. Isso exige domínio de ferramentas e técnicas específicas e uma postura profissional norteada pelo entendimento aprofundado, crítico e independente do seu contexto de atuação e os riscos emergentes com que está lidando.

A abordagem atrelada ao jornalismo vigilante está associada aos métodos adotados no processo de investigação jornalística e ao compartilhamento de informações de maneira mais segura e eficaz. Essa perspectiva está amplamente conectada aos agentes que buscam a manutenção da liberdade comunicacional na internet. A capacidade de intrusão sem precedentes (captação, identificação e manuseio de informações) revelada por atores ligados às possibilidades comunicacionais da internet demonstram um ponto de virada nas ações jornalísticas. Por mais que formas de vigilância sempre estiveram presentes no cotidiano jornalístico, o fenômeno contemporâneo é diferente e exige uma abordagem que enalteça os principais aspectos que estruturam essa diferenciação.

[4] O jornalismo cão-de-guarda está atrelado ao ato de vigiar os interesses da coletividade.

Nesse cenário, dois elementos relacionados aos Estados e às corporações se conectam. Por parte dos Estados, o terror e a segurança nacional são justificativas para tomadas de medidas e posições políticas. Nas corporações, as facilidades de comunicação do ambiente digital são "negociadas" pelas informações privadas dos usuários/jornalistas.

A partir de uma das premissas que orientam esse estudo, consideramos que o alto grau de utilização e dependência das possibilidades tecnológicas relacionadas à internet por parte dos jornalistas, paralelamente ao avanço progressivo das possibilidades de armazenamento e controle de dados disponibilizados pelas ferramentas e aparatos de vigilância, afetam a sedimentação e a legitimidade das investigações jornalísticas contemporâneas e desempenham um papel relevante nas relações de poder e fiscalização do Estado e de atores sociais que concentram elevado domínio econômico na sociedade. Consequentemente, a desproporção entre a capacidade de vigilância do Estado e de grandes corporações transnacionais em relação ao jornalismo gera consequências nocivas à democracia.

Em certa medida, o jornalismo sempre conviveu com formas de vigilância e intrusão. Contudo, elementos como as mídias sociais, por exemplo, estão facilitando a projeção de ações ligadas à parametrização algorítmica[5], fazendo emergir a urgência de novas medidas de proteção de dados, comunicações e fontes dos jornalistas. Conforme Bell (2016), esse cenário está provocando algo realmente dramático na paisagem da mídia, na esfera pública e na indústria jornalística sem o nível de análise e debate público que merece.

A capacidade de intrusão e instrumentalização de dados privados alcançou níveis massivos e sem precedentes. Nos reportamos às possibilidades de vigilância das comunicações, particularmente na internet, que identificamos como jornalismo vigiado. Nossa abordagem pretende clarear os riscos, vulnerabilidades, precauções e aspectos que emergem deste contexto e como estão sendo enfrentados pelos jornalistas. Atualmente, o jornalismo de interesse público focado em vigiar e expor atos de corrupção e desrespeito às leis vigentes depende da preservação e do fortalecimento da segurança digital, da defesa da internet livre e dos direitos, prerrogativas e liberdades dos jornalistas.

Imerso em mudanças e permeado pelas mídias sociais, o ecossistema de notícias acaba inserindo novas dinâmicas à prática jornalística. Essas novidades apresentam um número amplo de oportunidades e uma série de riscos que envolvem formas de vigilância e preservação da privacidade. "Estamos entregando o controle de partes importantes de nossa vida pública e privada a um número muito pequeno de pessoas, que não foram eleitas e não

[5] Processo de decisão e definição de parâmetros mecânicos para a identificação de dados e direcionamento de conteúdo para usuários.

nos devem explicações" (BELL, 2016, online). Seguindo a mesma linha de pensamento que a autora, precisamos garantir a igualdade no acesso e na disseminação do discurso público, assim como nas formas de expressão, que devem ser tratadas de maneira transparente, pois este é um requisito básico para o funcionamento da democracia.

O debate sobre as implicações da vigilância na sociedade e questões conectadas à intrusão da privacidade de cidadãos comuns e jornalistas vem sendo abordado por diversas perspectivas, por diferentes autores, tais como: Gary Marx (2003, 2015, 2016), Bruno (2009, 2013), Fuchs (2011), Bauman e Lyon (2014), Assange (2013), Greenwald (2014), Human Rights Watch (2014), Bauman *et al*. (2015), Lyon (2015, 2016, 2017, 2018), Christofoletti (2015), Fuchs e Trottier (2016), Bell e Owen (2017), Evangelista (2017), entre outros. De maneira geral, as abordagens têm pontos comuns que indicam que as transmutações comunicacionais não podem ser menosprezadas, tampouco enaltecidas, mas precisam ser entendidas e decifradas.

O surgimento de organizações como o WikiLeaks[6], de *whistleblowers*[7] como Edward Snowden, que em junho de 2013 revelou, por meio de ações jornalísticas, que a Agência Nacional de Segurança dos Estados Unidos estava fazendo registros de quase todos os telefonemas dos norte-americanos; e de fenômenos como o *Panama Papers*, conjunto de documentos (mais de dois *terabytes* de dados) vazados por uma fonte anônima para o jornal alemão *Süddeutsche Zeitung* em 2015, que deu origem a uma série de reportagens, resultado de um trabalho colaborativo que envolveu mais de 300 profissionais de 76 países e venceu o Prêmio Pulitzer de 2017, na categoria *Explanatory Reporting*, revelam a importância das mudanças que estamos vivenciando.

O problema de pesquisa que propomos emerge dessa perspectiva: diante da vigilância digital massiva realizada por governos e corporações, quais são as principais vulnerabilidades e potencialidades do jornalismo investigativo brasileiro? Nesse sentido, verificamos como os jornalistas que fazem investigações jornalísticas sobre temas sensíveis enfrentam as possibilidades de intervenção relacionadas à vigilância das comunicações, interceptação e armazenamento de dados pessoais e o monitoramento de ações jornalísticas no ecossistema digital. Esta pesquisa tem como objetivo geral examinar ações que envolvem o jornalismo investigativo, apontando potencialidades e vulnerabilidades no ecossistema digital. Como

[6] WikiLeaks é uma organização de mídia e um repositório de dados fundado pelo ativista Julian Assange em 2006. A organização é especializada na análise e publicação de grandes conjuntos de dados oficiais censurados ou restritos que envolvem guerra, espionagem e corrupção. Já publicou mais de 10 milhões de documentos e análises. Mais informações em: https://wikileaks.org/.

[7] Denunciantes que alertam para a existência de irregularidades na gestão, no funcionamento de empresas ou instituições, o termo não tem uma tradução equivalente em português.

objetivos específicos, o estudo pretende observar a emergência de tensionamentos relacionados ao jornalismo investigativo que são impostos pela vigilância, verificar implicações da possibilidade de intrusão comunicacional na atividade jornalística contemporânea e defender a necessidade de estímulos e convenções relacionadas com a formatação de uma cultura de riscos digitais para jornalistas.

Para tanto, a pesquisa se organiza em quatro etapas que em alguns períodos foram executadas paralelamente:

1ª Etapa – Pesquisa exploratória e revisão bibliográfica que discute questões teóricas e delimita os caminhos metodológicos mais adequados aos objetivos propostos. Articulamos a construção metodológica por meio de aportes teóricos (BENETTI; LAGO, 2007), práticos (desenvolvimento de protocolos de análise e proposição de tipificações) e técnicas de pesquisa (entrevistas em profundidade e aplicação de questionários). Nesta etapa, buscamos identificar relações entre vigilância e jornalismo, apontando maneiras distintas de apropriação de novas possibilidades de monitoramento e contravigilância no ambiente digital e como estas particularidades afetam perspectivas relacionadas ao jornalismo investigativo. Observamos a emergência de tensionamentos relacionados ao jornalismo investigativo que são impostos pela vigilância e verificamos implicações da possibilidade de intrusão comunicacional na atividade jornalística contemporânea. Estruturamos maneiras de verificar como jornalistas que trabalham com temas sensíveis respondem à potencial vigilância digital realizada por governos e corporações. Abordamos o papel significativo que as práticas de vigilância contemporânea ocupam nas ações de investigação jornalística e como atores governamentais e corporativos podem influenciar o trabalho de apuração dos jornalistas.

2ª Etapa – Mapeamento de casos concretos e ações jornalísticas relacionadas às diferentes formas de vigilância digital realizadas em contextos distintos. Verificação de implicações conexas à vigilância comunicacional e ao tratamento das informações jornalísticas a partir de apontamentos e condutas indicadas em relatórios de agressões aos jornalistas e ataques à liberdade de imprensa. Averiguação de formas e ferramentas de contravigilância para jornalistas em manuais e materiais específicos, elaboração de protocolos de análise.

3ª Etapa – Seleção de jornalistas investigativos para realização de pré-teste de entrevistas em profundidade com profissionais que atuam em Santa Catarina (3 entrevistados) e aplicação das entrevistas para aferir possíveis ajustes e adequações. Verificação dos resultados e aplicação da técnica com jornalistas (6 entrevistados) durante o 14ª Congresso Internacional de Jornalismo Investigativo da Associação Brasileira de Jornalismo

Investigativo (Abraji). Análise dos aspectos percebidos, adequados e negligenciados nas investigações jornalísticas realizadas em espaços vigiados e indicação da percepção dos jornalistas em relação à vigilância digital.

4ª Etapa - O objetivo desta etapa é apontar as ações que estão sendo desenvolvidas, perceber possíveis lacunas e problemáticas que envolvem a vigilância, o vazamento de dados e o acesso às novas fontes de informação. A partir da análise das entrevistas em profundidade e do mapeamento de relatórios e tipificação de casos concretos, avaliamos as melhores condições para estabelecer contato com jornalistas investigativos brasileiros para aplicação de questionário. Para tanto, projetamos a aplicação de uma *survey* baseada na técnica bola de neve (GOODMAN, 1961), que nos auxiliou na formação da amostragem. Basicamente, a bola de neve é uma técnica que permite fazer uma amostragem não probabilística que ocorre a partir da seleção, intencional ou de acordo com a conveniência, de um sujeito com características predefinidas. Com base em uma abordagem aleatória, que restringe o grupo analisado, os sujeitos selecionados indicam outros indivíduos para integrar a amostra.

A aplicação de questionários com jornalistas que trabalham com temas sensíveis buscou evidenciar regularidades e diferenças nas percepções sobre as possibilidades de vigilância digital contemporânea, apontando os seguintes elementos: métodos adotados em investigações jornalísticas no ambiente digital; aferição da consciência de riscos digitais; identificação de capacidades (utilização de ferramentas de segurança atreladas com a comunicação digital); vulnerabilidades (como são realizados os contatos com as fontes); ameaças (como são tratados os dados e informações sensíveis). Por fim, realizamos a avaliação de temas e apontamentos; limitações da abordagem; coleta e análise de dados; interpretação das informações; apresentação dos resultados.

Os apêndices apresentam o roteiro das entrevistas em profundidade (apêndice A), as bases para o formulário da *survey* (apêndice B), as seis entrevistas em profundidade (apêndice C), as principais ameaças, vulnerabilidades e capacidades digitais para jornalistas investigativos (apêndice D) e gráficos e tabelas da *survey* (apêndice E).

As etapas elencadas exploraram aspectos contextuais, a disseminação de informações, ações e condutas jornalísticas, *leaks*[8] como fontes de dados e apuração, noções técnicas ligadas à internet, ferramentas de segurança para jornalistas, criptografia de dispositivos e comunicações, bases de dados, proteção e armazenamento de dados coletados, interesses e conflitos conexos com a vigilância e políticas de internet.

[8] O termo se refere ao ato de vazar ou vazamento de informações, a palavra costuma ser utilizada para denotar o escapamento de informações privadas ou confidenciais que se tornam públicas.

Partimos da premissa de que o aumento da capacidade de vigilância comunicacional de governos e de corporações transnacionais modificou o jornalismo investigativo e apresenta aspectos que permitem o emprego de uma noção de jornalismo vigilante baseada em métodos (possibilidades/necessidades) e limitações (vulnerabilidades) associados à investigação jornalística contemporânea e ao contexto digital em que ela está inserida. Pretendemos demonstrar as principais mudanças na investigação jornalística no ambiente digital e a necessidade de apropriação de novos métodos associados com as possibilidades e vulnerabilidades do jornalismo investigativo diante da potencial vigilância nas comunicações digitais.

O *corpus* central do trabalho é composto por materiais distintos. Para examinar as principais vulnerabilidades e potencialidades do jornalismo investigativo brasileiro, exploramos diretrizes, relatórios e proposições de defensores de direitos digitais e organizações jornalísticas afetadas pelas possibilidades de vigilância digital. Um elemento fundamental são as percepções dos próprios jornalistas e os casos que envolvem a materialização das vulnerabilidades e potencialidades atreladas à vigilância digital.

Esta pesquisa parte dos seguintes pressupostos: a) A investigação jornalística envolvida pelas possibilidades tecnológicas pode ser limitada por ferramentas de vigilância comunicacional; b) As ferramentas de comunicação digital facilitam a projeção de ações ligadas ao jornalismo, ao ativismo e ao hacktivismo[9] e, paralelamente, fazem emergir a urgência da proteção das comunicações e fontes dos jornalistas; c) A desproporção entre a capacidade de vigilância do Estado e de grandes corporações transnacionais em relação ao jornalismo gera consequências nocivas à democracia.

Esta tese está dividida em quatro capítulos.

O primeiro capítulo caracteriza o conceito de vigilância em paralelo aos aspectos do jornalismo transpassados pelo ambiente digital. Trata de ciberativismo e vigilância inversa por meio das interseções entre segurança e liberdades, vigilância distribuída e autovigilância. Apresenta motivações e desafios relacionados com a atividade jornalística em tempos de vigilância em massa, intrusão comunicacional, exposição e propagação de dados em tempo real, a custos baixos, em volume gigantesco – o que não apenas dificulta seu tratamento e refinamento, mas também o consumo, guarda e proteção a partir da avaliação de casos

[9] Nesse estudo, entendemos hacktivismo como uma forma de ativismo por meio de técnicas e habilidades específicas (escrita de código fonte, manipulação de bits, etc.) para promover ideologia política relacionada à liberdade de expressão e aos direitos humanos.

jornalísticos. Indica a necessidade de adoção de uma cultura de segurança digital para jornalistas no ambiente virtual a partir de medidas de contravigilância.

O segundo apresenta as particularidades da relação entre o jornalismo e a vigilância e discute os seus entornos, buscando perceber elementos de tensão entre o papel de vigilante que os jornalistas exercem na sociedade em um contexto de intrusão comunicacional massiva onde os próprios jornalistas são vigiados e produzem conteúdos relacionados com informações jornalísticas sobre aparatos, casos e contextos monitorados. O capítulo trata das relações entre investigação jornalística e vigilância comunicacional, apresenta um quadro contextual do jornalismo investigativo contemporâneo no Brasil (aspectos econômicos, regulatórios, políticos e jornalísticos) e uma noção de "jornalismo vigilante".

No terceiro capítulo são mapeados e discutidos relatórios de entidades representativas (nacionais e internacionais) que registram a incidência de ataques digitais que têm como fundamento a proposição de uma tipificação própria. O capítulo debate vulnerabilidades, ameaças e capacidades digitais. Com base em uma equação que envolve os três fatores (riscos digitais = ameaças digitais x vulnerabilidades digitais/capacidades digitais), estruturamos um quadro de riscos digitais para jornalistas investigativos. O texto também aborda a segurança digital para jornalistas, apresenta um conjunto de ferramentas e possibilidades que podem ser exploradas pelos jornalistas e as suas implicações, particularmente relacionadas às formas de intrusão comunicacional.

O quarto capítulo apresenta os resultados alcançados nas entrevistas em profundidade e trata da *survey* aplicada no âmbito de jornalistas que abordam temas sensíveis. Descreve o contato e a realização de entrevistas que abordam elementos relacionados a métodos adotados em investigações jornalísticas no ambiente digital, percepção de riscos digitais por parte dos jornalistas investigativos, identificação das principais capacidades, vulnerabilidades e ameaças digitais. Nessa etapa, avaliamos os dados coletados, detalhes do percurso metodológico e a interpretação das informações.

Nas considerações finais, retomamos os principais aspectos desenvolvidos em cada um dos capítulos e o percurso percorrido, apresentamos as limitações do estudo e uma síntese dos resultados. Buscamos verificar entendimentos e transformações culturais que estão provocando revisões e adaptações nas práticas jornalísticas e oferecemos proposições, particularmente relacionadas ao processo de apuração e checagem na investigação de temas sensíveis.

1 ASPECTOS CONCEITUAIS DE VIGILÂNCIA E DO JORNALISMO NO AMBIENTE DIGITAL

> *Uma cultura de vigilância sem precedentes está emergindo. Sua principal característica é que as pessoas participem ativamente de uma tentativa de regular sua própria vigilância e a vigilância dos outros. Há evidências crescentes de padrões de perspectivas, panoramas ou mentalidades sobre vigilância, juntamente com alguns modos intimamente relacionados de estabelecer, negociar ou resistir à vigilância. Estes chamo de imaginários de vigilância e práticas de vigilância, respectivamente. Eles são analiticamente distinguíveis, mas não separáveis. Eles se somam um ao outro (LYON, 2017, p. 824, tradução livre)*[10].

O termo vigilância pode ser relacionado a uma ação, ato ou efeito de vigiar, permanecer alerta, de agir com precaução para não correr riscos, ao cuidado. Gary Marx (2016) destaca que na sociedade contemporânea o termo tem um significado muito amplo. Enquanto alguns significados são mais inclusivos, outros podem ser logicamente ligados, "embora possamos provocar significados sutis e distintos para cada um envolvendo um sentido, atividade ou função particular, todos eles refletem o que o filósofo Ludwig Wittgenstein chama uma família de significados dentro do conceito mais amplo"[11] (MARX, 2016, p. 15, tradução livre). Conforme Marx (2016), em muitas ocasiões a vigilância estratégica envolve um contexto contraditório onde o sujeito retém ou não oferece informações.

> Assim, a vigilância pode ter um componente de descoberta inquisitorial. Por sua vez, o sujeito pode se envolver em proteção de informações e outras práticas projetadas para moldar o que um agente descobre. Ou a vigilância pode envolver informações que estão aguardando para serem descobertas, reveladas, localizadas, criadas, coletadas ou intercaladas, ou pode envolver informações conhecidas, mas que precisam ser validadas[12] (MARX, 2016, p. 16, tradução livre).

Segundo o autor, o campo pode ser distinguido entre vigilância tradicional e nova vigilância. Na vigilância tradicional, a informação tende a permanecer local e compartimentada. Até a digitalização e os avanços que começaram na última metade do

[10] No original: An unprecedented surveillance culture is emerging. Its key feature is that people actively participate in an attempt to regulate their own surveillance and the surveillance of others. There is growing evidence of patterns of perspectives, outlooks, or mentalités on surveillance, along with some closely related modes of initiating, negotiating, or resisting surveillance. These I call surveillance imaginaries and surveillance practices, respectively. They are analytically distinguishable, but not separable. They shade into each other.

[11] No original: while we might tease out subtle and distinctive meanings for each involving a particular sense, activity, or function, they all reflect what the philosopher Ludwig Wittgenstein calls a family of meanings within the broader concept.

[12] No original: Thus, the surveillance may have an inquisitorial, discovery component. In turn, the subject may engage in information protection and other practices designed to shape what an agent discovers. Or the surveillance may involve information that is waiting to be discovered, unveiled, located, created, collected, or collated, or it may involve information that is known but needs to be validated.

século XX, os resultados da vigilância coletados em diferentes formas, lugares e tempos raramente eram combinados. Em relação à nova vigilância, destacam-se os novos meios de medição e armazenamento de dados e novas técnicas estatísticas que melhoraram a análise e significaram o aumento do uso da predição com base na modelagem do comportamento.

> Novas tecnologias extrativas são fundamentais aqui. Ao contrário das tecnologias de industrialização, as ferramentas não são bombas ou brocas, nem a substância extraída é valorada por suas propriedades físicas. As tecnologias são uma ampla família de computadores, sensores, transmissores, análises bioquímicas, espectrógrafos, lentes de vídeo, softwares e práticas de gestão que constroem a "nova vigilância" e que transcendem os sentidos, espaço e tempo, bem como as tradicionais fronteiras do eu, do corpo e do grupo. A substância é informação pessoal[13] (MARX, 2016, p. 1, tradução livre).

Marx (2016) aponta que a vigilância implica o acesso a certos dados pessoais por meio de um agente, bem como de ferramentas, regras ou configurações físicas e logísticas que permitem a descoberta. Por outro lado, a privacidade envolve um sujeito que pode restringir o acesso a seus dados pessoais através de meios relacionados. As duas dimensões envolvem esforços para controlar a informação, seja como descoberta, seja como proteção, e podem ser conectadas de várias maneiras.

Em linha com Marx (2016), Fuchs (2011) afirma que a vigilância é um tipo específico de recuperação de informação, armazenamento e processamento, avaliação e uso que envolvem dano potencial ou real, coerção, violência, relações de poder assimétricas, controle, manipulação, dominação e poder disciplinar. Esses aspectos podem gerar benefícios para certos grupos de interesse às custas de outros grupos ou indivíduos.

> A vigilância está baseada numa lógica de competição. Ela tenta fazer florescer ou evitar certos comportamentos de grupos ou indivíduos reunindo, armazenando, processando, difundindo, avaliando e usando informação sobre seres humanos de forma que a violência física, ideológica ou estrutural, potencial ou real, pode ser direcionada aos humanos de forma a influenciar seu comportamento. Esta influência é originada através de mecanismos coercitivos e traz benefícios para certos grupos em detrimento de outros (FUCHS, 2011, p. 129).

Conforme Fuchs (2011), a vigilância nunca beneficia a todos, entretanto certamente há processos de informação que visam o benefício coletivo. “Denomino tais processos de informação como monitoramento, envolvem o processamento de informações que visam o cuidado, benefícios, solidariedade, ajuda, e cooperação, benefícios a todos e se opõe à

[13] No original: New extractive technologies are central here. Unlike the technologies of industrialization, the tools are not pumps or drills, nor is the extracted substance valued because of its physical properties. The technologies are a broad family of computers, sensors, transmitters, biochemical assays, spectrographs, video lenses, software, and management practices that construct the “new surveillance” and that transcend the senses, space, and time, as well as the traditional borders of the self, the body, and the group. The substance is personal information.

vigilância" (FUCHS, 2011, p. 129). O autor aponta que formas de monitoramento podem facilmente se tornar formas de vigilância e as tecnologias de vigilância podem ser refinadas, de maneira a servir a propósitos solidários.

Um contexto que propicia formas amplas e eficazes de vigilância, particularmente as que envolvem o ecossistema digital, denota a consolidação de hábitos e condicionantes relacionados com a constituição de uma cultura de vigilância. Nessa esteira, Lyon (2017) percebe que a cultura de vigilância é um produto das condições contemporâneas, particularmente da modernidade digital, que ocorre desde o final do século 20, por meio de modos de vigilância corporativos e estatais, mediados pelas novas tecnologias, que estão cada vez mais rápidas e poderosas.

Lyon (2017) enaltece ainda a crescente dependência das ferramentas digitais nas relações cotidianas que são naturalizadas pelas instituições e pelo poder político-econômico, pela busca por segurança e pelo engajamento nas mídias sociais. "Nós concordamos como nunca antes em nossa própria vigilância, compartilhando - de forma voluntária ou intencional, ou não - nossas informações pessoais no domínio público online. A cultura de vigilância ajuda a situar isso" (LYON, 2017, p. 826, tradução livre)[14].

Nas últimas décadas, ocorreu uma profusão de formas de vigilância comunicacional impulsionada, principalmente, pela naturalização e consequente aceitação desses processos. Estamos vivenciando um momento de transição que se desenvolve há algum tempo e impacta de forma significativa nas investigações jornalísticas mediadas por ferramentas digitais. Tal transição está conectada com as possibilidades de vigilância comunicacional que estão minando liberdades, afetando direitos civis, interferindo em práticas jornalísticas e percepções sobre o jornalismo.

De acordo com Bauman *et. al.* (2015), grande parte das informações ligadas à vigilância comunicacional, especialmente sobre escala, alcance e sofisticação técnica dessas práticas, surpreendeu até mesmo observadores experientes e seu significado permanece obscuro.

> Isto se deve, em parte, à dificuldade de localização dos detalhes extensos acerca dos sistemas complexos expostos, embora muitos deles pareçam ter consequências graves e imediatas. Esses detalhes também parecem sugerir transgressões significativas nos entendimentos estabelecidos sobre o caráter e a legitimidade das instituições envolvidas em operações de segurança e inteligência, estimulando, assim, intensa controvérsia política. E se deve, em parte, e de modo ainda mais desconcertante, ao fato de que algumas revelações parecem confirmar transformações de longo prazo na política dos Estados, nas relações entre eles e nas

[14] No original: We collude as never before in our own surveillance by sharing—whether willingly or wittingly, or not—our personal information in the online public domain. Surveillance culture helps situate this.

> instituições e normas estabelecidas quanto: aos procedimentos democráticos; ao Estado de Direito; às relações entre Estado e sociedade civil; política pública e interesses econômicos - empresariais ou privados -; à aceitabilidade de normas culturais e, até mesmo quanto a conceitos de subjetividade (BAUMAN *et al.*, 2015, p. 9).

Os autores chamam a atenção para a necessidade urgente de avaliação sistemática da escala, do alcance e do caráter das práticas de vigilância contemporâneas, bem como das justificativas que atraem e das controvérsias que provocam. "Precisamos saber se essas práticas marcam uma reconfiguração significativa das relações entre coleta de informações, vigilância na Internet e outros sistemas de telecomunicações; ou se marcam desafios contínuos aos Direitos Fundamentais na esfera digital" (BAUMAN *et al.*, 2015, p. 9-10). Modernos sistemas de comunicação invasivos e orientados por interesses financeiros, políticos e ideológicos são verdadeiras armas, se forem utilizados para finalidades nocivas.

A grande transformação provocada pela propagação de formas e formatos conexos à vigilância comunicacional se traduz em impactos que um momento de transição pode causar em uma atividade profissional, principalmente em um contexto social que exige ressignificação e esvaziamento de sentido que possibilite uma nova percepção adaptada e reconfigurada pela realidade imposta. "Parece uma questão direta. Mas as instituições que controlam a nossa sociedade em caminhos críticos - grandes burocracias governamentais e empresas privadas poderosas - são cada vez mais opacas, particularmente quando se trata de privacidade e segurança nacional"[15] (SYED, 2017, p. 264, tradução livre).

Nossas proposições estão alinhadas à percepção de que estamos diante de significativas mudanças de instintos, de procedimentos, de hábitos, de interferências, que afetam até mesmo a leitura de cenários e a escrita/relato dos jornalistas. As respostas e constatações a esse respeito ainda são muito incipientes e pouco esclarecedoras. Novos instintos advindos da percepção sensorial dos usuários, tecnologias que captam demandas já existentes na sociedade, necessidades preenchidas por recursos tecnológicos e as ferramentas comunicacionais contemporâneas estão determinando um período histórico sem precedentes para o jornalismo.

> No mundo todo, o jornalismo está em um processo de tornar-se um tipo diferente de profissão. Uma vez organizada em instituições formais, onde os trabalhadores contratados produziriam conteúdo em condições de trabalho altamente estruturadas, embora informais, hoje a experiência vivida por jornalistas profissionais é muito mais precária, fragmentada e em rede. No centro do projeto de compreender o

[15] No original: It seems like a straightforward question. But the institutions that control our society in critical ways—sprawling government bureaucracies and powerful private companies alike—are increasingly opaque, particularly so when it comes to privacy and national security.

> jornalismo como uma profissão, com suas diferentes funções na sociedade, é preciso conceituar o jornalismo para além das antigas organizações jornalísticas (DEUZE; WITSCHGE, 2016, p. 8).

Deuze e Witschge (2016) apontam rupturas que desafiam fundamentalmente as formas dominantes de conceituar, teorizar e analisar as práticas jornalísticas. Para os autores, a teoria do jornalismo predominantemente tem tratado o jornalismo como um objeto estável que é incapaz de abarcar a complexidade, a mudança contínua e o estado do campo. "Em última análise, a nossa exploração dos desenvolvimentos disruptivos sugere que nós precisamos ver o jornalismo como um objeto em movimento" (DEUZE; WITSCHGE, 2016, p. 18). Nesse sentido, o jornalismo estaria evoluindo em níveis distintos interligados ao sistema social, ao contexto, às instituições, às práticas e à população, apresentando mudanças significativas. Os aparatos tecnológicos de vigilância criam um desequilíbrio entre os jornalistas e as ferramentas comunicacionais que eles utilizam, de modo que estão provocando reflexos profundos e singulares na sociedade e mais especificamente na atividade jornalística.

Bell (2017) indica que chegamos a um ponto de transição onde os espaços de notícias já não são de propriedade de noticiários. "A imprensa não é mais responsável pela imprensa livre e perdeu o controle das condutas principais através das quais as histórias chegam ao público"[16] (BELL, 2017, p. 412, tradução livre). De acordo com a autora, a esfera pública é efetivamente operada por um pequeno número de empresas comerciais, com base no Vale do Silício, que não estão sujeitas à regulamentação e à transparência que se deseja para o futuro das comunicações.

> Em grande parte, graças a essas plataformas tecnológicas em desenvolvimento e ao papel das mídias sociais na elevação de novas vozes, o jornalismo profissional agora é aumentado por um número incalculável de jornalistas cidadãos que quebram notícias, agregam contexto e relatam qualquer número de novas ferramentas[17] (BELL, 2017, p. 412, tradução livre).

Para Bell (2016), nenhuma outra plataforma de marca única na história do jornalismo teve a concentração de poder e atenção que o Facebook desfruta. A plataforma utiliza uma série de fórmulas para decidir quais notícias surgirão no topo da página dos usuários. Os algoritmos são mecanismos que ditam o que será difundido e fornecem a base do modelo de negócios para plataformas sociais. Conforme Marín (2016), o Facebook está estreitamente

[16] No original: The press is no longer in charge of the free press and has lost control of the main conduits through which stories reach audiences.
[17] No original: Largely thanks to these developing platform technologies and the role of social media in elevating new voices, professional journalism is now augmented by untold numbers of citizen journalists who break news, add context, and report through any number of new tools.

relacionado ao afeto que é estruturado por dados gerados, acumulados e analisados que produzem um novo ativo. O caráter econômico e o protagonismo como elemento organizador do cotidiano dos usuários o tornam um dispositivo de manipulação de afetividades consumíveis, mercadorias que o transformam em um componente de congregação.

> Se entendermos a liberdade, mesmo o negativo em seu estrato mais profundo, como proponho, como a capacidade de administrar nossas afeições, então parece que a rede, na verdade, constitui uma extensão de nossa liberdade. A dificuldade real da gestão do afetivo em um universo confuso e mudando como condições espaço-temporais reais, desaparece de repente, ao mover o problema para este reservatório emocional que cada usuário possui, para a sua própria conta que, em princípio, o usuário pode como soberano administrar sua biografia, as imagens que melhor se ajustam a cada imperativo, a determinação de quem são seus amigos, ordenar a relevância, determinar o que está sendo pensado, as preferências, fixar os estados emocionais, retornar ao passado de novo e de novo[18] (MARÍN, 2016, p. 36, tradução livre).

Em linha com Marín (2016), a essência do negócio do Facebook está localizada no deslocamento da amizade para a produção de valor econômico, esta característica transpassa o funcionamento da ferramenta que concentra dados pessoais em escala massiva. De acordo com Silveira, Avelino e Souza (2016), o mercado de dados pessoais pode ser entendido como as interações econômicas voltadas à compra e à venda das informações relativas a uma pessoa identificada ou identificável, direta ou indiretamente.

> O mercado de dados pessoais já é a principal fonte de receita para algumas das grandes corporações da economia informacional. Também se tornou fundamental para segmentar a publicidade e organizar amostras de consumidores em públicos mais dispostos a consumir determinados produtos e serviços. Organizado em camadas de captura, processamento, análise, venda de dados, o mercado permite realizar a modulação de comportamentos. Tudo indica que o uso massivo de dados pessoais terá efeitos ambivalentes em nossa sociedade. O cenário atual permite afirmar que o mercado de dados dará maior poder às corporações do que aos cidadãos em relação às trocas que realizam (SILVEIRA; AVELINO; SOUZA, 2016, p. 228).

Silveira, Avelino e Souza (2016) destacam que os interesses da economia informacional estão conectados aos interesses de vigilância dos aparatos de repressão do Estado e que os embates que envolvem os níveis de privacidade na internet definirão o tipo de sociedade em que viveremos. A opressão e o retrocesso democrático estão sendo

[18] No original: La dificultad real de esa gestión de lo afectivo en un universo confuso y cambiante como el de las condiciones espaciotemporales reales, desaparece de pronto al trasladarse el problema a ese depósito afectivo del que cada usuario es duenõ, a su propia cuenta en la que en principio el usuario puede como soberano administrar su biografia, las imágenes que mejor le acomoden a cada ininstante, la determinación de quienes son o no sus amigos, ordenar la relevancia, determinar e fijar que se está pensando, las preferencias, fijar los estados emocionales, regresar al pasado una y otra vez.

impulsionados pelas alardeadas conquistas tecnológicas que são utilizadas como instrumentos de monitoramento da sociedade, como demonstram Fuchs e Trottier (2016).

> As tecnologias não são a causa dessas mudanças, mas um campo, onde essas mudanças e as contradições resultantes se desenrolam. A convergência de atividades sociais e papéis nas mídias sociais resulta no fato de que os dados processados revelam imagens próximas da maioria dos aspectos de nossas vidas. O acesso a uma massa de dados sobre atividades convergentes em papéis sociais convergentes é a razão pela qual tanto as empresas da Internet, como o Facebook e o Google (as maiores agências de publicidade do mundo), bem como as instituições estatais repressivas têm um grande interesse em monitorar dados de redes sociais[19] (FUCHS; TROTTIER, 2016, p. 21, tradução livre).

Os autores enaltecem que o objetivo da vigilância não é apenas coletar dados, mas também usar esses dados para exercer controle social, por meio da cultura de consumo e da informática, que agregaram à vigilância uma perspectiva de rede, onipresente, focada no cotidiano e no consumo e organizada em tempo real. As vidas de grande parte dos indivíduos estão relacionadas com atividades em meios tecnológicos e nas redes de informação.

Nas próximas seções deste capítulo, vamos caracterizar algumas das formas de vigilância recorrentes que envolvem o ambiente de comunicação digital contemporâneo.

1.1 VIGILÂNCIA COMUNICACIONAL ESTATAL

O poder de vigilância e as possibilidades de intrusão comunicacional no ecossistema digital por parte do Estado estão largamente presentes nas formas de comunicação contemporâneas. De maneira geral, a vigilância estatal é realizada por agências de inteligência e amparada na segurança nacional dos países que se apoiam e buscam legitimação em uma política do medo. O desenvolvimento de tecnologias que facilitam ou protegem a segurança dos usuários está ocorrendo em paralelo às destinadas ao controle da vida das pessoas. O poder excessivo do Estado em relação à infraestrutura da internet proporciona o controle de dados, informações e atividades dos jornalistas na Rede.

> O problema é que a liberdade de todos depende cada vez mais de quem controla essa informação que está na internet, mas que nós, os humanos, manejamos. Os seres humanos escrevem as máquinas e os programas que a gerenciam. Os seres humanos

[19] No original: Technologies are not the cause of these changes, but a field, where these changes and resulting contradictions unfold. The convergence of social activities and roles on social media results in the fact that the processed data reveals close pictures of most aspects of our lives. The access to a mass of data about converging activities in converging social roles is the reason why both Internet companies such as Facebook and Google (the world's largest advertising agencies) as well as repressive state institutions have such a huge interest in monitoring social media data.

> continuam a fazer leis. E as leis, no caso da internet, estão nos códigos[20] (ZUAZO, 2015, p. 11-12, tradução livre).

Para Zuazo (2015), a guerra pela liberdade de expressão tem um novo campo de batalha que se formata nas plataformas digitais e envolve usuários, empresas e governos. A batalha pelo controle de dados pessoais e, consequentemente, pelo direito à privacidade está estreitamente conectada com as ferramentas comunicacionais proporcionadas pela internet e com a possibilidade dessa tecnologia ser utilizada como uma arma de vigilância global dos cidadãos. "Saber quem são seus donos, que parte cada um opera e como eles chegaram a ocupar seu lugar de poder nos permitirá entender as guerras que estão chegando e como nos defendermos nelas" [21] (ZUAZO, 2015, p. 36, tradução livre). Conforme a autora, o entendimento da infraestrutura das redes é algo mais simples do que parece e nem sempre os segredos que envolvem essas questões têm relação com as empresas de tecnologia. Em muitas ocasiões perguntas elementares sobre a trajetória que a vida digital dos usuários percorre não são realizadas.

Em uma sociedade de vigilância (MARX, 2015) que cultiva uma cultura de vigilância (LYON, 2017), desenvolvem-se práticas de controle social que envolvem o Estado, o setor privado e as relações interpessoais. Nesse panorama, nos colocamos diante de uma situação em que as possibilidades de vigilância comunicacional são uma ameaça à preservação da liberdade comunicacional. O entendimento desse contexto está estreitamente relacionado às estruturas e aos processos básicos que sustentam as possibilidades comunicacionais da internet. Os aspectos contextuais e o comportamento dos usuários na rede são elementos fundamentais para a finalidade dos instrumentos de vigilância digital na sociedade.

> Contexto refere-se ao tipo de instituição e organização em questão e aos objetivos, regras e expectativas aos quais eles estão associados. Comportamento refere-se ao tipo de comportamento esperado (baseado em lei ou em expectativas culturais menos formais) e, de fato, mostrado por aqueles em vários papéis de vigilância. Embora compartilhando alguns elementos, diferenças nos contextos de vigilância envolvendo coerção (governo), cuidado (pais e filhos), contratos (trabalho e consumo) e dados pessoais acessíveis livremente flutuantes (o pessoal e o privado dentro do público) precisam ser considerados[22] (MARX, 2015, p. 734, tradução livre).

[20] No original: El problema es que la libertad de todos depende cada vez más de quién controla esa información que está en internet, pero que la manejamos nosotros, los humanos. Los seres humanos escriben las máquinas y los programas que la manejan. Los seres humanos siguen haciendo las leyes. Y las leyes, en el caso de internet, están en los códigos.

[21] No original: Saber quiénes son sus dueños, qué parte opera cada uno y cómo llegó a ocupar su lugar de poder nos permitirá entender las guerras que vienen y cómo defendernos en ellas.

[22] No original: Context refers to the type of institution and organization in question and to the goals, rules, and expectations they are associated with. Comportment refers to the kind of behavior expected (whether based on law or less formal cultural expectations) of, and actually shown by, those in various surveillance roles. While

Nesse sentido, Marx (2015) defende que a vigilância pode ser considerada um processo genérico característico de sistemas vivos com fronteiras de informação e não algo restrito aos governos, espionagem ou sigilo. A simplificação desse processo provoca concepções precipitadas e pouco esclarecedoras. Em inúmeras ocasiões a relação entre vigilância e privacidade demonstra a dinâmica não linear que acompanha os entornos dessa problemática. Nelas, a privacidade é entendida como um elemento de oposição à vigilância. No entanto, a vigilância também pode ser um meio de assegurar a privacidade através de controles de acesso às informações pessoais. "Embora a atenção da mídia aos problemas associados à vigilância inadequada (particularmente pelo governo) esteja presente, também há problemas associados à falha em usar a vigilância quando for apropriado"[23] (MARX, 2015, p. 734, tradução livre). Como já ressaltamos, esse é um importante ponto de intersecção entre as possibilidades de vigilância comunicacional e a prática jornalística, pois em inúmeras ocasiões os canais de comunicação ratificam e legitimam uma percepção de insegurança e disseminam o medo.

Conforme Bauman e Lyon (2014), a vigilância é um aspecto cada vez mais presente nas notícias diárias e essa condição reflete sua crescente importância em muitas dimensões da vida em sociedade.

> À medida que esse mundo vem se transformando ao longo de sucessivas gerações, a vigilância assume características sempre em mutação. Hoje, as sociedades modernas parecem tão fluidas que faz sentido imaginar que elas estejam numa fase "líquida". Sempre em movimento, mas muitas vezes carecendo de certezas e de vínculos duráveis, os atuais cidadãos, trabalhadores, consumidores e viajantes também descobrem que seus movimentos são monitorados, acompanhados e observados. A vigilância se insinua em estado líquido (BAUMAN; LYON, 2014, p. 4).

As formas de vigilância têm se expandido de maneira silenciosa por muitas décadas, no entanto elas são uma característica básica do mundo moderno perpassado por possibilidades de monitoramento, rastreamento, localização, classificação e observação sistemática. Em linha com Marx (2015), Bauman e Lyon (2014) destacam o contexto como uma característica central para o entendimento do papel da vigilância no meio social.

No histórico de estudos relacionados às formas de vigilância que envolvem o controle social, destaca-se Foucault (1987), que buscou entender as formas externas e internas que

---

sharing some elements, differences in surveillance contexts involving coercion (government), care (parents and children), contracts (work and consumption) and free-floating accessible personal data (the personal and private within the public) need consideration.

[23] No original: While media attention to the problems associated with inappropriate surveillance (particularly by government) is present, there are also problems associated with the failure to use surveillance when it is appropriate.

constituem a sujeição à ordem estabelecida, por meio de processos disciplinadores relacionados ao contexto social.

> O momento histórico das disciplinas é o momento em que nasce uma arte do corpo humano, que visa não unicamente o aumento de suas habilidades, nem tampouco aprofundar sua sujeição, mas a formação de uma relação que no mesmo mecanismo o torna tanto mais obediente, quanto é mais útil, e inversamente. Forma-se então uma política das coerções que são um trabalho sobre o corpo, uma manipulação calculada de seus elementos, de seus gestos, de seus comportamentos. O corpo humano entra numa maquinaria de poder que o esquadrinha, o desarticula e o recompõe. Uma "anatomia política", que é também igualmente uma "mecânica do poder", está nascendo; ela define como se pode ter domínio sobre o corpo dos outros, não simplesmente para que façam o que se quer, mas para que operem como se quer, com as técnicas, segundo a rapidez e a eficácia que se determina. A disciplina fabrica assim corpos submissos e exercitados, corpos "dóceis" (FOUCAULT, 1987, p. 164).

Dessa forma, o controle social pode ser associado a um processo de constituição de regras e normas sociais que afetam as ações individuais de acordo com o que aprendemos ser certo ou errado. Segundo Foucault (1987), o processo de disseminação sistemática de dispositivos disciplinares permite a vigilância e o controle social mais eficazes. A partir da noção de panóptico empregada por Jeremy Bentham, Foucault (1987) aborda sua perspectiva de sociedade disciplinar. Bentham (1979) estudou o sistema penitenciário e criou o projeto de prisão circular que conta com um observador central que tem a capacidade de vigiar o presídio por meio do sistema panóptico.

> Se existe uma maneira de se tornar dono de tudo o que pode acontecer a um certo número de homens, de dispor de tudo o que os rodeia, para que eles causem a impressão que desejam produzir, para garantir suas ações, suas conexões e de todas as circunstâncias de sua vida, para que nada possa ser ignorado, nem reduzir o efeito desejado, não se pode duvidar que um instrumento desse tipo seja um instrumento muito enérgico e muito útil que os governos possam aplicar a diferentes objetos da maior importância[24] (BENTHAM, 1979, p. 33, tradução livre).

Para Bentham (1979), o sistema seria aplicável a prisões, escolas, hospitais, fábricas e facilitaria o controle desses estabelecimentos. Na perspectiva do conceito de panopticismo de Foucault (1987), o efeito panóptico produz sujeitos autodisciplinados que devem assumir que estão sendo vigiados em todos os momentos, mesmo quando ninguém esteja na torre vigiando. Diante da possibilidade um efeito incapacitante, atualmente, os sistemas

[24] No original: Si se hallára un medio de hacerse dueño de todo lo que puede suceder á un cierto número de hombres, de disponer todo lo que les rodea, de modo que hiciese en ellos la impresión que se quiere proclucir, de asegurarse de sus acciones, de sus conexiones, y de todas las circunstancias de su vida, de manera que nada pudiera ignorarse, ni coiltrariar el efecto deseado, no se puede dudar que un instrumento de esta especie, seria un instrumento muy enérgico y muy útil que las gobiernos podrian aplicar á diferentes objetos de la mayor irnportancia.

contemporâneos de vigilância digital operam em condições quase imperceptíveis para a maioria dos sujeitos. Os mecanismos são subsidiados por hardwares, cabos de fibra óptica, satélites e torres de telefone móvel.

Os estudos também passam pelas abordagens conectadas com a proteção da sociedade, especialmente após eventos de 11 de setembro de 2001[25], que aumentaram a atenção pública e acadêmica sobre o tema. De acordo com Marx (2015), a temática em sua forma moderna tem sido de interesse para estudiosos desde a década de 1950. "Isso está relacionado a uma maior conscientização das violações dos direitos humanos do colonialismo, do fascismo e do comunismo e do comportamento antidemocrático nas sociedades democráticas"[26] (MARX, 2015, p. 734, tradução livre). Na análise realizada por Marx (2015), a obra literária de Huxley (1932)[27], Orwell (1949)[28] e Kafka (1925)[29], o surgimento de computadores e outras novas tecnologias com suas profundas implicações para o comportamento social, a organização e a sociedade também são fatores cruciais para o desenvolvimento do campo.

No início do século XXI, nos deparamos com novas tecnologias comunicacionais que permitem novas formas de vigilância, a partir dessa perspectiva, Marx (2015) destaca que uma diversidade de abordagens sobre vigilância recorre aos escritores para descrever o surgimento de um novo tipo de sociedade, com novas formas e um novo ordenamento social.

Bauman e Lyon (2014) sugerem que essas premissas facilitam e direcionam a interpretação da difusão da vigilância como um fenômeno tecnológico ou como algo que lida simplesmente com controle social e o "Grande Irmão". Essas avaliações colocam toda a ênfase da problemática em instrumentos e tiranos, ignorando as motivações da vigilância, as

[25] Os eventos categorizados como atentados terroristas ocorreram simultaneamente no dia de 11 de setembro de 2001 e envolveram uma série de ataques suicidas contra os Estados Unidos da América. Dezenove terroristas sequestraram quatro aviões comerciais de passageiros, dois desses aviões colidiram intencionalmente nas Torres Gêmeas do complexo empresarial do World Trade Center, na cidade de Nova Iorque. O terceiro avião colidiu contra o Pentágono, sede do Departamento de Defesa dos Estados Unidos, no Condado de Arlington, Virgínia, nos arredores de Washington, já o quarto avião caiu em um campo aberto próximo de Shanksville, na Pensilvânia, depois de alguns de seus passageiros e tripulantes terem tentado retomar o controle da aeronave dos sequestradores, que a tinham reencaminhado na direção da capital estadunidense.

[26] No original: This is related to greater awareness of the human rights abuses of colonialism, fascism, and communism and anti-democratic behavior within democratic societies.

[27] Marx (2015) não cita especificamente as obras de cada um dos autores, no entanto, três obras distópicas destacam-se em relação aos escritores mencionados. *Admirável Mundo Novo*, romance escrito em 1931 por Aldous Huxley. Publicado em 1932, trata de uma história que se passa em Londres no ano 2540 (632 DF - Depois de Ford) e antecipa desenvolvimentos em tecnologia, manipulação e condicionamento que se combinam para modificar profundamente a sociedade.

[28] *1984* é um romance distópico de autoria do escritor inglês George Orwell que foi publicado em 1949. O romance apresenta a tirania, amparada pelas possibilidades de vigiar a sociedade, que é empregada pelo personagem "Grande Irmão".

[29] *O Processo* é um romance do escritor checo Franz Kafka, que conta a história de Josef K., que acorda certa manhã, é processado e sujeito a longo e incompreensível processo por um crime não especificado, todas as suas ações e toda a sua vida se tornam parte do julgamento, quer ele saiba ou não.

ideologias que a impulsionam, os eventos que a possibilitam e as pessoas comuns que concordam com ela, a questionam ou decidem que, se não podem vencê-la, é melhor juntarem-se a ela.

> São enormes os desafios que isso apresenta. Expressando de uma forma muito simples, as novas práticas de vigilância, baseadas no processamento de informações e não nos discursos que Foucault tinha em mente, permitem uma nova transparência, em que não somente os cidadãos, mas todos nós, por todo o espectro dos papéis que desempenhamos na vida cotidiana, somos permanentemente checados, monitorados, testados, avaliados, apreciados e julgados. Mas, claramente, o inverso não é verdadeiro. À medida que os detalhes de nossa vida diária se tornam mais transparentes às organizações de vigilância, suas próprias atividades são cada vez mais difíceis de discernir. À proporção que o poder se move à velocidade dos sinais eletrônicos na fluidez da modernidade líquida, a transparência simultaneamente aumenta para uns e diminui para outros (BAUMAN; LYON, 2014, p. 13).

A obscuridade das ações de vigilância comunicacional não são algo necessariamente planejado, entretanto as estratégias vinculadas às novas ferramentas de monitoramento têm a ver com aspectos técnicos sofisticados e fluxos de dados de difícil entendimento e organização. Outra parte dessa problemática que é destacada por Bauman e Lyon (2014) diz respeito ao sigilo que cerca a segurança nacional e a competição comercial.

Diante da modernidade líquida, grande parte das informações pessoais vigorosamente absorvidas pelas organizações é, na verdade, disponibilizada por pessoas que usam *smartphones*, realizam compras em *shoppings*, viajam de férias, divertem-se ou navegam pela internet. “Passamos nossos cartões, repetimos nossos códigos postais e mostramos nossas identidades de forma rotineira, automática, espontânea” (BAUMAN; LYON, 2014, p. 14). As formas de restrição de liberdade comunicacional e consequente intervenção no comportamento dos usuários da internet vêm se consolidando silenciosamente travestidas pela política da sensação de insegurança e pela naturalização das múltiplas formas de (auto)vigilância presentes no cotidiano dos indivíduos.

O poder de vigilância comunicacional estatal demonstrado pelas revelações de Edward Snowden apontou duas consequências importantes para o jornalismo. Em linha com Lyon (2016), tanto o que pode ser apreendido a partir dos documentos divulgados, quanto o que pode ser visto de seus impactos diretos fornecem a base para revisões sérias de algumas suposições sobre a vigilância no século XXI.

> Para dar um exemplo, o próprio termo “vigilância” pode exigir algumas novas qualificações. O que se sabe sobre as práticas da NSA levanta questões sobre a suposta clara distinção entre “vigilância de massa” e “vigilância orientada”, e o uso indiscriminado de “metadados” que coloca em primeiro plano debates de longa data sobre como definir “dados pessoais” (ou “informações pessoalmente identificáveis”). O que vale para o “sujeito” da vigilância aplica-se à “privacidade” também. Cada qual requer alguma reflexão séria (LYON, 2016, p. 25).

Lyon (2016) afirma que sem necessariamente estarmos cientes disso, todos nós fornecemos dados para a NSA e suas agências cognatas, apenas entrando em contato com os outros por via eletrônica. No momento em que as notícias surgiram pela primeira vez no jornal *The Guardian*, em 5 de junho de 2013, vários fatos foram surpreendentes. Uma gigante das telecomunicações (Verizon) foi convencida pela Agência de Segurança estadunidense a conceder informações sobre todas as ligações telefônicas dentro dos EUA e entre os EUA e outros países, realizadas em um determinado período.

A repercussão internacional desencadeada pelos fatos revelados sobre as ações de vigilância em massa demonstrou que os cidadãos estavam inconscientes e despreparados para lidar com a situação instalada. "O debate popular e na mídia sobre Snowden se concentrou, muito frequentemente, em estado de vigilância, principalmente como uma ameaça para os indivíduos, exceto quando o desafio a uma internet livre e aberta foi reconhecido" (LYON, 2016, p. 26). Conforme Lyon (2016), as práticas descobertas por Snowden têm uma longa história, não apenas nos órgãos estatais de inteligência e das agências nacionais de segurança, mas em dimensões que vão desde o policiamento e a administração pública, até o marketing de consumo. Esses aspectos são significativos para aqueles envolvidos no estudo acadêmico da vigilância e para qualquer cidadão que se preocupa com liberdade, democracia e justiça no século XXI.

No entender de Greenwald (2017), as revelações de Snowden desencadearam um momento muito intenso para os meios de comunicação que tiveram que modificar seus procedimentos e para vários países em diferentes continentes que aprenderam pela primeira vez que, ao contrário do que tinham sido levados a acreditar por muitos anos pelo governo dos EUA, este sistema ilimitado de vigilância não é direcionado para terroristas ou outras ameaças à segurança nacional, mas em vez disso é dirigido indistintamente.

> A razão pelas quais eu acho que a intensidade tem sido sustentada por tanto tempo é porque o debate que foi desencadeado por estas revelações realmente acabou sendo sobre muito mais do que apenas vigilância. De fato, os debates foram sobre uma grande variedade de outras questões, pelo menos tão importantes como a questão da vigilância[30] (GREENWALD, 2017, p. 86, tradução livre).

Dentre os debates levantados por Snowden destacam-se o reexame profundo da privacidade individual, o seu significado na era digital e porque ela é importante para manutenção das liberdades comunicacionais. "Este é o poder de um público informado.

[30] No original: The reason that I think the intensity has been so sustained for so long is because the debate that was triggered by these revelations actually ended up being about a lot more than just surveillance. In fact, the debates have been about a wide array of other issues, at least as significant as the question of surveillance.

Terminar a vigilância em massa de chamadas telefônicas privadas sob o *Patriot Act* é uma vitória histórica dos direitos de todos os cidadãos, mas é apenas o último produto de uma mudança na consciência global"[31] (SNOWDEN, 2015, online, tradução livre). As discussões evidenciaram os perigos contundentes que grandes governos, com imenso poder político e econômico, podem exercer.

Uma decisão da Corte Europeia de Direitos Humanos (ECHR) datada de setembro de 2018 aponta que, no Reino Unido, o Tempora, programa de vigilância desenvolvido pelo *Government Communications Headquarters* (GCHQ), permitiu um regime de coleta de dados que violasse os direitos humanos. Conforme os juízes, o sistema de vigilância que foi revelado por Snowden violou o direito à privacidade. "Os métodos do GCHQ para a interceptação em massa de comunicações online violaram a privacidade e não forneceram salvaguardas de vigilância suficientes, decidiu a Corte Europeia de Direitos Humanos"[32]. A decisão é baseada em uma avaliação abrangente alcançada pela Corte das operações de interceptação realizadas pela agência de inteligência britânica.

As ações judiciais foram apresentadas por jornalistas e por uma coalizão de 14 grupos de direitos humanos e organizações de privacidade. Os juízes pontuaram três aspectos da vigilância digital: a) interceptação de comunicações em massa; b) compartilhamento de inteligência; c) obtenção de dados de comunicações de provedores de serviços. Ainda conforme a decisão, o regime de vigilância comunicacional desenvolvido pelo GCHQ violava o artigo 8 da Convenção Europeia sobre Direitos Humanos, que garante a privacidade, sendo que o Tempora interceptava cabos e redes de comunicação, para obter grandes volumes de dados da internet. A jornalista Rachel Oldroyd, do *Bureau of Investigative Journalism*, apontou preocupações relacionadas à liberdade de expressão que envolvem a decisão.

> A liberdade de imprensa é uma pedra fundamental da democracia e os jornalistas devem poder proteger suas fontes. Estamos particularmente preocupados com o efeito inibidor que a ameaça de vigilância do Estado tem sobre denunciantes que querem denunciar irregularidades, e essa decisão forçará nosso governo a implementar salvaguardas[33].

[31] No original: This is the power of an informed public. Ending the mass surveillance of private phone calls under the Patriot Act is a historic victory for the rights of every citizen, but it is only the latest product of a change in global awareness.

[32] Disponível em: https://www.theguardian.com/uk-news/2018/sep/13/gchq-data-collection-violated-human-rights-strasbourg-court-rules. Acesso em: 27 set. 2018. No original: GCHQ's methods for bulk interception of online communications violated privacy and failed to provide sufficient surveillance safeguards, the European court of human rights has ruled.

[33] Disponível em: https://www.theguardian.com/uk-news/2018/sep/13/gchq-data-collection-violated-human-rights-strasbourg-court-rules. Acesso em: 27 set. 2018. No original: The freedom of the press is a vital cornerstone of democracy and journalists must be able to protect their sources. We are particularly concerned about the chilling effect that the threat of state surveillance has on whistleblowers who want to expose wrongdoing, and this ruling will force our government to put safeguards in place.

O debate estimulado pelas revelações de Snowden levantaram questões essenciais sobre o papel adequado do jornalismo em relação à sociedade e sua inserção em contextos democráticos a partir da perspectiva dos processos de vigilância comunicacional, especialmente do tratamento apropriado dispensado pelos jornalistas em relação àqueles que detêm o poder político e econômico.

1.2 VIGILÂNCIA COMUNICACIONAL PRIVADA

A vigilância comunicacional privada tem uma estreita relação com o capitalismo de vigilância (ZUBOFF, 2015). Em inúmeros casos, essas ações de vigilância ocorrem com a anuência dos usuários em diferentes ferramentas de comunicação e de modo mais marcante em plataformas digitais na internet. Grandes corporações transnacionais, como Google e Facebook, destacam-se por concentrar um grande volume de informações pessoais de milhões de usuários e consequente acesso aos parâmetros oriundos delas.

Nesse cenário, as convenções sociais que se desenvolvem no ecossistema digital originam um vetor econômico importante que emerge do big data[34] e é um componente basilar da nova lógica de acumulação de poder econômico que Zuboff (2015) chama de capitalismo de vigilância.

> Essa nova forma de capitalismo da informação visa prever e modificar o comportamento humano como meio de produzir receita e controle do mercado. O capitalismo de vigilância gradualmente se constituiu durante a última década, incorporando novas relações sociais e políticas que ainda não foram bem delineadas ou teorizadas. Embora os "big data" possam ser definidos para outros usos, aqueles não apagam suas origens em um extrativo projeto fundado na indiferença formal às populações que compreendem tanto suas fontes de dados, quanto seus alvos finais[35]. (ZUBOFF, 2015, p. 75-76, tradução livre).

As premissas de Zuboff (2015) ligadas ao capitalismo de vigilância estão essencialmente relacionadas ao big data, tanto no que diz respeito à condição contextual, quanto a uma expressão dessa lógica mercadológica emergente. Em meio ao estabelecimento de práticas perversas de verificação de condutas, as ações de vigilância diluem os direitos de privacidade através de uma redistribuição desigual de potencialidades de vigilância e

[34] O termo "big data" está relacionado a um grande volume de dados que podem estar estruturados ou não. Atualmente, esses dados estão gerando inúmeras questões sociais especialmente ligadas ao armazenamento, manipulação e finalidade das informações. Com capacidade de armazenamento e manejo, os big data podem se tornar um instrumento de vigilância.

[35] No original: This new form of information capitalismo aims to predict and modify human behavior as a means to produce revenue and market control. Surveillance capitalismo has gradually constituted itself during the last decade, embodying a new social relations and politics that have not yet been well delineated or theorized. While 'big data' may be set to other uses, those do not erase its origins in an extractive Project founded on formal indifference to the populations that comprise both its data sources and its ultimate targets.

preservação da segurança digital. A concentração das possibilidades de manutenção da privacidade, particularmente no que diz respeito às corporações transnacionais, instaura um regime de vigilância amplo e repleto de espaços de acúmulo de poder que se dá por meio do controle de dados e informações pessoais dos usuários.

A transparência aplicada no uso e processamento dos dados dos usuários não se aplica aos agentes comerciais que mantêm segredos sobre suas condutas e sobre suas "negociações". Esses instrumentos de manipulação e predição estão privando os usuários de escolhas conectadas às dimensões importantes das inter-relações sociais digitais e as grandes corporações estão obtendo informações por meio de artifícios e estratégias altamente obscuras.

> Os capitalistas de vigilância exploraram habilmente uma defasagem na evolução social, na medida em que o rápido desenvolvimento de suas habilidades para supervisionar o lucro superou a compreensão do público e o eventual desenvolvimento de leis e regulamentações que ele produz. Como resultado, os direitos de privacidade, uma vez acumulados e afirmados, podem ser invocados como legitimação para manter a obscuridade das operações de vigilância [36] (ZUBOFF, 2015, p. 83, tradução livre).

O capitalismo de vigilância apresenta características que podem ser associadas a um novo regime de controle de fatos e de fatores sociais abrangentes que é exercido por meio do monitoramento de dados e ações desenvolvidas no ecossistema digital. Estas situações impõem desafios aos jornalistas que, por meio de suas atividades cotidianas, precisam contrapor a tentativa de instalação de um novo tipo de poder soberano que pode gerar consequências sociais contundentes e imprevisíveis.

De acordo com Van Dijck (2017), as plataformas proprietárias costumeiramente compartilham os metadados agregados de seus usuários com terceiros, com o propósito de marketing personalizado em troca de serviços gratuitos. Até os vazamentos de Snowden não se sabia que as corporações de mídias sociais compartilhavam suas informações com agências de inteligência governamentais.

> Quando Barack Obama defendeu suas políticas administrativas de vigilância em massa, dizendo que não havia "conteúdo, apenas metadados" envolvidos no sistema Prism, acrescentou que os cidadãos não poderiam esperar cem por cento de segurança, cem por cento de privacidade, e nenhum inconveniente. A explicação do presidente ecoava o argumento das companhias de mídia sociais de que os usuários lhes forneciam parte de sua privacidade em troca de convenientes plataformas de serviços gratuitos. Em outras palavras, os metadados parecem ter se tornado a

[36] No original: Surveillance capitalists have skillfully exploited a lag in social evolution as the rapid development of their abilities to surveil for profit outrun public understanding and the eventual development of law and regulation that it produces. In result, privacy rights, once accumulated and asserted, can then be invoked as legitimation for maintaining the obscurity of surveillance operations.

> moeda corrente para os cidadãos pagarem por seus serviços de comunicação e segurança – um desconfortável equilíbrio se instalara na zona de conforto da maioria das pessoas (VAN DIJCK, 2017, p. 42).

Com base em Mayer-Schoenberger e Cukier (2013), Van Dijck (2017) afirma que a datificação pode ser entendida como a transformação da ação social em dados digitais quantificados que permitem o monitoramento em tempo real e análise preditiva dos usuários. Nessa perspectiva, as empresas e as agências governamentais exploram crescentes quantidades de metadados coletados a partir das mídias sociais e plataformas de comunicação, tais como Facebook, Twitter, LinkedIn, Tumblr, iTunes, Skype, YouTube, além de serviços gratuitos de e-mail, como o Gmail e o Hotmail, para rastrear informações sobre o comportamento humano.

> A datificação, como um legítimo meio para acessar, entender e monitorar o comportamento das pessoas está se tornando um princípio central, não apenas entre os adeptos da tecnologia, mas também entre os acadêmicos que a veem como uma revolucionária oportunidade de pesquisa para investigar o comportamento humano (VAN DIJCK, 2017, p. 43).

Van Dijck (2017) aponta que as noções de confiança e crença são particularmente relevantes quando se trata de entender a vigilância de dados (*dataveillance*). Como as revelações e documentos apresentados por Snowden demonstraram, a crença dos usuários nas instituições que armazenam e manuseiam os seus dados é algo essencial para a constituição de um senso de vulnerabilidade, que vale também para instâncias estatais de regulação. De maneira geral, a sensação de vulnerabilidade diante das situações instauradas de vigilância é desencadeada e alimentada por informações jornalísticas.

> Porém, como os jornalistas descobriram, a NSA constantemente desobedecia as decisões judiciais sobre o uso de dados, assim como as corporações estão constantemente testando os limites legais sobre a invasão de privacidade. De modo mais profundo, o caso Snowden alertou mais ainda as pessoas para as práticas inter-relacionadas da inteligência do governo, empresas e da academia na adaptação das premissas ideológicas do dataísmo. Assim, precisamos olhar para a credibilidade de todo o ecossistema de mídia conectiva. Quais são os distintos papéis do governo, corporações e academia em lidar com nossos dados? E qual tipo de atitude crítica é necessária frente a esse complexo sistema de fluxos de informação online? (VAN DIJCK, 2017, p. 43-44).

Para além de fomentar o debate sobre questões-chave relacionadas à vigilância, o jornalismo está interconectado à vigilância comunicacional privada por meio das possibilidades de parametrização de perfis de jornalistas por corporações transnacionais, da intervenção nas suas investigações e no contato com suas fontes de informação. O relatório

"Censura e Vigilância de jornalistas: Um negócio sem escrúpulos"[37], publicado pela RSF em 2017, exemplifica os fatores que permeiam essas possibilidades de vigilância e interceptação no ambiente digital.

> Em novembro de 2016, o New York Times (NYT) revelou que o Facebook - confidencialmente e com o apoio de seu fundador, Mark Zuckerberg - desenvolveu um programa para censurar o conteúdo dos usuários das redes sociais, de acordo com sua localização geográfica. Empregados do Facebook disseram que a empresa dos EUA procura responder às demandas do regime chinês em censura. Com essa ferramenta, a empresa vê seu retorno ao mercado chinês, do qual foi expulso em 2009, durante as rebeliões da minoria uigur no Xinjiang, que utilizou o Facebook para divulgar informações sobre a repressão dos protestos[38] (RSF, 2017, p. 5, tradução livre).

A vigilância comunicacional privada levanta preocupações, de maneira particular, devido à possibilidade de colaboração ativa das corporações com Estados repressores, desenvolvendo a supressão de informações jornalísticas e políticas opacas relacionadas ao controle de dados pessoais dos jornalistas e à moderação de conteúdos. Em 2016, o Twitter enfrentou acusações de censurar jornalistas em diversas ocasiões.

> Em 2016, na Turquia, a rede social, que afirma em seu site que só leva em conta solicitações válidas e corretamente definidas, fez todo o possível para aplicar as ordens dadas pelo regime dias após a tentativa de golpe de 15 de julho, censurando pelo menos vinte contas de jornalistas e meios de comunicação[39] (RSF, 2017, p. 6, tradução livre).

Simon (2017) aponta que associados a governos, atores não estatais estão encontrando formas inovadoras de reprimir a mídia. À medida que novos sistemas de controle de informações são desenvolvidos e tecnologias que permitem que dados sejam cooptados e usados para sufocar a liberdade de expressão, corporações privadas se notabilizam pela manutenção de processos sigilosos. Conforme o autor, atualmente, as estratégias para controlar e gerenciar informações se dividem em três grandes categorias: repressão 2.0, controle político dissimulado e tecnologia de captura.

[37] Disponível em: https://rsf.org/es/informes/censura-y-vigilancia-de-periodistas-un-negocio-sin-escrupulos. Acesso em: 10 jun. 2018.

[38] No original: En noviembre de 2016 The New York Times (NYT) reveló que Facebook de manera confidencial y con el apoyo de su fundador, Mark Zuckerberg – desarrollaba un programa para censurar los contenidos de los usuarios de la red social, según su ubicación geográfica. Empleados de Facebook señalaron que la empresa estadounidense busca poder responder a las exigencias del régimen chino en materia de censura. Con esta herramienta, la firma vislumbra su regreso al mercado chino, del que fue expulsada en 2009, durante las rebeliones de la minoría uigur en Xinjiang, que usaba Facebook para difundir información sobre la represión de las protestas.

[39] No original: En 2016 en Turquía la red social, que afirma en su sitio web que sólo toma en cuenta las solicitudes válidas y definidas correctamente, hizo todo lo posible por aplicar las órdenes dadas por el régimen días después del intento de golpe de Estado del 15 de julio, censurando al menos una veintena de cuentas de periodistas y de medios de comunicación.

A repressão 2.0 está relacionada a uma atualização de táticas antigas que vai da censura estatal à prisão de críticos, com novas tecnologias de informação que incluem *smartphones* e mídias sociais. Já o controle político dissimulado é um esforço sistemático para ocultar ações repressivas, revestindo-as com o aspecto de normas democráticas.

> Os governos podem justificar uma repressão à internet dizendo que é necessário suprimir o discurso de ódio e a incitação à violência. Eles podem encarcerar dezenas de jornalistas críticos justificando como um elemento essencial na luta global contra o terrorismo (SIMON, 2017, p. 2).

Por fim, a tecnologia de captura diz respeito à utilização das mesmas tecnologias que geraram a explosão da informação global para sufocar a dissidência, monitorando e vigiando críticos, bloqueando sites e utilizando *trolling*[40] para calar vozes críticas. De acordo com Simon (2017), a mais insidiosa de todas essas estratégias é semear a confusão através de propaganda e notícias falsas, sendo que elas centram-se no controle político e na manipulação. "Mas, é claro, os governos também procuram capturar a tecnologia que os jornalistas e outros dependem para disseminar informações críticas. Essas mesmas tecnologias podem ser usadas para a vigilância, bloqueio, *trolling* e disseminação de propaganda" (SIMON, 2017, p. 4).

Bell (2017) ressalta que as revelações de Edward Snowden levantaram uma bandeira sobre a convergência das tecnologias de comunicação e porque isso pode comprometer a integridade e segurança de jornalistas e fontes. Para Bell (2017), o exemplo mais nítido do atrito entre as novas plataformas e o papel tradicional da imprensa evidencia-se no conjunto notável de histórias publicadas sobre as atividades da NSA, trazidas à luz pelo material obtido por Snowden. "Estas divulgações especificam que as ferramentas que usamos para o jornalismo - Gmail, Skype, mídias sociais - estão fatalmente comprometidas por serem parte de um estado de vigilância"[41] (BELL, 2017, p. 422, tradução livre). Após os vazamentos de Snowden, plataformas digitais como Google ficaram supostamente surpresas com a forma como as suas infraestruturas foram aproveitadas para obter informações pelas agências de segurança governamentais.

O impacto de plataformas sociais e empresas de tecnologia no jornalismo é algo em andamento, caracterizando-se por sua difícil mensuração e descrição. A emergência de corporações como Facebook, Google e Twitter constituem um período de transição e desafios permanentes para os meios de comunicação e o jornalismo. Além de exercem competências

[40] Troll é uma gíria que designa um usuário cujo comportamento ou comentário busca desestabilizar uma discussão. Trolling é uma estratégia que explora comentários relacionados à ignorância, visando estimular atitudes odientas.

[41] No original: These disclosures spelled out that the tools we use for journalism—Gmail, Skype, social media—are already fatally compromised by being part of a surveillance state.

relacionadas com a distribuição de informações jornalísticas, as plataformas agem na monetização desses conteúdos. Para Bell *et. al.* (2017), as plataformas sociais influenciam o jornalismo em si ao incentivarem a produção de formatos específicos de conteúdo, por exemplo, o *streaming* ou ao ditar padrões gráficos aos meios.

Nessas situações, as plataformas assumem um papel claramente editorial. A estrutura e as métricas apresentadas pelas plataformas digitais não diferenciam a qualidade e a veracidade das informações jornalísticas. Dessa forma, os conteúdos disseminados por esses instrumentos contribuem para a formatação de um ecossistema de desinformação que atravessa o ambiente digital. "O jornalismo com valor cívico – o jornalismo que vigia os detentores do poder ou que fala a estratos menos favorecidos da sociedade – é preterido por um sistema que preza escala e *shareability*[42]" (BELL *et. al.*, 2017, p. 49).

A principal problemática relacionada à vigilância comunicacional privada que envolve o jornalismo está configurada nas limitações impostas pela impossibilidade de vigiar um sistema de hegemonia e poder ao qual o jornalismo está incorporado. As corporações que ofertam plataformas e ferramentas de comunicação digital cultivam a sensação de empoderamento dos usuários, no entanto essas mesmas empresas obtêm recursos financeiros com a venda de dados sobre o comportamento e ações de seus usuários.

> Paralelamente, ao adentrar setores altamente regulamentados (aeroespacial, automotivo, telecomunicações, segurança nacional), muitas empresas de tecnologia estão, cada vez mais, trabalhando em estreita parceria com o Estado, e sob direto controle deste. O resultado é que um pequeno número de empresas detém um controle considerável tanto da imprensa, como de setores que o jornalismo tradicionalmente cobre. Esse conflito põe em xeque a viabilidade do "accountability journalism", sobretudo do trabalho que exige a prestação de contas pelos detentores do poder no governo e em empresas. Esse trabalho exige um grau de independência difícil de imaginar em um mundo no qual a atividade de publicação da imprensa é exercida por controladoras de grandes plataformas digitais. A dúvida é saber como a imprensa vai vigiar os novos nós do poder quando essa mesma imprensa depende deles para distribuição, audiência e receita (BELL *et. al*., 2017, p. 81).

Aspectos como o controle de dados pessoais, constituição de espaços digitais de desinformação e vigilância comunicacional privada perpassam questões que envolvem a salvaguarda de investigações jornalísticas e dos próprios profissionais. Jornalistas, empresas de comunicação e projetos alternativos de jornalismo precisam encontrar formas de resguardar os seus dados e conquistar autonomia em relação às plataformas digitais transnacionais. As soluções possíveis estão conectadas com a utilização de instrumentos e ferramentas de comunicação digital abertas, além da adoção de estratégias e condutas

[42] O termo está relacionado à capacidade de compartilhamento dos conteúdos digitais.

condizentes com o grau de riscos e vulnerabilidades impostas pelo poder político e econômico das plataformas digitais emergentes.

1.3 VIGILÂNCIA DIGITAL DISTRIBUÍDA

A vigilância digital distribuída é uma forma de vigilância que pode ser observada, de maneira particular, através de duas angulações. Ela acontece mais frequentemente nas ferramentas e possibilidades atreladas às mídias sociais e se configura com formatos expressivos de pressão. A intersecção que mais se destaca com as ações jornalísticas, nesse caso, está relacionada à possibilidade de interação praticamente imediata entre os jornalistas e os usuários, assim como à produção de conteúdo por parte do público, que pode complementar ou contradizer as abordagens jornalísticas. A expressão vigilância distribuída proposta por Bruno (2013) pretende designar tanto um modo de funcionamento da vigilância, quanto o seu pertencimento ao contemporâneo, indicando em ambos os casos que as vias de captura e as vias de escape passam por este caráter distribuído.

> Proponho o termo vigilância distribuída como definição do estado geral da vigilância nas sociedades contemporâneas. Em linhas breves, trata-se de uma vigilância que tende a se tornar incorporada a diversos dispositivos, serviços e ambientes que usamos cotidianamente, mas que se exerce de modo descentralizado, não hierárquico e com uma diversidade de propósitos, funções e significações nos mais diferentes setores: nas medidas de segurança e circulação de pessoas, informações e bens; nas estratégias de consumo e marketing; nas formas de comunicação, entretenimento e sociabilidade; na prestação de serviços etc. Nota-se que em certos casos ela se exerce misturada a dispositivos que não são prioritariamente voltados para a vigilância, sendo assim uma função potencial ou um efeito secundário de dispositivos que são projetados inicialmente para outras finalidades – comunicação, publicidade, geolocalização, etc (BRUNO, 2009, p. 2).

Em um cotidiano social marcado pela proliferação de tecnologias comunicacionais digitais de acesso rápido e com o custo relativamente baixo, as práticas de vigilância coletiva tornaram-se algo comum. No âmbito jornalístico, essa possibilidade de pressão e interação coletiva imediata e simultânea gera consequências nocivas e intervenções diretas na prática jornalística. No ambiente digital, diversas mobilizações conexas com a vigilância distribuída exploram as potencialidades das mídias sociais para disseminar informações, compartilhar conteúdos e conectar pessoas. Conforme Bruno (2013), as comunicações cotidianas realizadas no ciberespaço estão cada vez mais sujeitas à coleta, ao registro e à classificação. Essa situação expõe questões sobre as implicações destes dispositivos tecnológicos para a vigilância, o controle e a formatação de relatórios sobre as inclinações, condutas e hábitos de indivíduos e populações.

No ecossistema digital, os formatos de vigilância são amplos e obscuros. “A esta altura, já está claro que, por vigilância distribuída, não se define uma tecnologia ou atividade particular, mas o modo de funcionamento das redes que constituem a vigilância como dispositivo nas sociedades contemporâneas” (BRUNO, 2013, p. 28). Com base nas premissas de Bruno (2013), a vigilância digital distribuída pode ser entendida como redes que ocupam o ambiente digital por meio de formatos participativos e colaborativos. Nesses espaços, que extrapolam o ecossistema digital, os indivíduos são mobilizados a desenvolver uma postura de atenção vigilante sobre o outro.

> Como se pode ver, não se trata de uma simples expansão de modelos historicamente conhecidos, mas de uma outra configuração das práticas e dispositivos em que a vigilância se torna um processo distribuído entre múltiplos agentes, técnicas, funções, contextos, propósitos, afetos etc. As características acima certamente não esgotam as muitas faces de um processo que não apenas é bastante complexo como está em pleno andamento e cujos desdobramentos ainda estão por vir (BRUNO, 2013, p. 36).

De acordo com Bruno (2013), a relação entre internet, mídias digitais e sociedade é relevante. Entretanto, mais importante que isso é ilustrar o grande potencial de aplicação prática dessa inter-relação. As sociedades informacionais envolvidas pelas possibilidades atreladas ao monitoramento coletivo fornecem subsídios para consolidação de relações e dimensões de poder que são desenvolvidos através de processos e estratégias de controle de dados e informações.

1.3.1 Autovigilância e a exposição voluntária

A autovigilância está diretamente atrelada aos dispositivos tecnológicos que fazem parte do cotidiano da sociedade atual e da atividade jornalística em particular. Em meio ao que Lyon (2017) classifica de cultura de vigilância, os jornalistas convivem com o monitoramento permanente e regular das suas ações em meios digitais através de iniciativas de autoexposição. Em muitas ocasiões, a autovigilância que ocorre em ferramentas digitais é consentida pelos jornalistas e exibe formas variadas que se modificam de maneira dinâmica.

> Como uma proporção cada vez maior de nossas relações sociais é mediada digitalmente, os sujeitos estão envolvidos, não meramente como os alvos ou portadores de vigilância, mas como participantes mais experientes e ativos. Isso ocorre mais obviamente através das mídias sociais e do uso da Internet em geral e, sem dúvida, intensificou uma adoção diária de variadas mentalidades e práticas de vigilância[43] (LYON, 2017, p. 828, tradução livre).

[43] No original: As an increasing proportion of our social relationships is digitally mediated, subjects are involved, not merely as the targets or bearers of surveillance, but as more-and-more knowledgeable and active participants.

Lyon (2017) aponta questões fundamentais para a discussão e o entendimento da autoexposição ou exposição voluntária de parcelas consideráveis dos usuários de meios digitais. A conformidade desses indivíduos, dentre os quais estão os jornalistas, em relação às formas de vigilância digital está alinhada com a participação ativa da própria vigilância. O acesso às ferramentas para atividades comunicacionais no ecossistema digital é apenas parte de um quadro mais amplo e complexo que envolve o uso e apropriação das tecnologias. As finalidades comunicacionais desses instrumentos não estão implícitas e não se dão de maneira linear e previsível, pois algumas ferramentas são adotadas de maneira massiva e ampla, enquanto outras são ignoradas e negligenciadas.

Esses fenômenos sociotécnicos dependem do engajamento social, noções e imaginários normativos. A própria ideia de cultura de vigilância empregada por Lyon (2017) implica destacar que questões de como pensar, comportar-se, agir e intervir são criadas dentro de um imaginário social, nesse caso um imaginário vigilante. Os assuntos comuns seguem para o domínio digital, criando consequências variadas que estão ligadas às regras básicas que possibilitam o surgimento de táticas e estratégias de vigilância. Imersos nessa cultura, os jornalistas se apropriam das novas tecnologias comunicacionais e se tornam alvos vulneráveis de formas variadas de vigilância digital.

As tecnologias comunicacionais digitais expandem o poder da Internet e consequentemente causam a expansão das possibilidades de vigilância que, conforme Marx (2016), não estão apenas voltadas para uma pessoa em particular, conhecida de antemão, mas para contextos, lugares e espaços geográficos, períodos de tempo específicos, redes e sistemas. “Por exemplo, esse é o caso da autovigilância, onde o indivíduo é sujeito e agente (por exemplo, monitorando a velocidade de condução de alguém para permanecer dentro do limite)”[44]. (MARX, 2016, p. 18, tradução livre). Para Marx (2016), a “nova vigilância” pode ser definida como um exame de indivíduos, grupos e contextos através do uso de meios técnicos para extrair ou criar informações.

> Nesta definição, o uso de "meios técnicos" para extrair e criar a informação implica a capacidade de ir além do que é naturalmente deslocado para os sentidos e mentes não suportados pela tecnologia, ou o que é voluntariamente relatado. Muitos dos exemplos ampliam os sentidos e as habilidades cognitivas usando artefatos materiais, softwares e processos automatizados, mas os meios técnicos para rootear também podem envolver formas sofisticadas de manipulação, sedução, coerção,

---

This occurs most obviously through social media and Internet use in general and has arguably intensified an everyday adoption of varied surveillance mentalities and practices.

[44] No original: For example, that is the case for self- surveillance, where the individual is both subject and agent (e.g., monitoring one’s driving speed to stay within the limit).

> decepção, infiltrações, informantes e habilidades especiais de observação[45] (MARX, 2016, p. 20, tradução livre).

Essas características afetam de maneira significativa a função vigilante do jornalismo. O jornalismo investigativo e vigilante está se autovigiando e, desta forma, sendo alterado por novas tecnologias de vigilância e comunicação. A disseminação de possibilidades comunicacionais ampliou e diversificou os formatos jornalísticos. No entanto, também apresentou armadilhas arquitetadas a partir de teias constituídas por redes de dados que realizam conexões entre formas de comunicação e vigilância indiscriminadas e diferenciadas. Essas capacidades tecnológicas de armazenamento e manipulação de dados e informações, massivas ou individuais, envolvem funções de extração de informações sensíveis ou imposição de condutas aos jornalistas vigilantes.

A sensibilidade das informações e dados de investigações jornalísticas é uma dimensão fundamental da análise e da noção de autovigilância que propomos. Essa intersecção entre a capacidade de monitoramento, por parte do Estado e de corporações, e a capacidade de manuseio de informações sensíveis, por parte dos jornalistas, apresenta problemáticas múltiplas e complexas que podem colocar em risco os profissionais e suas fontes.

Para além da utilização formal, legal e burocrática relacionada às restrições de acesso à informação do termo sensível no jornalismo, ele abrange métodos de coleta e gerenciamento de conteúdo. Em boa parte das investigações jornalísticas, informações sensíveis de governos e corporações são transmitidas por fontes de informação que revelam questões ligadas ao segredo, especificações e planos. Nesse sentido, a identidade das fontes está imersa em temáticas que podem envolver desde arquivos de inteligência até hábitos de vida de pessoas de interesse.

Quando nos reportamos à autovigilância a principal intersecção entre a vigilância comunicacional e a prática jornalística ocorre por meio dos aparatos tecnológicos que fornecem, na maior parte das vezes, de maneira ativa por parte de seus usuários, conteúdos e informações ligadas à geolocalização, fotos, áudios, contatos, entre outros. A característica mais nociva desta situação é a exposição “voluntária" das ações e conteúdos apurados pelos jornalistas.

[45] No original: In this definition the use of “technical means” to extract and create the information implies the ability to go beyond what is naturally offered to the senses and minds unsupported by technology, or what is voluntarily reported. Many of the examples extend the senses and cognitive abilities by using material artifacts, software, and automated processes, but the technical means for rooting out can also involve sophisticated forms of manipulation, seduction, coercion, deception, infiltrators, informers, and special observational skills.

1.3.2 Vigilância digital consentida

O ecossistema digital apresenta um universo amplo de ferramentas de comunicação digital oferecido "gratuitamente". Aplicações e instrumentos são negociados por dados e informações pessoais dos usuários. Nessa esteira, inúmeros jornalistas estão ofertando de maneira passiva e natural informações sensíveis que envolvem a segurança de fontes, dos envolvidos em investigações jornalísticas e dos próprios jornalistas. A possibilidade de acesso a esses dados e informações origina o que pode ser classificado de vigilância digital consentida. De maneira geral, esse consentimento se dá por meio de termos de uso e políticas de privacidade que raramente são de conhecimento dos usuários.

Bauman e Lyon (2014) nomeiam esses processos e atividades como possibilidades de vigilância norteada pelo consumismo. Essa premissa está ajustada à relação entre vigilância comunicacional e consumismo em mídias sociais. O consumo de plataformas digitais é instigado pelo acesso aos dispositivos eletrônicos.

> As bolhas de filtragem oferecidas pela mídia social, mas infladas por nós quando nelas sopramos nossas preferências e predileções a cada clique do mouse, simplesmente reproduzem essa "introversão" consumista, líquida moderna, que é ao mesmo tempo e paradoxalmente uma forma de extroversão, um desejo de publicidade (BAUMAN; LYON, 2014, p. 86).

Os autores destacam que esse é um processo de longo prazo que envolve as culturas ocidentais e está relacionado com a conexão do desejo de ser visto com a crescente ubiquidade das práticas de vigilância digital que gera inúmeros efeitos. "Um deles diz respeito ao óbvio envolvimento voluntário dos consumidores em sua própria vigilância" (BAUMAN; LYON, 2014, p. 87). Por meio de um processo de atração da atenção, encantamento e gratuidade para utilização, os usuários acabam negligenciando formas básicas de segurança digital e cedendo às estratégias de marketing das empresas de tecnologia. As formas de filtragem criadas no ambiente digital têm o intuito de transformar os dados em mercadorias.

Essa categorização de mercado contribui para a desinformação sobre outros usos negativos que podem ser efetuados a partir da mesma triagem. Para Bauman e Lyon (2014), a falta de cuidado para com as informações pessoais pode nos aquietar, tornando-nos mais complacentes em relação às nossas personas digitais.

> Em vez de perguntarmos por que a pessoa atrás do balcão nos pede número de telefone, identidade e código postal, ou questionarmos a exigência, pela máquina, de novos dados para que a transação se complete, presumimos que deve haver alguma razão que nos beneficiará. Por exemplo, quando se trata do uso, agora generalizado, de "cartões de fidelidade" de cadeias de lojas, linhas aéreas etc., um recente estudo

> internacional mostra que as pessoas "não conhecem ou não se importam" com as conexões entre esses cartões e a elaboração de perfis (BAUMAN; LYON, 2014, p. 87).

As plataformas digitais e as formas de obtenção de dados pessoais são objeto de estudos e discussões acadêmicas que adotam o termo vigilância para delinear práticas de monitoramento e exploração a partir do ecossistema digital, com reflexos claros no jornalismo investigativo. As práticas de vigilância comunicacional estão imersas em regras destinadas a garantir ou evitar certos resultados. Essas configurações de vigilância produzem consequências específicas e estão ligadas aos agentes que desenvolvem as ações, os temas e assuntos vigiados.

Conforme Marx (2016), plataformas como o Facebook, Twitter, Foursquare e as ferramentas de e-mail e telefones celulares utilizadas para fins de autopublicidade e sociabilidade podem ser instrumentos de drenagem de dados. Ferramentas de geolocalização e o histórico de navegação também são duas fontes importantes de extração de dados. Essa exposição pode se dar voluntariamente, de forma ativa ou passiva, e esses elementos podem ser usados para redução da autonomia e privacidade dos usuários. Diante dessas proposições, a vigilância digital consentida pode causar prejuízos contundentes para os jornalistas. A emergência de um espaço em que a vigilância é consentida levanta questões importantes em torno de novas ameaças à liberdade jornalística, à proteção de fontes de informação e aos dados sensíveis.

A vigilância direcionada para os jornalistas pode ter efeitos sobre as práticas relacionadas ao jornalismo investigativo, já que os jornalistas podem evitar cobrir histórias sensíveis e incluir vozes críticas por medo da vigilância comunicacional e das sanções associadas a ela. "O que é evidente a partir das contribuições para esta questão especial é que, à medida que a vigilância se torna cada vez mais abrangente e penetrante, o jornalismo como instituição e uma prática devem desenvolver as ferramentas para esclarecer e explicar essas práticas"[46] (BENNETT *et. al.*, 2017, p. 260, tradução livre).

O entendimento mínimo dos processos de vigilância digital vigentes na sociedade atual é algo obrigatório e vital para que os jornalistas possam promover direitos fundamentais relacionados à privacidade e à manutenção da cidadania digital. A compreensão relativamente limitada das formas de vigilância digital demonstra necessidades emergenciais de esclarecimento dos complexos regimes de monitoramento aos quais os jornalistas estão

[46] No original: What is apparent from the contributions to this special issue is that as surveillance is becoming increasingly all-encompassing and pervasive, journalism as an institution and a practice must develop the tools to shed light on and explain these practices.

expostos e a importância de entendimentos mais claros das formas emergentes de cidadania digital.

1.3.3 Vigilância digital odienta

As ameaças e constrangimentos que emergem das possibilidades comunicacionais e interativas disponibilizadas pelo ambiente digital, particularmente nas mídias sociais, corroboram para a consolidação de um tipo de vigilância digital que visa afetar os jornalistas e consequentemente o trabalho que desenvolvem. O relatório "Violações à Liberdade de Expressão (2015)", produzido pela Artigo 19 [47], demonstra possíveis consequências e desdobramentos nocivos do ambiente digital no cotidiano dos jornalistas.

> Um exemplo de uma dessas campanhas aconteceu no início de 2016, quando um jornal impresso de Minas Gerais veiculou uma entrevista falsa comigo em sua manchete de capa, afirmando que eu teria dito que aposentados são inúteis e mereciam ser reciclados. Isso gerou uma onda de ódio fomentado por sites e páginas em redes sociais e, consequentemente, mais ameaças de morte de todo o país (ARTIGO 19, 2015, p. 26).

No texto "A dimensão real do ódio virtual" do jornalista Leonardo Sakamoto, o autor expressa preocupação com a formatação de grupos que empregam o que chamamos de "vigilância digital odienta". Esses grupos realizam campanhas que tentam colocar em dúvida o trabalho jornalístico e, em última instância, em risco a integridade física e a vida dos jornalistas. No mesmo documento, a Artigo 19 entrevistou a jornalista Lola Aronovich, autora do blog "Escreva Lola, Escreva"[48], que é vítima frequente de ameaças e intimidações na esfera digital. A jornalista afirma que recebe ameaças de morte, estupro, tortura, espancamento, destacando que, por vezes, as formas de intimidação se estendem aos seus familiares.

> Os criminosos divulgam meu endereço residencial, põem fotos da fachada da minha casa, prometem atentados à universidade onde leciono e às faculdades em que sou convidada para palestrar. Ameaçam também meu marido e minha mãe, uma senhora de 80 anos. Além disso, fazem montagens grosseiras com fotos minhas e criam blogs e tuítes falsos em meu nome, dizendo coisas que eu jamais diria (ARTIGO 19, 2015, p. 28).

Os ataques e ameaças relacionados ao ecossistema digital podem ser enquadrados como violações à liberdade de expressão. Atualmente, apesar de inúmeros casos denunciarem a possibilidade de controle e monitoramento da comunicação digital, particularmente por

[47] Disponível em: https://artigo19.org/?p=8022. Acesso em: 24 ago. 2018.
[48] Disponível em: http://escrevalolaescreva.blogspot.com. Acesso em: 24 ago. 2018.

agentes do Estado, a presença de relatos que considerem o espaço digital como um local de risco e ameaça é inexpressivo.

Percebe-se como aspecto preponderante a evidenciação de ataques físicos e de ameaças à integridade de profissionais e, de uma maneira geral, desconsidera-se que, ao longo dos anos, há incidências e um aumento progressivo de casos envolvendo o ambiente digital. Esses episódios apresentam potenciais desdobramentos danosos e consequências nocivas que estão sendo desconsiderados ou precariamente delineados. Evidenciamos a necessidade premente de consideração, alerta e tipificação de ataques digitais relacionados ao jornalismo, tema que abordaremos no capítulo 4. No contexto atual, esses ataques digitais podem ser considerados formas de violência, limitação e controle da atividade jornalística.

A preservação da liberdade comunicacional vai além da possibilidade de expressão, sendo imprescindível a utilização de ferramentas e métodos de manutenção da privacidade dos jornalistas. A possibilidade de sigilo na troca de informações, a conscientização de riscos e a adoção de práticas seguras para minimização de ameaças são elementos essenciais para o jornalismo investigativo contemporâneo.

Em linha com essas premissas, a Associação Brasileira de Jornalismo Investigativo (Abraji) lançou a cartilha "Como lidar com assédio contra jornalistas nas redes (2018)"[49] que evidencia que, nos últimos anos, o ambiente digital tem se tornado um espaço onde se alastram comportamentos extremos. "Pela natureza investigativa da sua profissão, o jornalista está suscetível a críticas. Mas é importante separar a crítica ao trabalho de ofensas à pessoa. Também é fundamental não naturalizar os assédios como se fossem ossos do ofício ser alvo de ataques" (ABRAJI, 2018, p. 3). A publicação ressalta a necessidade de sensibilização de veículos, jornalistas, empresas de tecnologia, entidades ligadas ao jornalismo e à liberdade de expressão e autoridades policiais e da justiça para a gravidade do assédio online, além de recomendar a elaboração de protocolos de defesa digital para jornalistas.

> A Abraji entende que registrar comportamentos abusivos e eventualmente buscar seus direitos na Justiça são meios de mostrar aos agressores que há consequências para a violência praticada na internet. Recentes ataques coordenados a jornalistas nas redes sugerem a atuação de grupos organizados, com diferentes vieses ideológicos, que agem de má-fé para desqualificar o trabalho do jornalista. Tais acontecimentos contribuem para uma desconfiança geral na imprensa, o que não é saudável para nenhuma democracia (ABRAJI, 2018, p. 3).

A exposição às formas de vigilância digital odienta pode provocar danos emocionais e as ações de assédio podem gerar impactos na saúde dos jornalistas e consequentemente nos

[49] Disponível em: http://abraji.org.br/publicacoes/cartilha-como-lidar-com-assedio-contra-jornalistas-nas-redes. Acesso em: 28 ago 2018.

seus cotidianos profissionais. “O assédio virtual é assimétrico porque a vítima não tem controle sobre suas causas e o fim do ciclo de agressão depende quase sempre de uma decisão dos perpetradores” (ABRAJI, 2018, p. 4). Para jornalistas investigativos, a precaução e a utilização de formas de mitigação das vulnerabilidades impostas pelo ambiente digital são fundamentais para evitar o uso de informações e dados pessoais dos profissionais contra suas atividades de investigação. Esses aspectos serão aprofundados nos capítulos 4 e 5 desta pesquisa.

1.4 CONTRAVIGILÂNCIA E FORMAS DE RESISTÊNCIA

Os movimentos e iniciativas atrelados à contravigilância provêm de segmentos sociais e grupos de indivíduos que buscam coibir ações de vigilância por meio de formas de neutralização e resistência praticadas por governos e por corporações transnacionais. De acordo com Marx (2003), os movimentos de contravigilância buscam vigiar aqueles que estão exercendo formas de vigilância a partir da emergência de tecnologias que possibilitaram a "democratização da vigilância". “Certamente há uma maior igualdade no acesso e uso de tecnologias de vigilância hoje do que na maior parte da história. No entanto, estamos certamente longe da equivalência aqui” [50] (MARX, 2003, online, tradução livre). Os pressupostos da contravigilância estão conectados com a defesa da liberdade e da privacidade no ecossistema digital através da proteção dos dados pessoais de usuários.

No entender de Marx (2016), a vigilância tem sido um tema crucial para o contexto social porque está no cerne da ideia de democracia, de dignidade da pessoa e do tipo de sociedade possível. Para o autor, as pesquisas sobre vigilância, tecnologia e sociedade têm impactos sociais, econômicos e culturais relacionados à informação, essenciais para compreender o conjunto de ações e comportamentos de indivíduos e grupos sociais. Marx (2016) aponta que as vantagens dos formatos de monitoramento tecnológicos e de outras estratégias de vigilância são de curta duração e contêm vulnerabilidades. Isso também se aplica aos novos esforços empreendidos para contrariar a vigilância.

O jornalista está no limiar das questões que envolvem a vigilância comunicacional e as possibilidades de resistência a ela. Essa fronteira entre o dever de vigiar os meandros do ecossistema digital e a necessidade de resistir à vigilância presente nele é porosa e de difícil

[50] No original: Certainly there is greater equality in access to and use of surveillance technologies today than in much of recorded history. However, we are certainly far from equivalence here.

identificação. Alguns aspectos contextuais, a complexidade do sistema e a interconectividade tornam as formas de resistência e mitigação das vulnerabilidades algo necessário e essencial.

> A relação entre jornalismo, cidadania e práticas de vigilância, historicamente, tem sido complexa. Por um lado, damos por certo que o jornalismo atua como um cão de guarda sobre as concentrações de poder, garantindo a responsabilidade das instituições na sociedade. Isso inclui prestar atenção às ações das agências de inteligência e aos governos facilitando e subscrevendo suas ações. Fazer isso é particularmente desafiador, dado o choque estrutural entre o segredo institucional dos serviços de inteligência e os principais princípios jornalísticos de transparência e responsabilidade (BENETT *et. al.*, 2017, p. 258).

Os resultados da ampla exposição aos aparatos de vigilância no ambiente digital envolvem a passividade e descrença dos jornalistas em relação ao potencial nocivo e lesivo imposto por esse panorama. Os novos cenários e mercados amparados por tecnologias criam inadvertidamente espaço para contratecnologias. Atualmente, a consolidação de uma imprensa livre e da liberdade comunicacional na internet estão profundamente ligadas às ações, convenções e posturas de resistência diante da vigilância massiva operada por corporações e governos. De acordo com Marx (2016), orientações e informações sobre formas de resistência estão disponíveis e acessíveis.

> Há guias para usar telefones celulares para filmar a polícia. E pode-se encontrar facilmente várias lojas de spyware e catálogos para tecnologias de vigilância e neutralização, embora possa ser difícil para o possível resistente dizer quais ferramentas realmente funcionam (a maioria dos sites da Web relata orgulhosamente sua política de privacidade). O fato de que é difícil dizer qual propósito a ferramenta encobre e suaviza a tendência cultural em relação à espionagem. A autodefesa e o direito de saber são, afinal, valores importantes[51] (MARX, 2016, p. 142, tradução livre).

Ainda conforme Marx (2016), as ações de resistência que os usuários empregam para vencer métodos de vigilância de uma determinada aplicação são muitas vezes encobertas para maximizar a eficácia e/ou evitar suspeitas e sanções. A resistência direta ou a evasão de aplicações que possibilitam a vigilância digital contrastam com uma ampla resposta estratégica, como desafiar uma lei ou incentivar um boicote.

Marx (2016) elenca doze tipos de movimentos e técnicas de neutralização de atividades de vigilância:

- Descoberta (*Discovering*: descubra se a vigilância está em operação e, se estiver, onde, por quem e como);

[51] No original: There are guides for using cell phones to film police. And one can easily find numerous spyware stores and catalogues for surveillance and neutralization technologies, though it may be difficult for the would-be resister to tell what tools actually work (most with web sites proudly reporting their privacy policy). The fact that it is oft en difficult to tell which purpose the tool has shrouds and softens the cultural tilt toward spying. Self-defense and the right to know are, after all, important values.

- Evitando (*Avoiding*: escolha locais, períodos de tempo e meios não sujeitos à vigilância);

- *Piggybacking* (Acompanhe ou acesse um objeto elegível ou qualificável);

- Comutação (*Switching*: transferir um resultado autêntico para alguém ou algo em que a vigilância não se aplique);

- Distorção (*Distorting*: altere a entrada de modo que um resultado tecnicamente válido apareça, mas a inferência extraída dele seja inválida);

- Bloqueio (*Blocking*: elimine ou torne os dados inacessíveis);

- Mascaramento (*Masking*: bloqueie, mas com engano em relação a certos fatores como identidade e localização);

- Quebra (*Breaking*: torne o dispositivo de vigilância inoperável);

- Recusando (*Refusing*: recuse a vigilância e o que é destinado a impedir);

- Explicando (*Explaining*: Contabilize um resultado desfavorável ao reformulá-lo de forma aceitável ou oferecer dados alternativos e reivindicações de especialistas rivais, fazendo reivindicações de direitos e violações processuais);

- Cooperando (*Cooperating;* Faça movimentos com estabelecimento de confiança entre os agentes);

- Contravigilância (*Countersurveillance*; inverta os papéis, para que os sujeitos apliquem as táticas aos agentes de vigilância; aproveitando o potencial de dois gumes das ferramentas).

A contravigilância busca explorar formas de neutralização e combate à vigilância por meio do ativismo baseado em pressupostos conectados com a liberdade de informação. Ações de antivigilância consideram princípios democráticos de responsabilidade e transparência. Movimentos disruptivos buscam romper a vigilância secreta e obscura por meio de mudanças políticas e ações de neutralização em um sistema dinâmico que inclui e antecipa o comportamento de agentes de vigilância.

Nessa esteira, os *cypherpunks* se notabilizam por defenderem a utilização da criptografia e de métodos similares como meio para provocar mudanças sociais e políticas. O Movimento *Cypherpunk* está relacionado à estruturação de um contraponto aos métodos intrusivos realizados por governos e corporações, é uma luta pela liberdade por meio da criptografia. O termo *cypher* tem relação com criptografia ou com criptógrafo e *punk* está conectado com a noção de liberdade. A junção das duas palavras expressa a ideia de liberdade

pela criptografia. Na perspectiva do movimento, criado no início dos anos 90, o mundo está avançando a passos largos na direção de uma nova distopia transnacional.

> Esse fato não tem sido reconhecido de maneira adequada fora dos círculos de segurança nacional. Antes, tem sido encoberto pelo sigilo, pela complexidade e pela escala. A internet, nossa maior ferramenta de emancipação, está sendo transformada no mais perigoso facilitador do totalitarismo que já vimos. A internet é uma ameaça à civilização humana. Essas transformações vêm ocorrendo em silêncio, porque aqueles que sabem o que está acontecendo trabalham na indústria da vigilância global e não têm nenhum incentivo para falar abertamente. Se nada for feito, em poucos anos a civilização global se transformará em uma distopia da vigilância pós-moderna, da qual só os mais habilidosos conseguirão escapar. Na verdade, pode ser que isso já esteja acontecendo (ASSANGE, 2013, p. 16).

Os movimentos de contravigilância são frutos de uma ordem de ações que abrem perspectivas instigantes e viáveis para o jornalismo investigativo. A contravigilância está conectada com a utilização das mesmas ferramentas que os agentes que empregam tipologias de vigilância digital utilizam (registrar o comportamento dos usuários, suas interações com outros sujeitos e defender informações e dados) para vigiar essas ações e minimizar essa condição desfavorável. “Aqui, há uma inversão de papéis, à medida que os sujeitos se tornam agentes e os observadores se tornam observados”[52] (MARX, 2016, p. 166, tradução livre).

O relatório “Violações à Liberdade de Expressão” (2015), produzido pela Artigo 19[53], aborda uma dimensão da liberdade de expressão que extrapola a batalha contra o silenciamento e envolve o direito de acesso e liberdade no espectro eletromagnético e no ciberespaço. No texto “Censura - velhos e novos métodos”, o jornalista Ricardo Gonzalez enaltece que em ambientes supostamente democráticos os meios de censura alcançaram níveis de sofisticação sem precedentes. Esses métodos podem se manifestar por meio de leis que pretendem combater o terrorismo e o crime organizado. Conforme Gonzalez, nos últimos anos, a proliferação de leis contra o terrorismo abrangeu pelo menos 30 países e as ambiguidades de seus conteúdos têm servido para restringir ou inibir o direito de livre expressão.

> Além da vulnerabilidade que esse tipo de lei, ilegítima e desproporcional, gera, o auge e a expansão do ciberespaço e o uso das tecnologias de comunicação e informação abriram um novo capítulo na lista de oportunidades bem como de ameaças ao exercício pleno da liberdade de expressão. A vigilância massiva das comunicações por parte dos Estados e corporações, as restrições ao acesso do ciberespaço, bem como o filtro e o bloqueio de conteúdos, são alguns dos elementos que tem nos obrigado a moderar o otimismo inicial a respeito do uso da internet como veículo propício para o exercício de direitos e liberdades (ARTIGO 19, 2015, p. 8).

[52] No original: Here, there is role reversal, as subjects become agents and the watchers become the watched.
[53] Disponível em: https://artigo19.org/?p=8022. Acesso em: 24 ago. 2018.

A intersecção entre o jornalismo e a vigilância, no caso da contravigilância, está especialmente baseada em atividades relacionadas à segurança da informação e fontes alternativas de conteúdo. A contravigilância ocorre em contextos específicos que podem envolver informações secretas e ações coordenadas. O recorrente número de ameaças relacionadas às ferramentas de comunicação e à vulnerabilidade da autonomia comunicacional de fontes e jornalistas está contribuindo para instauração de um clima de intimidação, o que está exigindo posturas de prudência e conscientização por parte dos jornalistas.

Percebe-se que as limitações ligadas ao monitoramento comunicacional, particularmente no ambiente digital, podem condicionar de forma determinante as ações dos jornalistas e colocar em risco os profissionais, suas fontes e os conteúdos de suas apurações. Nesse sentido, a conscientização e as medidas e ações baseadas nas premissas da contravigilância são necessárias e fundamentais para manutenção da liberdade jornalística no ecossistema digital.

Bennett *et. al.* (2017) afirmam que a era digital oferece novas maneiras para os cidadãos resistirem e contestarem a vigilância através de iniciativas próprias de monitoramento e coleta de dados que podem ser utilizadas para documentar negligências e enfrentar as autoridades.

> Mais do que tudo, o trabalho emergente sobre a cidadania digital demonstra que temos alguma maneira de alargar o desenvolvimento de ferramentas conceituais e práticas para nos ajudar a entender as implicações da vigilância na era digital. Aqui, o jornalismo desempenha um papel fundamental[54] (BENNETT *et. al*., 2017, p. 258, tradução livre).

Como já evidenciamos, Bennett *et. al.* (2017) ratificam que a relação entre jornalismo, cidadania e práticas de vigilância tem sido historicamente complexa. Atualmente, a atuação do jornalista como um cão de guarda sobre as concentrações de poder buscando garantir a responsabilidade das instituições na sociedade é particularmente desafiadora. “Por outro lado, se a cidadania digital envolve facilitar a compreensão, a participação e a agência dos cidadãos, envolve a responsabilidade jornalística de informar os cidadãos sobre questões-chave, incluindo a vigilância”[55] (BENNETT *et. al.*, 2017, p. 258, tradução livre).

[54] No original: More than anything, emerging work on digital citizenship demonstrates that we have some way to go in developing both the conceptual and practical tools to help us understand the implications of surveillance in the digital era. Here, journalism plays a key role.

[55] No original: On the other hand, if digital citizenship involves facilitating understanding, participation and the agency of citizens, it involves journalistic responsibility for informing citizens about key issues, including surveillance.

Contextos políticos e sociais específicos formam diversificados modos de envolvimento dos jornalistas com questões relacionadas à vigilância comunicacional digital, lembrando que essas questões podem ser articuladas e contestadas de maneiras distintas e dinâmicas. “O que é claro é que as complexidades da vigilância na era digital, e como contestar e resistir, são insuficientemente compreendidas e comunicadas pelos jornalistas”[56] (BENNETT *et. al.*, 2017, p. 259, tradução livre).

As plataformas digitais, com o compartilhamento de informações e processos de interação propiciados pelos meios de comunicação digital, potencializam elementos propositivos por meio de arranjos que podem ampliar formas de participação social positivas ou negativas. O uso estratégico dessas possibilidades pode ocasionar ações de intervenção informais estruturadas com fins democráticos ou antidemocráticos. A participação dos membros da audiência em questões que envolvem o jornalismo aproxima os usuários de plataformas digitais dos processos de decisão e acesso às informações que causam impactos no exercício da investigação e disseminação jornalística.

1.4.1 Vigilância inversa

Diante da necessidade de adoção de medidas de proteção e preservação de dados por meio de técnicas de contravigilância em um ambiente digital altamente monitorado, a função jornalística acaba entrelaçada com as atividades de vigilância inversa. Nesse sentido, a noção de contravigilância abarca a ideia de vigilância inversa associada à possibilidade de vigiar o “vigilante” que tem como base os estudos do pesquisador canadense Steve Mann. Mann (2004) criou o termo que descreve essa função de resistência e autodefesa. Na língua inglesa, a palavra *surveillance* significa vigilância. No termo derivado do francês, o prefixo “sur” significa “acima”. Para contrastar com essa perspectiva, o autor cunhou o neologismo *sousveillance* em que “sous” significa “abaixo”. No entender de Mann (2004), a palavra indica a possibilidade de estabelecer formas de monitoramento das ações dos “vigilantes” pelos “vigiados”.

Consideramos essa abordagem como um desdobramento da contravigilância, pois do ecossistema digital emergem ações de vigilância inversa costumeiramente orquestradas por grupos de hacktivismo que buscam a liberdade de informação baseada na cultura hacker através de motivações político-sociais.

[56] No original: What is clear is that the complexities of surveillance in the digital era, and how to contest and resist it, are insufficiently understood and communicated by journalists.

> O hacktivismo é um acrônimo formado pelas palavras hacker e ativismo. À primeira vista, é entendido como a fusão de hacking e ativismo que leva ao uso de ferramentas de hackers para apoiar uma causa social ou política. O termo hacker é usado em referência ao seu significado original, ou seja, um usuário de computador com conhecimento superior em programação, redes e sistemas operacionais, enquanto o ativismo é definido como a prática de ação direta e militante para manifestar-se em favor de uma causa[57] (GÓMEZ, 2017, p. 39-40, tradução livre).

Gómez (2017) afirma que internacionalmente o hacktivismo demonstrou sua capacidade de instalar problemas em discussões públicas, sendo o caso mais significativo o do WikiLeaks, que em 2010 demonstrou que até mesmo a diplomacia mais experiente e a potência militar mais forte do mundo são vulneráveis na era da comunicação global e no avanço das tecnologias da informação.

A partir de uma concepção mais ampla, o WikiLeaks pode ser considerado um símbolo de uma forma de resistência realizada por grupos que têm problematizado as práticas de captura contínua e rotineira de dados pessoais de usuários. Um exemplo disso ocorreu em março de 2017 quando o WikiLeaks realizou uma série de vazamentos chamado de "Vault 7". A ação foi considerada uma das maiores publicações de documentos confidenciais da Agência Central de Inteligência dos Estados Unidos (CIA) e o vazamento mais importante sobre vigilância desde as revelações de Snowden em 2013. Os documentos revelam um programa da CIA chamado "*Weeping Angel*" que acessa TVs Samsung Smart, permitindo que o microfone embutido do controle por voz fosse manipulado remotamente enquanto a TV aparentemente permanecia desligada.

A primeira parte completa da série é composta por milhares de documentos e arquivos de uma rede isolada de alta segurança, situada dentro do Centro de Inteligência Cibernética da CIA, e foi obtida através de uma fonte não identificada, que queria iniciar um debate público sobre a proliferação de armas cibernéticas. Os documentos reafirmam o estado de vigilância em massa e revelam um quadro de avanço permanente dos instrumentos de intrusão. Os vazamentos, que incluem documentos datados de 2013 a 2016, reforçam a necessidade de um debate aprofundado das armas cibernéticas. "Em meio ao coro de empresários que oferecem soluções de monitoramento e jornalistas que oferecem respostas instantâneas, é fácil confundir a retórica com a realidade das novas tecnologias e ignorar as consequências

[57] No original: Hacktivismo es un acrónimo formado con las palabras hacker y activismo. A primera vista se entiende como la fusión del hacking y el activismo que desemboca en la utilización de herramientas hacker para apoyar una causa social o política. El término hacker se utiliza en referencia a su significado original, es decir, un usuario de computadoras con un conocimiento superior en lo que respecta a la programación, redes y sistemas operativos, mientras que activismo se define como la práctica de la acción directa y militante para manifestarse a favor de una causa.

indesejadas” [58] (MARX, 2016, p. 190, tradução livre). Para além da possibilidade de processamento e armazenamento de informações estão dimensões de análise, cruzamento, apropriação e gerenciamento que podem indicar formatos de controle e manipulação de investigações jornalísticas, além de modos de parametrização na difusão e distribuição de conteúdos jornalísticos.

Uma aproximação entre ações hackativistas e o jornalismo está conectada ao Jornalismo Guiado por Dados (JGD)[59]. Conforme Träsel (2013), o JGD compreende diversas práticas profissionais cujo ponto em comum é o uso de dados como principal fonte de informação para a produção de notícias. O objetivo do JGD é produzir, tratar e cruzar grandes quantidades de dados para permitir modos eficientes de recuperação de informações. “Principalmente, as técnicas de JGD permitem ao jornalista encontrar informação com valor noticioso em bases de dados com milhares ou milhões de registros, dificilmente manejáveis sem a ajuda de computadores” (TRÄSEL, 2013, p. 2). Para Träsel (2013), alguns indicativos demonstram que os profissionais envolvidos na prática do JGD compartilham traços característicos da cultura hacker, como a tendência à apropriação de tecnologia, à valorização da liberdade de informação e à disposição para o trabalho colaborativo.

Christofoletti (2008) aponta a força e a amplitude dessa cultura derivada da internet que transformam o ciberespaço em um ambiente fértil de inteligência, sensibilidade e imaginação que influencia o jornalismo. “A emergência de uma ética hacker, por exemplo, contamina o debate sobre a democratização do conhecimento e da informação” (CHRISTOFOLETTI, 2008, p. 103). O tripé da ética hacker que corresponde a liberdade, colaboração e conhecimento pode ser associado ao urgente e necessário debate sobre a liberdade de informação e compartilhamento no ecossistema digital, além da utilização de softwares e ferramentas de código aberto, por parte dos jornalistas vigilantes.

Nessa perspectiva, Kanashiro (2016) afirma que é importante sublinhar o surgimento de novas formas de resistência e contestação que debatem e atuam sobre a captura de informações realizada pelo mercado e nos movimentos que buscam problematizar os mesmos dispositivos e sistemas que servem à captura de dados a partir de sua reapropriação.

[58] No original: Amid the chorus of entrepreneurs offering monitoring solutions and journalists delivering instant answers, it is easy to confuse the rhetoric with the reality of new technologies and to ignore unwanted consequences.

[59] Träsel (2014) aprofunda aspectos do JGD associados à cultura hacker na tese: Entrevistando planilhas: estudo das crenças e do ethos de um grupo de profissionais de jornalismo guiado por dados no Brasil. Disponível em: http://tede2.pucrs.br/tede2/bitstream/tede/4590/1/461784.pdf. Acesso em: 16 nov. 2019.

> As formas de resistência e construção de alternativas são muitas, indo desde o uso de câmeras de celulares para denúncia, até os laboratórios experimentais, sendo mais ricas e frutíferas aquelas que buscam as respostas sem se deslocar de onde já estamos inseridos. É a partir da reapropriação da tecnologia e da construção e proliferação de saberes que se pode propor alternativas e não negando a tecnologia ou falsamente se ausentando de alguns sistemas de comunicação (KANASHIRO, 2016, p. 23).

A vigilância inversa se apresenta como um dos principais aspectos e elementos problematizadores quando o tema é vigilância de informações e demonstra a necessidade de constituição de novas formas de resistência. Para Castells (2015)[60], a mercantilização das informações transforma as pessoas em dados e posteriormente em capital. "A vigilância digital transforma os humanos em objetos digitais"[61]. Entre iniciativas estatais e privadas, a vigilância parece ser totalizante e de forma mais marcante no ambiente digital.

Castells (2015) sugere que estamos vivenciando uma mudança profunda nas formas de comunicação e, nesse cenário, a vigilância digital é preponderante. "As nossas vidas estão relacionadas a atividades em meios tecnológicos e nas redes de informação"[62]. Um conjunto de empresas controla e armazena informações privadas que os usuários podem não querer que se tornem públicas. "Não há privacidade nesse macrotexto em que vivemos"[63]. O autor aponta que a democracia está ameaçada pela vigilância comunicacional, contudo existem espaços para ações de contravigilância.

Essas ações estão envolvidas pelas possibilidades dos usuários vigiarem os abusos do estado, até mesmo do próprio jornalismo, e denunciarem medidas de violação à privacidade por meio de um tipo de vigilância espontânea. Além disso, essas ações são impulsionadas pelas premissas e pelos espaços de liberdade da internet, que devem ser preservados e complementados por ações de autodefesa. A liberdade do ambiente digital está relacionada com a possibilidade das pessoas se manifestarem e defenderem a sua privacidade.

Inúmeras organizações estão engajadas na defesa da liberdade de jornalistas e cidadãos nos espaços digitais, por meio de ações de ciberativismo e de hackativismo ligadas à luta tecnológica que estão estabelecendo espaços de contrapoder e contravigilância. Essas possibilidades autônomas de organização e estruturação de movimentos que buscam mudanças sociais por meio de canais alternativos de informação demonstram que o principal antídoto para a vigilância massiva das comunicações é a própria comunicação a partir de ações ligadas ao jornalismo, ao ciberativismo e ao hackativismo.

[60] Palestra em comemoração ao cinquentenário da Universidade do Estado de Santa Catarina (Udesc) realizada em 14 de maio de 2015. Manuel Castells: "Vigilância, privacidade, poder e contrapoder na era digital".
[61] Idem.
[62] Idem.
[63] Idem.

2 PONTOS DE INTERSECÇÃO ENTRE JORNALISMO E VIGILÂNCIA

> *O plano era fazer contato de forma anônima com jornalistas interessados nas liberdades civis. Jornalistas cujas credenciais e integridades não pudessem ser postas em dúvida. E vazar para eles documentos ultrassecretos roubados – muito embora ainda estivesse um pouco vago como isso seria feito. Documentos que mostrassem evidências da ilegalidade da NSA, que provassem que a agência conduzia programas que violavam a Constituição dos EUA. A julgar pelo que disse mais tarde, o objetivo de Snowden não era expor segredos de Estado no atacado. Pelo contrário: queria entregar uma seleção do material a repórteres e deixá-los exercer seu próprio julgamento editorial (HARDING, 2014, p. 38).*

Historicamente o jornalismo tem uma relação estreita com aspectos ligados à vigilância. Particularmente, o segmento conexo ao jornalismo investigativo carrega em sua essência o dever de vigiar a sociedade. Para além de métodos de coleta e tratamento das informações, o que caracteriza esse tipo de ação jornalística é a busca por revelações, abusos de poder e danos sociais. De acordo com Waisbord (2000), esse tipo de jornalismo está diretamente atrelado aos aspectos contextuais que determinam a prática e as condições oferecidas para o desenvolvimento do papel de vigilante na revelação do que está oculto. Em linha com Waisbord (2000), Reyes (1996) aponta uma caracterização mais ampla que concebe o jornalista investigativo como um especialista em unir elementos dispersos que, em muitas ocasiões, alguém quer esconder.

> Às vezes, todas as peças são obtidas pelo jornalista e outras chegam as suas mãos porque alguém descobre que ele está procurando por elas, mas em ambos os casos, sua perseverança, o fato de estar sempre aí ouvindo queixas e rumores, olhando documentos e seguindo pistas, é a chave para obter uma informação que ficaria oculta se não fosse pelo seu olfato inquisitivo[64] (REYES, 1996, p. 12-13, tradução livre).

Marcet (1997) chama a atenção para as controvérsias relacionadas com a definição de jornalismo investigativo tanto para os profissionais que o praticam, quanto para alguns autores que defendem pontos de vista contraditórios ao analisar essa atividade jornalística. "As discrepâncias surgem no momento de caracterizar o jornalismo investigativo como especialização jornalística ou simplesmente jornalismo bem conduzido" (MARCET, 1997, p. 13). Para Marcet (1997), a técnica do jornalismo investigativo consiste em aplicar todas as diretrizes jornalísticas em certos tópicos que o jornalista investigativo obtém com seu próprio esforço fora dos canais habituais de informação. "Uma coisa é investigar, verificar e

[64] No original: Algunas veces todas las piezas son obtenidas por el periodista y otras llegan a sus manos porque alguien se entera de que las está buscando, pero en ambos casos, su perseverancia, el hecho de estar siempre ahí escuchando quejas y rumores, mirando documentos y siguiendo pistas, es la clave para obtener una información que quedaría oculta si no fuera por su olfato inquisitivo.

contrastar com meticulosidade tudo o que é publicado - pesquisa jornalística - e outra é praticar o jornalismo investigativo" (MARCET, 1997, p. 18). Ainda segundo o autor, essas discrepâncias da origem do jornalismo investigativo significam que não existe uma definição unívoca para essa prática jornalística, no entanto ele adota uma caracterização que aponta para uma atividade jornalística peculiar determinada pela metodologia utilizada pelo profissional para obter os dados, estabelecer um relacionamento especial com certas fontes de informação e buscar objetivos específicos relacionados ao papel crítico que o jornalismo deve desempenhar em uma sociedade democrática.

Segundo estudos de Hanson e Hunter (2013), o jornalismo investigativo envolve expor ao público questões que estão ocultas, seja por meio de uma fonte relacionada ao poder, seja revelando o que está por trás de uma massa desconexa de fatos e circunstâncias que obscurecem entendimentos. Essa prática jornalística requer o uso tanto de fontes e documentos secretos, quanto de informações e dados divulgados. Os autores demarcam diferenças entre o jornalismo convencional e o jornalismo investigativo com base em três elementos centrais das rotinas jornalísticas: pesquisa, relação com as fontes e resultados. A proposta de Hanson e Hunter (2013) pode ser observada no quadro 1.

Quadro 1: Diferenças entre jornalismo convencional e jornalismo investigativo.

JORNALISMO CONVENCIONAL	**JORNALISMO INVESTIGATIVO**
Pesquisa	
As informações são reunidas e relatadas em um ritmo fixo (diário, semanal, mensal).	As informações não podem ser publicadas até que a sua coerência e completude estejam garantidas.
A pesquisa é completada com rapidez. Não se faz uma pesquisa adicional uma vez que a história esteja completa.	A pesquisa continua até que a história esteja confirmada e pode continuar após a sua publicação.
A história se baseia em um mínimo necessário de informações e pode ser bastante curta.	A história se baseia no máximo possível de informações e pode ser bastante longa.
As declarações das fontes podem substituir a documentação.	A reportagem requer uma documentação capaz de apoiar ou negar as informações das fontes.
Relações de fontes	
A boa fé das fontes é presumida, frequentemente sem verificação.	A boa fé das fontes não pode ser presumida; qualquer fonte pode fornecer informações falsas; nenhuma informação pode ser utilizada sem verificação.
As fontes oficiais fornecem informações ao(à) repórter livremente, para promoverem a si e suas metas.	As informações oficiais são ocultadas do(a) repórter, porque a sua revelação pode comprometer os interesses de autoridades ou instituições.
O(a) repórter deve aceitar a versão oficial da história, ainda que ele ou ela possa contrastá-la com comentários ou afirmações de outras fontes.	O(a) repórter pode desafiar ou negar explicitamente a versão oficial de uma história, com base nas informações de fontes independentes.

O(a) repórter dispõe de menos informações do que a maioria das suas fontes.	O(a) repórter dispõe de mais informações do que qualquer uma das suas fontes, considerada individualmente, e de mais informações do que a maioria delas em conjunto.
As fontes são quase sempre identificadas.	As fontes frequentemente não podem ser identificadas, em nome de sua segurança.
Resultados	
A reportagem é vista como um reflexo do mundo, que é aceito assim como ele está dado. O(a) repórter não espera obter resultados além de informar o público.	O(a) repórter se recusa a aceitar o mundo como ele se apresenta. A história visa penetrar ou expor uma dada situação, para que seja reformada ou denunciada, ou, em certos casos, para que se promova um exemplo de um caminho melhor.
A reportagem não requer um engajamento pessoal por parte do(a) repórter.	Sem um engajamento pessoal do(a) repórter, a história nunca será completada.
O(a) repórter busca ser objetivo(a), sem viés ou juízo de valor em relação a qualquer uma das partes envolvidas em uma história.	O(a) repórter busca ser justo(a) e escrupuloso(a) em relação aos fatos da história. Com base nisso, pode designar as suas vítimas, heróis e malfeitores. O(a) repórter também pode oferecer um juízo de valor ou veredito sobre a história.
A estrutura dramática da reportagem não é de grande importância. A história não precisa ter um final, pois as notícias continuam.	A estrutura dramática da história é essencial para o seu impacto e leva a uma conclusão que é oferecida pelo(a) repórter ou por uma fonte.
Erros podem ser cometidos pelo(a) repórter, mas eles são inevitáveis e, normalmente, não têm muita importância.	Os erros expõem o(a) repórter a sanções formais e informais, e podem destruir a credibilidade do(a) repórter e do(s) meio(s) de comunicação.

Fonte: Hanson e Hunter (2013).

Apesar de apresentar alguns aspectos controversos e algumas definições específicas, o quadro de Hanson e Hunter (2013) auxilia na delimitação do jornalismo investigativo como uma prática jornalística que apresenta especificidades relacionadas a um grupo de profissionais que aborda temas sensíveis e situações singulares. O ponto convergente entre várias definições de jornalismo investigativo é a necessidade de ações de investigação do jornalista, através de canais próprios, sobre fatos que alguém deseja esconder.

Na proposta de periodização da história do jornalismo ocidental realizada por Sousa (2008), os anos sessenta e setenta são enaltecidos como importantes períodos para o jornalismo investigativo. De acordo com o autor, esses momentos históricos foram marcados por vários trabalhos de investigação de iniciativa jornalística sobre temas relevantes que expuseram conspirações e dados ocultos, sendo que o mais importante foi o caso *Watergate* (1972-1974). Esse caso alegórico da história do jornalismo pode ser considerado como o momento inicial de uma transformação e da redefinição das atividades relacionadas à vigilância jornalística dos fatos sociais. A ênfase e a importância das revelações, que ocorreram a partir de vazamentos, formataram o episódio e parametrizaram práticas jornalísticas que consolidaram o aspecto vigilante das ações de jornalistas nos anos posteriores.

O trabalho realizado pelos jornalistas Carl Bernstein e Bob Woodward, do jornal norte-americano *The Washington Post*, detalhado no livro "Todos os homens do presidente"[65], indicou que o presidente republicano Richard Nixon estava ligado a um caso de espionagem realizado no comitê do Partido Democrata. A espionagem foi efetivada através de escuta ilegal no Edifício Watergate, em Washington, por agentes ligados ao governo republicano. Na época, Nixon era candidato à reeleição nos Estados Unidos e o objetivo da espionagem era estruturar uma fonte de vazamentos de informações.

Na oportunidade, os jornalistas do *The Washington Post* aprofundaram-se nas investigações ao longo de dois anos (1972-1974) e acessaram informações importantes fornecidas por uma fonte da Casa Branca que ficou conhecida como Garganta Profunda (Mark Felt, ex-agente do *Federal Bureau of Investigation* – FBI). Na epígrafe do livro que aborda o caso, Bernstein e Woodward fazem referência à importância das fontes para a formatação da investigação jornalística.

> Aos outros homens e mulheres da Presidência, que, na Casa Branca e em outros lugares, correram riscos para nos fornecer informações confidenciais. Sem eles, a história do Watergate não teria sido contada pelo Washington Post (BERNSTEIN; WOODWARD, 1978, p. 8).

Com o processo contínuo de investigação e consequentemente pressão, especialmente por meio de conteúdos jornalísticos, Richard Nixon renunciou à presidência no ano de 1974.

Os reflexos de *Watergate* demonstram uma intersecção importante entre o jornalismo e a vigilância, pois o caso evidenciou a capacidade de modificação social, com consequências políticas importantes, a partir do trabalho de apuração e checagem jornalística. Para além da sua função de informar a sociedade, as atividades conectadas ao jornalismo investigativo demonstraram a importância e o potencial de fontes que detêm informações secretas, fato que já tinha sido evidenciado de maneira significativa no caso que ficou conhecido como *Pentagon Papers,* em 1971. Na época Daniel Ellsberg[66] entregou um documento secreto com milhares de páginas que revelavam informações internas do governo estadunidense sobre a Guerra do Vietnã ao *The New York Times*, ao *Washington Post*, entre outros jornais. Os documentos foram retirados clandestinamente dos arquivos do governo estadunidense pela fonte. Nos dois casos, a partir da utilização de técnicas específicas, denúncias levaram aos

[65]BERNSTEIN, Carl. WOODWARD, Bob. Todos os homens do presidente. Livraria Francisco Alves Editora S.A. 1978.

[66]Daniel Ellsberg é um ex-analista militar estadunidense, empregado pela instituição RAND Corporation e posteriormente funcionário do Pentágono. Mais informações sobre o caso: ELLSBERG, Daniel. SECRETS: A Memoir of Vietnam and the Pentagon Papers. Londres: Penguin Books, 2003.

desvios, a sociedade pode reivindicar esclarecimentos e o jornalismo investigativo consolidou o seu potencial vigilante.

Atualmente, existem padrões perceptíveis e identificáveis nessas ações de vigilância jornalística que são desempenhadas por iniciativas jornalísticas independentes e por organizações tradicionais. Nestes casos, atos ilegais do governo, corrupção corporativa e injustiça social são alvos de investigação e do trabalho jornalístico. Este aspecto vigilante é evidenciado por Traquina (2012) como uma característica mitológica da comunidade jornalística atrelada ao papel de servidores do público que buscam saber o que ninguém sabe, o cão de guarda que protege os cidadãos contra abusos, desempenha o papel de quarto poder que vigia os outros poderes e atua como herói do sistema democrático. "Com o desenvolvimento do 'direito da informação' como norma numa democracia, o jornalista foi reconhecido como sendo o agente social que tem como missão 'informar o público' (TRAQUINA, 2012, p. 52). O *ethos* jornalístico define que os membros desta comunidade têm um papel social que envolve o dever de informar e proteger os cidadãos por meio de ações de vigilância social que formatam uma espécie de contrapoder.

Nesse sentido, o contrapoder é entendido como uma forma de poder com potencial de contestar outros poderes, especialmente o poder político e o poder econômico, ou seja, a ação jornalística pode abrandar e, em algumas situações, impedir os excessos do Estado e a hegemonia econômica de entes privados. Desvios, prepotências, injustiças, o conceito de *watchdog*[67] é confrontado diariamente em um contexto social permeado por escândalos, corrupção e formas de exploração que projetam o jornalismo investigativo e sua função social. "O movimento de jornalismo cívico entende que o jornalismo não pode oferecer apenas o que é interessante, mas sobretudo o que é importante para os cidadãos" (TRAQUINA, 2005, p. 212). A característica vigilante do jornalismo seria benéfica para a sociedade por se aproximar da verdade, pela premissa de buscar justiça e o esclarecimento da população.

Kovach e Rosenstiel (2014) destacam princípios basilares de que o jornalismo necessita para fornecer aos cidadãos conteúdos adaptados às exigências da vida em um mundo cada vez mais complexo: a obrigação do jornalismo com a verdade, a lealdade com os cidadãos, a necessidade da verificação, a independência e a vigilância do poder. Os autores ressaltam a manutenção da autonomia e a liberdade para monitorar sistematicamente as outras

[67]Ações jornalísticas que buscam resguardar e assegurar os interesses da coletividade com métodos e técnicas conectados ao monitoramento e à vigilância de desvios de autoridades e injustiças sociais.

forças e instituições poderosas da sociedade como condições imprescindíveis para prática jornalística.

> As raízes da reportagem investigativa foram firmemente estabelecidas nos primeiros periódicos, nas primeiras noções sobre o significado de uma imprensa livre e da Primeira Emenda, e na motivação dos jornalistas ao longo da história da profissão. Estas raízes são tão fortes, elas formam um princípio fundamental: Jornalistas devem ser um monitor independente do poder. (KOVACH; ROSENSTIEL, 2014, p. 119, tradução livre)[68].

Conforme Kovach e Rosenstiel (2014), no contexto jornalístico contemporâneo o princípio da vigilância está sendo ameaçado pelo uso excessivo desta prerrogativa de uma forma enviesada e por um novo tipo de conglomerado empresarial que busca novos modelos para captação de receitas. Este poder de vigilância concedido ao jornalismo revelou-se problemático diante de uma série de incógnitas que surgiram a partir de apropriações inadequadas e transpassadas por fatores imponderáveis dos pressupostos de investigação. Entretanto, diante de novas possibilidades, o jornalismo investigativo formata regularmente alternativas experimentais que se aprimoram com o passar do tempo. Tanto a geração de informações, quanto a recepção destas informações estão sendo adaptadas e adequadas diante do cenário de evolução tecnológica progressiva e constante.

As ferramentas e os aparatos de comunicação carregam em sua essência uma perspectiva que impacta diretamente na sociedade e nas práticas jornalísticas. Essas novas características acabam enaltecendo as particularidades do jornalismo investigativo relacionadas com a vigilância e obtêm importância singular no contexto atual, especialmente para a consolidação e reafirmação dos pressupostos jornalísticos, como destacam Russell e Waisbord (2017).

> A história da Agência Nacional de Segurança de bisbilhotagem global da rede que foi descoberta pelas revelações de Edward Snowden em 2013 sugere novas dinâmicas na mudança da ecologia global da informação. Os relatórios de accountability sobre vigilância governamental e invasão de privacidade foram gerados não exclusivamente a partir de notícias tradicionais, mas também por ativistas e inovadores do jornalismo. As revelações foram divulgadas e sustentadas em um ambiente híbrido onde jornalismo independente e tradicional, criação de mídia, opinião pública e ativismo em rede cooperam e competem para disseminar e dar forma a histórias e estimular reações públicas e políticas (RUSSELL; WAISBORD, 2017, p. 858, tradução livre)[69].

[68] No original: Investigative reporting's roots were firmly established in the very first periodicals, in the earliest notions of the meaning of a free press and the First Amendment, and in the motivation of journalists throughout the profession's history. These roots are so strong, they form a fundamental principle: Journalists must serve as an independent monitor of power.

[69] No original: The story of the National Security Agency global dragnet snooping that was uncovered by Edward Snowden's revelations in 2013 suggests new dynamics in the changing global information ecology. Accountability reporting about government surveillance and invasion of privacy was generated not exclusively from traditional news outlets but also by activists and journalism innovators. The revelations were disseminated

De acordo com Russell e Waisbord (2017), esta nova ecologia comunicacional é caracterizada pelo surgimento de um novo modelo de vigilância baseado em uma fusão entre o tradicional e o alternativo representado por organizações, por exemplo, o WikiLeaks, que não se encaixam nas definições convencionais de organizações de notícias ou de ativismo. Fatos recentes revelaram a dimensão gigantesca dos elementos de vigilância e contravigilância em um ambiente digital largamente interconectado. Atores políticos como Julian Assange e Edward Snowden se notabilizaram pela luta contra os atos de vigilância e o sigilo de informações públicas.

> Se olharmos para a transição da nossa sociedade global para a internet, quando fizemos essa transição a liberdade de circulação pessoal permaneceu basicamente inalterada. A liberdade de comunicação foi enormemente expandida em alguns aspectos, no sentido de que agora podemos nos comunicar com um número muito maior de pessoas; por outro lado, ela também foi enormemente reduzida, porque não temos mais privacidade e as nossas comunicações podem ser interceptadas, armazenadas e, como resultado, usadas contra nós. Então a interação elementar que temos fisicamente com as pessoas acabou se degradando (ASSANGE, 2013, p. 89).

Estudos de Assange (2013) revelam que a vigilância não constitui um problema apenas para a democracia e para a governança, mas também representa um problema geopolítico. “A vigilância de uma população inteira por uma potência estrangeira naturalmente ameaça à soberania. Intervenção após intervenção nas questões da democracia latino-americana nos ensinaram a ser realistas” (ASSANGE, 2013, p. 18). Assange (2013) aponta os riscos inerentes à penetração de corporações estadunidenses, como o Facebook[70], que ocorre por meio da oferta de serviços relacionados às mídias sociais.

O jornalismo investigativo enfrenta inúmeros dilemas e diversas questões, mas atualmente um dos dilemas mais emblemáticos e importantes é o que envolve e confronta de um lado o conformismo e a sujeição diante do quadro de vigilância comunicacional massiva, e de outro a combatividade e a indignação com essa situação. Esse elemento ambivalente se sobressai em contextos opressivos que pretendem restringir liberdades. É o que estamos vivenciando com o amplo avanço das formas de intrusão comunicacional, a capacidade massiva de apropriação e manipulação de dados pessoais e das possibilidades de vigilância digital, por parte de Estados e corporações transnacionais. Para além do monitoramento dos indivíduos está a possibilidade de vigiar as ações de jornalistas. Esses elementos transpassam

---

and sustained in a hybrid environment where independent and traditional journalism, media start-ups, public opinion, and networked activism cooperate and compete to disseminate and shape stories and spur public and political reactions.

[70] É uma mídia social digital, lançada em 4 de fevereiro de 2004, de propriedade privada, que em 2017 superou a marca de 2 bilhões de usuários.

as investigações jornalísticas contemporâneas e podem interferir de maneira determinante na prática cotidiana dos profissionais, particularmente dos que abordam temáticas sensíveis.

Aspectos contextuais atrelados à vigilância comunicacional, particularmente em meios digitais, e características específicas relacionadas com as principais particularidades do jornalismo investigativo brasileiro estão conectados com a tese central desse estudo que está alinhada à necessidade dos jornalistas investigativos cultivarem um senso permanente de sua vulnerabilidade no ambiente digital e adotarem medidas preventivas que fomentem uma cultura de segurança digital para jornalistas.

2.1 AÇÕES JORNALÍSTICAS SOB VIGILÂNCIA

A ampla possibilidade de vigilância do ambiente digital está reconfigurando as relações entre jornalistas e fontes, assim como formatando zonas de tensão entre o jornalismo, o Estado, as corporações transnacionais e a sociedade. A condição de vulnerabilidade dos jornalistas é ratificada pela organização internacional *Human Rights Watch* (2014), que verificou os efeitos da vigilância eletrônica em larga escala sobre a prática jornalística. O estudo da organização envolveu 46 jornalistas estadunidenses e evidenciou as preocupações e mudanças de comportamento dos profissionais em um contexto de vigilância comunicacional em larga escala. Os resultados demonstram que os jornalistas sentem cada vez mais a necessidade de adotar etapas elaboradas para proteger suas fontes e informações e eliminar qualquer rastreamento digital de suas investigações, desde o uso de criptografia de alta qualidade, até abandonar todas as comunicações online e tentar encontrar suas fontes pessoalmente.

> Jornalistas entrevistados para este relatório descreveram a dificuldade de obter fontes e abranger tópicos sensíveis em uma atmosfera de incerteza sobre o alcance e efeito do poder do governo sobre eles. Tanto as investigações de vigilância, quanto os vazamentos surgiram amplamente neste contexto, especialmente na medida em que pode haver uma relação entre os dois (HUMAN RIGHTS WATCH, 2014, p. 22, tradução livre)[71].

As informações e dados apresentados pelo relatório ratificam que a maioria dos jornalistas entrevistados têm dificuldades para enfrentar os novos desafios relacionados ao aumento dos processos de vazamento e à vigilância comunicacional praticada pelo governo

[71] No original: Journalists interviewed for this report described the difficulty of obtaining sources and covering sensitive topics in an atmosphere of uncertainty about the range and effect of the government's power over them. Both surveillance and leak investigations loomed large in this context—especially to the extent that there may be a relationship between the two.

dos Estados Unidos da América (EUA). Para os profissionais, a intrusão comunicacional e o armazenamento de metadados e comunicações tornam a proteção das investigações jornalísticas e consequentemente das suas fontes mais difícil.

> Mesmo com a rápida evolução de técnicas para conduzir pesquisas e entrar em contato com fontes, os jornalistas expressaram preocupação de que uma ampla vigilância governamental restrinja sua capacidade de investigar e divulgar questões de interesse público e, em última instância, mina os processos democráticos impedindo um debate aberto e esclarecido (HUMAN RIGHTS WATCH, 2014, p. 24, tradução livre)[72].

Alinhada à necessidade de proteger as fontes, os dados e a própria segurança, muitos jornalistas relataram que estão modificando suas práticas para realizar investigações, se comunicar e proteger os seus dados. Os reflexos dessas alterações, profundamente conectadas aos métodos e técnicas empregadas por jornalistas investigativos, evidenciam o impacto da vigilância comunicacional em suas atuações. O relatório da *Human Rights Watch* (2014) destaca ainda três grandes tipos de mudanças no comportamento dos jornalistas: a) aumento do uso de tecnologia avançada de privacidade; b) diminuição da dependência de ferramentas eletrônicas; c) modificação no uso de métodos convencionais para proteção de informações e fontes. Em muitas oportunidades e em casos específicos os jornalistas entrevistados empregam uma combinação de medidas ligadas às três categorias elencadas.

Em um contexto de vigilância comunicacional massiva, os jornalistas que teriam o papel de vigiar abusos e negligências estão expostos às inúmeras possibilidades de vigilância nociva. Em 5 de junho de 2013, as denúncias de espionagem massiva e monitoramento global realizadas por Edward Snowden chamaram a atenção para o colossal aparato técnico da *National Agency of Security* (NSA), agência de segurança estadunidense.

> Os documentos revelaram ordens judiciais secretas que exigiam que a Verizon transmitisse registros telefônicos de todos os usuários ao governo. A NSA estava fazendo registros de quase todos os telefonemas nos Estados Unidos. As divulgações expuseram detalhes estruturais de dois programas-chave da NSA, PRISM e XKeyscore e do Tempora, que se baseava no Reino Unido sob os auspícios do Government Communications Headquarters (GCHQ). O programa de vigilância PRISM permitiu que a NSA obtivesse entrada por backdoor nos dados de nove gigantes empresas de internet, incluindo Google e Facebook (BELL; OWEN; KHORANA, 2017, p. 29, tradução livre)[73].

[72] No original: Even with rapidly evolving techniques for conducting research and contacting sources, journalists expressed concern that widespread government surveillance constrains their ability to investigate and report on matters of public concern, and ultimately undermines democratic processes by hindering open, informed debate.
[73] No original: The documents revealed secret court orders requiring Verizon to pass on phone records for all its users to the government. The NSA had been making records of nearly every phone call in the United States.1 The disclosures exposed structural details of two key NSA programs, PRISM and XKeyscore, and of Tempora, which was based in the United Kingdom under the auspices of Government Communications Headquarters (GCHQ). The surveillance program PRISM had allowed the NSA to gain backdoor entry into the data of nine giant Internet companies, including Google and Facebook.

Bell, Owen e Khorana (2017) garantem que as revelações de Edward Snowden abalaram os alicerces do sistema de vigilância estadunidense e de seus principais parceiros: Reino Unido, Austrália, Canadá e Nova Zelândia [74]. Os fatos expostos por Snowden detalharam ao mundo as possibilidades sem precedentes de vigilância eletrônica apresentadas por aparatos e ferramentas tecnológicas. O caso também se notabilizou pela sua vertente jornalística, pois Snowden procurou jornalistas para difundir as suas revelações. Snowden acreditava que sozinho não poderia avaliar e mensurar adequadamente a importância ou a ameaça associada às informações que obteve. A crença e as convicções de uma das fontes mais importantes da história do jornalismo e a singularidade de suas revelações nos motivaram a selecionar o caso Snowden como um dos casos abordados neste estudo.

A relação de Edward Snowden com o jornalista Gleen Greenwald e com a documentarista Laura Poitras revelou aspectos emblemáticos sobre as vulnerabilidades e as potencialidades do tratamento de informações e dados sensíveis em um ambiente digital vigiado. O contato de Snowden com Greenwald, relatado no livro "Sem lugar para se esconder" (2014), trata de alguns desafios impostos aos profissionais. Para se comunicar com a fonte, Greenwald precisava adotar um padrão de criptografia chamado PGP [75]. As dificuldades do jornalista em adotar o padrão de comunicação foram um empecilho para o contato com Snowden, que utilizava o pseudônimo de Cincinnatus.

> A criptografia é importante, e não só para espiões e adúlteros. "Instalar um programa de e-mail criptografado", segundo Cincinnatus, "é uma medida de segurança crucial para qualquer um que deseje se comunicar com o senhor". Para me motivar a seguir seu conselho, ele acrescentou: "Há pessoas por aí com quem o senhor adoraria conversar, mas que nunca vão poder entrar em contato a menos que saibam que suas mensagens não poderão ser lidas em trânsito" (GREENWALD, 2014, p. 7).

Conforme Greenwald (2014), as agências de inteligência mais avançadas do mundo têm softwares com capacidade para quebrar senhas de um bilhão de tentativas por segundo, mas os códigos PGP são tão compridos e aleatórios que mesmo o mais sofisticado dos softwares precisa de muitos anos para quebrá-los. Esse padrão é utilizado por agentes de inteligência, ativistas dos direitos humanos e hackers que temem ter suas comunicações monitoradas.

[74] Os cinco países formaram uma aliança de espionagem que ficou conhecida como Cinco Olhos (Five Eyes) e foi apontada por especialistas como um dos maiores acordos de espionagem da história.
[75] O padrão que em inglês significa Pretty Good Privacy foi criado em 1991 e foi constantemente aprimorado até se tornar uma sofisticada ferramenta de proteção para e-mails e outras formas de contato online.

> Diante da minha inércia, C. intensificou seus esforços: produziu um vídeo de dez minutos chamado "PGP para jornalistas"[76]. Usando um software que gera vozes computadorizadas, o vídeo me ensinava a instalar o programa, passo a passo, de um modo fácil, que incluía gráficos e imagens. Mesmo assim, continuei sem fazer nada. Nesse momento, como ele me contou mais tarde, C. ficou frustrado. "Aqui estou eu", pensou, "prestes a arriscar minha liberdade e talvez até minha vida para entregar a esse cara milhares de documentos ultrassecretos do mais secreto órgão público desta nação – um vazamento que vai gerar dezenas, se não centenas, de enormes furos jornalísticos, e ele não é capaz nem de se dar ao trabalho de instalar um programa de criptografia". Eis quão perto cheguei de ignorar um dos maiores e mais influentes vazamentos de segurança nacional da história dos Estados Unidos (GREENWALD, 2014, p. 8).

A impossibilidade de estabelecer formas de comunicação que mitigassem as vulnerabilidades e fortalecessem a segurança das informações colocou em risco a revelação de um volume sem precedentes de documentos ultrassecretos que geraram interesse e debates mundiais sobre a vigilância eletrônica em massa e a privacidade na era digital. Após o contato de Snowden com Greenwald e Poitras, os documentos selecionados foram compartilhados, relatados e publicados por uma rede de instituições de mídia tradicionais em todo o mundo.

Na série de denúncias, jornalistas publicaram documentos revelando que a NSA havia monitorado cidadãos de todo o mundo e trinta e cinco líderes mundiais, incluindo a chanceler alemã Angela Merkel e a presidente brasileira Dilma Rousseff. As revelações expuseram que governos democráticos estavam vigiando as atividades privadas de cidadãos comuns, dentre os quais os próprios jornalistas.

Diante desse panorama, dilemas e questões relacionadas à sensação de vulnerabilidade e às capacidades ligadas ao ambiente digital emergem e atravessam o cotidiano dos jornalistas investigativos. Um dos desdobramentos mais importantes que tangencia esse contexto está relacionado com a possibilidade de preservar a privacidade comunicacional dos profissionais. De acordo com Christofoletti (2015), no contexto brasileiro, a intimidade é um direito fundamental previsto na Constituição Federal e a privacidade está entre os direitos e garantias fundamentais de todos os cidadãos. Christofoletti (2015) enaltece que aspectos importantes desses elementos estão ligados à capacidade do indivíduo de se reservar, buscar proteção de ambientes e situações públicas.

> Em meio ao cenário de convergência midiática e de intensificação das tecnologias de informação e comunicação, a privacidade ganha novos contornos porque se tornam mais complexas as formas de gerenciamento da vida íntima e da imagem pública. Isto é, existem hoje muitas maneiras de exibir o que antes circulava de forma restrita, aumentando a necessidade de mais cuidados para a preservação dos próprios dados (CHRISTOFOLETTI, 2015, p. 128).

[76] Vídeo disponível em: https://www.dailydot.com/layer8/edward-snowden-gpg-for-journalists-video-nsa-glenn-greenwald. Acesso em: 10 jun. 2018.

Em relação ao jornalismo, Christofoletti (2015) destaca a intensificação da criptografia para troca de mensagens e pacotes de dados, a adoção de precauções mais severas nos contatos com as fontes e esforços para uma especialização de jornalistas em cibersegurança. O autor também evidencia a importância do papel do Estado como moderador das relações econômicas, fazendo prevalecer os interesses da coletividade, o papel mais atuante do usuário na condição de consumidor, exigindo o atendimento às leis vigentes no país e dos jornalistas que deveriam se engajar mais nas questões que envolvem elementos imprescindíveis para investigações jornalísticas.

Conforme Shirky (2017), uma questão essencial para o jornalismo é como os jornalistas podem fortalecer a sua capacidade de relatar notícias importantes em um período de crescente interferência. A intervenção está alinhada aos movimentos significativos de restrição dos relatos jornalísticos e dos vazamentos de informação. Novos elementos como os *leaks*[77] estão revelando debilidades jornalísticas. O volume grandioso e a complexidade das informações disponibilizadas revelam a necessidade de readequações e adaptações para o melhor aproveitamento e tratamento dos dados.

O norte parece estar no trabalho de depuração e dimensionamento do impacto de revelações e colaborações. Shirky (2017) aponta uma tendência de aumento no volume de informações reveladas e indica que os jornalistas devem maximizar a sua capacidade de relatar notícias e minimizar a interferência do governo por meio de três competências. A primeira competência está relacionada com a obtenção de bons canais de comunicação criptografada onde, no mínimo, os repórteres se sintam confortáveis ao se comunicarem por e-mails criptografados. A segunda indicação diz respeito ao contato dos jornalistas com "vazadores" por meio de um plano que envolva outros jornalistas. A terceira competência aponta que os jornalistas devem descobrir a quem eles podem ser úteis como um terceiro destinatário dos segredos que serão publicados, como uma forma de backup. Por fim, fontes corajosas vão exigir jornalistas corajosos e cooperação entre concorrentes em algum momento.

As revelações de Snowden fortaleceram inúmeros indícios que apontam que jornalistas e fontes de informação estão expostos. Investigações jornalísticas que abordam temas sensíveis podem ser controladas por grandes empresas e instituições estatais. Poderosas ferramentas de controle social estão sedimentadas em nossos cotidianos e os próprios usuários abastecem as redes, plataformas e aparatos com informações e dados pessoais que fortalecem

[77] O termo se refere ao ato de vazar ou vazamento de informações, a palavra costuma ser utilizada para denotar o escapamento de informações privadas ou confidenciais que se tornam públicas.

cada vez mais as possibilidades de dominação e instrumentalização das ações jornalísticas e consequentemente da sociedade.

Em um contexto permeado por aparatos de intrusão comunicacional massiva e o desequilíbrio entre a capacidade de vigilância do Estado e de grandes corporações transnacionais em relação ao jornalismo, acreditamos que o monitoramento das ações jornalísticas pode interferir na competência investigativa do jornalismo contemporâneo. Um caso exemplar que apresenta potencialidades (colaboração e capilaridade das informações) e vulnerabilidades (falta de mecanismos de segurança digital) do ambiente digital é o projeto *Colaboración sin Fronteras*[78]. A iniciativa, realizada entre abril e outubro de 2012, reuniu jornalistas de quatro organizações que desenvolvem jornalismo investigativo em meios digitais na América Latina: *Verdad Abierta*[79] (Colômbia); *El Faro*[80] (El Salvador); *Plaza Pública*[81] (Guatemala); *Animal Político*[82] (México). Contou com a participação da fundação *InSight Crime*[83], que realiza estudos sobre o crime organizado na América Latina e no Caribe, e com o financiamento da organização não governamental *Internews*[84]. A proposta visava desenvolver projetos digitais de jornalismo investigativo relacionados ao crime organizado na região[85].

Conforme Constantaras (2013), o trabalho de colaboração dos meios digitais demonstrou um nível baixo de conscientização e ação de segurança digital dos jornalistas que participaram da iniciativa. Para a autora, esses são indícios de que há necessidade de mais treinamento e recursos nessa área, além da formatação de um plano de segurança digital para colaborações de alto risco.

> Apesar de ter procedimentos de segurança implementados, todos os participantes tinham aversão ao risco em compartilhar informações devido à falta de mecanismos de segurança digital e, portanto, compartilhavam informações apenas uma vez que todas as informações sensíveis fossem anonimizadas e as matérias estivessem quase prontas para publicação. Como eles não conseguiam compartilhar fontes durante as investigações ativas, era quase impossível para os participantes descobrir conexões entre os criminosos que operam em cada país[86] (CONSTANTARAS, 2013, online, tradução livre)[87].

[78] Mais informações em: https://www.insightcrime.org/investigations/the-mafias-shadow-highlights-the-human-rights-consequences-of-organized-crime/. Acesso em 10 jun. 2018.
[79] Disponível em: https://verdadabierta.com/. Acesso em: 17 nov. 2019.
[80] Disponível em: https://elfaro.net/. Acesso em: 17 nov. 2019.
[81] Disponível em: https://www.plazapublica.com.gt/. Acesso em: 17 nov. 2019.
[82] Disponível em: https://www.animalpolitico.com/. Acesso em: 17 nov. 2019.
[83] Disponível em: https://www.insightcrime.org/about-us/. Acesso em 10 jun. 2018.
[84] Disponível em: https://www.internews.org/. Acesso em 10 jun. 2018.
[85] Mais informações em: https://www.insightcrime.org/uncategorized/slaves-organized-crime-latin-america/. 10 jun. de 2018.
[86] No original: Despite having security procedures in place, all the outlets were somewhat more risk averse in sharing information due to lack of digital security mechanisms and therefore only shared information with each

Constantaras (2013) ratifica que o aumento da segurança está atrelado a uma avaliação abrangente de segurança física e digital para colaborações que envolvem temas sensíveis e desenvolvimento de um protocolo de segurança ao qual todos os parceiros estejam envolvidos. A falta de mecanismos de segurança digital fez com que os participantes evitassem compartilhar informações sensíveis por meio de canais digitais e esse aspecto afetou o potencial da colaboração através da troca de informações.

A emergência de casos concretos de vigilância eletrônica representa um alerta para alguns grupos, como o grupo dos jornalistas investigativos, pois para eles, os riscos são mais iminentes e perigosos. "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" (CHRISTOFOLETTI; TORRES, 2018, p. 2). No contexto atual, os jornalistas investigativos, particularmente os que trabalham com temas sensíveis, estão atuando em zonas de alto risco. Diante da dependência e centralidade do ecossistema digital na atividade jornalística e do aumento contundente da capacidade de vigilância comunicacional do Estado e de empresas privadas, podemos afirmar que o monitoramento das comunicações digitais é uma realidade que pode gerar constrangimentos e consequências significativas para os profissionais.

As vulnerabilidades em relação à segurança digital e ao acesso a informações sensíveis dos jornalistas materializam-se em casos de espionagem a partir de dispositivos de comunicação e ações de violação à privacidade dos profissionais. Esses ataques têm como base formas de constrangimento, cerceamento e impedimento que ameaçam a liberdade dos jornalistas. Um caso emblemático ocorreu em junho de 2017, quando um grupo de jornalistas acusou o governo mexicano de usar um *software* para espionar seus celulares. O presidente mexicano, Enrique Peña Nieto, negou a ação e o episódio passou a ser conhecido como *Gobierno Espía*[88].

O caso foi detalhado em um relatório divulgado pela *Red en Defensa de los Derechos Digitales, SocialTIC e Article 19 México y Centroamérica*[89]. As ações de vigilância comunicacional do governo mexicano ocorreram por meio de um *software* utilizado para

---

other once all sensitive information had been anonymized and stories were nearly ready for publication. Since they were unable to share sources during the active investigations, it was nearly impossible for outlets to uncover connections between criminal actors operating in each country.

[87] Disponível em: http://mediashift.org/2013/01/lessons-learned-from-a-collaboration-without-borders-in-latin-america010/. Acesso em 10 jun. 2018.

[88] Mais informações 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/. Todos os acessos em: 10 de jun. 2018.

[89] Disponível em: https://r3d.mx/gobiernoespia. Acesso em: 10 de jun.2018.

vigiar dispositivos eletrônicos. O *malware Pegasus,* produzido pela empresa israelense *NSO Group,* afetou seis jornalistas. Segundo informações do *The New York Times*[90], pelo menos três agências federais mexicanas investiram 80 milhões de dólares em *softwares* de espionagem da *NSO Group*. A própria corporação assegura que seus produtos são vendidos exclusivamente para governos e operacionalizados por agências governamentais autorizadas.

O *Pegasus* possibilita acesso remoto aos 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 expostas afetam, particularmente, a capacidade investigativa do jornalismo.

Em outubro de 2019, o Comitê de Direitos Humanos das Nações Unidas [91] questionou o México sobre os casos de vigilância com uso do *Pegasus.* Durante a 127ª sessão do Comitê da ONU, o Estado mexicano foi questionado sobre suas ações em relação a casos de vigilância contra jornalistas, ativistas e defensores de direitos humanos. Após mais de dois anos da divulgação das informações relacionadas ao uso de sofisticadas ferramentas de vigilância para espionar, assediar e intimidar pelo menos 25 pessoas, o caso permanece impune.

No mesmo mês de outubro, a Anistia Internacional revelou um novo caso ligado à utilização do *Pegasus* no Marrocos[92], dois defensores de direitos humanos foram alvos de tentativas de ataque digital com uso do *malware*. Em junho de 2019, o relator especial da ONU para a liberdade de expressão, David Kaye, pediu a imposição de uma moratória à concessão de licenças de exportação para tecnologias de vigilância. Kaye solicitou que as empresas cessem imediatamente a venda, transferência e suporte dessas tecnologias até que possam fornecer evidências de que estão tomando medidas para mitigar os riscos de abuso de direitos humanos vinculados ao uso dessas ferramentas.

Nos últimos anos, diversos casos de intrusão, armazenamento e manipulação de dados pessoais de jornalistas foram registrados em diferentes partes do mundo por inúmeros relatórios produzidos por organizações não governamentais nacionais e internacionais (Federação Nacional dos Jornalistas – Fenaj, *Freedom House*, Repórteres Sem Fronteiras – RSF, Comitê de Proteção aos Jornalistas – CPJ, entre outras). No relatório "Censura e

[90] Disponível em: https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group espionaje/?mcubz=1. Acesso em: 10 jun. 2018.
[91] Disponível em: https://r3d.mx/2019/10/18/el-comite-de-derechos-humanos-de-la-onu-cuestiona-a-mexico-por-casos-de-vigilancia-con-pegasus/. Acesso em: 17 nov. 2019.
[92] Disponível em: https://r3d.mx/2019/10/14/amnistia-internacional-revela-nuevo-caso-vinculado-a-pegasus-en-marruecos/. Acesso em: 17 nov. 2019.

Vigilância de jornalistas: Um negócio sem escrúpulos”[93], divulgado pela RSF em 2017, são tratadas questões relacionadas com a vigilância comunicacional e formas de censura que estão ocorrendo regularmente em diferentes partes do mundo.

> A vigilância na web e nas telecomunicações é uma prática inerente dos "Inimigos da Internet" - os países mais repressivos do mundo em termos de liberdade de informação na Internet - que geralmente realizam evocando os "interesses vitais da nação na Internet". Na liderança deste grupo estão regimes autoritários como a China, o Irã, a Síria e o Uzbequistão, que adquiriram e continuam abastecendo-se com tecnologia que lhes permite traçar o mínimo ato ou gesto de jornalistas críticos, blogueiros e usuários de internet. No caso de países democráticos - como a França, o Reino Unido, os Estados Unidos, a Austrália e o México - que recorrem à vigilância em nome da segurança do país, surge a questão da proteção de fontes jornalísticas (ISMAIL; MOINI; VIALLE, 2017, p. 8, tradução livre)[94].

O relatório da RSF (2017) também ressalta características da realidade enfrentada por jornalistas mexicanos, particularmente as relações comerciais que existem entre agências governamentais e um dos principais exportadores de ferramentas e aparatos de vigilância. Diante disso, questiona qual é a margem para que os jornalistas investiguem de forma independente e para que protejam suas fontes. Nesse contexto, a opacidade das ações empregadas por autoridades quanto ao uso dessas tecnologias de vigilância faz crescer a sensação de insegurança e a falta de garantias sobre o uso sistemático delas contra investigações jornalísticas.

> O que aconteceu com o jornalista argentino Rafael Cabrera, caso em que a empresa israelense *NSO Group* esteve envolvida, mostra o abuso na vigilância cometida pelas autoridades mexicanas. Em agosto de 2016 *Citizen Lab* e *Look out* relataram que havia um programa de espionagem que permitia controlar completamente o iPhone aproveitando suas falhas de segurança (que foram posteriormente corrigidas): "Pegasus". O software malicioso (*malware)* foi instalado no telefone celular da vítima da seguinte maneira: a pessoa recebeu uma mensagem SMS no telefone (aparentemente confiável) seguido de um link; quando aberto, o seu telefone foi infectado e o *malware* pode acessar todas as suas informações pessoais (contatos), ver suas fotos e arquivos, o conteúdo das suas chamadas, ler suas mensagens SMS, e-mails, conversas no WhatsApp, Skype e até mesmo Telegram (sistema de mensagens que é conhecido por sua segurança). Ele também pode usar a câmera do iPhone remotamente, ouvir suas conversas ligando o microfone e sempre saber onde seu dono está, ativando o GPS (ISMAIL; MOINI; VIALLE, 2017, p. 10, tradução livre)[95].

[93] Disponível em: https://rsf.org/es/informes/censura-y-vigilancia-de-periodistas-un-negocio-sin-escrupulos. Acesso em: 10 jun. 2018.

[94] No original: La vigilancia de la Web y de las telecomunicaciones es una práctica inherente a los “Enemigos de Internet” – los países más represivos del mundo en materia de libertad de información en la Red–, que estos suelen llevar a cabo evocando los “intereses vitales de la Nación”. A la cabeza de este grupo se encuentran regímenes autoritarios como China, Irán, Siria e Uzbekistán, que han adquirido y continúan abasteciéndose de tecnología que les permite rastrear el mínimo acto o gesto de periodistas, blogueros e internautas críticos. En el caso de países democráticos –como Francia, Reino Unido, Estados Unidos, Australia y México – que recurren a la vigilancia en nombre de la seguridad del país, surge la cuestión de la protección de las fuentes periodísticas.

[95] No original: Lo que le ocurrió al periodista de investigación mexicano Rafael Cabrera, caso en el que estuvo implicada la empresa israelí NSO Group, muestra el abuso en la vigilancia cometido por las autoridades

O relatório da RSF (2017) ainda apresenta a posição da corporação *NSO Group* em relação ao caso. Conforme a manifestação da empresa, a sua intenção é tornar o mundo mais seguro, fornecendo às agências governamentais autorizadas tecnologias que auxiliem no combate ao terror e ao crime. "Os clientes podem usar nossos produtos exclusivamente para a investigação e prevenção do crime e do terror. O uso ético e legal desses produtos pelos clientes é de suma importância para a empresa" (ISMAIL; MOINI; VIALLE, 2017, p. 11)[96]. O posicionamento da corporação evidencia argumentos amplamente questionáveis e o uso e apropriação das tecnologias, por parte dos governos e da própria empresa, aponta para a falta de restrições que garantam o uso "adequado" dos aparatos e ferramentas de vigilância comunicacional.

As inúmeras possibilidades de vigilância das comunicações estão se manifestando de maneira contundente e em muitas ocasiões de forma imperceptível e ampla. Nesse cenário em que jornalistas investigativos podem estar sendo vigiados, buscamos clarear como as investigações jornalísticas estão sendo desenvolvidas e que potencial essas ações apresentam para garantir zonas de comunicação menos vulneráveis.

Um contexto vigiado gera o que pode ser classificado de liberdade parcial e essa constatação implica formas de opressão e constrangimento. Desempenhar o jornalismo investigativo nessas condições significa sujeitar-se e correr o risco de não explorar o potencial que o jornalismo investigativo tem em relação ao desenvolvimento da sociedade e da democracia.

---

mexicanas. En agosto de 2016 Citizen Lab y Look out informaron que existía un programa espía que permitía controlar por completo los iPhone aprovechando sus fallas de seguridad (que después fueron corregidas): "Pegasus". El software malicioso (malware) se instalaba en el teléfono móvil de la víctima de la siguiente manera: la persona recibía un mensaje SMS en su teléfono (en apariencia confiable) seguido de un link; al abrirlo, su teléfono quedaba infectado y el malware podía tener acceso a toda su información personal (contactos), ver sus fotos y archivos, los contenidos de sus llamadas, leer sus mensajes de SMS, correos electrónicos, conversaciones en WhatsApp, Skype e incluso Telegram (sistema de mensajería que no obstante es conocido por su seguridad). También podía usar a distancia la cámara del iPhone, escuchar sus conversaciones encendiendo el micrófono y saber en todo momento dónde se encontraba su propietario, activando el GPS.

[96] No original: Los clientes pueden utilizar nuestros productos exclusivamente para la investigación y la prevención del crimen y el terror. El uso ético y legal de estos productos por parte de los clientes es de importancia capital para la empresa.

2.2 JORNALISMO VIGILANTE[97]

As implicações das vigilâncias comunicacionais estatais e corporativas sobre as práticas e preceitos do jornalismo investigativo contemporâneo formatam um contexto que exige habilidades alinhadas ao tratamento e proteção de dados sensíveis e os desafios técnicos impostos à atuação de jornalistas em espaços digitais vigiados. Projetos jornalísticos autônomos têm demonstrado a possibilidade de produzir iniciativas jornalísticas independentes, que resultam em pequenos e grandes atos de denúncia, indo ao encontro do que Bell, Owen e Khorana (2017) apontam como uma ferramenta de poder.

> Um papel histórico central do jornalismo tem sido tomar a decisão final sobre o que as pessoas devem saber. Os jornalistas têm a capacidade de relatar, revelar e contextualizar informações que estão sendo retidas dos cidadãos e, como resultado, têm as ferramentas para defender o poder - seja poder do Estado, poder corporativo ou outras formas de poder institucional[98] (BELL; OWEN; KHORANA, 2017, 42, tradução livre).

As decisões subjacentes a estes processos jornalísticos têm sido muitas vezes envoltas em segredo. Relações históricas entre o jornalismo e o poder, especialmente a emergência da capacidade de vigilância do poder por meio de ações jornalísticas, contrastam com aspectos do contexto de vigilância comunicacional em massa que os profissionais vivenciam atualmente.

> Confidencialidade não significa nada se um terceiro pode de uma forma razoavelmente fácil divulgar com quem um jornalista tem falado através de seus registros telefônicos, listas de contatos, e-mails, textos, ou divulgar quem mais estava em um determinado local, em um determinado momento (RUSBRIDGER, 2017, p. 64, tradução livre) [99].

Aspectos contextuais atrelados às tecnologias comunicacionais ampliam as imbricações entre jornalismo investigativo e vigilância, promovendo a emergência de conceitos como ciberativismo e contravigilância, que permitem a formatação de uma noção de jornalismo vigilante. Para além dos aspectos normativos propositivos empregados na definição de jornalismo investigativo, propomos a necessidade de um senso de

[97] A noção proposta nesse tópico foi apresentada no 40º Congresso Brasileiro de Ciências da Comunicação (Intercom), realizado em 2017, na cidade de Curitiba-PR, e foi publicada nos anais do evento. Disponível em: http://portalintercom.org.br/anais/nacional2017/index.htm. Acesso em: 30 out. 2019.

[98] No original: A central historical role of journalism has been to make the ultimate decision about what people should know. Journalists have the capacity to report, reveal, and contextualize information that is being withheld from citizens, and as a result they have the tools to stand up to power—be it state power, corporate power, or other forms of institutional power.

[99] No original: Confidentiality means nothing if a third party can reasonably easily work out to whom a journalist has been talking—through their phone logs, contacts lists, e-mails, texts, or by working out who else was in a certain location at a certain time.

vulnerabilidade atrelado ao fomento de uma cultura de riscos digitais para jornalistas que trabalham com temas sensíveis em ecossistemas digitais.

A noção que propomos está vinculada com as características emergentes ligadas à investigação jornalística que demarcam novas condicionantes presentes nas ações empregadas por jornalistas investigativos. Em condições adequadas, o jornalismo vigilante seria combativo e desempenharia um papel significativo no fortalecimento dos princípios democráticos com potencial para influenciar a formação de agendas públicas e governamentais, intermediar relações entre grupos com interesses em comum e atribuir elementos informativos sobre temas específicos à opinião de inúmeras pessoas, como afirmam Karam (2014), Castells (2013), Waisbord (2000), Traquina (2005, 2012), entre outros. O jornalismo se aproxima deste ideal quando revela segredos do Estado e situações até então inconcebíveis, por meio de métodos de checagem e apuração.

Nestes casos, em tese, o jornalista sabe o que ninguém sabe fora de uma determinada rede de poder e controle. O jornalismo crítico e independente tem entre as suas prioridades a vigilância social coerente e socialmente engajada. Não pode ceder às exigências e pressões do Estado e do mercado, ao alinhamento político, aos estímulos ideológicos extremos que afetam concepções de direitos humanos e de liberdade de expressão. Alienar esta função compromete a credibilidade e pode denunciar intenções obscuras e informações imersas em negociatas privadas. Canais de comunicação e jornalistas norteados pela característica vigilante da atividade jornalística devem estar dispostos e preparados para confrontar os benefícios e favores do Estado e de contratos privados, pois manter a consistência e o movimento dinâmico depende, necessariamente, de um caminho tortuoso e incerto.

O cerne deste trabalho de investigação está atrelado aos métodos que concedem ao jornalista mediador a consolidação e reafirmação dos pressupostos do sistema democrático e um papel de fiscalizador, defendido por Waisbord (2000), Nascimento (2010) e Fortes (2005), por meio do *accountability*[100]. Waisbord (2000) deposita grandes esperanças na prática jornalística democrática que deve monitorar o poder, expressar uma diversidade de opiniões, tornar os cidadãos informados e promover o debate público. Esses pressupostos são elementos vitais da vida democrática. Para Fortes (2005), a avaliação dos resultados de iniciativas de vigilância garante à atividade jornalística um tipo de credibilidade que poucas instituições têm.

[100] O termo está relacionado à obrigação de agentes políticos institucionais prestarem contas de suas ações às instâncias controladoras e à sociedade, de uma forma geral. Envolve os conceitos de responsabilidade, democracia, transparência e fiscalização de instituições públicas.

> Refiro-me ao efeito direto da vigilância e, por que não dizer, do medo que a investigação jornalística impõe aos agentes públicos, principalmente àqueles que se utilizam do espaço governamental para se locupletarem por meio de corrupção e tráfico de influência (FORTES, 2005, p. 38).

Enquanto agentes que desenvolvem, iniciam e evidenciam processos de *accountability,* os jornalistas desempenham ações que transformam o jornalismo não só em uma instância legítima de vigilância dos atores sociais, como também em um espaço para proposição e realização do debate cívico. Maia (2006) ressalta que a exposição de escândalos de maneira isolada não é o suficiente para eliminá-los, para modificar as atuações de representantes ou para desencadear processos de investigação e de punição das instituições competentes.

> Como vimos, a exposição nos meios de comunicação constrange os representantes políticos ou as autoridades públicas a responder e a explicar suas próprias ações e omissões, tornando as ações abertas ao escrutínio e à avaliação externa. Em outras palavras, os media não criam a accountability, mas ajudam a adicionar esforços para criar uma sociedade mais vigilante e crítica (MAIA, 2006, p. 23).

Conforme a autora, a questão da *accountability* é fundamental para a qualificação da democracia moderna, pois origina o dever dos representantes políticos, diante de seus poderes e obrigações, de responder aos cidadãos. Nesse contexto, o jornalismo vigilante está capacitado a promover controle na partilha de poder por meio do monitoramento dos dirigentes vinculados às instituições públicas e organizações privadas, a partir de mecanismos e técnicas específicas. Como já observamos, além de se relacionar com o poder, o jornalismo é um importante instrumento de resistência e oposição a ele.

Correia (2011) salienta que no contexto das atuais democracias, os jornalistas intervêm decididamente na configuração do agir político, propondo e impondo uma agenda de questões sobre as quais decorrem muitos dos debates e das controvérsias politicamente relevantes. O autor salienta a migração de uma parte significativa de diversas formas de comunicação pública para os novos meios digitais, paralelamente com a concretização e o aparecimento, em alguns momentos experimentais e em outros consolidados, de novas formas de jornalismo. "O recente protagonismo do site da organização WikiLeaks mostra como os media tradicionais não têm, de modo algum, o monopólio da circulação da informação no espaço público" (CORREIA, 2011, p. 5). Christofoletti e Oliveira (2011) reafirmam a importância do WikiLeaks, caracterizando-o como um fator potencialmente transformador da atividade jornalística.

> Neste bojo, a hipótese de um jornalismo pós-WikiLeaks considera a chegada do site no cenário comunicativo como um divisor de águas, capaz de alterar condutas dos profissionais e políticas internas das empresas jornalísticas de tratamento das fontes (CHRISTOFOLETTI; OLIVEIRA, 2011, p. 236).

De acordo com Christofoletti e Oliveira (2011), ao suscitar o debate sobre o papel da imprensa na fiscalização do poder, o WikiLeaks aponta para a necessidade do jornalismo retomar e reafirmar a liberdade em sua dimensão mais profunda, enquanto princípio e direito humano fundamental de todos. Uma situação contemporânea que se reflete na prática do jornalismo é o da Agência Pública, que foi criada em 2011 para exercer um papel independente, focado em jornalismo investigativo. A iniciativa busca maneiras alternativas de viabilizar a prática jornalística e tem se notabilizado por abordagens experimentais inovadoras que nos motivaram a elencar um projeto desenvolvido em 2013 como um dos casos paradigmáticos analisados neste estudo.

Trata-se do projeto PlusD (Biblioteca de Documentos Diplomáticos dos EUA), desenvolvido pelo WikiLeaks em parceria com a Agência Pública e outros 17 veículos internacionais. Em vez de trazer vazamentos, constitui-se como uma ferramenta para buscar documentos de domínio público. Esta ferramenta reúne mais de 1 milhão de documentos diplomáticos do período de 1973 a 1976 e mais de 200 mil de 2003 a 2010. Os documentos vieram a público em um dos vazamentos mais famosos do WikiLeaks, conhecido como o *Cablegate*[101]. A WikiLeaks PlusD é uma das inúmeras séries especiais produzidas pela Agência Pública, contando com 11 reportagens que foram publicadas entre os dias 07 e 14 de abril de 2013 e aborda documentos que tratam da relação diplomática entre os EUA e o Brasil, particularmente relacionados à ditadura brasileira, entre 1973 e 1976.

> Para o Brasil, o novo projeto do WikiLeaks tem especial importância. Embora parte dos documentos já tenha sido publicada pela imprensa brasileira, o arquivo completo expõe em detalhe as ações de Kissinger em relação à ditadura brasileira entre 1973 e 1976 – em especial, durante o governo do general Ernesto Geisel. Até agora não se sabia a real dimensão deste arquivo. São mais de 8.500 documentos enviados pelo Departamento de Estado dos EUA para o Brasil e mais de 13.200 documentos enviados da embaixada americana em Brasília e consulados a Washington – mais de 1.400 são confidenciais, e mais de 115 secretos (VIANA, 2013, online).

O conteúdo jornalístico oferecido pela Agência Pública, por meio da ferramenta do WikiLeaks, apresenta aspectos importantes do jornalismo vigilante em relação à memória de um período histórico brasileiro. As entranhas do poder expostas pela série WikiLeaks PlusD da Agência Pública rementem à possibilidade de reinterpretação dos fatos através do acesso às

[101] *Cablegate* é um vazamento, iniciado em 2010, em que o WikiLeaks disponibilizou um conjunto de mais de 250 mil telegramas do Departamento de Estado dos EUA e que passou a ser referência para reportagens de jornais em todo o mundo.

formas de comunicação diplomática secretas desse período histórico, como pode ser observado na quadro 2.

Quadro 2 – Reportagens do especial WikiLeaks PlusD.

Título da reportagem	*Data da publicação*	*Tema principal da reportagem*
Conheça o PlusD, a Biblioteca de Documentos Diplomáticos do WikiLeaks	07/04/2013	Apresentação da ferramenta PlusD do WikiLeaks e da série de reportagens relacionada ao material coletado.
Para justificar assistência militar à ditadura, EUA diziam que tortura era exceção	07/04/2013	Apoio EUA à ditadura brasileira.
Desfecho de caso Elbrick irritou Kissinger	07/04/2013	Libertação de Cláudio Torres da Silva, após cumprir sete anos de prisão por ter sequestrado, em 1969, o embaixador americano Charles Elbrick.
Tão americano quanto João da Silva	07/04/2013	Diferença de tratamento entre o norte-americano Fred Morris e Paulo Stuart Wright, que possuía dupla nacionalidade, ambos presos e torturados durante a ditadura brasileira.
Retrato em branco e preto	07/04/2013	Telegrama secreto de 1976 em que o embaixador americano John Hugh Crimmins qualifica governo militar de paranoico.
“Estamos barateando visitas de militares”	08/04/2013	Telegrama do embaixador americano John Hugh Crimmins que expressa preocupação com as repetidas visitas de americanos de alta patente para o Brasil em curto intervalo de tempo.
A pedido do Departamento de Estado, empresa americana veio ao Brasil pesquisar “terrorismo”	08/04/2013	Telegramas de 1974 demonstram que a RAND, empresa de pesquisa norte-americana, esteve no Brasil para estudar casos de sequestros políticos.
Ligações perigosas: a DEA e as operações ilegais da PF brasileira	08/04/2013	Documentos demonstram que o ex-diretor da Polícia Federal efetuou prisões e extradições ilegais a pedido do departamento antidrogas norte-americano.
EUA fizeram lobby pró-censura durante governo militar	09/04/2013	Embaixada norte-americana pediu a repórter da TV americana para ouvir Roberto Marinho, da Globo, e Nascimento Brito, diretor do Jornal do Brasil, vozes menos críticas à censura oficial.
Crimes, mentiras e telegramas	11/04/2013	Cumplicidade de Pinochet e norte-americanos nas violações de direitos humanos no Chile expressa-se em troca de telegramas.
My Dear Henry	14/04/2013	Cartas entre Henry Kissinger e o chanceler brasileiro Antônio da Silveira descrevem aliança para manter Cuba fora da OEA.

Fonte: Elaborado pelo autor, 2017.

Os arquivos disponibilizados pelo WikiLeaks possibilitaram aos jornalistas da Agência Pública uma abordagem crítica e investigativa sobre documentos históricos que fizeram emergir indícios e elementos significativos para uma rememoração e possível reinterpretação de fatos históricos. O conteúdo avaliado apresenta sutilezas de documentos históricos que foram descritos de forma consistente, amparadas em um processo de apuração, e que denotam uma perspectiva ligada ao esclarecimento e à investigação. Nas reportagens do especial da Agência Pública foram observados elementos singulares de abordagem e tratamento das informações que refletem alguns esforços que visam à ampliação de eixos e de problemáticas merecedoras de notoriedade, como no caso da reportagem "EUA fizeram lobby pró-censura durante governo militar", onde são evidenciados elementos de censura à imprensa no período ditatorial no Brasil.

Documentos disponibilizados no PlusD, do WikiLeaks, demonstram que a diplomacia norte-americana defendeu a censura do regime militar brasileiro perante um jornalista de um importante canal de TV dos EUA. Na época, o correspondente da CBS na América Latina, George Nathanson, estava em São Paulo, produzindo material sobre a censura à imprensa brasileira e a embaixada norte-americana sugeriu ao profissional que "tentasse obter todos os lados da história da censura no Brasil". Para tanto, indicou fontes da mídia brasileira que estavam mais alinhadas ao regime, como Roberto Marinho, das Organizações Globo, e Nascimento Brito, do Jornal do Brasil, assim como fontes oficiais do governo. A reportagem apresenta ainda uma visão abrangente sobre a censura aos veículos de comunicação no período ditatorial. Essas características que estão presentes nos conteúdos de inúmeras reportagens produzidas pela Agência Pública na série demonstram como ferramentas tecnológicas e fontes independentes de informação podem ser determinantes para ações jornalísticas de investigação.

Iniciativas como o especial WikiLeaks PlusD demonstram a possibilidade da implementação de avanços apoiados nas possibilidades tecnológicas no jornalismo vigilante contemporâneo. No entanto, as alardeadas conquistas tecnológicas também estão sendo utilizadas como instrumentos de controle da sociedade e de suas formas de contestação. Os espaços de privacidade estão sendo cada vez mais interditados por possibilidades de monitoramento e, consequentemente, jornalistas e cidadãos estão expostos às ferramentas de vigilância comunicacional indiscriminada, conforme aponta Spannos (2017).

> Hoje, governos e corporações controlam partes importantes da rede, incluindo mapeamento de domínios, cabos submarinos, softwares e hardwares, códigos de programação e data centers. Isto significa que a rede está agora altamente

> centralizada, vigiada, estudada, manipulada e sujeita a vazamentos prejudiciais de dados (SPANNOS, 2017, p. 2).

Conforme já afirmamos, o poder de vigilância comunicacional pode minar liberdades e direitos civis, empresas e governos exploram, manipulam e administram modernos sistemas invasivos motivados por interesses financeiros, políticos e ideológicos. Ironicamente, os jornalistas que teriam o papel de vigiar os abusos e negligências também estão sendo vigiados. Investigações e fontes de informação estão expostas, o trabalho jornalístico pode estar sendo controlado por grandes empresas e instituições estatais.

Os jornalistas têm um papel fundamental a desempenhar na luta pela reapropriação, descentralização, experimentação e exploração das possibilidades tecnológicas no que elas têm de melhor: a liberdade. Todos devem estar cientes dos riscos aos quais estão expostos em um contexto que está extinguindo ambientes pessoais e espaços privados. Os governos e as grandes empresas estão mais preparados do que os cidadãos para essa disputa desigual pela liberdade nos ambientes digitais. O jornalismo deve demonstrar o nível de risco que estamos enfrentando e o WikiLeaks é uma das tantas iniciativas contemporâneas que encorajam e possibilitam a realização desta função que depende fundamentalmente de disposição e dedicação.

2.3 JORNALISMO INVESTIGATIVO BRASILEIRO VIGIADO

As rotinas jornalísticas desenvolvidas no ecossistema digital permeadas pela vigilância e intrusão comunicacional são diretamente afetadas pelo contexto atual da economia política do jornalismo. As questões relacionadas ao jornalismo e à vigilância das comunicações são perpassadas por vetores econômicos relacionados com a comercialização de dados pessoais e por dimensões políticas ligadas aos aspectos regulatórios atrelados com a privacidade comunicacional, segurança da informação, limbos de regulação e investimento público em tecnologias intrusivas.

No contexto brasileiro, a dimensão regulatória pode ser enaltecida por meio de duas leis que atravessam ecossistema digital e se relacionam diretamente ao jornalismo investigativo contemporâneo. Tratam-se do Marco Civil da Internet[102] e da Lei de Acesso à Informação[103] (LAI). Christofoletti (2015) explica que o Marco Civil da Internet estabelece

[102] Lei número 12.965, de 23 de abril de 2014 que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
[103] Lei número 12.527, de 18 de novembro de 2011 que regula o acesso a informações previsto na Constituição Federal.

direitos básicos para o usuário, determinando contrapartidas dos provedores de serviços e definindo responsabilidades de setores públicos. Para Christofoletti (2015), o elemento regulatório oferece instrumentos para cidadãos e jornalistas resguardarem seus dados de navegação e de aplicações.

> A resposta é afirmativa, embora algumas dessas armas sejam ainda débeis. Daí a importância do momento atual, quando se busca regulamentar a lei. Os dispositivos auxiliares da lei terão que expressar os interesses dos usuários, reforçando a figura da privacidade e enaltecendo a intimidade como direito inalienável de base para a internet. Se os próximos capítulos jurídicos seguirem essa direção, haverá mais equilíbrio nas relações entre usuários, fornecedores de serviços, governos e outras partes interessadas (CHRISTOFOLETTI, 2015, p. 225).

Em linha com essa perspectiva, em agosto de 2018 foi aprovada a lei geral de proteção de dados[104], que tem o objetivo de proteger os direitos relacionados à liberdade e à privacidade dos cidadãos. Da mesma forma, a LAI regulamenta o direito constitucional de obter informações públicas. A norma que entrou em vigor em 16 de maio de 2012 criou mecanismos que possibilitam a qualquer pessoa (física ou jurídica) o recebimento de informações públicas dos órgãos e instituições. Entidades privadas sem fins lucrativos também são obrigadas a dar publicidade a informações referentes ao recebimento e à destinação dos recursos públicos obtidos.

> Além de promover o acesso a dados mantidos e/ou produzidos por órgãos públicos, o direito à informação reflete o próprio sentido republicano do governo a serviço do povo. Porém, para os jornalistas, a aprovação da Lei de Acesso à Informação também representou a conquista de uma nova ferramenta de trabalho, uma alternativa às assessorias de imprensa dos órgãos públicos para buscar informações oficiais (DUTRA, 2015, p. 83).

Para Dutra (2015), os jornalistas desempenham uma importante função no processo de amadurecimento democrático ao fazer uso deste instrumento, apontar suas falhas e divulgá-las. Em janeiro de 2019, um decreto federal[105] exemplificou como o Estado pode retroceder rapidamente através de medidas autoritárias. A nova regulação que buscava promover alterações no procedimento de classificação de documentos e informações como sigilosas no

[104] Lei número 13.709, de 14 de agosto de 2018 que trata da proteção de dados pessoais e altera o Marco Civil da Internet. Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade. A lei está fundamentada no respeito à privacidade, à autodeterminação informativa, à liberdade de expressão, de informação e de comunicação. O regulamento brasileiro tem como base o *General Data Protection Resolution*, regulação da União Europeia sobre a proteção de dados e privacidade, cujo objetivo é oferecer aos cidadãos o controle sobre os seus dados pessoais. Da mesma forma, a lei geral de proteção de dados brasileira pretende permitir que o cidadão tenha mais controle sobre o tratamento que é dado às suas informações pessoais.

[105] O Decreto federal 9.960/2019 alterava regras de aplicação da LAI no Executivo federal, ampliando o grupo de agentes públicos autorizados a colocar informações públicas nos mais altos graus de sigilo: ultrassecreto (25 anos, renováveis por mais 25) e secreto (15 anos).

governo federal poderia afetar diretamente o trabalho de jornalistas investigativos. Após intensa mobilização da sociedade civil, em fevereiro de 2019, o decreto foi revogado. A pressão de organizações contrárias ao retrocesso na transparência no Governo Federal foi essencial para a revogação.

Mosco (2016) define que os aspectos regulatórios são elementos políticos de controle e organização interna que podem ser comparados aos aspectos econômicos relacionados à sobrevivência.

> Controle se refere especificamente à organização interna de membros de um grupo social e ao processo de adaptação à mudança. Já sobrevivência diz respeito a como as pessoas produzem o que é necessário para a reprodução social e sua continuidade. Processos de controle são amplamente políticos, na medida em que constituem a organização social das relações dentro de uma comunidade, e processos de sobrevivência são principalmente econômicos porque dizem respeito à produção e à reprodução (MOSCO, 2016, p. 43-44).

Na perspectiva de Mosco (2016), em contextos capitalistas, aqueles que controlam os mercados são capazes de exercer um alto grau de controle sobre o conteúdo jornalístico. Dentre as tendências existentes ligadas à economia política do jornalismo que foram apontadas pelo autor estão o reconhecimento da importância das novas formas de jornalismo, especialmente a partir das mídias sociais, e a relevância da tecnologia, tanto como uma força social, quanto como uma ferramenta ideológica.

Para Silveira (2017), as sociedades informacionais são perpassadas por arranjos empresariais que dominam o sistema político e utilizam dados pessoais com fins econômicos. A neutralidade de rede[106] é um exemplo das intersecções que envolvem questões políticas, especialmente regulatórias, e lógicas econômicas que refletem no jornalismo. A tentativa de controle do acesso e divulgação de informações na internet pode ser verificada em diferentes países e em distintos contextos. O controle de acesso e os "pacotes de conteúdo" formatam um contexto semelhante ao das TVs por assinatura, onde a tendência é que poucas empresas dominem o ecossistema digital e o manipulem por meio de relações políticas, do dinheiro e da concentração de poder. De acordo com Silveira (2017), a quebra da neutralidade de rede denota a possibilidade de controle da internet por empresas de telecomunicações.

> As "teles" possuem a concessão estatal dos cabos por onde passa a comunicação em rede. Caso possam filtrar o tráfego e cobrar diferenciadamente pelos diferentes tipos de uso da internet, as operadoras obteriam o poder sobre o futuro da criatividade, uma vez que os protocolos e tecnologias que ainda não foram criadas não estariam previstos em seus pacotes de uso. Desse modo, alguém que criasse uma nova tecnologia na rede teria que necessariamente pedir passagem para as operadoras de

[106] A neutralidade de rede obriga os provedores de internet a tratarem igualmente todos os dados, sem poder discriminar ou privilegiar nada do que passa por suas redes.

> telecomunicação. Se isso ocorresse, teríamos o fim da predominância da lógica da liberdade na rede com a sua substituição pela lógica da permissão (SILVEIRA, 2017, p. 38).

As relações sociais que originam dados e informações a partir da utilização e da apropriação das tecnologias comunicacionais produzem um tipo de ativo econômico valoroso que é fornecido de maneira voluntária às grandes corporações que estão acumulando poder político e econômico. Nesse contexto, de acordo com uma das premissas desse estudo, o Estado pode utilizar o seu poder regulatório de forma perversa e, em algumas ocasiões, alcançar um potencial de controle e intrusão comunicacional com consequências significativas nas investigações jornalísticas que podem causar danos à democracia.

Muitos dos efeitos conectados às ações de vigilância na prática jornalística contemporânea são velados e opacos, entretanto inúmeras evidências demonstram que atos de vigilância podem estar relacionados com atitudes de repressão, pressões, prisões e até outros riscos para profissionais e fontes. Boa parte dos jornalistas está ciente dos riscos atrelados com a comunicação digital, contudo a maior parte destes profissionais não utiliza medidas básicas de segurança nas suas ações cotidianas. Uma pesquisa global divulgada pelo *International Center For Journalists* em 2017 demonstrou que 53% dos jornalistas e 54% das redações não usam nenhuma ferramenta de segurança digital[107]. O cenário apresentado demonstra que mesmo diante de elementos incisivos do estado de vigilância comunicacional um número significativo de jornalistas opta pela omissão perante esta realidade.

Aspectos políticos relacionados com a circulação de informações jornalísticas em meios digitais, dispositivos regulatórios e elementos ligados às ações de *lobby* de empresas transnacionais, como o Facebook, colocam em risco liberdades comunicacionais oferecidas pela internet. Atualmente, as discussões ligadas às *fake news* e ao discurso de ódio em espaços digitais expõem indícios dessa problemática.

Em entrevista concedida à *Folha de S. Paulo*, o pesquisador Steve Coll destacou que os maiores desafios do jornalismo contemporâneo são resistir aos ataques de governos populistas e a proliferação das *fake news*. Segundo Cool, é imprescindível desenvolver métodos para investigar e responsabilizar os novos donos do poder. “Nos dias de hoje, isso inclui fazer engenharia reversa dos algoritmos que determinam tantas decisões, seja nas redes

[107]Disponível em: http://www.icfj.org/sites/default/files/ICFJTechSurveyFINAL.pdf. Acesso em: 16 jan. 2018.

sociais, empresas ou governos"[108]. As mudanças na estrutura de poder que vivenciamos passam pelos algoritmos[109].

A perspectiva de veracidade de toda e qualquer informação que é apresentada nas plataformas digitais é extremamente preocupante e denuncia a negligência de uma grande parcela dos usuários em relação às suas fontes de informação. A consolidação das mídias sociais como importantes canais de informação, que podem influenciar o posicionamento dos usuários em relação às inúmeras questões centrais de interesse público, demonstra que essas arenas de discussão redesenham o acesso e o consumo de informações de parte significativa da sociedade, enaltecendo questões levantadas pelas *fake news* e o discurso de ódio.

Em dezembro de 2017, organizações da América Latina e do Caribe que defendem a liberdade de expressão e a governança democrática da Internet lançaram uma carta pública durante o Fórum da Governança da Internet, realizado em Genebra. No documento, as organizações afirmam que estamos lidando com um problema de informação e desinformação.

> Campanhas de desinformação têm sido uma estratégia dos monopólios tradicionais da mídia para ameaçar e desmantelar democracias há décadas. Não podemos desconsiderar anos de trabalho e debates dos movimentos de democratização das comunicações e adotar o termo "fake news" como um fenômeno completamente novo na América Latina. Desconsiderar antigas e novas assimetrias de poder relativas à concentração da propriedade dos meios, monopólios das redes sociais e interesses políticos governamentais para controlar e manipular discursos - dentro e além de suas fronteiras - abre espaço para sérias consequências[110].

Entre as consequências e desdobramentos possíveis apontados pelo documento estão a abertura de espaço para vigilância, manipulação de conteúdo e censura por parte das plataformas e o incentivo à vigilância e à censura dos governos. Em relação às plataformas de mídias sociais é evidenciada a utilização de ferramentas para classificar e bloquear conteúdos, qualificados como "falsos", "reais" ou "confiáveis", orientadas por algoritmos que basicamente estão relacionados a uma sequência de instruções, executadas mecanicamente por meios opacos e manipuláveis.

A vigilância e a censura dos governos se dá por meio de leis e ações governamentais que visam vigiar e regular ativamente as atividades online, além de delegar a verificação de fatos às autoridades. No Brasil, uma iniciativa governamental aponta essa intenção. Trata-se

[108] Disponível em: http://www1.folha.uol.com.br/mundo/2017/09/1922725-governos-populistas-e-fake-news-ameacam-jornalismo-diz-steve-coll.shtml. Acesso em: 16 jan. 2018.
[109] São mecanismos que ditam o que será difundido e fornecem a base do modelo de negócios para plataformas digitais a partir de uma sequência de instruções, executadas mecanicamente por meios opacos e manipuláveis.
[110] Disponível em: https://direitosnarede.org.br/p/carta-aberta-americalatinaecaribe-igf2017/. Acesso em: 16 jan. 2018.

da criação de um grupo de trabalho composto por integrantes da Polícia Federal (PF), do Exército, da Agência Brasileira de Inteligência (ABIN) e outros órgãos federais para monitorar "notícias falsas" durante as eleições de 2018.

Dentre as ações previstas pelo grupo estava a criação de uma nova legislação específica sobre as *fake news,* que poderia permitir que a polícia adotasse medidas mais duras de repressão à prática, como operações de busca e apreensão para coleta de provas[111]. Nesse caso, as notícias falsas poderiam se tornar um álibi para vigiar, constranger e restringir liberdades comunicacionais de todos os usuários da internet, inclusive os jornalistas.

O jornalismo vigilante está relacionado com a apuração e checagem de temas sensíveis por meio de ferramentas digitais. Consideramos que no Brasil esta atividade está sendo desenvolvida em zonas vigiadas e de alto risco. Como já afirmamos, devido à dependência, à centralidade do ecossistema digital na atividade jornalística e o aumento contundente da capacidade de vigilância comunicacional do Estado e de corporações podemos afirmar que a vigilância das comunicações digitais é uma realidade que pode gerar constrangimentos e consequências significativas para os profissionais.

As vulnerabilidades atreladas com a segurança digital e o acesso às informações sensíveis dos jornalistas materializam-se em casos de espionagem a partir de dispositivos de comunicação e ações de violação à privacidade dos profissionais. Esses ataques têm como base formas de constrangimento, cerceamento e impedimento que ameaçam a liberdade dos jornalistas.

No Brasil, um dos casos de vigilância de ações jornalísticas mais contundente ocorreu em 2012 e envolveu a jornalista Leniza Krauss e o produtor Lumi Zúnica da *TV Record*. O caso registrou a invasão de computadores, rastreamento de e-mails pessoais e grampo de telefones celulares e fixos dos profissionais e de seus familiares. Na oportunidade, Krauss e Zúnica investigavam a morte de Geralda Guabiraba, caso que ficou conhecido como "Pedra da Macumba", em referência ao local da morte de Geralda. Em entrevista ao *Observatório da Imprensa,* a jornalista falou sobre a situação.

> As represálias para o produtor chegavam pelo telefone da mulher dele. Eu recebia ligações e ameaças no meu celular. Uma vez estávamos no DEIC prestando depoimento e ligaram, simultaneamente, avisando que sabiam que tínhamos buscado ajuda policial. A jornalista explica que seu computador foi invadido e todos seus passos eram seguidos. Não era ninguém "blefando", eles sabiam o conteúdo dos *e-mails* trocados e tudo que conversávamos[112].

[111] Mais informações em: http://www1.folha.uol.com.br/poder/2018/01/1947872-pf-cria-grupo-para-auxiliar-outros-orgaos-no-combate-as-fake-news.shtml. Acesso em: 15 jan. 2018.
[112]Disponível em: http://observatoriodaimprensa.com.br/caderno-da-cidadania/_ed760_a_mudanca_na_vida_de_jornalistas_que_sofreram_violentas_represalias/. Acesso em: 15 jan. 2018.

Uma investigação apurou que nas ações praticadas contra os profissionais da *TV Record* foram utilizadas tecnologias avançadas que são normalmente empregadas por hackers e policiais especializados. Em 2014, após mais de dois anos de investigações, o Departamento de Homicídios e de Proteção à Pessoa (DHPP) concluiu que Geralda não foi assassinada e classificou o caso como suicídio. No entanto, o primeiro médico legista que analisou o corpo descartou essa possibilidade. A Justiça acatou a conclusão do DHPP e arquivou o caso[113].

Diante das vulnerabilidades que afetam todos os usuários da internet[114], órgãos do Estado e grandes empresas privadas têm capacidade e podem estar vigiando as comunicações eletrônicas de jornalistas sem supervisão judicial. Rusbridger (2017) afirma que os órgãos estatais querem controlar as ferramentas digitais. Para ele, as razões pelas quais o Estado quer domar, penetrar e controlar o universo digital são as mesmas que o tornam um instrumento de liberdade. O que está em jogo são interesses públicos concorrentes e conflitantes, incluindo aqueles representados por corporações, libertários civis, agências de inteligência, advogados, jornalistas e políticos.

A atividade jornalística está exposta aos riscos explícitos e implícitos do ecossistema digital. Os jornalistas convivem com dilemas que envolvem privacidade, segurança, liberdade de expressão, problemas e implicações relacionados à vigilância das comunicações. Eles se deparam corriqueiramente com situações que envolvem abusos e ataques, restrições visíveis e invisíveis.

O exercício do jornalismo em meios digitais estabelece a necessidade de condutas de precaução para preservação de liberdades ligadas à privacidade comunicacional dos jornalistas. Grande parte do trabalho jornalístico depende da confidencialidade de suas fontes e de suas apurações. No caso de que diferentes formatos de intrusão possam identificar os registros de telefone, a lista de contatos, os e-mails, os textos, a localização, os metadados e os conteúdos produzidos pelos jornalistas, estamos tratando de uma zona de vulnerabilidades e riscos significativos.

Ao evidenciar aspectos ligados aos riscos impostos por ferramentas de vigilância comunicacional e ações governamentais relacionadas à defesa dos "interesses nacionais" que podem afetar a atividade jornalística no Brasil, destacam-se indicadores de investimento em tecnologias de intrusão e a atuação da Agência Brasileira de Inteligência (ABIN) como

[113] Mais informações em: http://g1.globo.com/sao-paulo/noticia/2014/07/apos-dois-anos-policia-conclui-laudo-de-dona-de-casa-morta-em-mairipora.html. Acesso em 15 jan. 2018.
[114]Mais informações em: https://br.reuters.com/article/topNews/idBRKBN1ET136-OBRTP?feedType=RSS&feedName=topNews. Acesso em: 16 jan. 2018.

elementos norteadores para mapear evidências e possíveis implicações da vigilância sobre atividades jornalísticas.

Quanto ao investimento em aparatos intrusivos efetuado por órgãos do Estado, as informações são escassas e na maioria dos casos secretas, pois estão amparadas por questões conectadas à "segurança nacional". No entanto, um relatório publicado em 2016 pela ONG chilena *Derechos Digitales* com o título *Hacking Team malware para la vigilancia en América Latina*[115] apresentou investimentos do governo brasileiro em tecnologias intrusivas oferecidas pela empresa de segurança italiana *Hacking Team*.

O relatório baseado em um vazamento de 400 *gigabytes* (GB) de informações da empresa italiana demonstra que em 2015 a Polícia Federal (PF) assinou um contrato com uma empresa intermediária chamada *YasniTech,* a fim de comprar o *software* produzido pela *Hacking Team* para a realização de um projeto piloto. Conforme o relatório, o valor investido inicialmente foi de R$ 75 mil, contudo se o projeto fosse aprovado, o contrato seria de 1 milhão e 750 mil euros. Uma reportagem divulgada pela Agência Pública em 2015 descreve detalhes da atuação da *Hacking Team* junto à Polícia Federal, o Exército e diversos órgãos governamentais brasileiros desde 2011[116].

> O negócio da *Hacking Team* é desenvolver maneiras de "infectar" diferentes aparelhos digitais para permitir seu monitoramento ao vivo, 24 horas por dia, a chamada "tecnologia de segurança ofensiva" – ou espionagem digital. Seus equipamentos permitem às polícias realizar vigilância seletiva e também vigilância massiva, em milhares de celulares e computadores ao mesmo tempo. Seu principal produto é o Sistema de Controle Remoto "Da Vinci", que permite invadir e controlar uma máquina, driblando as comunicações criptografadas, além de espionar *Skype* e comunicações por *chat*. Segundo a empresa, o Da Vinci pode ligar remotamente microfones e câmeras de computadores e celulares e depois gravar todo o conteúdo. E, mesmo com o computador desconectado da internet, pode acessar históricos, conversas, fotos e deletar ou modificar arquivos[117].

Os testes realizados com o *software* da *Hacking Team* apresentam indícios das ferramentas intrusivas que estão à disposição e podem estar sendo usadas por diferentes órgãos governamentais brasileiros. Uma das principais frentes governamentais relacionadas ao processo de controle das possibilidades comunicacionais é a ABIN, que foi criada em 1999 e é um órgão vinculado ao Gabinete de Segurança Institucional (GSI) da Presidência da República. Dentre suas funções primordiais estão o fornecimento de informações e análises estratégicas que fomentem o processo de decisão do presidente e dos ministros.

[115] Disponível em: https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf. Acesso em: 16 jan. 2018.
[116] Mais informações em: https://apublica.org/2015/07/hackeando-o-brasil/. Acesso em: 16 jan. 2018.
[117] Disponível em: https://apublica.org/2015/07/hackeando-o-brasil/. Acesso em: 16 jan. 2018.

Em 2013, o ex-oficial de inteligência da ABIN tenente-coronel do Exército André Costa Soares afirmou que em 2004 foi convocado para atuar em uma operação clandestina chamada de "Operação Mídia". Conforme o ex-oficial, a operação visava espionar jornalistas e donos de meios de comunicação[118]. Os fatos são baseados em um documento escrito por Soares e apesar dos poucos esclarecimentos, o caso demonstra a possível inadequação da atuação da agência. Tendo em vista o papel central de produzir informações que balizem tomadas de decisão do Estado e que direcionem outras instituições, as ações da ABIN podem influenciar de maneira determinante a adoção de políticas e regulações relacionadas com a comunicação digital.

Um reflexo concreto dessa possibilidade de intervenção pode ser associado aos desdobramentos da Operação *Hashtag*, deflagrada oficialmente em julho de 2016 pela ABIN, Polícia Federal (PF), Forças Armadas e agências de informação internacionais. A Operação *Hashtag* foi a primeira ação da Polícia Federal após a sanção da lei Antiterrorismo[119] e realizou as primeiras detenções de brasileiros por suspeita de ligação com grupos terroristas. Alguns aspectos que transpassaram a operação apontam que ações de vigilância estão em curso no Brasil. Em entrevista ao portal G1, o procurador da República, Rafael Brum Miron, integrante da operação, afirmou que as investigações que prenderam os suspeitos de ligação com o Estado Islâmico começaram com um alerta do *Federal Bureau of Investigation* (FBI). As ações classificadas como atividades terroristas foram vigiadas em aplicativos (WhatsApp[120] e Telegram[121]) que usam sistemas de criptografia. De acordo com Silveira (2016), os aparatos de segurança e de justiça agem cada vez mais de modo extremo e hiperdimensionado.

> Seus expoentes clamam pelo fim das restrições ao acesso das autoridades aos dados armazenados pelos cidadãos e pela possibilidade de interceptação plena da comunicação em rede. Sem isso, dizem, não poderão enfrentar os quatro cavaleiros do infoapocalipse: o terrorismo, o tráfico de drogas, a pedofilia e a lavagem de dinheiro[122].

[118] Mais informações em: https://josiasdesouza.blogosfera.uol.com.br/2013/11/09/abin-espionou-a-midia-sob-lula-diz-ex-analista/. Acesso em: 16 jan. 2018.
[119] Lei 13.260 sancionada por Dilma Rousseff em 16 de março de 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm. Acesso em: 16 jan. 2018.
[120] É um aplicativo multiplataforma que oferece serviços criptografados de mensagens de texto e áudio, chamadas de voz e vídeo, envio e recebimento de diversos tipos de arquivos, além do compartilhamento de localização entre os usuários.
[121] Serviço de mensagens instantâneas baseado em nuvem.
[122] Disponível em: https://noticias.uol.com.br/opiniao/coluna/2016/03/14/vigilancia-na-internet-nao-reduz-crimes-apenas-restringe-liberdade.htm. Acesso em: 16 jan. 2018.

Na perspectiva de Silveira (2016), esse descabido grau de vigilância não reduzirá os crimes, apenas tornará a democracia mais frágil e os cidadãos mais cerceados. Nesse sentido, atos relacionados com a "segurança nacional" associados ao poder de vigilância do Estado podem estar minando liberdades e direitos civis. Em uma realidade em que empresas e governos exploram, manipulam e administram modernos sistemas invasivos motivados por interesses financeiros, políticos e ideológicos, investigações e fontes de informação jornalísticas estão expostas e o trabalho jornalístico está sendo atravessado por interferências de grandes empresas e instituições estatais.

Uma circunstância que demonstra o potencial controle de espaços expressivos de consumo e distribuição de informações jornalísticas por empresas transnacionais, como o *Facebook,* ocorreu no dia 11 de janeiro de 2018, quando o fundador da plataforma, Mark Zuckerberg, anunciou uma alteração no algoritmo, para que publicações de amigos e familiares ganhem mais destaque do que notícias no *feed*[123] dos usuários. A recalibragem do algoritmo demonstra a fragilidade que a dependência de ferramentas digitais terceirizadas impõe aos veículos jornalísticos tradicionais e independentes.

Esse grau de controle da informação concentrado no *Facebook* também pode ser associado às tentativas e intenções nocivas de regulação do ambiente digital. Uma medida regulatória adotada na reforma eleitoral de 2017[124] que permite o impulsionamento de conteúdos em plataformas digitais favorece economicamente a empresa de Zuckerberg. A nova regulação eleitoral brasileira que foi aprovada pelo Congresso Nacional em outubro de 2017 traz mudanças importantes nas campanhas eleitorais realizadas nos meios digitais e, de certa forma, fortalece o poder econômico e político do *Facebook*[125].

Além das intenções veladas do poder público, que podem violar garantias individuais, convivemos com práticas de entidades privadas que buscam o lucro por meio da exploração do mercado de dados. Seguindo uma lógica perversa, as informações pessoais dos cidadãos são expostas, enquanto os dados e conhecimentos gerados pelas corporações são opacos e praticamente inacessíveis. Enquanto as informações sobre os usuários estão vulneráveis, os dados ligados às empresas são protegidos e blindados.

Esses desdobramentos apontam riscos acionados pela dinâmica tecnológica acelerada, tais como a dificuldade de acesso às informações sobre a atuação de empresas privadas,

[123] *Feeds* são utilizados para que os usuários da plataforma possam acompanhar as novas publicações.
[124] Mais informações em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13488.htm. Acesso em: 16 jan. 2018.
[125] Mais informações em: http://www.valor.com.br/politica/5158354/reforma-eleitoral-abre-espaco-para-impulsionar-conteudo-em-rede-social. Acesso em: 16 jan. 2018.

estratégias adotadas pelo Estado, segredos e dados públicos e a restrição de liberdades comunicacionais dos indivíduos, particularmente dos jornalistas, que podem interferir de maneira determinante no sistema democrático brasileiro.

3 RISCOS DIGITAIS PARA JORNALISTAS

> *Eu sabia que nenhuma quantidade de documentos, nem de jornalismo, seria suficiente para enfrentar a ameaça que assolava o mundo. As pessoas precisavam de ferramentas para se proteger, e precisavam saber usá-las. Dado que eu também estava tentando fornecer essas ferramentas aos jornalistas, preocupava-me que minha abordagem houvesse se tornado técnica demais. Depois de tanto tempo dedicado a dar palestras a colegas, essa oportunidade de simplificar a minha abordagem ao assunto diante de uma audiência geral me beneficiaria bastante. Além disso, eu sinceramente sentia falta de lecionar; fazia um ano que não ficava diante de uma classe, e assim que voltei a essa posição, percebi que estivera ensinando as coisas certas às pessoas erradas o tempo todo (SNOWDEN, 2019, p. 280-281).*

O risco é um elemento intrínseco à atividade jornalística que é envolvida por perigos e ameaças de dimensões distintas. Essas ameaças podem atingir a integridade física e mental dos jornalistas. No contexto atual, para além das agressões físicas, mortes e perseguições somam-se os perigos inerentes ao ecossistema digital. Elementos tangíveis demonstram a possibilidade de impactos consistentes na prática profissional em dimensões que abarcam principalmente a privacidade, a vigilância das comunicações e violações específicas desse contexto.

> 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 (CHRISTOFOLETTI; TORRES, 2018, p. 5).

Conforme a nossa perspectiva, 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. Já quando *devices* ou *gadgets* usados pelos jornalistas servem de porta de entrada para ameaças à sua privacidade e à segurança profissional, é possível afirmar que os riscos são derivados do manejo desses equipamentos. Por fim, 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 caracterização demonstra a multiplicidade de pontos potencialmente vulneráveis nas ações e condutas jornalísticas.

> 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 (CHRISTOFOLETTI; TORRES, 2018, p. 5).

Nesse sentido, os riscos digitais estão diretamente associados aos ataques advindos do ecossistema digital. Conforme Paterson (2018), o jornalismo investigativo não pode existir sem a confiança do público na capacidade dos jornalistas de protegerem as suas fontes. Atualmente, uma questão fundamental está relacionada à capacidade de proteger fontes diante dos desenvolvimentos tecnológicos que representam uma ameaça substancial ao anonimato.

> Uma questão importante da preocupação atual refere-se à proteção limitada disponível para os chamados metadados, juntamente com os requisitos legais em algumas jurisdições para que os provedores de telecomunicações e provedores de serviços de Internet retenham os metadados para que possam ser acessados pelas agências[126] (PATERSON, 2018, p. 15, tradução livre).

Ainda de acordo com Paterson (2018), as tecnologias que ameaçam a proteção das fontes dos jornalistas podem ser divididas em três grupos: tecnologias que comprometem a capacidade de os indivíduos permanecerem anônimos em locais públicos; tecnologias que possibilitam identificar a localização física dos indivíduos e movimentos geográficos e tecnologias que comprometem a segurança dos dados armazenados ou comunicados eletronicamente. McGregor e Watkins (2016) apontam que os riscos de segurança digital para jornalistas e organizações jornalísticas aumentaram nos últimos anos.

> Somente em 2013, uma série de grandes organizações noticiosas - incluindo o New York Times, o Wall Street Journal, Bloomberg e The Washington Post - revelaram que seus sistemas de comunicação digital haviam sido alvo de ataques digitais patrocinados pelo Estado[127] (MCGREGOR; WATKINS, 2016, p. 34, tradução livre).

Em alguns dos casos citados, o objetivo dos ataques apontava a tentativa de identificação das fontes dos jornalistas, em outros, os esforços pareceram mais retaliatórios, apesar da ampla gama de ameaças e consequências tangíveis desses ataques. Como já indicamos, estudos (PEW RESEARCH CENTER, 2015; MCGREGOR; WATKINS, 2016; TSUI; LEE, 2019) apontam que a maioria dos jornalistas investigativos não adotam medidas

[126] No original: A key issue of current concern relates to the limited protection that is available for so- called metadata, coupled with legal requirements in some jurisdictions for telecommunications providers and internet service providers to retain metadata so that it can potentially be accessed by agencies.
[127] No original: During 2013 alone a host of major news organizations—including The New York Times, The Wall Street Journal, Bloomberg, and The Washington Post—revealed that their digital communications systems had been the target of state-sponsored digital attacks.

práticas de mitigação de riscos, no que diz respeito à segurança da informação ou das comunicações.

Desde o final do século passado, as mudanças tecnológicas e culturais tornaram a tarefa de caracterizar segurança e liberdade dos jornalistas ainda mais complexa. A digitalização da informação e a descentralização de bancos de dados fizeram com que a internet se consolidasse como uma plataforma de comunicação e informação. O acesso a equipamentos que ampliam o tempo e a experiência de conexão contribuiu para a hiperconectividade (JENKINS; FORD; GREEN, 2014), a multimidialidade (SALAVERRÍA, 2014), a ubiquidade (PAVLIK, 2014) e a ampliação da vida digital. Todos os aspectos da experiência humana sofreram modificações, inclusive o jornalismo.

Conforme Christofoletti e Torres (2018), os riscos digitais podem ser considerados perigos mais extensivos que os demais, isto é, nem todo jornalista atua em zonas de conflito ou arrisca a vida, mas não há jornalista que não utilize computadores, *smartphones*, internet ou sistemas de informação em seu cotidiano profissional.

> 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 (CHRISTOFOLETTI; TORRES, 2018, p. 4-5).

A fim de verificar a existência de indicativos relacionados aos riscos digitais para a atividade jornalística e caracterizá-los, analisamos 80 relatórios sobre agressões a jornalistas e ataques à liberdade de imprensa de nove organizações não governamentais [128] . São documentos reconhecidos pela categoria e pela indústria, que permitem a formulação de políticas para o setor e o aperfeiçoamento do mercado. A análise compreende categorias de ataques que elaboramos a partir da bibliografia na área. A partir desse quadro, sugerimos uma definição de risco digital e indicamos possíveis descrições para os ataques digitais, objetivando sensibilizar os jornalistas a essas ameaças.

[128] Esses dados serão detalhados no decorrer desse capítulo.

3.1 ATAQUES DIGITAIS COMO MODALIDADE DE RISCO PROFISSIONAL[129]

Em um panorama no qual diversas organizações não governamentais classistas e humanitárias monitoram violações a direitos e casos de violência contra jornalistas em suas atividades profissionais, os registro e relatórios que revelam e sistematizam agressões auxiliam na composição de uma paisagem dos constrangimentos, cerceamentos e impedimentos que ameaçam o livre e pleno exercício jornalístico, podendo se desdobrar, ainda, em danos à cidadania e à democracia. Esses relatórios cumprem um papel significativo em relação aos inúmeros atentados à vida e à integridade física desses profissionais, pois permitem aferir aspectos voláteis, como liberdade de expressão, de imprensa e comunicação, autonomia e independência editorial, solidez e consistência democrática.

Ameaças, que antes estavam presentes apenas na vida tangível, tiveram seus derivados no espelho online, o que nos leva a defender que riscos digitais também deveriam ser considerados como formas de violência contra jornalistas em relatórios sobre liberdade de imprensa. Na medida em que esses (novos) perigos atualizam ações que violentam a prática jornalística, impactando na qualidade, diversidade, pluralidade e integridade das informações, é importante identificá-los, caracterizá-los e quantificá-los.

Em situações práticas que potencialmente afetam rotinas jornalísticas, identificamos 19 ataques que são percebidos conforme a Tabela 1:

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 de histórico de navegação

[129] Essa proposição foi apresentada no artigo "Jornalistas expostos e vulneráveis: ataques digitais como modalidade de risco profissional" publicado na **Revista Famecos**, Porto Alegre, v. 25, n. 3, em 2018. Disponível em: http://revistaseletronicas.pucrs.br/ojs/index.php/revistafamecos/article/view/29210. Acesso em: 30 out. 2019.

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*
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.

Fonte: Christofoletti & Torres, (2018). Categorias elaboradas a partir de Artículo 19 (2013), Carlo & Kamphuis (2014), Sierra (2013).

Interessados em mapear e avaliar os ataques digitais a jornalistas, recorreremos 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 realidades específicas ou contextos globais. Tais critérios permitiram alcançar os seguintes documentos de nove organizações, conforme relatado a seguir:

Tabela 2– Relatórios avaliados.

Documento	Origem	Quant.	Período
Relatório Sobre Liberdade de Imprensa no Brasil		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	Comitê 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	Artigo 19 – Brasil	01	2012

Jornalistas e Defensores dos Direitos Humanos			
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 por Christofoletti & Torres, 2018, a partir do corpus de análise.

Para analisar a amostra, utilizamos como método os parâmetros da pesquisa documental e da pesquisa bibliográfica, associados à coleta e à análise de dados. Com o propósito de realizar a análise documental, desenvolvemos um protocolo específico, que pode ser observado no Quadro 3.

Quadro 3 – Protocolo de pesquisa.

Questões centrais analisadas:		
a) Os ataques digitais da Tabela 1 são inventariados nos *reports* das ONGs mencionadas 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: Elaborado por Christofoletti & Torres, 2018.

Ao verificarmos os relatórios, percebemos a variedade nos formatos e na estrutura dos documentos, fatores que dificultam a identificação imediata de ataques digitais e consequentemente reduzem seu peso e importância no contexto de ameaça aos jornalistas. De forma predominante, o enquadramento dos riscos apresentados pelos documentos não está alinhado ao ecossistema digital. Foi possível perceber, porém, a ocorrência de situações regulatórias e contextos com altos riscos de ameaças e violações das comunicações privadas de jornalistas em diferentes partes dos relatórios.

Com o intuito de facilitar a identificação de episódios de ataques digitais nos documentos avaliados, recorremos a uma lista de 40 palavras-chave relacionadas com o uso de tecnologias de comunicação e informação e a 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. Os termos aparecem na nuvem de palavras-chave da figura 1.

Nesta etapa da avaliação, percebemos que os ataques digitais aparecem nos relatórios de diferentes maneiras, sem padrão de apresentação e, na maior parte das vezes, associados à ameaça física dos jornalistas. Essa é uma condição que demonstra uma abordagem situacional das questões propostas e seus entornos. 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. Da mesma maneira, as ameaças que abordam temas sensíveis emergem como problemáticas com potencial real de interferência e modificação nas condutas e ações jornalísticas.

Figura 1 – Nuvem de palavras-chave.

Fonte: Elaborado por Christofoletti & Torres, 2018.

Com base nos critérios que estabelecemos, identificamos 452 ataques nos 15 anos do período observado, taxa que pode ser considerada baixa, se levarmos em conta o alcance geográfico, a janela temporal e a larga disseminação dos usos e apropriações tecnológicas entre os jornalistas. Tendo em vista os dados coletados, podemos afirmar que, em média, um ataque digital contra jornalistas aconteceu a cada 12 dias no planeta. A baixa ocorrência permite algumas inferências, no que diz respeito aos ataques digitais como modalidade de

risco profissional. As ameaças podem não ter sido graves o suficiente para serem registradas, podem não ter sido notificadas ou elas sequer foram notadas.

Esses elementos apontam para uma possível negligência, por parte dos profissionais, em relação ao potencial nocivo desses ataques em âmbitos tangíveis, como constrangimentos e restrições, e intangíveis, por exemplo, modulação[130] e inviabilidade do trabalho jornalístico. De acordo com Tsui e Lee (2019), para entender a relação entre vigilância e liberdade de imprensa, precisamos distinguir a "liberdade da vigilância" e a "liberdade de privacidade e segurança comunicacional".

> Considerando que a liberdade de vigilância acentua a ausência de vigilância, a liberdade de comunicação privada e segura enfatiza, em vez disso, a capacidade de um usuário se comunicar de forma privada e segura, mesmo na presença da vigilância. Para entender a liberdade de imprensa na era digital, é fundamental examinar até que ponto os jornalistas estão cientes e capazes de usar ferramentas de segurança digital[131] (TSUI; LEE, 2019, p. 2, tradução livre).

Tsui e Lee (2019) evidenciam a importância de entender com mais profundidade que tipo de mentalidade os jornalistas têm, no que abrange à segurança digital. Também destacam como os jornalistas não só percebem os riscos e ameaças ligadas à vigilância digital, mas também como eles são conscientes de possíveis soluções para sanar os perigos apresentados pelo ecossistema digital. Em seu estudo "Como os jornalistas entendem as ameaças e oportunidades de novas tecnologias: um estudo de mentalidades de segurança e suas implicações para a liberdade de imprensa"[132], os autores buscaram estudar mentalidades e práticas de segurança digital de jornalistas baseados em Hong Kong, incluindo aqueles que viajam e trabalham na China.

> Muitos jornalistas de Hong Kong precisam trabalhar regularmente na China para cobrir notícias sobre o continente. Portanto, dependendo da sua abordagem e tópico de foco, os jornalistas em Hong Kong enfrentam condições de trabalho que variam de um ambiente de relatórios relativamente livres (Hong Kong) a um ambiente em que os jornalistas enfrentam uma ampla gama de ameaças, incluindo vigilância,

[130] Nesse estudo, abordamos modulação a partir da perspectiva de Fernanda Bruno (2016), que trata da "modulação das subjetividades" em um cenário multifacetado que envolve a exposição das tecnologias e redes de comunicação. Nesse contexto, o controle social contemporâneo modula o comportamento pela promessa da otimização da performance e pela exigência de melhores resultados nos diversos planos da vida, dentre os quais destacam-se o profissional, o pessoal e o social.

[131] No original: Whereas the freedom from surveillance emphasizes the absence of surveillance, the freedom to private and secure communication instead emphasizes the capacity of a user to communicate privately and securely, even in the presence of surveillance. To understand press freedom in the digital age, it is therefore critical to examine to what extent journalists are aware of and able to use digital security tools.

[132] No original: "How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom".

> assédio físico ou até mesmo ameaças de prisões (China)[133] (TSUI; LEE, 2019, p. 2, tradução livre).

As ambivalências destacadas pelo estudo de Tsui e Lee (2019) que permitem ver como os diferentes ambientes de atuação interferem no pensamento e comportamento dos jornalistas em relação à segurança digital podem ser associadas à diversidade das ocorrências registradas nos relatórios analisados. Dos 19 tipos investigados, 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 o último implica em reconhecer desatenção e até negligência na garantia de segurança digital.

O tipo de ataque a jornalistas detectado com mais frequência foi a ameaça por telefone (AT), com 106 registros, quase um quarto dos episódios. Violação e interceptação de e-mail foram relatadas 76 vezes e ameaças em redes sociais 60. Somados, os três tipos de ataques mais comuns ultrapassam 53% dos casos, apontando 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 7 relatos cada; furto de senhas por meio de *phishing* ou *pharming* (FPP) e quebra de criptografia (QC), com 6 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

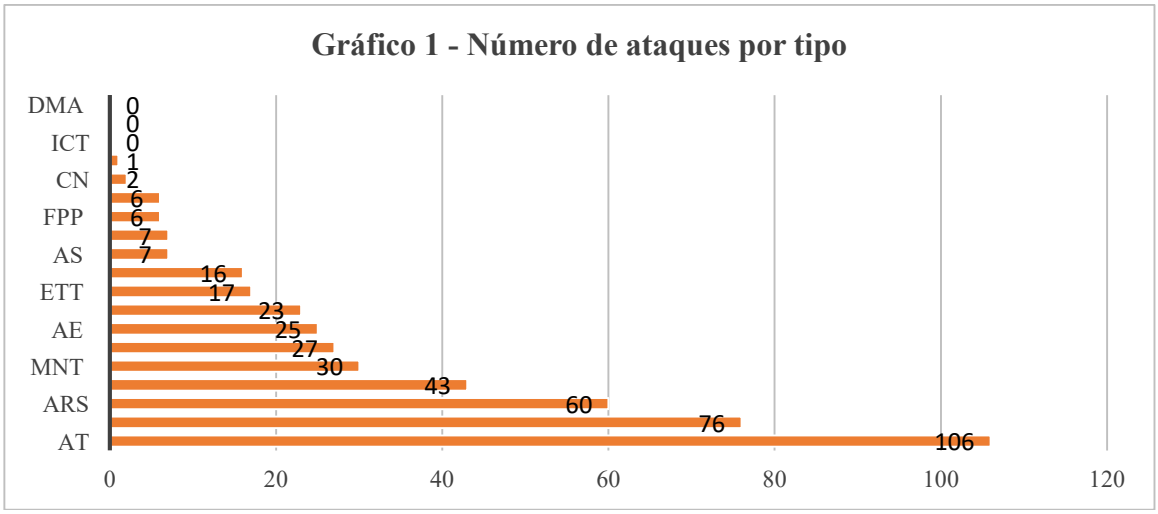
[133] No original: Many Hong Kong journalists need to work regularly in China to cover news about the mainland. Therefore, depending on their beat and topical focus, journalists in Hong Kong face working conditions ranging from a relatively free reporting environment (Hong Kong) to an environment where journalists face a wide range of threats, including surveillance, physical harassment, or even the threats of arrests (China).

autorização na casa de jornalista ou em seu telefone celular/smartphone (ETC) e nos 17 casos de escutas na redação ou local de trabalho (ETT), que podem ocorrer mediante invasão física, infiltração e até mesmo de forma remota.

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 a Freedom House abrange 15 dos 19 tipos de ataques listados. Os relatórios dos Repórteres Sem Fronteiras totalizaram 62 casos, divididos 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, enquanto que a Federação Internacional de Jornalistas fez 20 registros de 4 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.

Amplos, variados, intensos e invisíveis, os riscos digitais permitem ataques digitais que podem comprometer o controle e a integridade das informações, assim como a proteção pessoal de jornalistas e de suas fontes. Desta forma, afetam a liberdade de imprensa e a segurança de repórteres, redatores e editores. Esses ataques são inventariados de formas diversas nos relatórios das organizações que fazem algum tipo de monitoramento em relação ao trabalho realizado pelos jornalistas (CHRISTOFOLETTI; TORRES, 2018).

Gráfico 1 – Número de ataques digitais por tipo no período 2001-2016.



Fonte: Elaborado por Christofoletti & Torres, 2018.

Os aspectos evidenciados pela análise dos relatórios contribuem para a visualização de um panorama mais amplo sobre segurança digital e liberdade comunicacional e de imprensa através da estruturação de um quadro de incidências de episódios relacionados à segurança de jornalistas, que pode ser aplicado em diferentes contextos. Alinhado com essa possibilidade está a constituição de elementos que possibilitem a consolidação de mentalidades que alimentem um "senso de vulnerabilidade permanente" que fortaleça uma "cultura de segurança digital para jornalistas".

Entender a perspectiva de segurança digital de um conjunto específico de jornalistas é importante para podermos compreender também os níveis de liberdade de imprensa e de liberdade comunicacional de determinados contextos. Jornalistas mais conscientes têm mais condições de aproveitar as oportunidades oferecidas pelas novas tecnologias, assim como para mitigar e se proteger das inúmeras possibilidades de vigilância a que podem estar expostos. Quanto maior o alcance e sensibilidade dos temas e histórias investigadas, maior a necessidade de um campo jornalístico que tenha liberdade, robustez e potência.

3.2 JORNALISTAS EXPOSTOS E VULNERÁVEIS

A fim de obter as informações necessárias para realização do seu trabalho mais elementar, isto é, de desenvolver relatos cotidianos, os jornalistas transitam por zonas e situações de confronto que, de maneira geral, envolvem personagens que oferecerem potenciais situações de perigo. Nessas ocasiões, ficam sujeitos a condições insalubres, exaustivas e estressantes que exploram a lógica adversarial de pessoas e grupos poderosos e, muitas vezes, ficam na linha de tiro que as separa. A exposição pública e o contato com ameaças diversas tornam a profissão altamente arriscada.

"Para mitigar um problema, precisamos reconhecê-lo como um problema". Essa é uma máxima constantemente repetida, no entanto verídica, quando tratamos da segurança digital, integridade física e psicológica dos jornalistas brasileiros. A presença e atuação jornalística no ambiente digital expõem os profissionais a riscos regulares e iminentes. Atualmente, a dimensão dos problemas contextuais e ambientais impostos ao ecossistema jornalístico no Brasil são um fato contundente e avassalador.

Conforme a Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), em 2019, o Brasil era o sexto país mais perigoso para o exercício da atividade jornalística no mundo. Um relatório divulgado em 2019 se debruça sobre o assassinato de jornalistas, que é a forma mais definitiva de censura. "No entanto, é apenas a ponta do iceberg

dos ataques contra jornalistas, que vão desde ataques físicos não letais, sequestros, detenções ilegais, ameaças, assédio online e offline, até retaliações a membros da família" (UNESCO, 2019, p. 1).

Em abril de 2019, o Conselho Nacional do Ministério Público (CNMP) apresentou dados específicos do Brasil sobre assassinatos decorrentes do exercício do jornalismo, no período de 1995 a 2018. "A situação brasileira é preocupante e revela um cenário sistemático. O país soma sessenta e quatro episódios de homicídios desses agentes desde 1995, praticados em todas as cinco regiões" (CNMP, 2019, p. 3). Informações apresentadas pela organização não governamental Repórteres Sem Fronteiras (RSF) indicam "um período sombrio que se anuncia" diante da quantidade assustadora de ameaças, agressões e assassinatos que afetam frontalmente os jornalistas que atuam no país, um dos mais violentos da América Latina para quem exerce esse ofício.

De acordo com a RSF, em 2018, ao menos quatro jornalistas foram assassinados no país, em decorrência da sua atividade, sendo que, na maioria dos casos, os profissionais mortos cobriam e investigavam temas sensíveis ligados à corrupção, políticas públicas e crime organizado, particularmente em cidades de pequeno e médio porte. Os dados estão alinhados aos 156 ataques digitais e físicos a jornalistas registrados pela Associação Brasileira de Jornalismo Investigativo (Abraji) em 2018.

A Federação Nacional dos Jornalistas (Fenaj) ratifica o diagnóstico ameaçador no relatório "Violência contra jornalistas e liberdade de imprensa no Brasil" (2018), informando que a violência contra jornalistas no Brasil voltou a crescer em 2018. O número de agressões chegou a 135, atingindo 227 jornalistas, visto que em muitos casos mais de um profissional foi atingido. O relatório "Violações à liberdade de expressão" (2018), divulgado pela Associação Brasileira de Emissoras de Rádio e Televisão (Abert), demonstra preocupação com o panorama do jornalismo no Brasil: "Em todo o mundo, a tarefa de informar se transformou em risco de morte e os jornalistas continuam sendo tratados como alvos. No Brasil, não é diferente" (ABERT, 2018, p. 9).

Em seu sexto relatório abordando o tema liberdade de expressão no Brasil, que recebe o título de "Violação à liberdade de expressão" (2017), a Artigo 19 procura destacar o cenário de hostilidade e ataques a comunicadores, de uma forma geral. Este cenário busca impedir a efetivação da liberdade de expressão e do direito à informação no país. "Isso se configura de maneira ainda mais intensa em um ambiente de comunicação como o brasileiro, marcado por um grande 'deserto de notícias', em que mais de um terço da população vive em cidades sem nenhum jornal impresso ou online local" (ARTIGO 19, 2017, p. 6). A desinformação e as

diversas formas de violência praticadas contra jornalistas afetam a democracia e a liberdade de maneira significativa.

Com uma situação semelhante a do Brasil, o México registrou o assassinato de cinco jornalistas nos primeiros cinco meses de 2019, um número que é trágico e ao mesmo tempo comum em países altamente letais para exercer este ofício no mundo. Alvos dos cartéis de drogas, tanto a corrupção estatal, como a policial aliam-se a um sistema de justiça ineficiente e compõem o quadro que transformou o México em um território de risco para ações jornalísticas.

> Apenas em 2018, organizações da sociedade civil documentaram os assassinatos de 48 defensores dos direitos humanos e oito jornalistas. Com esses indicadores, o México continua sendo um dos países mais perigosos do mundo para ativistas e comunicadores, com um custo sério em termos de luta pelos direitos humanos, liberdade de expressão e responsabilidade do governo[134] (PBI; WOLA, 2019, p. 6, tradução livre).

Os casos apresentados pelo relatório *"Cambiando el curso de la impunidad"*, produzido pela Brigadas Internacionais de Paz (PBI) e pela Oficina em Washington para Assuntos Latinoamericanos (WOLA), são ocorrências de uma escalada da violência contra jornalistas no México. No continente americano, o segundo país a oferecer mais riscos é o Brasil. Brasil e México têm os maiores produtos internos brutos (PIBs) da América Latina, mas também são os países mais populosos. Órgãos oficiais estimam populações nas casas dos 200 milhões e 120 milhões, respectivamente. Somadas, essas populações equivalem a mais da metade dos habitantes da América Latina. Além de características econômicas ou demográficas, o histórico de impunidade em crimes contra esses profissionais aproximam os dois países.

Nos últimos anos, estes países têm sido os locais mais perigosos do subcontinente para se atuar[135], onde há mortes, agressões, perseguições e impunidade nos crimes contra jornalistas. 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.

Nos 80 relatórios em que identificamos ataques digitais, Brasil e México somaram 137 casos. No Brasil foram 119 registros de riscos à integridade física e ofensas. As ameaças e constrangimentos em mídias sociais (ARS) apareceram 49 vezes. Em alguns documentos,

[134] No original: Solo en 2018, organizaciones de la sociedad civil documentaron los asesinatos de 48 personas defensoras de derechos humanos y ocho periodistas. Con estos indicadores, México continúa siendo uno de los países más peligrosos en el mundo para activistas y comunicadores, con un grave costo en cuanto a la lucha por los derechos humanos, la libertad de expresión y la rendición de cuentas del gobierno.

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

emerge uma preocupação com a formação de grupos que empregam o que classificamos, nesse estudo, de "vigilância digital odienta". 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 (CHRISTOFOLETTI; TORRES, 2017).

Em 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). 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 [136] (2014) aparece como um importante instrumento regulatório alinhado à privacidade e à liberdade de expressão, mas parcialmente regulamentado (CHRISTOFOLETTI; TORRES, 2017).

Os documentos avaliados apontam que os riscos digitais para jornalistas ainda são tratados de forma superficial pelas organizações de notícia, jornalistas e autoridades que devem enfrentar e coibir crime e violência. Para fomentar formas de entendimento e esclarecimento dessas situações, propomos definições de riscos e ataques digitais no campo jornalístico. Conforme Christofoletti e Torres (2017), 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 no ecossistema digital e a importância de condutas de precaução para preservação de liberdades ligadas a privacidade comunicacional dos jornalistas (CHRISTOFOLETTI; TORRES, 2017, p. 109-110).

[136] Lei número 12.965, de 23 de abril de 2014 que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

O dia 3 de maio é marcado pela celebração do Dia Mundial da Liberdade de Imprensa, proclamado pela Assembleia Geral da Organização das Nações Unidas (ONU) em 1993, em seguimento à aprovação em sessão da Conferência Geral da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), realizada em 1991. O dia é marcado pela defesa da mídia de ataques contra a sua independência e presta tributo aos jornalistas que perderam a vida no exercício de sua profissão. Também é uma ocasião singular para refletir sobre as tentativas de censura e cerceamento da liberdade jornalística, por meio de perseguições, ataques e assassinatos (TORRES, 2019). Em mensagem, a diretora-geral da UNESCO, Audrey Azoulay, enalteceu a dimensão dos ataques aos jornalistas.

> A impunidade por crimes cometidos contra jornalistas é uma ameaça que afeta todas as nossas sociedades. Essa ameaça exige de nós um constante estado de vigilância. Devemos agir de forma conjunta para proteger a liberdade de expressão e a segurança dos jornalistas (UNESCO, 2019) [137].

A transição que envolve a transformação de situações corriqueiras de vigilância nociva em problemas significativos está intrinsecamente ligada ao olhar que lançamos sobre contextos e fatos. Em muitas ocasiões, essa mudança de perspectiva é perpassada por uma decisão que envolve os próprios jornalistas. Essa decisão abarca elementos que vão além do comprometimento com a transmissão de informações de maneira íntegra e profissional. Ela precisa ser balizada por elementos de contextualização histórica e condições de atuação que, em última análise, impõem riscos severos aos jornalistas.

> A clareza deste panorama destrutivo não está diretamente associada ao convencimento dos profissionais, não importa dizer qual a perspectiva retórica mais acertada, mas sim apresentar possibilidade de ampliação de entendimentos a partir do conhecimento de dados tangenciados por formas de apuração e verificação. As formas de opressão envolvem métodos violentos e refinados que estruturam um modo operatório repressivo ampliado pelas novas tecnologias. Os ataques aos jornalistas estão relacionados às tentativas de controle social ardilosas que podem corroer instituições democráticas e dar aos detentores de poder econômico e político um nocivo grau de manipulação dos fatos sociais, pois, em inúmeras ocasiões, a falta de densidade informativa é proposital e estratégica (TORRES, 2019, p. 1).

Nesse cenário, opiniões pessoais e a resignação diante da incompreensão das zonas de risco impostas aos jornalistas são subterfúgios acessíveis. Esconder, negligenciar e subestimar são características que envolvem os riscos cotidianos enfrentados por jornalistas, particularmente em abordagens de temas sensíveis. A definição de risco digital e tipificação

[137] UNESCO. Punir o crime, não a verdade: destaques do relatório de 2018 da Diretora-Geral da UNESCO sobre a segurança dos jornalistas e o perigo da impunidade, 2019. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000266151_por. Acesso em: 5 out. 2019.

de ataques digitais revela que os ataques e ameaças digitais compõem um cenário pouco ameaçador. Vale ressaltar que esta definição foi feita a partir de ocorrências registradas 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.

Entretanto, sua variedade de modos e ampla difusão estão 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. O número baixo de registros em relação ao período avaliado (452 registros em uma década e meia) aponta a necessidade de que as organizações de monitoramento revejam suas metodologias para reunir mais informações sobre esses tipos de violência profissional, de maneira a permitir leituras mais profundas das reais ameaças que rondam as redações, coletivos e projetos jornalísticos independentes.

3.3 SEGURANÇA DIGITAL PARA JORNALISTAS

Ao longo desse estudo, evidenciamos elementos concretos e objetivos que demonstram a urgência da discussão e da conscientização sobre os riscos e ameaças que o ecossistema digital impõe à prática do jornalismo. Particularmente, as iniciativas ancoradas no jornalismo investigativo necessitam de um senso de vulnerabilidade diante da exposição aos riscos digitais. Também apontamos que as práticas conectadas e em rede trazem potencialidades à reportagem, apuração, edição e difusão de conteúdos jornalísticos.

Em um contexto de vigilância digital massiva, o jornalismo vigilante precisa balizar o seu trabalho e levar em conta a vigilância comunicacional e a necessidade de preservação da privacidade dos jornalistas. Cabe ratificar que, neste estudo, quando tratamos do conceito de vigilância nos reportamos ao monitoramento de ações jornalísticas e à possibilidade de intrusão das comunicações, através da interceptação e do armazenamento de dados pessoais.

Aspectos dessas problemáticas já aparecem em diversos relatórios de riscos e agressões bem como em materiais de apoio a jornalistas, particularmente nos últimos 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.

De acordo com Christofoletti e Torres (2018), a bibliografia sobre cibersegurança é vasta na informática e tem se espalhado também na forma de referências para usuários não especializados. Moore (2016) trata da privacidade, da segurança e da responsabilidade em

uma abordagem que sugere uma gama diversificada de perspectivas filosóficas e argumentos sobre por que ou se a privacidade pode ser mais ou menos importante do que a segurança e se uma pode prejudicar a outra, em um contexto de tecnologias avançadas que estão transformando a forma como os cidadãos veem conceitos como privacidade e segurança.

Taylor, Floridi e Sloot (2017) chamam a atenção para as tecnologias analíticas de dados que estão focadas nas vidas e no comportamento dos usuários e para conceitos como anonimização, proteção de identidades individuais e salvaguarda de informações pessoais. Ações direcionadas a grupos específicos, possibilitadas por análises de dados, permitem uma visão ampla que pode resultar em decisões que originam riscos reais.

As obras sobre quebra de privacidade e necessidade de aumento da segurança digital dirigidas a jornalistas também têm surgido com mais vigor nos últimos anos. Elas tratam do fenômeno dos *whistleblowers*[138] e dos grandes vazamentos de informação (GREENBERG, 2012; BREVIN *et al.* 2013; GOLDFARB, 2015; RUBY *et al.*, 2016) e passam ainda pelo desenvolvimento de habilidades digitais específicas para incremento da segurança pessoal dos profissionais e das próprias fontes de informação (BÜCHI *et al.*, 2016; BRADSHAW, 2016; WASSERMAN, 2017).

É importante registrar 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 dos jornalistas que entendam os conceitos de segurança de informação na teoria e nunca deixem de aprender sobre proteção na prática.

A Fundación para la Libertad de Prensa, a Organização das Nações Unidas, a Fundação Karisma e os Repórteres Sem Fronteiras elaboraram um manual prático para jornalistas (FLIP, 2015). Para além das recomendações e diagnósticos, este manual apresenta noções elementares que podem propiciar a constituição de um ambiente digital mais seguro para atuação de jornalistas. Estes elementos formatam um escopo que envolve o comportamento e a experiência digital dos profissionais e o desenvolvimento de capacidades de segurança digital.

> Para que as práticas robustas de segurança jornalística sejam eficazes, elas devem oferecer as proteções reais que as fontes merecem e devem ser razoáveis o suficiente

[138] Denunciantes que alertam para a existência de irregularidades na gestão, no funcionamento de empresas ou instituições, o termo não tem uma tradução equivalente em português.

> para integrarem-se ao processo de coleta e publicação de notícias. Para atingir esses objetivos, qualquer abordagem deve ser fundamentada em um entendimento fundamental dos quadros técnicos e legais em que nossas comunicações digitais existem e como suas intersecções, às vezes estranhas, influenciam a forma como os jornalistas devem operar[139] (MCGREGOR, 2014, p. 2, tradução livre).

Outras organizações formularam seus documentos: Committee for Journalist Protection (2012), Artículo 19 (2013), International Center For Journalists e Freedom House (SIERRA, 2013), Repórteres Sem Fronteiras (2017, 2018, 2019). Fernandez e Mancini (s/d) enfatizaram a urgência de repórteres praticarem um "criptojornalismo", isto é, um jornalismo fundamentado na criptografia como medida de autoproteção e segurança de informações e fontes. Dagan (2017) vai além e enaltece o anonimato, os mecanismos de buscas mais seguros, entre outras medidas.

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

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"*[140]. Na publicação, as autoras mapearam desafios tecnológicos, institucionais, psicossociais e econômicos para enfrentar os riscos que afetam jornalistas e organizações de mídia.

> Paralelamente à crescente digitalização do jornalismo, que traz benefícios sem precedentes tanto para jornalistas, quanto para o público, tem havido ameaças preocupantes: comunicações eletrônicas de meios informativos, blogueiros críticos e outros indivíduos ou organizações que disseminam informações tornaram-se alvos. O perigo emana de várias fontes, de atores estatais a terceiros. Existe vigilância digital que transcende os padrões internacionais de privacidade e liberdade de expressão. Há hacking de dados e ataques disruptivos em sites e sistemas de computadores. De forma mais extrema, alguns agentes de mídia estão sendo mortos

[139] No original: For robust journalistic security practices to be effective, they must both offer the real protections that sources deserve and be reasonable enough to integrate into the process of newsgathering and publication. To achieve these ends, any approach must be grounded in a fundamental understanding of the technical and legal frameworks in which our digital communications exist, and how their sometimes strange intersections influence the way that journalists must operate.

[140] Disponível em: http://proledi.ucr.ac.cr/wp-content/uploads/2018/10/Seguridad-digital-para-el-periodismo.pdf. Acesso em: 23 jun. 2019.

> por seu jornalismo na rede[141] (HENRICHSEN; BETZ; LISOSKY, 2016, p. 10, tradução livre).

Conforme Henrichsen, Betz e Lisosky (2016), entre 2011 e 2013, 37 dos 276 assassinatos de jornalistas condenados pela UNESCO eram de profissionais cujas plataformas principais eram baseadas na internet. As ferramentas digitais são utilizadas no trabalho jornalístico todos os dias, o que, para as autoras, pode expor estes profissionais de várias maneiras, pois alguns riscos à segurança simplesmente mudaram do domínio *offline* para o ambiente online.

> As ameaças de morte agora são enviadas por e-mail e podem responder a conteúdo publicado na Internet, e não em jornais impressos ou em emissoras de rádio. Um escritório de mídia ou uma gráfica ainda podem ser alvo de uma bomba, mas atualmente é mais comum negar serviços para derrubar o site de um meio de comunicação. No entanto, outras ameaças assumem uma nova dimensão em sua forma digital. À medida que mais dados são gerados, armazenados, transmitidos e pesquisados, ameaças antigas, como o assédio sexual, podem se intensificar. Questões relacionadas à privacidade e liberdade de expressão também surgem. Por exemplo, expondo os movimentos dos jornalistas através de dados de geolocalização vinculados a telefones celulares, tornar visível a sua vida privada em mídias sociais e extrair metadados de suas comunicações[142] (HENRICHSEN; BETZ; LISOSKY, 2016, p. 10, tradução livre).

No documento, as autoras identificaram 12 ameaças digitais, dentre as quais estão vigilância digital ilegal ou arbitrária, rastreamento de locais e explorações de *software* e *hardware* sem conhecimento do indivíduo alvo, *phishing*, ataques de domínio falso, ataques intermediários (MitM), ataques de negação de serviço (DoS), alteração de sites, contas de usuários comprometidas, confisco ou roubo de seus recursos digitais, campanhas de intimidação, desinformação e difamação online. Ao mesmo tempo, reconhece-se que a segurança digital passa por mudanças constantes e existem ainda desafios político-legais que

[141] No original: En paralelo a la creciente digitalización del periodismo, que aporta beneficios sin pre-cedentes tanto a los periodistas como a las audiencias, han surgido amenazas preocupantes. Las comunicaciones electrónicas de los medios informativos, los blogueros críticos y otros individuos u organizaciones que difunden información se han convertido en objetivo. El peligro emana de diversas fuentes, desde actores estatales a terceros. Existe una vigilancia digital que trasciende los estándares internacionales sobre privacidad y libertad de expresión. Existe hacking de datos y ataques perturbadores a sitios web y sistemas informáticos. De forma más extrema, algunos agentes de los medios de comunicación están siendo asesinados por su periodismo en la red.

[142] No original: Las amenazas de muerte ahora se envían por correo electrónico y pueden responder a contenidos publicados en Internet más que en periódicos impresos o en radiodifusoras. Una oficina de medios de comunicación o una imprenta todavía pueden ser objeto de una bomba, pero actualmente es más común la negación de servicios para echar abajo el sitio web de un medio de comunicación. Sin embargo, otras amenazas adoptan una nueva dimensión en su forma digital. A medida que se generan, almacenan, transmiten y buscan más datos, pueden intensificarse viejas amenazas como el acoso sexual. También surgen cuestiones relacionadas con la privacidad y la libertad de expresión. Por ejemplo, exponer los movimientos de periodistas a través de datos de geolocalización vinculados a teléfonos celulares, hacer visible su vida privada en medios sociales y extraer metadatos de sus comunicaciones.

envolvem governos, ONGs, corporações e outras entidades, o que torna a problemática multifacetada, complexa e dinâmica.

Diversos atores[143] e iniciativas[144] trabalham e abordam segurança digital por meio de diferentes perspectivas, identificam vulnerabilidades e apresentam lacunas de conhecimento, ao mesmo tempo, indicam estratégias de mitigação de riscos e conscientização em relação às ameaças e à vigilância digital. Nessas abordagens, os riscos de segurança digital são apresentados em seus aspectos tecnológicos, institucionais, econômicos, políticos, legais, psicológicos e físicos.

Em junho de 2019, a Repórteres Sem Fronteiras (RSF) lançou um "Guia de Segurança Digital" para jornalistas, com orientações que podem ser adotadas durante a rotina de trabalho dos profissionais. A RSF enaltece a hostilidade crescente que está sendo enfrentada pelos jornalistas, manifestada de forma mais intensa no ambiente digital, que passou a ser um espaço recorrente de ameaças, campanhas de difamação e linchamentos virtuais.

De maneira geral, a abordagem adotada no guia da RSF (2019) segue premissas comuns entre as diversas publicações feitas nesse formato para jornalistas. Elas apresentam ferramentas e possibilidades de mitigação de riscos, indicando eixos principais ligados à proteção de dispositivos eletrônicos, preservação de informações pessoais e prevenção de invasões maliciosas em sistemas informáticos.

A publicação aponta sete tópicos específicos: proteção de dispositivos (formas seguras de armazenamento de dados sensíveis durante coberturas jornalísticas); a senha é a primeira barreira (definição de senhas fortes e seguras); como cuidar das mídias portáteis (ferramentas existentes para proteção de dados); navegação com segurança (cuidados ao se conectar a redes públicas e sugestões de serviços); os riscos das redes sociais (comportamentos suspeitos nas

[143] Comitê Gestor da Internet no Brasil (www.cgi.br/); Tedic (www.tedic.org); Instituto Brasileiro de Defesa do Consumidor (idec.org.br); Coding Rights (www.codingrights.org); Freedom of the Press Foundation (freedom.press); IFEX (ifex.org); International News Safety Institute (newssafety.org); Derechos Digitales (derechosdigitales.org); Eletronic Frontier Foundation (www.eff.org); Fundación Karisma (stats.karisma.org.co); Knight Center for Journalism in the Americas (knightcenter.utexas.edu); Human Rights Watch (www.hrw.org); Anistia Internacional (anistia.org.br); Artigo 19 (artigo19.org); Committee to Protect Journalist (cpj.org); International Federation of Journalists (www.ifj.org); Repórteres Sem Fronteiras (rsf.org); Freedom House (freedomhouse.org); Federação Nacional dos Jornalistas (fenaj.org.br); Tow Center for Digital Journalism (towcenter.columbia.edu).

[144] Rede latino-americana de estudos sobre vigilância, tecnologia e sociedade (lavits.org); Oficina Antivigilância (antivigilancia.org); Privacidade para jornalista (privacidadeparajornalistas.org); Tem boi na linha? (www.temboinalinha.org); Labjor/Unicamp (www.labjor.unicamp.br); MediaLab UFRJ (medialabufrj.net); Observatório da Privacidade e Vigilância (www.privacidade.net); Pimentalab (pimentalab.milharal.org); Surveillance Studies Centre (www.sscqueens.org); The Citizen Lab (citizenlab.ca); Privacy tools (www.privacytools.io); Prism Break (prism-break.org); Datactive (data-activism.net); Privacy International (privacyinternational.org).

mídias sociais); cuidados com o e-mail (utilização de e-mails encriptados); como me organizar em viagens (cuidados com informações e equipamentos).

Além das recomendações, apontamos a necessidade contínua da promoção de mecanismos de proteção para os jornalistas no ambiente digital, que estejam associados à possibilidade de sensibilização de maneira mais ampla e perene, a fim de que as vantagens que a internet oferece não sejam ofuscadas pelos seus riscos. O repórter da *Folha de S. Paulo*, especialista em ciberseguranca, Raphael Hernandes, destaca que, nas redações existem problemas para habitar o ecossistema digital, sendo que "histórias sensíveis são um alvo mais qualificado"[145]. Para Hernandes, o ecossistema digital é um ambiente hostil para jornalistas, com possibilidades de ataque acessíveis que exigem o mapeamento de vulnerabilidades.

O especialista ressalta a quebra de sigilo de fonte, a difamação e a quebra de confiabilidade como possíveis riscos e evidencia quatro estratégias regularmente utilizadas por atacantes: backdoors[146]; engenharia social[147]; ataques legais (realizados pela Justiça e por autoridades ligadas ao Estado); furtos (senhas, informações pessoais e dados sensíveis). Também ressalta a necessidade de atenção permanente, por parte dos jornalistas, e a consciência em relação aos custos de usabilidade e conveniência que ferramentas de mitigação de vulnerabilidades impõem.

O cuidado perpassa dados armazenados nos dispositivos dos profissionais e os dados em trânsito ou movimento, com estratégias de defesa em profundidade que garantam várias camadas de controle de segurança de informações sensíveis. Hernandes é autor do site "Privacidade para Jornalistas"[148], onde alerta os jornalistas para possíveis contextos críticos e de ameaça no ecossistema digital.

> Quando se trata da proteção de fontes e das informações que já foram coletadas, é bastante claro quem é o principal adversário. Dependendo da pessoa ou organização que está sendo investigada, os recursos disponíveis para cercear os jornalistas podem variar. Portanto, as ferramentas e habilidades devem estar à altura. A escolha das ferramentas e práticas adequadas deve ir ao encontro da "análise de ameaças" (HERNANDES, 2017, online).

É fundamental que o jornalista compreenda quem são os possíveis atacantes por meio de três questões-chave: Quem está tentando te prejudicar? O que eles buscam? O que você

[145] Palestra "HACKER AQUI: cibersegurança do jornalista" realizada durante o 14º Congresso Internacional de Jornalismo Investigativo da Associação Brasileira de Jornalismo Investigativo (Abraji), São Paulo, 2019.
[146] Método não documentado de entrada em sistemas (software, plataformas, dispositivos, etc.) que pode ser usado de forma legítima por fabricantes para restaurar acessos. Porém, pode ser explorado para dar acesso remoto a um centro de comando e controle externo ao sistema invadido, criando uma via permanente para futuras contaminações.
[147] Método de ataque que faz uso da persuasão, da ingenuidade ou confiança do usuário, a fim de obter informações que podem ser utilizadas para obtenção de acesso não autorizado a computadores ou informações.
[148] Disponível em: privacidadeparajornalistas.org. Acesso em: 24 jun. 2019.

pode fazer quanto a isso? Baseado nesse conjunto de informações, o profissional pode selecionar ferramentas de segurança e de privacidade, também pode orientar suas práticas para se defender e proteger as suas fontes.

Os cuidados para mitigação de ameaças envolvem desde ações simples, como atualização de sistemas operacionais, aplicativos e *softwares,* até a análise da relação entre possíveis atacantes e defesas disponíveis. Shelton (2015) indica que hábitos simples de proteção à privacidade podem mitigar a exposição dos jornalistas, se adotados como regularidade.

> Por exemplo, alguns jornalistas criptografam seu computador e telefone em discos rígidos, mantêm senhas longas e usam plug-ins de navegador que melhoram a privacidade. Essas abordagens exigem pouco trabalho adicional depois de algum esforço inicial, em comparação com a maioria das outras técnicas que exigem mais tempo e esforço para aprender e exigem manutenção contínua[149] (SHELTON, 2015, p. 133, tradução livre).

Ferramentas de segurança digital complexas, que consequentemente exigem mais investimento de tempo e de conhecimento, acabam rechaçadas pelos jornalistas. De acordo com Shelton (2015), alguns jornalistas evitam utilizar as ferramentas do ecossistema digital durante as suas investigações. Desta forma, não realizam registros eletrônicos, evitam conversação online, encontram pessoalmente fontes sensíveis, entregam e recebem manualmente documentos sensíveis e pagam despesas relacionadas ao trabalho em dinheiro.

> Finalmente, até mesmo jornalistas altamente motivados ficaram insatisfeitos com o uso de certos tipos de ferramentas de segurança porque são desnecessariamente difíceis de usar e entender - por exemplo, a criptografia de e-mail PGP. Usabilidade é um sério desafio para inúmeras ferramentas de comunicação. Os efeitos de rede agravam ainda mais o problema. Quando os problemas de usabilidade desencorajam os usuários, eles não são afetados isoladamente, as pessoas ao seu redor também não podem usar ferramentas de comunicação que aprimoram a privacidade e a segurança[150] (SHELTON, 2015, p. 134, tradução livre).

Nesse sentido, a perspectiva de segurança digital para jornalistas perpassa a necessidade de adequação das ferramentas ao cotidiano dos profissionais, levando em conta a sua usabilidade e aplicação durante o trabalho de investigação de temas sensíveis. *Softwares* e

[149] No original: For example, some journalists encrypt their computer and phone hard drives, keep lengthy passwords, and use privacy-enhancing browser plug-ins. These approaches require little additional work after some initial effort, compared to most other techniques that take more time and effort to learn and require continued maintenance.

[150] No original: Finally, even highly motivated journalists were often unhappy about using certain types of security tools because they are unnecessarily difficult to use and understand—for example, PGP email encryption. Usability is a serious challenge for countless communication tools. Network effects further exacerbate the problem. When usability problems discourage users, they are not affected in isolation; the people around them may not use privacy- and securityenhancing communication tools either.

padrões de segurança não podem alcançar níveis de complexidade incompatíveis com a capacidade de assimilação dos jornalistas e com a possibilidade de serem usados no processo de comunicação dos jornalistas com suas fontes.

No ecossistema digital, os jornalistas se deparam com vulnerabilidades que exigem escolhas que envolvem oportunidades de preservação da privacidade. Essas escolhas podem ser realizadas através da implantação de medidas que podem variar dependendo do nível de risco e potencial de vigilância que os temas que estão sendo investigados apresentam. É importante entender essas possibilidades como potencialidades de proteção que exigem entendimentos específicos, para reduzir os custos financeiros e de usabilidade dos aparatos de segurança.

3.3.1 Proteção como potencialidade do jornalismo vigilante

Medidas de segurança requerem esforço e tempo, mas também podem se transformar em uma potencialidade, quando assimiladas e implementadas às rotinas dos jornalistas, por meio de protocolos e práticas. De maneira geral, os jornalistas investigativos desenvolvem um trabalho solitário, no entanto as possibilidades comunicacionais apresentadas pelo ecossistema digital favorecem o trabalho coletivo, consórcios que são estruturados, especialmente, para manusear e explorar grandes volumes de dados. Esses casos exigem a adoção de medidas extraordinárias de proteção e resistência às formas de vigilância eletrônica contemporâneas.

Noções e técnicas de segurança precisam levar em conta todos os elementos e as variáveis relacionados à comunicação que envolvem o contexto onde as ações jornalísticas estão sendo desenvolvidas. As problemáticas ligadas aos processos de vigilância que podem ter os jornalistas como alvos se sobrepõem as dos cidadãos comuns, apesar de que ambos os grupos costumam usar as mesmas tecnologias. Entretanto, a abordagem de temas sensíveis impõe aos jornalistas a necessidade de contramedidas de vigilância.

> A proliferação de softwares de comunicação criptografados coincide com o desenvolvimento e adoção de novas ferramentas de segurança para dar suporte às notícias. O SecureDrop, um projeto de código aberto atualmente gerenciado pela Freedom of the Press Foundation, permite que as fontes entreguem documentos de forma segura e anônima para as organizações de notícias. Organizações de notícias, incluindo The Guardian, Washington Post, ProPublica, The Intercept, e outros, apoiam o SecureDrop, facilitando a transferência anônima de documentos entre denunciantes e organizações de notícias[151] (SHELTON, 2015, p.71, tradução livre).

[151] No original: The proliferation of encrypted communication software coincides with the development and adoption of novel security tools to support the news. SecureDrop, an open-source project currently managed by

Shelton (2015) explica que o *SecureDrop* exige que os usuários se conectem através da rede de anonimato do Tor antes de fazer o *upload* de documentos. O jornalista deve baixar os documentos em um computador conectado à internet e usar unidades *flash USB* para transferir e descriptografar os dados em um computador secundário não conectado à internet. Esse esquema de criptografia, transferência e descriptografia oferece um nível relativamente seguro para jornalistas e fontes, permitindo a transmissão de documentos confidenciais por pessoas de qualquer lugar do mundo. Shelton (2015) ainda ressalta que as ferramentas de anonimato e criptografia complementam as atividades de coleta de informações para um número restrito de organizações de notícias e não podem substituir o trabalho tradicional de contato com as fontes e coleta de informações para investigações jornalísticas.

De acordo com Eguren (2005), o nível de risco enfrentado por um grupo que trabalha com temas sensíveis aumenta de acordo com as ameaças recebidas e a sua vulnerabilidade frente a estas ameaças. Nesse sentido, as ameaças representam a possibilidade de que alguém viole a integridade física ou moral de outra pessoa, por meio de uma ação intencionada.

Avaliar uma ameaça significa analisar a possibilidade de que esta ameaça se concretize na forma de ataque. Já a vulnerabilidade é o grau em que as pessoas estão suscetíveis a perdas e danos em caso de um ataque. A vulnerabilidade é dinâmica, varia de acordo com o indivíduo ou grupo, e modifica-se com o tempo. “As vulnerabilidades são sempre relativas, porque todas as pessoas e grupos são vulneráveis em certo grau. Entretanto, toda pessoa possui seu próprio nível e tipo de vulnerabilidade, de acordo com as circunstâncias” (EGUREN, 2005, p. 19). A vulnerabilidade deve ser colocada em contexto e contrastada com as capacidades de mitigação dos indivíduos.

Conforme Eguren (2005), as capacidades são os pontos fortes e os recursos que um indivíduo ou um grupo podem acessar, para conseguir um nível razoável de segurança. O risco gerado pelas ameaças e vulnerabilidades pode ser mitigado se os jornalistas dispõem de capacidades. Eguren (2005) diz que para reduzir o risco a níveis toleráveis e aumentar o nível de proteção é necessário: “reduzir as ameaças”; “reduzir os fatores de vulnerabilidade”; “aumentar as capacidades de proteção”. A partir dessa perspectiva, surge a possibilidade de medir o nível de risco.

> Se colocarmos dois pesos com nossas ameaças e vulnerabilidades num dos pratos da balança, e outro peso com nossas capacidades no outro prato, veremos como nosso

---

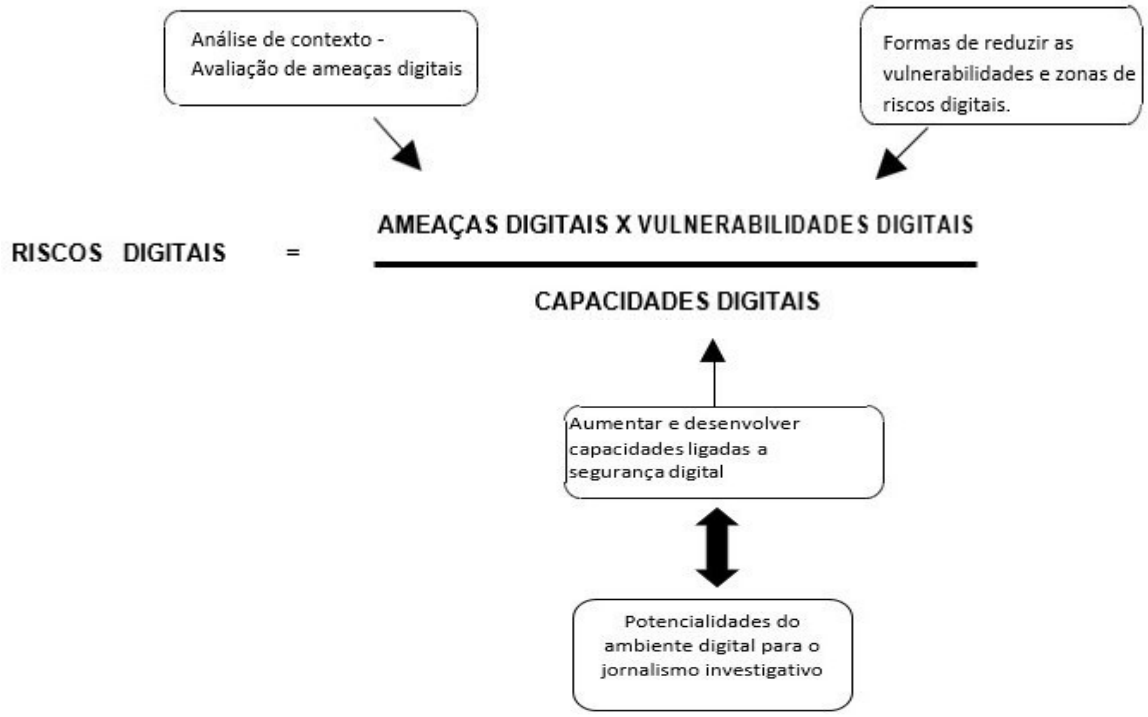
the Freedom of the Press Foundation, allows sources to securely and anonymously deliver documents to news organizations. News organizations including the Guardian, the Washington Post, ProPublica, the Intercept, and others support SecureDrop, facilitating the anonymous transfer of documents between whistleblowers and news organizations.

> risco aumenta ou se reduz. Quanto mais vulnerabilidades e ameaças temos, mais risco enfrentamos. Quanto mais capacidades tenhamos, menos risco enfrentaremos. E para reduzir o risco, também podemos reduzir nossas ameaças e vulnerabilidades, assim como aumentar nossas capacidades (EGUREN, 2005, p. 28-29).

Jornalistas investigativos têm motivações específicas alinhadas aos seus conhecimentos e comportamentos para adotar ou não ferramentas de mitigação de riscos digitais e vigilância comunicacional. Diante de situações de exposição e vulnerabilidade iminentes, com base teórica e estrutural no *"*Manual de Proteção para Defensores de Direitos Humanos"[152], elaboramos uma equação que envolve três fatores: **riscos digitais = ameaças digitais x vulnerabilidades digitais/capacidades digitais.** A partir desses elementos, elaboramos a figura 2.

Os fluxos que tratam dos riscos digitais, apresentados na figura 2, contam com uma etapa prévia de análise de contexto/avaliação de ameaças digitais. Essas são contrastadas com as vulnerabilidades digitais e zonas de risco percebidas. Esses fatores deverão ser reduzidos aos menores níveis possíveis. Na etapa seguinte, projetamos a avaliação das capacidades digitais relacionadas à segurança e à preservação dos dados e comunicações digitais dos jornalistas.

Figura 2 – Avaliação do nível de vulnerabilidade, ameaças e capacidades digitais



Fonte: Elaborada pelo autor, 2020.

[152] O manual foi elaborado por Enrique Eguren (2005) e publicado pela Fundação Internacional para a Proteção dos Defensores de Direitos Humanos - Front Line.

Dessa forma, percebemos a possibilidade de mitigação de riscos digitais na investigação de temas sensíveis como uma combinação de fatores que envolve a análise de contexto*,* por meio da avaliação de ameaças digitais*,* que são multiplicadas pelo mapeamento de vulnerabilidades e zonas de riscos digitais. Na equação, as ameaças e vulnerabilidades devem ser comparadas com as capacidades digitais relacionadas à segurança digital que são apresentadas pelo jornalista investigativo. Após essa avaliação, propomos a divisão da multiplicação (ameaças x vulnerabilidades) pelo fator alcançado nas capacidades digitais. A relação entre as capacidades e níveis de riscos observados implica na utilização efetiva das potencialidades ofertadas pelo ambiente digital aos jornalistas investigativos.

Nessa perspectiva, se as capacidades conseguirem sanar o quadro de ameaças e vulnerabilidades, os potenciais riscos digitais são mitigados e a utilização das ferramentas ofertadas pelo ecossistema digital (bancos de dados, possibilidades de compartilhamento de informações, ferramentas comunicacionais, entre outras) pode potencializar a investigação jornalística, resguardando os profissionais, suas fontes, apurações e dados sensíveis.

Mesmo se tentarmos aumentar nossas capacidades no momento em que estivermos enfrentando ameaças grandes ou severas, a balança mostrará um alto nível de risco. Aplicamos essa perspectiva em relação ao jornalismo investigativo no ambiente digital, para evidenciar aspectos importantes da verificação de riscos digitais.

A parametrização das variáveis para a equação exige a identificação da melhor forma de tratamento dessas situações de risco e dos padrões de ameaça que permeiam o fluxo de trabalho dos jornalistas no ecossistema digital. Os jornalistas podem classificar algumas condições críticas a partir de níveis de risco (alto, médio ou baixo) em diferentes etapas do trabalho jornalístico: troca de informações, no tratamento das informações, compartilhamento em rede e após a publicação do conteúdo jornalístico, levando em conta as principais situações de exposição, riscos e cuidados que foram elencadas no apêndice D.

Ainda em relação a recomendações de segurança digital, o “Guia de privacidade na internet para jornalistas”, indicado pelo coletivo de comunicadores e ativistas latino-americanos Nodo Común[153], apresenta medidas importantes para mitigação de riscos que foram desenvolvidas por Dagan (2017), algumas delas estão elencadas na tabela 3:

Tabela 3 – Medidas de mitigação de riscos.

Proteção de aplicativos e funções no dispositivo	Redução da "superfície de ataque", por meio da limitação de aplicativos instalados ao máximo.

[153] Disponível em: https://nodocomun.org/privacidad-internet-periodistas. Acesso em: 01 ago. 2019.

Cautela no mundo digital e no mundo real	Não escrever o nome da fonte em aplicativos ou em qualquer documento armazenado no computador, nem em nada que esteja armazenado na nuvem.
Sempre codifique tudo	A decodificação de arquivos aumenta o grau de esforço necessário que deverá ser realizado por possíveis atacantes. O Advanced Encryption Standard (AES) e ferramentas como PGP ou OpenVPN são métodos de criptografia disponíveis.
Codificação de todo o disco	Essa medida evita acessos indesejados do computador ou telefone e pode ser feita usando FileVault [154], VeraCrypt ou BitLocker[155].
Não fale com as fontes por telefone	Todas as empresas telefônicas armazenam dados relacionados ao número do chamador e a pessoa que recebe a chamada, bem como a localização dos dispositivos e o horário em que as chamadas foram feitas.
Priorize aplicações de troca de mensagens seguras	Todo o texto é completamente visível para aqueles que podem interceptá-lo. O Signal e o Telegram são considerados os mais seguros (embora Telegram, bem como os aplicativos do WhatsApp já foram violados). De acordo com alguns especialistas, você também pode considerar o uso do SMSSecure, Threema e mesmo do WhatsApp. Você também deve ter em mente que o Facebook Messenger e o WhatsApp são de propriedade do Facebook. Você também pode usar o Messenger Tor, o que provavelmente é o mais seguro de todos. Você também deve se lembrar de excluir as mensagens do seu telefone, embora isso não seja suficiente, caso seu dispositivo caia nas mãos erradas.
Não use bate-papo de empresas	Evite usar aplicações como Skype e Hangouts, do Google, para conversas privadas. Eles são fáceis de violar, portanto é melhor evitá-los. Isso deve ser feito não só quando se trata de conversas com fontes, mas também aquelas que você mantém entre colegas, editores, etc., quando você precisa passar informações que você recebeu da sua fonte, cuja identidade deve ser protegida.
Proteja o seu computador com senha	É muito fácil decodificar senhas normais, mas pode levar anos para decodificar frases codificadas, ou seja, combinações aleatórias de palavras. Ferramentas seguras de gerenciamento de senha, como LastPass, 1Password e KeePassX, podem auxiliar. Especialistas em segurança da informação afirmam que senhas seguras devem ter mais de 20 caracteres.
Sensibilize suas fontes	É necessário proteger a informação e se esforçar para garantir que as informações estejam ocultas: privilegie locais protegidos e se comunique através de dispositivos seguros. Oriente a fonte para que ela possa lidar com informações confidenciais.
Use um sistema seguro e dedicado para receber documentos	Substitua Dropbox ou Google Drive e use algo menos popular, mas mais seguro, por exemplo, o SecureDrop. Este é um sistema que permite que você receba arquivos de fontes anônimas com segurança.
Não faça anotações	Em laptop, calendários, listas de contatos em seu telefone, no computador, na nuvem - não mantenha

[154] É um programa de criptografia de disco do Mac OS X 10.3 e posterior.
[155] É um sistema de criptografia que consiste em codificar partições, protegendo documentos e arquivos do computador contra o acesso não autorizado.

	registros de seu nome, iniciais, número de telefone, e-mail ou nome de usuário nos programas de mensagens.
Modo de navegação privada	A maneira mais básica e popular, embora insuficiente, é navegar com informações em modo privado, uma opção que a maioria dos navegadores oferecem. Seu histórico de navegação não será salvo e as tecnologias de rastreamento básicas usadas pelos anunciantes, como os cookies HTTP, não poderão criar seu perfil detalhado.
Use navegadores alternativos	Entre os navegadores alternativos, o mais seguro é o Tor. Ele permite que você opere em uma rede oculta, realize comunicações privadas e estabeleça sites anonimamente. O sistema operacional mais popular para Tor é Tails. Tails pode ser iniciado a partir de um dispositivo USB ou DVD, e faz todas as informações anônimas.
Buscador alternativo	O Google, mecanismo de pesquisa mais usado, guarda seu histórico de pesquisa, para otimizar os resultados. É preferível usar um mecanismo de pesquisa como o DuckDuckGo.
Use uma Virtual Private Network (VPN)	É uma rede de comunicações privada, construída sobre uma rede de comunicações pública (por exemplo, a Internet). Uma VPN criptografa todas as suas comunicações, de modo que possíveis atacantes não conseguem saber a quem você enviou um e-mail, quais serviços você usou, etc.
Máquinas virtuais	Este truque engenhoso é, na verdade, um segundo computador (virtual), que funciona como uma aplicação em seu sistema operacional. Você pode baixar arquivos ou abrir links, então seu computador está menos exposto a software malicioso ou spyware[156] de qualquer tipo.
Fornecedores de e-mail seguros	Serviços de e-mail alternativos podem proporcionar mais segurança do que as redes comerciais que são utilizadas habitualmente.
Endereços de e-mail descartáveis	Este é um e-mail criado com um propósito específico, que é completamente anônimo e é excluído imediatamente após usá-lo.
Codificar o seu e-mail	Criptografar mensagens de e-mail pode ser difícil. Muitas vezes requer que o usuário e a fonte estejam preparados para usar ferramentas como PGP para codificá-las e decodificá-las (PGP - Pretty Good Privacy - é um programa de criptografia que fornece privacidade criptográfica e autenticação para comunicação de dados). Com a codificação PGP, você tem uma chave pública e uma chave privada. A chave privada deve ser armazenada com segurança, como qualquer outra informação confidencial. Então, quando uma fonte quiser enviar-lhe informações, ela usará sua chave pública para criptografar seu e-mail, que somente uma chave privada pode desbloquear.

Fonte: Nodo Común, adaptada pelo autor. Disponível em: https://nodocomun.org/privacidad-internet-periodistas. Acesso em: 01 ago. 2019.

[156] É um *software* espião que tem o objetivo de observar e roubar informações pessoais do usuário que utiliza o computador em que o programa está instalado, retransmitindo-as para uma fonte externa, sem o conhecimento ou consentimento do usuário.

Finalmente, é importante destacar que todas as atividades digitais que envolvam investigações jornalísticas de temas sensíveis merecem proteção, por exemplo, no âmbito comunicacional (e-mails, mensagens, telefonemas, etc.), no armazenamento (nuvem ou em dispositivo), na navegação, nas mídias sociais, no uso de ferramentas e dispositivos de localização. Conforme já demarcamos, um dos aspectos mais importantes é verificar quem quer e quem pode atacá-lo e, consequentemente, se está interessado em suas atividades ou informações.

Os possíveis interessados em conhecer as atividades digitais de um jornalista investigativo podem apresentar grande vontade de obter essas informações, mas não ter capacidade de obtê-las. No entanto, também pode haver grandes capacidades e os detentores desse potencial não se importarem com o que o jornalista está fazendo. Alguém com baixa capacidade, mas grande vontade pode melhorar as suas possibilidades de ataque ou alguém com pouca vontade que apresente grande capacidade pode desenvolver interesses para acessar a atividade digital de um profissional.

A publicação de informações privadas em mídias sociais e a utilização e dependência de dispositivos móveis pelos jornalistas são vulnerabilidades latentes e com vasto potencial nocivo. Reconhecer essa realidade e as formas de segurança disponíveis pode ajudar os jornalistas a transformarem suas fraquezas em forças. As ferramentas de segurança digital devem atender as necessidades apresentadas pelo contexto em que o jornalista atua e os temas que está abordando. A única maneira de aferir esses elementos é avaliar os riscos digitais a que está exposto, para dimensionar de maneira adequada as melhores formas de atuação.

No próximo capítulo, buscamos clarear de que maneira os jornalistas investigativos percebem o contexto de vigilância digital e comunicacional, compreendem as vulnerabilidades, valoram as ameaças e as capacidades do ecossistema digital. Os objetivos são verificar a percepção dos profissionais sobre essas questões e o possível desenvolvimento de uma cultura que envolva práticas de segurança digital perenes para o jornalismo investigativo.

4 JORNALISMO VIGILANTE SOB VIGILÂNCIA NOCIVA

Neste capítulo, detalharemos os métodos utilizados para alcançar os objetivos projetados para a pesquisa e os resultados obtidos na última etapa do estudo que envolveu entrevistas em profundidade e a aplicação de uma *survey* a jornalistas que abordam temas sensíveis. Mais especificamente, buscamos indicar os riscos e as possibilidades encontradas em espaços digitais que apresentam vulnerabilidades e potencialidades para as investigações jornalísticas contemporâneas.

4.1 PERCURSO METODOLÓGICO

Após uma etapa inicial de pesquisa exploratória e revisão bibliográfica sobre questões teóricas relacionadas ao jornalismo e à vigilância, delimitamos um percurso metodológico que envolveu o mapeamento de casos concretos e ações jornalísticas que dizem respeito às diferentes formas de vigilância digital realizadas em contextos distintos a partir de apontamentos e condutas indicadas em relatórios de agressões à jornalistas e ataques à liberdade de imprensa.

Na sequência, desenvolvemos uma série de ações que envolveram a produção de artigos, participação em eventos científicos, oficinas e palestras que serviram de base para o relatório de qualificação e para o processo submetido ao Comitê de Ética em Pesquisa com Seres Humanos da Universidade Federal de Santa Catarina (CEPSH-UFSC). A pesquisa foi aprovada pelo CEPSH (anexo A) e pela banca de qualificação que sugeriu a combinação da técnica de entrevistas em profundidade com a aplicação da *survey* como uma forma de alcançar os objetivos propostos pelo estudo. Avaliamos e acatamos a sugestão da banca, substituindo a estratégia inicialmente projetada (análise de casos) pela realização de entrevistas em profundidade.

Buscando ratificar que o contexto atual de vigilância comunicacional em meios digitais exige dos jornalistas investigativos um senso permanente de vulnerabilidade e a adoção de medidas relacionadas a uma cultura de segurança digital para profissionais que abordam temas sensíveis, verificamos como jornalistas com essas características percebem as possibilidades de intervenção relacionadas à vigilância das comunicações no ecossistema digital.

Para tanto, selecionamos jornalistas para realização de entrevistas em profundidade. A definição do perfil dos sujeitos de pesquisa teve como base os seguintes critérios: jornalistas

investigativos que trabalham com temas sensíveis; preferencialmente associados à Associação Brasileira de Jornalismo Investigativo (Abraji); preferencialmente profissionais que tenham mais de 3 anos de experiência; profissionais que estejam na ativa; jornalistas investigativos que tenham diferentes níveis de conhecimento relacionado à segurança da informação; profissionais que atuem em veículos jornalísticos tradicionais, alternativos e independentes; jornalistas investigativos que atuem a partir de diferentes formatos e plataformas de comunicação; profissionais que se reconhecem como jornalistas investigativos; jornalistas que trabalhem em seguimentos distintos, como justiça criminal, segurança nacional, segurança da informação, negócios e tópicos locais em diferentes cidades brasileiras.

Com base nos conceitos trabalhados no primeiro capítulo, nas principais possibilidades de vigilância apresentadas no segundo capítulo e nas modalidades de riscos digitais desenvolvidas no terceiro capítulo, estruturamos um roteiro (apêndice A) para a etapa de entrevistas em profundidade e um formulário (apêndice B) para aplicação da *survey*.

Inicialmente, realizamos pré-testes presenciais com três sujeitos de pesquisa. Por uma questão de proximidade, selecionamos profissionais que atuam no Estado de Santa Catarina. Cabe salientar que por tratarmos de temáticas, estratégias e percepções que envolvem a segurança dos profissionais, optamos por não revelar a identidade de nenhum dos sujeitos de pesquisa. Essas entrevistas tiveram o objetivo de identificar a necessidade de ajustes e aprimoramentos no roteiro de perguntas, possíveis constrangimentos e dúvidas para os participantes.

Os pré-testes realizados durante o mês de maio de 2019 apontaram aspectos como estimativa de tempo das entrevistas, formas de abordagem, avaliação dos objetivos das questões e como as respostas subsidiavam a tese. As entrevistas duraram em média 30 minutos e demostraram-se exitosas em relação aos seus objetivos. Os entrevistados indicaram algumas dúvidas relacionadas às questões que apresentavam termos específicos, mas não demonstraram constrangimento durante os testes, todos leram e assinaram o Termo de Consentimento Livre e Esclarecido – TCLE (apêndice F). Dessa forma, o roteiro das entrevistas em profundidade foi validado.

Com a validação do roteiro, definimos que iríamos realizar as entrevistas em profundidade em São Paulo durante o 14ª Congresso Internacional de Jornalismo Investigativo da Associação Brasileira de Jornalismo Investigativo (Abraji) que aconteceu em junho de 2019. Fizemos essa escolha porque o evento reúne jornalistas que preenchiam as características previstas para os sujeitos de pesquisa e pelas facilidades relacionadas à logística e ao agendamento prévio dos encontros presenciais.

Optamos pela técnica de entrevistas em profundidade com a intenção de avaliar elementos e aferir a percepção dos jornalistas no que diz respeito a aspectos percebidos, adequados e negligenciados nas investigações jornalísticas realizadas em espaços digitais vigiados. Como já destacamos, diante da vigilância digital massiva realizada por governos e corporações, buscamos clarear quais são as principais vulnerabilidades e potencialidades do jornalismo investigativo brasileiro. A realização de perguntas elementares pretendeu entender melhor como os jornalistas investigativos percebem o impacto da possibilidade de vigilância em seus cotidianos, bem como detalhes dos seus hábitos de segurança digital.

Dentre os tópicos explorados pelas entrevistas estão os desafios apresentados pelas possibilidades de vigilância digital na rotina de jornalistas que abordam temáticas sensíveis e que medidas estão sendo adotadas em relação a esse contexto. As principais mudanças e potencialidades para as investigações jornalísticas transpassadas pelo ecossistema digital foram enaltecidas por meio das experiências e casos vivenciados pelos profissionais. Também foram abordados aspectos específicos a respeito do contato com fontes e utilização de ferramentas digitais, além de verificar a noção de vulnerabilidade apresentada pelos entrevistados em relação a atuação deles nos espaços digitais e suas preocupações ligadas à vigilância comunicacional.

Entre os dias 27 e 29 de junho de 2019 realizamos seis entrevistas que foram balizadas por 12 questões-chave (apêndice A) alinhadas aos objetivos e aos principais temas que tangenciam a pesquisa. Conforme já destacamos, anonimizamos os participantes da pesquisa que serão identificados com a palavra “Sujeito” acompanhada dos números de “1 a 6”. Os jornalistas investigativos entrevistados têm um perfil heterogêneo, abordam temáticas sensíveis e iniciaram suas trajetórias em períodos históricos que disponibilizavam possibilidades tecnológicas distintas para realização das ações de apuração. Todos relataram experiências profissionais e atuação em investigações jornalísticas emblemáticas e singulares, os jornalistas apresentaram diferentes níveis de conhecimento sobre segurança digital e utilização das potencialidades ofertadas pelo ecossistema digital.

4.1.1 Jornalistas imersos em possibilidades de vigilância digital

Para assinalar os argumentos dos jornalistas entrevistados, selecionamos citações específicas alinhadas aos objetivos propostos neste estudo, sendo que as respostas dos participantes são apresentadas na íntegra no apêndice C. Na primeira questão, buscamos aferir

a percepção dos entrevistados sobre as possibilidades de vigilância comunicacional no espaço digital. O Sujeito 1 (S1) ressaltou que esse é um tema novo até mesmo para o jornalismo.

> Realmente, eu confesso que era um pouco ingênuo até um tempo atrás, em relação a esses cuidados durante o nosso trabalho de investigação, de não estarmos sendo vigiados. Recentemente, eu até coloquei uma fita na frente da câmera do meu notebook, porque pode haver uma invasão, enfim a gente trabalha com temas sensíveis que interessam muito a criminosos.

Para S1, os jornalistas precisam estar atentos à questão da vulnerabilidade imposta pelas mídias e meios digitais. O entrevistado citou um caso em que tomou precauções e medidas de segurança comunicacional, dentre as quais destacam-se o uso de um celular empresarial exclusivamente para aquela apuração que envolvia o contato com milicianos. "Pela primeira vez, eu tive muito cuidado mesmo, nesse preparo contra uma eventual espionagem contra mim, porque a gente está acostumado a espionar os outros, no bom sentido, investigar os outros, mas ser investigado é algo bastante complicado".

O Sujeito 2 (S2) indicou que o *stalking*[157] é uma vulnerabilidade cada vez mais real e nociva para os jornalistas, particularmente, diante da utilização de dispositivos eletrônicos que permitem inúmeras maneiras de intrusão por meio de aplicativos, sistemas operacionais e até mesmo câmeras que em algumas ocasiões são praticamente irrastreáveis. De acordo com o Sujeito 3 (S3), o trabalho de investigação jornalística exige a preservação das fontes e das informações apuradas pelo jornalista.

> Eu acho que a essência do repórter é o trabalho solitário, por mais que às vezes esteja trabalhando em equipe, mas a essência é essa relação dele com o seu objeto de apuração e, nesse sentido, não é de agora, ele vai querer se preservar. Ele não vai querer que aquilo passe para ninguém. Então a essência dele é essa relação única e exclusiva com a fonte dele, com o objeto. Está intrínseco no repórter esse drama mais que uma preocupação é o temor da apuração dele ser compartilhada por outros, a informação ser compartilhada por outros antes dele dar corpo a essa informação, antes dele ter o controle dessa informação e da forma que ele quer que ela passe.

O desamparo dos jornalistas investigativos em relação à segurança também foi enaltecido por S3 que apontou que nem mesmo as empresas de comunicação mais consolidadas conseguem garantir condições seguras para o desenvolvimento de investigações de temas sensíveis. "Então, não é de hoje, isso é uma conjuntura histórica, o repórter brasileiro, ele sempre foi um bicho, um ser que atuou de forma muito solitária nesse campo de preservação de sua integridade e da integridade do seu material".

[157] *Stalking* é um tipo de perseguição persistente, uma forma de violência, na qual sujeitos invadem repetidamente a privacidade das vítimas, empregando táticas de perseguição por meios diversos (mídias sociais, ligações telefônicas, envio de mensagens por SMS, correio eletrônico, publicação de fatos ou boatos em sites da Internet, também conhecido como *cyberstalking*).

Nesse sentido, o entrevistado aponta que as novas tecnologias impõem mudanças e adaptações associadas à capacitação dos profissionais. “Até os anos 90, os arapongas da Abin que ficavam ali e faziam suas gravações. Hoje não, hoje você tem uma plataforma digital toda conectada com possibilidade de entrada aqui e acolá. Então, você está em um jogo muito diferente, muito mais sofisticado”. Questões primordiais ligadas à segurança, à proteção e às possibilidades de atuação de maneira menos vulnerável são evidenciadas pelo Sujeito 3 como elementos essenciais e urgentes que, em última instância, envolvem risco de vida.

O Sujeito 4 (S4) afirmou que toma alguns cuidados, especialmente nas formas de comunicação adotadas durante coberturas sensíveis, utilizando aplicações como o Telegram[158] e o Signal[159], principalmente com pessoas que estão em situação de ameaça, proteção, fontes em *off* e fontes de governo.

Para o Sujeito 5 (S5), existe um tipo de vigilância padrão instalada em qualquer plataforma digital comercial que coleta dados sem distinção, isto é, de todos os usuários, jornalista e pessoas comuns.

> As pessoas querem saber o que você está fazendo para monetizar isso depois. E aí ainda que a intenção não seja de vigiar é uma instrumentalização que se quisesse ser usada para vigiar pode ser usada. Então, é muito difícil escapar de qualquer vigilância, de todas as vigilâncias em qualquer espaço digital seja por navegador, redes sociais, enfim.

O entrevistado indicou que atualmente, na sua atuação como jornalista, não percebe algo sistemático conectado a vigilância por parte do governo e das empresas, no entanto acredita que há espaço possível para que isso exista: “Eu não me sinto perseguido ou vigiado quando estou fazendo o meu trabalho, mas eu acho que há espaço para que se alguém quisesse conseguisse”. Sendo assim, aponta que em investigações sensíveis o cuidado tem que ser redobrado e as medidas de mitigação de riscos devem ser adotadas desde a fase inicial das ações de investigação.

Conforme o Sujeito 6 (S6), no Brasil, as questões relacionadas às formas de vigilância digital ainda são muito obscuras e são perpassadas por dispositivos legais presentes no Marco Civil da Internet[160]. Para ele, os jornalistas estão em uma situação extremamente vulnerável a esse tipo de vigilância comunicacional. “Não é possível dizer o quanto ela é feita em cima do jornalista pela prática da profissão em si, mas dá para dizer que se for feita, o estrago pode ser

[158] É um serviço de mensagens instantâneas baseado em nuvem que está disponível para diversas plataformas. Permite enviar mensagens e trocar fotos, vídeos, stickers e arquivos de qualquer tipo.
[159] É um serviço de mensagens criptografadas para várias plataformas.
[160] Lei número 12.965, de 23 de abril de 2014 que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

bastante grande, as consequências podem ser bastante nefastas nesse tipo de caso". De maneira geral, as respostas obtidas reforçam a ideia que expressamos na tese de que as ferramentas digitais expõem os jornalistas investigativos a riscos e vulnerabilidades.

A segunda questão buscou entender como que o contexto de vigilância digital afeta as ações dos jornalistas durante investigações que envolvem temas sensíveis relacionados a segredos, vazamentos e crimes. O principal objetivo desse questionamento foi clarear possíveis alterações no processo de investigação jornalística, particularmente durante a apuração, contato com fontes, tratamento de dados e informações sensíveis. Também buscamos compreender se os jornalistas estão adotando medidas de mitigação de riscos digitais.

S1 afirmou que possíveis ações de vigilância comunicacional em ferramentas digitais afetam sua conduta durante investigações sensíveis. Por exemplo, em temas mais agudos, o jornalista opta por encontrar as fontes pessoalmente e não leva dispositivos eletrônicos para o encontro. Ele demonstrou estar consciente de riscos relacionados com o rastreamento e a revelação da identidade da fonte. "O jornalismo caminha, cada vez mais, para o uso de ferramentas digitais e, por isso, a gente está sujeito também ao reverso, a quem nos vigia usar essas ferramentas como contrainformação". S2 também demonstrou preocupação no cuidado com as fontes que apresentem informação sensíveis, disse que utiliza ferramentas de criptografia e aplicativos que considera seguros para a mitigação de riscos digitais.

Devido aos riscos e ataques digitais, S3 evita a utilização de formas de comunicação eletrônica e adota o contato pessoal na abordagem de temas delicados. O jornalista narrou experiências no contato com militares e agentes da Agência Brasileira de Inteligência (ABIN).

> Eu fiz também um trabalho, trabalhei muito com militares da ditadura e foi por experiência própria, esses caras, por exemplo, o "personagem 1" por exemplo, que é o cara que me passava muita informação, ele chegava fazendo barulho ou se não eu ia para uma cidadezinha e ele me levava em uma caixa de som em um bar para ter muito ruído para ser uma porcaria a gravação e ali a gente conversava e só ali que ele falava, nos momentos mais finais do trabalho, ele escrevia no papel, eu perguntava, ele escrevia no papel, mostrava o papel, eu olhava, ele colocava no bolso para não criar prova.

S3 expressou preocupação e disse não conhecer nada que considere seguro para abordagens sensíveis. Sem essas alternativas, descreveu que busca métodos de investigação que proporcionem a maior sensação de segurança possível. S4 disse que a possibilidade de intrusão comunicacional afeta as suas ações de maneira frontal, pois as fontes estabelecem uma relação de confiança com os jornalistas que poderia ser abalada de maneira significativa com possíveis atos intrusivos de vigilância.

S5 expressou novamente a preocupação com segurança digital desde a etapa inicial das investigações que envolvem informações, temas e maneira de comunicações sensíveis. Afirmou também que existem mudanças na apuração, nos meios de comunicação entre os jornalistas, entre jornalista e fonte, apontando que algumas dessas investigações reúnem vários jornalistas e consequentemente troca de documentos e informações que demandam um maior grau de segurança.

S6 informou que no seu cotidiano se comunica frequentemente com hackers e, para isso, toma uma série de medidas de segurança digital. “Alguns eu só consegui conversar pessoalmente até hoje, nunca pude gravar essas conversas. Alguns me permitem anotar, porque são pessoas que vão me descrever o passo a passo para cometer um crime, um crime virtual”. S6 demonstrou a necessidade de uma avaliação de contexto e de possibilidades de ataques digitais que vão variar de caso a caso. Também afirmou que é imprescindível não entrar em uma paranoia. As modalidades de segurança vão desde noções de segurança aplicadas no dia a dia para prevenção de ataques genéricos, golpes, roubos de identidade até medidas de segurança mais complexas que vão deixar o profissional menos suscetível a ataques.

> E aí enquanto jornalista é a questão de você avaliar caso a caso mesmo com quem você está lidando, quem pode estar interessado naquilo e quais medidas você vai tomar, e também o conhecimento técnico da sua fonte, como eu lido bastante com hacker, isso tende a não ser um problema. É muito mais eu ter que correr atrás e entender como que eu vou fazer para me comunicar com essa pessoa, do que eu ter que ensinar essa pessoa a se comunicar comigo por meio seguro.

S6 informou que em algumas interações utiliza aplicativos como o WhatsApp e em outras situações, dependendo do conteúdo da conversa, sistemas mais seguros. Conforme projetamos, as respostas da pergunta 2 proporcionaram um panorama um pouco mais aprofundado das alterações e adaptações adotadas pelos jornalistas vigilantes na abordagem de temas sensíveis e descreveram algumas experiências e atuações em situações relacionadas à vigilância digital.

A terceira questão buscou verificar a percepção dos entrevistados sobre as principais mudanças relacionadas ao jornalismo investigativo contemporâneo perpassado pelas possibilidades de vigilância comunicacional. S1 acredita que o jornalismo investigativo não mudou e que as ferramentas do jornalismo ainda são as mesmas: entrevista, coleta de dados, telefone, entre outras. Acha que os elementos da reportagem continuam os mesmos, entretanto afirma que as grandes corporações e o Estado, de um modo geral, avançaram muito nos

aspectos ligados à vigilância e que investigações que envolvem altas autoridades podem tornar os jornalistas alvos.

S1 citou casos emblemáticos que ocorreram nos últimos anos, como os vazamentos do WikiLeaks e o escândalo da NSA que mencionamos no capítulo 3.

> Quer dizer, como que essas agências de inteligência do governo, a gente tem a Abin no Brasil, atuam. Esse jogo é muito pesado. Eu tenho fontes na Abin, até agora essas fontes sempre me trataram com muito respeito, eu não acredito que tenham feito algum tipo de malefício a mim, mas é uma coisa que você fica atento.

Para S1, os jornalistas investigativos têm que ficar atentos, pois a luta contra o poder do Estado é ingrata, pode ser altamente constrangedora e trazer consequências sérias para os profissionais. S2 acredita que as mudanças relacionadas ao jornalismo investigativo ainda não estão devidamente esclarecidas entre os jornalistas e que pouca gente presta a atenção que deveria prestar em relação a essas questões.

S3 acredita que as mudanças já podem ser nitidamente percebidas, não só em relação ao aumento da vigilância por parte de governos e corporações, mas também por meio das mídias sociais que permitem uma interação mais direta e estratégias organizadas de ataques digitais. Segundo S4, as mudanças impõem maiores cuidados aos jornalistas, no entanto não cercearam nada além do que já estava posto. S4 percebeu avanços relacionados à transparência e ao acesso à informação nos últimos anos.

Conforme S5, as mudanças podem ser percebidas, principalmente, nos últimos cinco anos. A partir do momento que a internet virou peça central de qualquer investigação jornalística, seja ela baseada em dados digitais ou não.

> A partir do momento que a internet virou o principal meio de transmissão de informação, mudou tudo, eu acho. As preocupações passaram a ser outras, os problemas passaram a ser outros e aí tudo mudou. As ferramentas mudaram, a forma de comunicar mudou, a forma de passar dados de um lado para o outro mudou.

S5 cita uma transformação significativa nas últimas décadas, mesmo não tendo vivenciado a fase anterior à internet, o jornalista acredita que as ações jornalísticas eram distintas das praticadas hoje. De acordo com S6, a modificação está em andamento, é algo em transformação que não envolve só o jornalismo, mas a sociedade como um todo. Mudanças em dimensões conectadas com a privacidade motivadas por casos como o da *Cambridge*

Analytica[161] e os vazamentos da Vaza Jato[162] despertam o interesse e debates sobre temas associados à vigilância digital e à intrusão comunicacional.

De acordo com S6, a preocupação dos jornalistas ainda está centrada no mundo físico, mas isso está mudando aos poucos a partir do entendimento e relevância do universo digital, da noção de que as consequências de ataques digitais podem ser tão nefastas quanto a dos ataques realizados pessoalmente.

Cabe salientar que o episódio da Vaza Jato, citado por alguns jornalistas durante as entrevistas, se notabilizou e se tornou um caso emblemático para esse estudo, pois envolveu o vazamento de informações relacionadas com a comunicação digital e a negligência, no que diz respeito à segurança de informações sensíveis por autoridades de alto escalão do Poder Judiciário no Brasil. As informações jornalísticas ligadas ao episódio começaram a ser divulgadas pelo *The Intercept Brasil* em junho de 2019, mês de realização das entrevistas em profundidade. Durante o processo de disseminação das informações, outros veículos (*Veja, Folha de S. Paulo*, entre outros) se associaram ao *The Intercept* na disseminação e tratamento jornalístico ao conteúdo vazado.

O vazamento da interação realizada por meio de um aplicativo de troca de mensagens entre os integrantes da operação Lava Jato indica desdobramentos de longo prazo, sendo que ainda não é possível tangenciar os resultados das ações realizadas durante o caso para o jornalismo investigativo brasileiro. No entanto, diante da repercussão e da importância das temáticas abordadas, especialmente por conta da forma de tratamento e obtenção das informações, pode-se afirmar que esse é um caso paradigmático que corrobora com as premissas relacionadas com a necessidade de formatação de uma cultura de segurança digital para jornalistas que abordam temáticas sensíveis.

As percepções dos entrevistados na questão três corroboram parcialmente com as premissas que apresentamos, no que diz respeito à modificação e às adaptações do jornalismo

[161] A *Cambridge Analytica* é uma empresa de análise de dados que utiliza comportamentos para direcionar conteúdos. Em 2018, jornalistas do *The New York Times* e *Observer of London*, ligado ao *The Guardian,* revelaram um esquema de coleta, venda e uso indevido de dados de milhões de norte-americanos. As reportagens demonstram como a empresa, fundada em 2013 e conhecida por seus trabalhos nas campanhas pró-Brexit no Reino Unido e de Donald Trump nos EUA, montou perfis baseados em traços da personalidade de cerca de 50 milhões de pessoas, com o objetivo de formar opiniões e direcionar votos ao candidato republicano. Em 2017, o *The Guardian* já demonstrava o interesse da empresa de inteligência britânica em direcionar a população do Reino Unido a adotar uma visão a favor da saída do país da União Europeia. Mais informações: https://www.nexojornal.com.br/expresso/2018/03/19/O-uso-ilegal-de-dados-do-Facebook-pela-Cambridge-Analytica.-E-o-que-h%C3%A1-de-novo. Acesso em: mar. 2019.

[162] Vaza Jato é a denominação do caso que envolveu o vazamento de conversas no aplicativo Telegram entre integrantes da Operação Lava Jato. A divulgação foi realizada pelo portal *The Intercept Brasil*, em junho de 2019. A repercussão do caso contou com a participação do jornalista estadunidense Glenn Greenwald, que atua no *The Intercept* e foi um dos protagonistas do caso do vazamentos de Snowden relacionados a NSA.

investigativo diante das possibilidades de vigilância digital a que os jornalistas estão expostos. Mesmo os profissionais que não percebem mudanças significativas apontam a necessidade de adaptações na conduta e nas ações de investigação jornalística.

4.1.2 Estratégias de segurança digital em investigações jornalísticas

Na questão número 4, buscamos aproveitar a experiência dos entrevistados e entender com mais clareza as suas vivências em relação a temas centrais do estudo ligados à vigilância comunicacional e à segurança digital. Em relação a casos emblemáticos que ocorreram durante a carreira dos profissionais, S1 citou as investigações sobre a morte da vereadora do Rio de Janeiro Marielle Franco, ocasião em que adotou medidas preventivas de mitigação de riscos digitais que nunca tinha adotado antes. Dentre as principais medidas implementadas, S1 relatou a utilização de um celular corporativo no contato com algumas fontes para evitar o mau uso de suas informações pessoais. No final da apuração, o número telefônico utilizado foi descartado.

S2 afirmou que já participou de alguns casos que envolviam protocolos de segurança digital que visavam mitigar possibilidades de vigilância e intrusão. Em um caso[163] de grande repercussão, o entrevistado revelou que os protocolos foram reforçados, no entanto o "veículo"[164] em que ele atua já tem protocolos de comunicação e gestão de dados que são utilizados regularmente durante apurações sensíveis. "A gente se preocupa muito com isso, até pela natureza do site. Desde uso de VPN[165] para navegação, até GPG[166], já é uma coisa incorporada a nossa rotina".

S3 não vivenciou casos emblemáticos que envolvessem protocolos de segurança digital, mas citou que formas de vigilância em relação aos jornalistas podem ocorrer de maneiras distintas, por exemplo, por meio de relatórios detalhados sobre repórteres e suas condutas, estratégia utilizada para interromper investigações. Para S3, estamos vivenciando um novo momento que indica o fim dos segredos e exige dos jornalistas atuações mais públicas e transparentes.

Casos regulares de vigilância digital odienta foram relatados por S4, que convive com ameaças e mensagens de desqualificação por meio de mídias sociais, especialmente durante

[163] Não revelamos o caso citado para evitar a identificação do entrevistado.
[164] Não revelamos o nome do veículo para evitar a identificação do entrevistado.
[165] VPN significa Virtual Private Network ou Rede Virtual Privada.
[166] GPG é uma criptografia assimétrica que emprega um par de chaves para alcançar seu objetivo (uma chave pública e uma chave privada). É um software livre alternativo ao conjunto de softwares criptográficos PGP.

investigações que envolvem presídios. “Nenhuma ameaça de morte explícita, mas coisas que me fizeram repensar a minha segurança, então, por exemplo, eu tenho um botão de pânico[167] no meu celular”. S4 revelou que utiliza protocolos de segurança para fazer coberturas em situações específicas, mas que estas estratégias envolvem mais riscos físicos do que riscos cibernéticos.

O *Panama Papers*[168] foi citado por S5 como um caso emblemático de sua carreira. A investigação jornalística realizada junto ao Consórcio Internacional de Jornalistas Investigativos (ICIJ)[169] envolveu mais de 300 jornalistas de 76 países. De acordo com S5, o ICIJ desenvolveu um método para realizar grandes investigações, com a participação de inúmeros jornalistas de diferentes partes do mundo, devido à utilização de ferramentas tecnológicas próprias.

> Eles desenvolveram plataformas próprias com um grau de segurança que não se compara com qualquer outra plataforma aberta na internet para a comunicação interna e para a comunicação com as fontes. Então, mais do que criptografia, eles desenvolveram sistemas internos para que esses jornalistas tivessem comunicação entre si segura, com várias etapas e várias camadas de segurança, desde o login até criptografia de arquivo, acesso ao banco de dados, criação de banco de dados próprio para não ter que depender, várias ações para criar um espaço seguro para que centenas de jornalistas pudessem trocar informações com segurança, informações sensíveis que não podiam ser divulgadas.

As principais recomendações para os jornalistas que participaram das investigações do *Panama Papers* foram não usar nenhuma rede estabelecida de comunicação, não usar e-mail tradicional, não usar mídias sociais para se comunicar sobre a investigação e jamais deixar qualquer contato dos documentos avaliados em bancos de dados públicos acessíveis. Conforme S5, esse protocolo de segurança foi formalizado entre os jornalistas que foram capacitados para utilização plena das ferramentas digitais de comunicação oferecidas. “Então, foram várias camadas de mediação e segurança para evitar que a informação vazasse. Nos dois casos, tanto no *Panama Papers,* quanto no *Paradise Papers*[170] e outras investigações, ninguém sabe quem é a fonte até hoje, exceto quem recebeu lá na ponta”.

[167] O botão de pânico alerta três pessoas que recebem a localização do dispositivo que começa a gravar automaticamente.

[168] O vazamento de um conjunto de documentos (mais de dois terabytes de dados) realizado por uma fonte anônima para o jornal alemão *Süddeutsche Zeitung,* em 2015, deu origem a uma série de reportagens, resultado do trabalho colaborativo que envolveu mais de 300 profissionais de 76 países e venceu o Prêmio Pulitzer de 2017, na categoria *Explanatory Reporting*.

[169] O Consórcio Internacional de Jornalistas Investigativos (ICIJ) foi fundado em 1997 pelo *Center for Public Integrity* e reúne jornalistas de mais de 65 países que buscam investigar delitos internacionais, atos de corrupção, abuso de poder, etc.

[170] O caso teve como base um conjunto de mais de 13 milhões de documentos eletrônicos confidenciais de natureza fiscal obtidos pelo jornal alemão *Süddeutsche Zeitung* e compartilhados com o ICIJ. A divulgação

S6 informou que passou por dois ataques digitais, violação ou interceptação de e-mail pessoal do jornalista (VE) e furto de senhas por meio de *phishing*[171] ou *pharming*[172] (FPP). Após os ataques, S6 começou a adotar medidas de segurança mais estritas que contam com várias profilaxias digitais para mitigação de riscos.

Durante as entrevistas, também buscamos verificar se os jornalistas vigilantes estão preocupados com segurança digital, todos eles responderam de maneira afirmativa. As respostas a respeito de quando eles despertaram para esse aspecto da investigação jornalística variaram bastante. S1 começou a se preocupar com medidas de mitigação de riscos após cobrir um caso emblemático (assassinato da vereadora Marielle Franco) e de grande repercussão em 2018. Já S2 busca informações e recursos relacionados à segurança digital há cerca de dez anos: "Já dei curso sobre isso também, já dei curso sobre TOR[173], sobre navegação anônima, sobre VeraCrypt[174], sobre arquivos criptografados, já é uma coisa que me interessa há bastante tempo".

Por conta das preocupações com os riscos do ecossistema digital, S3 imprime todos os documentos coletados durante investigações de temáticas sensíveis e evita a utilização do computador. Quando não consegue evitar a utilização de arquivos digitais, coloca em um HD externo[175]. A sua preocupação com segurança digital ficou mais aguda no desenvolvimento de uma investigação jornalística em que enfrentou um processo judicial. O processo pretendia tomar os arquivos coletados durante a apuração. No mesmo período, o jornalista teve a sua casa arrombada.

O caso ocorreu entre os anos de 2010 e 2011. "Era um grupo de militares que ficavam atrás dessas informações também. Ali eu tinha um problema, foi terrível, casa arrombada, justiça na porta". S3 relatou que em algumas ocasiões prefere realizar ações de investigação em *lan house* ao invés de utilizar o seu computador pessoal, também cria e-mails exclusivos para algumas apurações.

---

jornalística ocorreu em 2017. As revelações apontam investimentos *offshore* de mais de 120 mil grandes corporações, celebridades e pessoas de várias nações.

[171] Termo que designa tentativas de obtenção de informações pessoais através de golpes com identidades falsas balizadas por estratégias de engenharia social. Normalmente ocorre por meio de falsificação de comunicação digital, como e-mail, portais de instituições bancárias e administradores de sistemas.

[172] É uma prática fraudulenta semelhante ao *phishing*, com a diferença de que, nesta modalidade, o tráfego de um site legítimo é manipulado para direcionar os usuários para páginas falsas, que instalam *softwares* maliciosos nos dispositivos para coletar dados pessoais, senhas, etc.

[173] TOR é um software livre e de código aberto que possibilita comunicação anônima na navegação pela Internet e em atividades online.

[174] VeraCrypt é um programa que realiza criptografia em arquivos e discos do computador. Cria arquivos ocultos e protegidos dentro do sistema operacional, no HD e em dispositivos externos, como pendrives.

[175] O HD (Hard Disc) externo é um dispositivo portátil que armazena dados digitais (arquivos, fotos, documentos, etc).

Em 2013, durante os protestos no Brasil[176], S4 percebeu o início de uma onda de ódio contra os veículos e a atuação da imprensa. Nesse momento, começou a tomar mais cuidados em relação a sua segurança digital. S5 afirmou que toma medidas de mitigação de riscos digitais desde o começo da sua carreira, pois ingressou no jornalismo em uma época (2015) que as possibilidades cibernéticas já estavam consolidadas. Na mesma linha, S6 afirmou que mantém uma preocupação básica com segurança digital desde sempre, mas foi após os ataques digitais que sofreu que começou a adotar medidas de segurança digital mais rígidas.

As preocupações e as motivações para a tomada de medidas de segurança digital apresentadas pelos entrevistados auxiliam no entendimento de situações que podem indicar caminhos para o fomento de uma cultura de riscos digitais para jornalistas. A maioria dos jornalistas vigilantes que participaram deste estudo tomaram medidas de prevenção de riscos digitais após situações traumáticas ou casos extremos que os fizeram refletir sobre a necessidade de uma nova tomada de posição em relação as suas vulnerabilidades.

Um dos momentos mais delicados que expõem jornalistas e suas fontes a riscos digitais, especialmente durante investigações de temas sensíveis, são as formas de contato e interação. Durante as entrevistas em profundidade, verificamos possíveis mudanças na relação dos profissionais com as suas fontes e algumas estratégias de contato que estão sendo adotadas em situações críticas onde são abordados temas relacionados a segredos, vazamentos, crimes, etc. S1 informou que nesses casos sempre encontra as fontes pessoalmente, face a face e em locais públicos. Em algumas oportunidades, utiliza o WhatsApp para o contato, porque a ferramenta é criptografada.

Por questão de segurança, S2 não detalhou quais são as formas de contato com as fontes. “A gente faz o contato conforme a fonte se sente mais confortável ou a gente indica para ela maneiras de se contatar que ela não corra o risco de ser rastreada, então, por isso, não posso dizer quais são”. Da mesma forma, S3 indica que esse tipo de contato depende muito do perfil da fonte, do momento e do contexto da apuração.

> Esse tipo de fonte já está preparada. Ela que deixa claro a forma de preservação dela mesma, pelo menos essas fontes de governo. Tem também, porque veja, quando é uma fonte dessas, as coisas são muito integradas, se o cara pegar um dado sigiloso vai deixar rastros, então as quebras de informações, elas ocorrem hoje, no contexto atual, por grupos. O Ministério Público, ele decidiu, foi uma decisão, eu diria assim, de um colegiado, que vamos vazar isso. Assim é o governo também. Então quando essas informações chegam, elas já chegam com seus escudos, as suas proteções.

[176] As manifestações populares que foram denominadas como “Manifestações dos 20 centavos”, “Jornadas de Junho”, dentre outras, ocorreram por todas as regiões do país, principalmente nas capitais. Inicialmente surgiram para contestar os aumentos nas tarifas de transporte público, depois passaram a defender bandeiras difusas. Elas estão entre as maiores mobilizações registradas na história do Brasil.

S3 explicou que vazamentos realizados por órgãos do Poder Judiciário ou governamentais passam por entendimentos internos e convenções entre atores que têm acesso a informações sensíveis. S4 disse que toma todos os tipos de cuidado para que suas fontes não sejam identificadas e estabelece uma relação de confiança mútua que envolve segurança e manutenção do anonimato. Costuma utilizar o Signal[177] para estabelecer contato em situações que envolvem riscos digitais e, se possível, prefere encontrar as fontes pessoalmente.

Na percepção de S5, as condicionantes comunicacionais e o tipo de documentos envolvidos na apuração modificam os protocolos de segurança que cada situação exige. S5 costuma adotar algumas medidas preventivas em seus dispositivos eletrônicos.

> Tudo que tem documento tenho acesso com dois fatores de autenticação[178], todos os sistemas têm as recomendações básicas de criação de senha, troca de senha sempre. As recomendações básicas de segurança eu sigo todas, as mais normais e alguns casos exigem passos além do que esses, por exemplo, tem fonte que não fala por linha telefônica porque pode ser grampeado e só faz ligação com WhatsApp por exemplo, que é criptografado e você não consegue, o WhatsApp eventualmente não vai conseguir fornecer o áudio para ninguém, e não tem como grampear que é por dados. Esse é o exemplo mais simples. Aí tem fontes que você não se preocupa com isso porque o assunto que você está falando com ela por telefone não tem nenhum problema, e aí envio de dados, não usar o e-mail pessoal para mandar os dados, eventualmente criar contas de e-mail específicas para tratar de algum assunto. A criptografia de arquivos sempre. Enfim, aí cada caso é um caso, tem caso que realmente não exige esse tipo de preocupação, aí o contato é mais livre.

S5 explica que nas investigações do ICIJ, os protocolos de segurança digital são muito rígidos e preveem várias situações de risco, além da utilização de ferramentas próprias para realização das investigações e trocas no ambiente digital.

As estratégias de mitigação de riscos digitais de S6 no contato com suas fontes variam de acordo com o nível de importância das informações que estão envolvidas na apuração. Costumeiramente, as conversas podem ocorrer em aplicativos de trocas de mensagem, como o WhatsApp, em um *chat* secreto no Telegram ou por meio de um sistema mais escuso. “Teve gente que já pediu para entrar em contato comigo por meio de chat de jogo. Nós dois entramos no mesmo jogo ao mesmo tempo, como se estivesse jogando, por lá a gente conversou”.

O contato e a possibilidade de exposição das fontes é um indicativo importante das vulnerabilidades impostas pelo ecossistema de comunicação digital. De maneira geral, todos os entrevistados demonstraram preocupação e medidas específicas para tratamento de fontes

[177] É um serviço de mensagens criptografadas para várias plataformas.
[178] É um recurso oferecido por vários prestadores de serviços online que acrescentam uma camada adicional de segurança para o processo de login da conta, exige que o usuário forneça duas formas de autenticação, por exemplo, uma senha, um SMS ou um código enviado por e-mail.

que forneçam informações sensíveis por meio de ferramentas digitais. Também adotam estratégias e medidas específicas em situações pontuais e condutas no ecossistema digital. S1 adota cuidados em relação à utilização de mídias sociais: "Um deles é nunca postar fotos da minha família. Eu não costumo postar fotos da minha família em rede social, só minhas, por conta do meu trabalho sensível. É uma forma, eu creio, de preservar a família".

S5 dá atenção especial a cuidados com logins e acessos, desde a conta de e-mail até o bloqueio do celular, além da troca regular de senhas e utilização de combinações que não possam ser facilmente deduzidas. Adota cuidados relacionados à manipulação de arquivos utilizando criptografia e verifica os canais mais seguros para o envio dessas informações. Também evita conversas por meio de aplicativos que são abertos, como chat do Gmail ou do Facebook, para tratar de assuntos sensíveis. O uso de senhas mais fortes e autenticação em duas etapas[179] também são precauções utilizadas por S6.

> Tomo cuidado com todas as redes que eu me conecto, na verdade que eu não me conecto, no geral. É muito, muito raro você me ver conectado ao wi-fi público, por exemplo, ou wi-fi compartilhado, ou wi-fi que eu não conheça. Se eu fizer isso eu vou adotar medidas de cautela. Eu uso sistemas para proteger o meu telefone, os meus computadores, eu tenho muitas medidas de segurança em prática.

Diante da complexidade dos temas abordados, por exemplo, a necessidade de anonimato e de segurança apresentadas pelos casos e por situações do dia a dia, a utilização de sistemas operacionais distintos também fazem parte das condutas de S6 na utilização das possibilidades digitais. S6 recomenda a compartimentalização das informações, evitando armazenar arquivos e informações em um lugar só, especialmente quando se está trabalhando em investigações complexas.

> Criptografia em tudo. O meu telefone é criptografado, o meu computador é criptografado, mas assim, tem que ter toda uma noção, entender qual é o sistema, o que você está usando, quais são as limitações e quais são os benefícios dele. Porque às vezes você vai ter um custo de usabilidade, vai ser conforme você vai adotando medidas de segurança. Chega o momento que o negócio fica tão inconveniente que você pode acabar, você é ser humano, sendo displicente com aquilo e deixar algo desligado que, enfim, isso te expõe.

Para S6 é importante refletir sobre as medidas de prevenção digital em relação aos custos de usabilidade que elas apresentam. O entrevistado sugere que em alguns momentos é recomendável baixar um pouco o nível de segurança, mas permanecer com alguma segurança. Também é importante não usar níveis mais altos de segurança digital em atividades cotidianas

[179] Com a verificação em duas etapas você adiciona uma camada extra de segurança à sua conta. Depois de configurar esse recurso, você fará login na sua conta em duas etapas, usando, por exemplo, algo que você conhece (senha) e algo que você possui (chave de segurança).

e utilizá-los apenas em situações específicas, em que houver necessidade: “Porque eu sei que vai chegar o momento que vai ser inconveniente, eu vou acabar simplesmente desligando e ficar totalmente descoberto”. A análise contextual que envolve o caso, o bom senso e a atenção, em tempo integral, a possíveis riscos e vulnerabilidades devem ser condutas permanentes dos jornalistas. As respostas dos entrevistados apresentam medidas e estratégias de prevenção que estão sendo adotadas por jornalistas investigativos no ambiente digital e serviram de embasamento para algumas perguntas do formulário aplicado na *survey*.

4.1.3 Vulnerabilidades e potencialidades apontadas pelos jornalistas

Para entender mais detalhadamente as principais vulnerabilidades enfrentadas por jornalistas que desenvolvem investigações em um contexto de vigilância massiva das comunicações digitais, perguntamos como os entrevistados percebiam esta condição. S1 acredita que a comunicação é a principal vulnerabilidade enfrentada pelos profissionais. “O WhatsApp, por exemplo, se alguém eventualmente conseguir quebrar a criptografia de uma conversa de WhatsApp, eu sei que é possível já fazer isso, isso seria altamente danoso para gente, vai estar exposto muita coisa que eu não quero que esteja exposto”. Na opinião de S1, as formas de comunicação digital podem expor os jornalistas. Diante disso, S1 evita a utilização de e-mail e de aplicativos como o Telegram.

O desconhecimento e o fato das pessoas acreditarem que as questões e problemáticas relacionadas à vigilância comunicacional e à segurança digital não são importantes são as principais vulnerabilidades apontadas por S2. Aspectos atrelados à vida pessoal do jornalista são indicados por S3 como as principais vulnerabilidades presentes no ecossistema digital. A exposição da família e a falta de condições de jornais e empresas no que diz respeito à segurança para os profissionais foram enaltecidos pelo entrevistado.

> Eu, por exemplo, tive que bloquear minha família inteira, mãe, pai, irmãos, sobrinhos todo mundo para evitar as conexões, as pessoas começarem a me rastrear, chegar aqui e compor a minha árvore genealógica, da minha família, para me atingir, porque eles vão nas crianças, é terrível. Chegam nos meus sobrinhos que estão há quilômetros de onde eu trabalho. Nas redes sociais eu tenho um código interno, com a minha família, assim, ninguém curte as minhas coisas, ninguém coloca nada nas minhas coisas e eu também não compartilho informações pessoais com a minha família. Eu já não garanto a minha segurança, vou garantir de alguém.

S3 citou uma situação em que investigou um caso que envolvia o crime organizado no Espírito Santo e ataques de grupos de ódio que atuavam nas mídias sociais. Ele relatou que sofreu ameaças pelo telefone: “Essa matéria teve muito destaque no jornal na época. Ali, para

mim, ficou muito claro essa rede toda e ficou claro também como a gente estava vulnerável, porque, de repente, nas ligações, os caras já falavam: 'você tem família, esse tipo de coisa'". Para S3, esses grupos de ódio, organizados no ambiente digital, estabelecem uma forma de vigilância altamente nociva e com ampla capacidade de gerar danos para os jornalistas.

A falta de conhecimento que os jornalistas têm em relação aos riscos presentes no ambiente digital também foi elencada como a principal vulnerabilidade por S4. De maneira geral, S4 acredita que há baixo nível de conhecimento sobre internet nas redações, até mesmo as coberturas sobre temas como Deep Web[180] são superficiais. Esses fatores indicam um alto grau de exposição dos jornalistas. "Então a gente não têm o menor conhecimento disso, se a gente tivesse, a gente teria identificado a chegada das *fake news*, isso é um problema. Uma omissão nossa, a gente não está investindo nisso". Casos que envolveram colegas de S4 foram relatados para exemplificar as vulnerabilidades e riscos dos espaços digitais. Em algumas ocasiões, S4 utiliza o *ProtonMail*[181] nas suas investigações.

O descuido com a segurança digital e as possibilidades de vigilância comunicacional, seja por parte dos jornalistas, seja da parte das fontes, é apontada por S5 como a principal vulnerabilidade enfrentada pelos profissionais.

> A vigilância, ela só é feita se você permite. Ela está em todo lugar, em maior ou menor grau e aí o quão você vai deixar ela chegar aos seus dados é uma coisa que depende muito de você, de que níveis de obstáculos que você vai adotar, aí pode chegar a um nível extremo de você não usar um navegador de internet comum, a selecionar o navegador para limpar os cookies do meu histórico de navegação, então têm todos esses níveis e aí a principal vulnerabilidade é que as outras pessoas envolvidas não tomem esse cuidado que você está tomando ou que todo mundo deveria estar tomando.

Conforme S5, a negligência de qualquer um dos envolvidos nas trocas de informações durante as apurações pode comprometer todo o processo de investigação e colocar em risco os envolvidos: "A vulnerabilidade é sempre ou ignorância da pessoa, ou o erro, ou a negligência, ou imperícia, a vulnerabilidade maior é sempre a falta de procedimento, de seguir o protocolo de segurança". Na mesma direção, S6 aponta a displicência como principal vulnerabilidade enfrentada pelos jornalistas que abordam temas sensíveis.

> Você não ter essa noção do ambiente em que você está inserido, você achar que isso é seguro. Enfim, você adotar uma ou outra medida de segurança e ter uma falsa noção de que você está realmente coberto, mas, na verdade, você não está porque você não entende realmente como aquilo que você está usando funciona e você não se dá ao trabalho de perguntar para alguém que realmente entenda.

[180] É uma parte da web que não é indexada pelos mecanismos de busca (exemplo: Google) e, desta forma, fica oculta ao público massivo. O termo geral classifica diversas redes de sites distintas que não se comunicam.
[181] É um serviço de correio eletrônico criptografado.

S6 acredita que os jornalistas devem se preocupar em entender os protocolos, os processos de comunicação digital e a infraestrutura que oferece essas possibilidades, como que os profissionais podem influenciar nesse meio, quem pode querer interceptar esses dados, o que essa pessoa pode fazer com essas informações. S6 destaca que de maneira geral os jornalistas não conhecem essa área, reforçando que não conhecer não é o problema, mas que isso passa a ser displicência a partir do momento em que os profissionais não procuram conhecer e entender o ambiente em que estão inseridos para proteger minimamente as suas fontes. O entendimento dessas problemáticas passa por reconhecer a existência dos riscos digitais, saber quais são, sem necessidade de um conhecimento técnico profundo, mas com uma consciência e um senso de vulnerabilidade permanente.

Em relação às principais potencialidades do ecossistema de comunicação digital para o trabalho de investigação jornalística, S1 enalteceu que as inúmeras bases de dados digitais são vitais para o trabalho dos jornalistas e que atualmente seria impensável fazer jornalismo investigativo sem acesso a sistemas digitais. Para S2, os principais potenciais do ambiente digital estão conectados as possibilidades de pesquisa, obtenção de documentação, acesso a dados públicos e bancos de dados. "É possível fazer jornalismo com fontes abertas de uma maneira que não se fazia antes, as coisas estão mais transparentes".

Conforme S3, as mudanças são agudas e envolvem todo o setor de comunicação. Uma nova plataforma que, de certa forma, têm um *know how* que foi produzido ao longo de dois séculos oferece inúmeras oportunidades para o jornalismo. S4 observa que o advento de dispositivos tecnológicos facilita o trabalho dos jornalistas, apesar dos níveis de exposição e vulnerabilidade, o acesso a bancos de dados e pesquisas, como as do *Google Trends*[182], são importantes ferramentas de apuração.

As possibilidades comunicacionais são apontadas por S5 como a principal potencialidade apresentada pelo ecossistema digital. "O que fez, o que permitiu um salto incalculável nas possibilidades de investigação jornalística, em relação ao que não existia antes, são os meios de comunicação entre as pessoas". As condições enaltecidas por S5 são amplamente perceptíveis em investigações como as desenvolvidas pelo ICIJ. Elas reúnem centenas de jornalistas de diversos países, exigem alto grau de sigilo e a utilização de ferramentas de comunicação moduladas por protocolos avançados de segurança digital.

> Hoje em dia você consegue fazer banco de dados que você não conseguia fazer antigamente, ferramentas de acesso a esses bancos de dados, porque não adianta também se ter todos os dados organizados se não for fácil e compreensível acessá-

[182] É uma ferramenta que mostra os mais populares termos buscados em um passado recente.

> los. Assim, o avanço da tecnologia possibilitou ao jornalismo coisas inimagináveis há 20 anos atrás e aí têm todos os problemas que isso traz.

Em relação às problemáticas e às vulnerabilidades, S6 identifica avanços no que tange à mitigação de riscos dos espaços digitais utilizados por jornalistas.

> Por exemplo, é muito mais fácil você interceptar ligações e interceptar comunicação na verdade não ligações, mas SMS, enfim, numa rede 2G do que em uma rede 3G, que é mais fácil do que uma rede 4G, que vai ser mais fácil que uma rede 5G. Então essas coisas vão se atualizando e criam canais seguros. Canal de ligação criptografada, é muito mais fácil você grampear um telefone do que você grampear uma ligação para um aplicativo de VoIP. Acho que isso traz possibilidades que antes você não tinha tanto para o lado negativo, quanto para o lado positivo.

Os relatos dos entrevistados fortalecem e ratificam a importância desse estudo em relação a algumas de suas premissas e objetivos, particularmente nos aspectos que tratam das limitações das investigações jornalísticas impostas pelas formas de intrusão comunicacional do ambiente digital, a urgência da proteção das comunicações digitais de jornalistas que abordam temas sensíveis e ao objetivo principal do estudo que é examinar ações que envolvem o jornalismo investigativo, apontando potencialidades e vulnerabilidades no ecossistema digital.

4.1.4 Vazamentos e a necessidade de uma cultura de segurança digital

Os vazamentos que subsidiam investigações e a relação dos jornalistas investigativos com os *whistleblowers*[183] apresentam novas características quando as interações e as ações jornalísticas são mediadas pelas possibilidades do ecossistema digital. As condutas e condicionantes que perpassam as apurações tornam esses elementos e as questões que os tangenciam aspectos fundamentais do jornalismo investigativo contemporâneo. S1 lembrou que há 15 anos vivenciou um caso que envolvia a interação com um *whistleblower* e apuração mediada por tecnologia digital.

> Evidentemente o uso da tecnologia digital era muito incipiente em 2004, na época, eu investiguei, com a ajuda desse hacker, um esquema de roubo de senhas bancárias, uso de Cavalo de Troia. Na época isso era uma novidade ainda, hoje mal se usa isso, aqueles programas espiões que você baixa sem querer e eles pegam a sua senha. Era um megaesquema em Santa Catarina, era chefiado por lá, mas eu estava no interior de São Paulo e tinha um braço no interior de São Paulo, eu divulguei isso e até ganhei um prêmio nesse caso.

[183] Denunciantes que alertam para a existência de irregularidades na gestão, no funcionamento de empresas ou instituições, o termo não tem uma tradução equivalente em português.

Esse é um caso marcante para S1, pois foi a primeira vez que ele trabalhou com tecnologia digital em uma reportagem e com fontes especializadas que exigem condutas específicas por parte do jornalista, particularmente por envolver práticas criminosas relacionadas ao ambiente digital.

> Há que se tomar muito cuidado com a fronteira ética nesse tipo de situação. O hacker vaza milhões de dados sobre conversas, anos de conversa no WhatsApp ou no Telegram, o que fazer com esse material? É uma dúvida que eu tenho, se isso acontecesse comigo, eu teria noites sem dormir com certeza. É justamente nesse entrave ético, nesse debate ético de publicar ou não.

S1 citou o caso que ficou conhecido como Vaza Jato [184] para evidenciar a complexidade da atuação em casos que envolvem o vazamento de um grande volume de informações. Diante do evidente interesse público da situação emergem reflexões de outra ordem, particularmente relacionadas à origem dos dados e às condutas adotadas pela fonte para obtenção deles. De acordo com S1, essa é uma problemática polêmica e não há uma resposta pronta para esse tipo de situação que deve ser debatida pelos jornalistas.

Em relação a como se preparar para isso, S1 aponta que não é um *expert* em tecnologia, mas para ele, os fundamentos da reportagem são os mesmos, o que muda é o ambiente, os filtros do jornalista permanecem inalterados. “O jornalismo continua com as mesmas balizas éticas e de prática”.

S2 também abordou o episódio da Vaza Jato, indicando que essa é uma investigação jornalística significativa, especialmente para o jornalismo independente, que demonstra que é possível fazer jornalismo de alto nível em outro formato, de um outro jeito, com uma outra visão, com outra identidade, outra linguagem, em uma perspectiva diferente do que é o jornalismo e de como ele tem que ser feito. Para S2, esse caso paradigmático não aconteceria sem as possibilidades oferecidas pelo ecossistema digital.

S2 comenta que já existe um histórico e profissionais que já lidaram com vazamentos. “Claro que não todos, porque também não são todos os jornalistas que trabalham com esse tipo de material, mas já tem um aprendizado de como lidar com esse tipo de material, inclusive fazendo parcerias e tal. Acho que tem bastante massa crítica”. S2 diz que as experiências ao longo da carreira o prepararam para trabalhar com vazamentos e vazadores: “Tem uma lógica que é muito precisa, assim, a lógica da proteção de fontes, é a mesma lógica da proteção de documentos, a mesma lógica que você vai usar para todas as coisas”.

[184] Vaza Jato é a denominação do caso que envolveu o vazamento de conversas no aplicativo Telegram entre integrantes da Operação Lava Jato. A divulgação foi realizada pelo portal *The Intercept Brasil*, em junho de 2019. A repercussão do caso contou com a participação do jornalista estadunidense Glenn Greenwald, que atua no *The Intercept,* e foi um dos protagonistas do caso dos vazamentos de Snowden relacionados a NSA.

S3 citou o *Panama Papers* e a Vaza Jato como casos emblemáticos relacionados à gestão de vazamentos e dilemas impostos por essas situações, como o fato de repassar o conteúdo obtido na íntegra ou resguardá-lo para tratar jornalisticamente.

> Um repórter que pegou as informações e acha que tem todo o tempo do mundo para preparar o material, a informação que ele quer, isso é da essência do repórter, e do outro o profissional que acha que o interesse público é maior naquele momento e tem que ser naquele momento, repassar tudo e é igual agora estão questionando o *The Intercept*.

Para S3, os vazamentos são tradicionalmente utilizados como base para investigações jornalísticas. "É tradição do jornalismo publicar o que chegou na mão do repórter, vazou e ponto final. Mas isso não é legal? É tradição, foi assim que a imprensa se consolidou". S3 também ressaltou o importante papel do jornalismo no processo democrático ao longo da história e que em inúmeros momentos esse papel foi transpassado por vazamentos de informações.

S3 acredita que está preparado para lidar com essas situações, mas aponta que as empresas não estão. Os grandes vazamentos sempre existiram, entretanto, na sua trajetória de 18 anos no jornalismo, presenciou o declínio do número de profissionais nas redações, o que dificulta o tratamento de grandes volumes de informações. Também evidencia elementos essenciais para lidar com vazamentos, como o conhecimento do repórter em relação ao tema, a formação do repórter e a densidade das informações obtidas.

Em um momento em que grandes bancos de dados estão sendo base de ações jornalísticas, S4 indica que está ocorrendo um processo de aprendizado por meio do trabalho executado durante essas investigações. Os casos do *Panama Papers* e da Vaza Jato propõem inúmeros desafios aos profissionais e uma série de cuidados que precisam ser adotados em determinadas situações.

S4 aponta que o grande volume de informações e de jornalistas envolvidos no *Panama Papers* demonstra o aprendizado que está em curso para condutas dos jornalistas investigativos no ambiente digital. S4 acredita que a estratégia do *The Intercept Brasil,* ligada ao tratamento das informações de maneira jornalística e divulgação do conteúdo obtido em etapas, é acertada e serve de base para outras situações. "Acho que ninguém estava e tinha se preparado especificamente para receber um conteúdo de tanta informação vazada assim. E eu acho surpreendente, o acontecimento jornalístico mais importante dos últimos anos no Brasil".

Grandes vazamentos que servem de base para o trabalho jornalístico exigem dos jornalistas precauções e habilidades que envolvem o recebimento e a depuração de dados

digitais. S5 exalta que alguns grupos de jornalistas estão preparados e organizados para realizar esse tipo de investigação.

> O ICIJ talvez seja o exemplo mais evidente no mundo que conseguiu conduzir, o *Panama Papers,* em específico, acho que foi um caso muito paradigmático. Foi a primeira investigação desse tamanho com uma quantidade de dados inacreditável, quase 3 teras de dados brutos. Então, eu acho que esse procedimento mostra que é possível e também abriu caminhos para que novos casos como esse aconteçam no futuro.

Segundo S5, o caso da Vaza Jato, denunciado pelo *The Intercept Brasil,* é outra prova de que atualmente existem jornalistas preparados para lidar com isso. "Obviamente não são todos, obviamente se aprende muito ao longo do processo, erros podem ser cometidos, mas eu acho que sim, hoje em dia já existe jurisprudência profissional para tratar casos como esse". Outro caso paradigmático que ajudou a constituir formas de aprendizagem para o cenário digital foi o caso do WikiLeaks, que realizou grandes vazamentos de dados e documentos brutos que foram disponibilizados na internet.

> A cada caso os jornalistas estão mais preparados, porque você consegue ver o que deu certo e o que deu errado. E acho que esse caso aqui no Brasil, está tendo agora do *The Intercept*, vai ser importante para isso também, porque é um caso também inédito, de troca de mensagens entre juiz e procuradores da operação mais importante, e como lidar com isso e como publicar o conteúdo. São muitos fatores que têm que ser considerados e também é o caso que eles, com certeza, estão aprendendo à medida que estão desenvolvendo. É muito complexo, um sem número de questões éticas, técnicas, de opinião pública. É um assunto muito nocivo na opinião pública.

S5 aponta para um processo de aprendizado permanente tangenciado pela evolução técnica e deontológica da ética, do como divulgar e como falar, como tratar esses dados brutos que o jornalista teve acesso. Na mesma linha, S6 percebe que a experiência no ambiente digital é um fator essencial para o tratamento de grandes vazamentos e *whistleblowers.* O entrevistado salienta que alguns jornalistas têm medidas impostas para atuar nessas situações, mas, de maneira geral, os profissionais não estão preparados para trabalhar nesses casos. "Nesses casos muitas vezes a noção de segurança parte muito mais do *whistleblower* do que do jornalista, porque não é o jornalista pedindo para alguém tomar essa medida, mas parte dessa pessoa". S6 sugere que o fato de o jornalista sentir que está preparado para atuar nessas abordagens também pode ser um problema, porque o contexto digital muda constantemente.

> O protocolo que hoje é seguro amanhã pode não ser. Então, você tem que se manter sempre atualizado em relação a essa esfera e descobrir quais são as vulnerabilidades que foram descobertas hoje. Algo que há alguns anos era o estado da arte ou quase estado da arte em segurança, que é o protocolo PGP para criptografia de e-mails, já foi quebrado. Então assim, hoje ele não é tão seguro quanto ele era há alguns anos, amanhã ele vai ser menos seguro do que hoje. Nesse meio tempo surgiram outros

> protocolos que fazem essa mesma função e são mais seguros. Amanhã também não vão ser. Acho que é sempre um processo de você se preparar e conhecer tecnologias novas, técnicas novas e vulnerabilidades novas também.

As respostas dos entrevistados apontam dificuldades e ações que facilitam o tratamento e aproveitamento das possibilidades abertas pelo ecossistema digital, particularmente em relação aos grandes vazamentos e ao surgimento de *whistleblowers* que subsidiam e originam investigações jornalísticas. A partir desse contexto, defendemos a necessidade de estímulos e convenções relacionadas com a formatação de uma cultura de riscos digitais para jornalistas. Vale ressaltar que todos os entrevistados apontaram que esse é um elemento importante para o jornalismo investigativo contemporâneo.

S1 justificou a sua percepção salientando que esse é um aspecto extremamente importante, porque os jornalistas que abordam temas sensíveis estão sujeitos a riscos digitais consideráveis como, por exemplo, atos de intrusão comunicacional.

> Como a gente já conversou, nós, jornalistas investigativos, lidamos com fontes muito sensíveis, muito sensíveis. Qualquer vazamento de uma conversa pode colocar em risco a vida do jornalista e da fonte também. Isso é muito sério, tem que ser levado muito em consideração e eu acho que o jornalismo não está preparado para esse tipo de ato criminoso contra si mesmo. O jornalismo, de um modo geral, e eu me incluo nisso, não está suficientemente preparado para lidar com uma invasão desse tipo, por exemplo.

Na mesma direção, S2 acredita que o grande problema é a desinformação e o consequente despreparo dos profissionais que não estão aculturados sobre isso, não se dão conta da importância de proteger dados que parecem banais, mas que se caírem nas mãos erradas ou forem descontextualizados podem virar tragédia. S3 também acredita que o mais importante é a formação do repórter. “Você tem um novo contexto no jornalismo, na política, no jogo do poder e que a imprensa não está preparada, nem um pouco preparada”. A inexistência de uma cultura de investigação para atuação em um novo contexto, a falta de recursos e a falta de estrutura diminuem a capacidade de pensar sobre uma possível cultura de riscos digitais para jornalistas.

> Hoje, o mundo global, o crime cibernético, o crime digital, toda essa questão das relações dos crimes organizados, a gente está passando batido por isso. Nós estamos longe desse contexto, desse novo jogo, da forma que está sendo jogado e o Brasil é um país ilhado, nós não temos relações com ninguém.

S4 garante que possibilidades de capacitação são fundamentais para viabilização de uma cultura de riscos digitais para jornalistas. “Cursos, acho que formação sistemática nas redações seria muito importante. Na universidade também, é muito importante. E acho que as organizações de jornalismo também tinham que ter cursos específicos para quem quisesse

fazer isso". S5 também aponta a capacitação para meios digitais como ferramenta essencial para a constituição de uma cultura de segurança digital para os jornalistas vigilantes.

> O trabalho pode ser muito comprometido se a pessoa não tiver conhecimento de algumas coisas, às vezes, bem básicas de segurança digital, sigilo e privacidade. Aí entra tanto as questões éticas, relacionamento com a fonte, quanto as questões técnicas de segurança mesmo. É preciso sim e em um mundo ideal isso seria discutido nas faculdades e na formação básica do jornalista que quer trabalhar com jornalismo investigativo, é base para poder realmente fazer as investigações.

Os entrevistados percebem como positiva a possibilidade de constituição de uma cultura de riscos digitais para jornalistas que abordam temas sensíveis, o que está associado a um dos elementos centrais defendidos por essa tese. Por fim, verificar possíveis formas de fomento dessa cultura foi o intuito da última questão das entrevistas.

S1 enalteceu o papel da Abraji na oferta de treinamentos e oficinas, mas lembrou que infelizmente muitos jornalistas não levam isso a sério. "Eu acho que esse caso da Vaza Jato também coloca essa perspectiva, quer dizer, até que ponto eu posso estar sendo hackeado. As pessoas estão mais conscientes desse problema hoje do que há cinco anos atrás".

S2 destacou o papel das universidades, sugerindo que as redações jornalísticas não treinam os jornalistas suficientemente para estas situações. S3 ressalta a busca por parcerias como uma das ações importantes para o fomento de uma cultura digital, observando que a discussão isolada sobre as problemáticas tecnológicas, que mudam constantemente, afetam o jornalismo e o sistema democrático, especialmente o processo eleitoral por meio das mídias sociais.

Para S5, os jornalistas precisam falar sobre este assunto, pois debates e discussões podem conscientizar profissionais que eventualmente vão trabalhar com essas questões. "Formação de jornalistas, faculdade, curso, capacitação de jornalistas que já estão formados e principalmente fazer desse assunto uma pauta discutida sempre em grupos, entre os jornalistas".

S6 acredita que, infelizmente, os jornalistas investigativos vão precisar de mais sustos, educação e tempo para estruturarem uma cultura de segurança digital. A oferta de treinamentos, possibilidades de conscientização e posturas dos gestores das redações pode gerar percepções que transformem a segurança digital em algo fundamental, isto é, algo tão importante quanto a segurança física dos jornalistas.

> Não é necessário, novamente, um grande conhecimento técnico, você não precisa virar um especialista em cibersegurança, você não precisa virar um hacker, mas você precisa ter a noção de que essas ferramentas que você usa têm limitações e quais são essas limitações, para que em um caso mais específico você possa procurar ajuda, se

> for o caso, para lidar com isso. Enfim, tudo passa no fim pela educação mesmo, treinamento.

As respostas dos entrevistados apontam indícios e motivações para o estabelecimento de possibilidades associadas a um senso de vulnerabilidade permanente e a condutas mais adequadas para as situações de risco apresentadas pelos espaços digitais. Apresentam práticas jornalísticas relevantes relacionadas às possibilidades de vigilância das comunicações digitais e alguns aspectos negligenciados pelos profissionais. Também são identificadas algumas ferramentas e posturas que podem minimizar formas de intrusão comunicacional e vulnerabilidades presentes nas investigações jornalísticas contemporâneas.

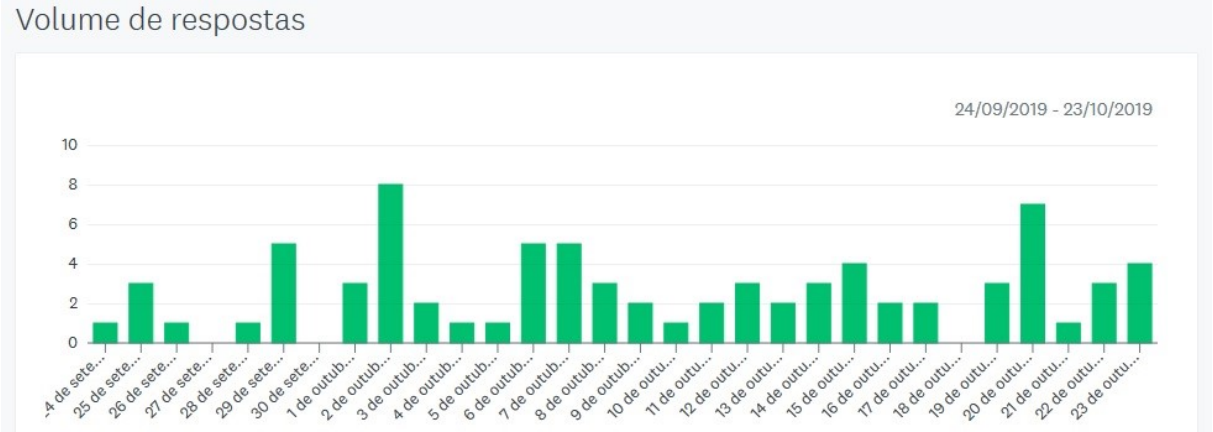
4.2 PERCEPÇÕES DOS JORNALISTAS QUE ATUAM EM UM CONTEXTO DE RISCO

Na última etapa do estudo, utilizamos a técnica de pesquisa *survey,* baseada na amostragem bola de neve (GOODMAN, 1961) que serviu de base para estruturação da amostra, e para aplicação de questionários a jornalistas investigativos ligados à abordagem de assuntos sensíveis. A partir da análise das entrevistas em profundidade e do mapeamento de relatórios e tipificação de casos concretos, avaliamos e estabelecemos contato com jornalistas investigativos brasileiros para aplicação do questionário. Basicamente, a bola de neve é uma técnica que permite fazer uma amostragem não probabilística que ocorre a partir da seleção, intencional ou de acordo com a conveniência, de um sujeito com características predefinidas. A partir de uma abordagem aleatória, que restringe o grupo analisado, sujeitos selecionados indicam outros indivíduos para integrar a amostra.

Para elaboração do roteiro de perguntas do questionário, estabelecemos elementos para aferir a percepção dos jornalistas no que diz respeito a aspectos percebidos, adequados e negligenciados nas investigações jornalísticas realizadas em espaços digitais vigiados. A partir dos subsídios das etapas anteriores do estudo, discutimos e verificamos pontos relevantes e as bases para o formulário da *survey* (apêndice B). De maneira geral, as condições estabelecidas foram: convite personalizado para recrutamento e pedido para indicação de mais profissionais; recrutamento por e-mail e por ferramentas digitais; possibilidade de convite para participações pontuais por meio de canais de comunicação da preferência dos jornalistas (aplicativos de mensagens de texto criptografados, ferramentas criptografadas de bate-papo de áudio e vídeo, telefone pessoal e telefone fixo); questionários com tempo de resposta estimado entre 10 e 15 minutos; anuência com Termo de Consentimento Livre e Esclarecido – TCLE (apêndice F).

Após avaliarmos algumas ferramentas de pesquisa online, optamos pela utilização do serviço pago oferecido pela *SurveyMonkey* que viabiliza pesquisas personalizáveis e oferece possibilidades de análise e representação de dados. Inserimos o questionário na ferramenta no dia 24 de setembro de 2019 e iniciamos a coleta no dia seguinte. Optamos por realizar a coleta durante 30 dias (25 de setembro de 2019 a 25 de outubro de 2019) e recebemos o volume de respostas apresentado na figura 3.

Figura 3 – Volume de respostas por dia de coleta.



Fonte: Elaborada pelo autor, 2019.

Com base na definição do perfil dos sujeitos de pesquisa, que foi apresentado no início desse capítulo, formatamos uma lista com mais de 200 contatos de jornalistas para envio do formulário de pesquisa. Ao longo do período proposto enviamos 217 e-mails com formulário (nove foram devolvidos e quatro cancelados) e 27 links em aplicativos de mensagem (WhatsApp e Messenger). A rotina de coleta contava com o envio de cerca de 10 coletores por dia e lembretes com intervalo de cerca de quatro dias (foram enviados até seis lembretes para o mesmo contato).

Elaboramos uma estratégia de engajamento que contava com um processo de sensibilização dos jornalistas por meio da apresentação das características do estudo e dos objetivos da pesquisa de maneira transparente e concisa. No final do período de coleta, recebemos 78 respostas, com uma taxa de conclusão de mais de 80% e uma média de 8 minutos e 17 segundos para a conclusão do formulário. Após a revisão dos dados coletados na *survey,* os formulários incompletos foram excluídos da amostra, restando 60 respostas que foram validadas e apresentadas em gráficos e tabelas que podem ser vistas no apêndice E.

Figura 4 – Taxa de conclusão e tempo médio das respostas.

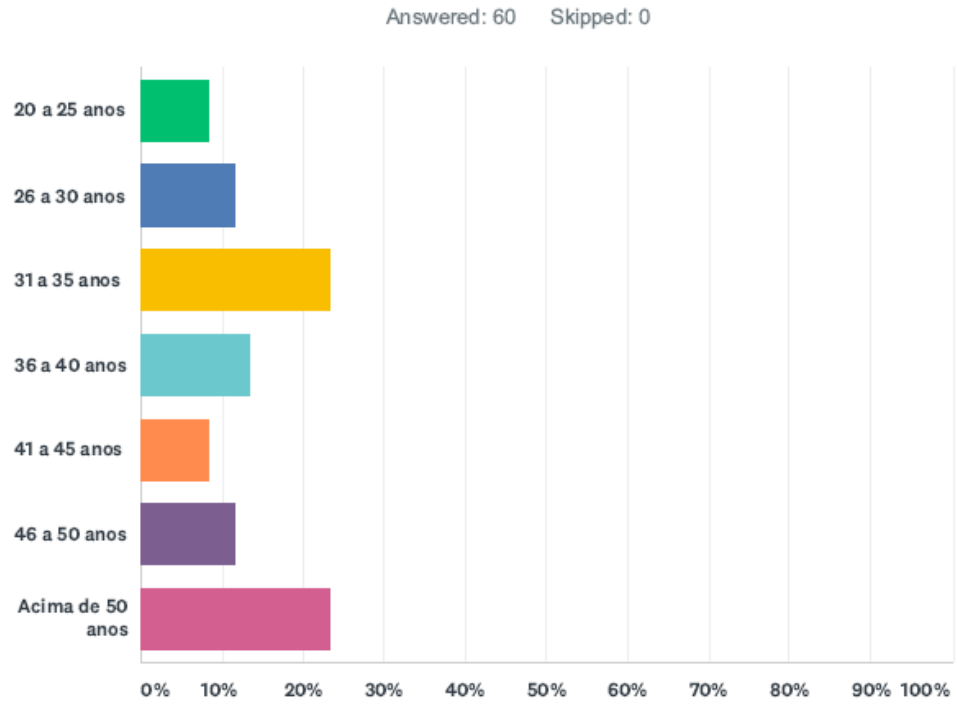
Fonte: Elaborada pelo autor, 2019.

Realizamos o backup dos resultados gerais e de todas as respostas individuais (conforme exemplo): *coletor - email invitation; iniciado em: segunda-feira, 30 de setembro de 2019 11:56:07; última modificação: segunda-feira, 30 de setembro de 2019 12:22:41; tempo gasto: 00:10:34; e-mail; endereço IP.* Cabe destacar, que não vamos disponibilizar as respostas individuais, para preservar o anonimato dos participantes da *survey.*

Os respondentes têm características pessoais e profissionais distintas, sendo que 40 são homens e 20 são mulheres. Vale destacar que o volume maior de respostas de homens está alinhado ao número de contatos obtidos durante o levantamento inicial, em sua maioria os jornalistas que preenchiam os critérios eram do sexo masculino. As respostas vieram das cinco regiões do Brasil, com predominância para a região Sudeste. (Norte - 3,33% [2]; Centro-Oeste - 11,67% [7]; Sul - 20,00% [12]; Nordeste - 21,67% [13]; Sudeste - 43,33% [26]). A maioria dos respondentes tem entre 31 a 35 anos (23,33% - 14) e mais de 50 anos (23,33% - 14) de idade.

A grande maioria dos jornalistas tem mais de 10 anos de carreira (43 respondentes) (10 deles têm de 6 a 10 anos e sete até 5 anos) e trabalha predominantemente na internet (68,33% [41]), sendo que 13 trabalham em jornal, 3 em TV, 2 em revista e 1 em rádio. Para 51 dos respondentes as ferramentas tecnológicas digitais são muito importantes para o jornalismo investigativo, oito acreditam que elas sejam importantes e um está indiferente. As respostas ratificam que o ambiente digital é um elemento central no cotidiano desses profissionais e na atuação durante investigações jornalísticas.

Gráfico 2 – Idade dos respondentes.



Fonte: Elaborado pelo autor, 2019.

Quanto ao nível de preocupação dos jornalistas com segurança digital, 42 respondentes afirmaram que em algumas oportunidades se preocupam com seus níveis de segurança no ecossistema digital, já 16 sempre estão preocupados, 1 nunca e 1 não sabia opinar. O número significativo de jornalistas investigativos preocupados, mais de 96%, combinado com a percepção sobre a possibilidade de ser vigiado digitalmente, que sempre está presente para 37 e às vezes para 20 dos respondentes, apenas 3 nunca se preocupam, indica que as problemáticas relacionadas às possibilidades de vigilância digital e intrusão comunicacional é significativa no universo de profissionais avaliados.

Esse fator é emblemático, pois está alinhado com a percepção dos jornalistas investigativos que participaram das entrevistas em profundidade. Diante desses dados, podemos afirmar que de maneira geral os jornalistas investigativos apresentam um nível significativo de preocupação e entendem que suas ações investigativas podem estar sendo vigiadas.

4.2.1 Aspectos ambientais e contextuais ligados às tecnologias digitais

As tendências indicadas a respeito das preocupações que tangenciam a vigilância digital envolvendo jornalistas investigativos foram consolidadas na verificação da utilização

da ampla gama de recursos e aspectos relacionados ao ambiente digital. As respostas dos jornalistas apresentaram elementos analiticamente relevantes sobre práticas de prevenção e segurança da informação jornalística. Em relação à existência de políticas de proteção de comunicações e informações no ambiente digital no local de trabalho dos jornalistas investigativos, 16,67% afirmaram que têm acesso a esse aspecto, 8,33% desconhecem a existência, a maioria (30%) não têm nenhum tipo acesso e 23,33% recebem apenas orientações para lidar com o tema, 21,67% não estão vinculados a uma empresa.

De forma particular, os respondentes acreditam que de alguma maneira os avanços tecnológicos das últimas décadas fizeram com que os jornalistas se preocupassem mais com segurança digital, 33,33% concordam totalmente com essa premissa e 65% parcialmente. Apenas um respondente discorda totalmente disso. A maioria dos participantes (55%) concorda que atualmente os jornalistas enfrentam formas de vigilância comunicacional digital por governos e corporações no Brasil, 35% concorda parcialmente com essa percepção e 10% não sabem responder.

Cabe salientar que as respostas referentes a possibilidade de vigilância nos espaços digitais está conectada com a percepção geral apresentada na etapa de entrevistas em profundidade, assim como o sentimento de necessidade de intensificação dos cuidados com a privacidade das fontes e pessoas mencionados em investigações sensíveis. 45% sempre tomam essas medidas e 55% aumentam os cuidados em situações específicas.

Quando perguntados sobre as providências ou atitudes relacionadas à própria proteção diante de possibilidades de vigilância comunicacional digital, a maioria (48,33%) apontou que às vezes adota medidas de prevenção de riscos digitais e 43,33% sempre estão munidos delas. Apenas 8,33% dos respondentes afirmaram que nunca adotaram estratégias e medidas de prevenção. Em relação ao nível de preocupação sobre as formas de vigilância empregadas no ambiente digital, boa parte dos respondentes se dizem preocupados (56,67%) ou muito preocupados (31,67%) com o contexto de atuação dos jornalistas. 10% estão pouco preocupados e apenas um está despreocupado com a situação.

Aproximadamente 88% dos respondentes relataram estar preocupados com as possibilidades de vigilância em relação a diferentes vulnerabilidades presentes no trabalho de investigação jornalística, como o sigilo das fontes e informações sensíveis. Neste momento, a pesquisa aponta que a vigilância comunicacional digital tem afetado as condutas dos jornalistas no Brasil. Mais da metade dos participantes acredita que o governo brasileiro possivelmente coleta os seus dados (51,67%) e 23,33% têm certeza disso, 18,33% não sabem responder e 6,67% acreditam que o governo não coleta os seus dados. A compreensão dos

impactos mais dramáticos da vigilância digital sobre os jornalistas perpassa essas inúmeras percepções e as condicionantes que podem modular as suas ações durantes investigações.

4.2.2 Tratamento da informação e contato com fontes diante da vigilância digital

Múltiplas arenas moldam a interseção entre vigilância digital e jornalismo investigativo, aspectos relacionados à transparência das ações e o cuidado durante investigações que impõem riscos digitais desempenham papéis distintos. No cenário ideal, os jornalistas procuram simultaneamente expor as informações de interesse público e preservar os dados sensíveis da apuração. Neste contexto, o tratamento das informações e o contato com as fontes, que devem permanecer anônimas, ganham nuances importantes atrelados a práticas de segurança da informação e contramedidas de vigilância digital que podem mitigar riscos conectados ao jornalismo investigativo contemporâneo.

No que diz respeito ao tratamento da informação, a possibilidade de intrusão comunicacional interfere em algumas oportunidades (53,33%) no cotidiano de trabalho da maioria dos jornalistas que abordam temas sensíveis, sendo que para 11,67% dos profissionais essa possibilidade sempre afeta a rotina cotidiana. Na opinião de 21,67% dos respondentes, as formas de intrusão comunicacional nunca afetam as suas atividades, já 13,33% não sabiam opinar. Um número significativo de respondentes demonstra que os problemas decorrentes das vulnerabilidades comunicacionais já afetam o trabalho de inúmeros jornalistas investigativos.

Na opinião da ampla maioria dos participantes (66,67%), a preservação dos seus dados pessoais é muito importante para que desempenhem o trabalho de investigação jornalística, 25% acham importante, 6,67% dos respondentes estão indiferentes a preservação dessas informações e um acredita que elas não têm nenhuma importância. Como já ressaltamos neste estudo, o campo do jornalismo investigativo enfrenta inúmeros desafios ligados à segurança digital que demandam esforços para manutenção de dados e informações confidenciais, no entanto as dimensões de vulnerabilidade alcançaram também a esfera pessoal e a privacidade dos profissionais.

Alinhado a essas demandas recentes, 55% dos jornalistas adotam medidas de segurança para preservar os seus dados pessoais às vezes, 40% têm medidas de mitigação de riscos digitais permanentes. Apenas 5% dos profissionais nunca se previnem contra essas vulnerabilidades digitais. As respostas apontam que a segurança digital está se tornando uma questão crucial para os jornalistas investigativos e, consequentemente, em um contexto

histórico mais amplo, a segurança da informação jornalística pode ser fomentada por medidas de aculturação de um grupo específico do segmento profissional.

Há algumas décadas, os jornalistas passaram a utilizar tecnologias digitais para realizar atividades de investigação jornalística, se comunicar com suas fontes e disseminar os resultados do trabalho. Imersos nessa realidade, a maioria dos respondentes (53,33%) faz uso pontual de ferramentas de criptografia e outras formas de segurança digital. Outros 26,67% sempre fazem uso dessas possibilidades e 16,67% nunca lançam mão dessas alternativas. Dois participantes não sabiam opinar sobre essa questão.

Em um ambiente de vigilância digital generalizada, particularmente sobre atividades comunicacionais, o contato com fontes sensíveis tornou-se uma interação de alto risco. No que tange às estratégias para proteção das fontes, 76,67% dos respondentes sempre adotam medidas para resguardar as suas identidades, 21,67% tomam medidas em algumas oportunidades e um não sabia responder. As formas de contato que habitualmente são adotadas nas interações com fontes que têm informações sensíveis variam bastante, entretanto a maior parte dos participantes (80%) apontou o contato pessoal como estratégia predominante e mais da metade (51,67%) utiliza aplicações de mensagens para estabelecer contato, 6,67% dos jornalistas investigativos descreveram outras formas de interação com as fontes, em geral, eles utilizam e-mail, aplicativos de mensagem e sistemas criptografados, chave PGP[185] e contatos via Deep Web[186].

> No caso do e-mail, utilizo criptografado (geralmente os que dão possibilidade de usar mensagens autodestrutivas, como o ProtonMail[187]). O trabalho obriga a usar vários e-mails. No meio deles, há não criptografados e criptografados. No contato com fontes de temas sensíveis, uso o criptografado[188].

A grande maioria dos respondentes (70%) sempre utiliza servidores de e-mail de corporações transnacionais, por exemplo, o Gmail, o Yahoo e a Microsoft, 26,67% às vezes utilizam e apenas 3,33% nunca usam esses serviços.

[185] O padrão que em inglês significa Pretty Good Privacy foi criado em 1991 e foi constantemente aprimorado até se tornar uma sofisticada ferramenta de proteção para e-mails e outras formas de contato online contravigilância.
[186] É uma parte da web que não é indexada pelos mecanismos de busca (exemplo: Google) e desta forma, fica oculta ao público massivo. O termo geral classifica diversas redes de sites distintas que não se comunicam.
[187] É um serviço de correio eletrônico criptografado.
[188] Fragmento da resposta alternativa da questão número 21.

Figura 5 – Formas de contato com fontes sensíveis.

OPÇÕES DE RESPOSTA		RESPOSTAS	
Contato por telefone		41,67%	25
Contato por e-mail		36,67%	22
Contato por aplicações de mensagem		51,67%	31
Contato por redes sociais		13,33%	8
Contato pessoalmente		80,00%	48
Adoto outras formas de contato (quais?)	Respostas	6,67%	4

Fonte: Elaborada pelo autor, 2019.

Quando questionados sobre a utilização de contas de e-mail "falsas" ou participação de fóruns online e salas de bate-papo usando nomes de usuários anônimos durante investigações jornalísticas 26,67% dos participantes indicaram que já utilizaram essas estratégias e 73,33% não fizeram uso desses artifícios. A maioria dos respondentes adota medidas preventivas durante investigações jornalísticas que abordam temas sensíveis. Desta forma, 8,33% sempre tomam essas atitudes e 53,33% adotam em situações pontuais. Um número significativo de jornalistas (35%) nunca faz isso e dois não sabiam responder.

Em relação ao uso de criptografia para se comunicar com fontes por meios digitais, mais da metade dos respondentes indicaram a utilização destes métodos em algumas oportunidades (56,67%), 16,67% dos profissionais sempre utilizam essa possibilidade e 20% nunca fazem uso. Além disso, 6,67% não sabiam responder. Quando responderam o formulário, 58,33% dos profissionais estavam trabalhando pontualmente em investigações jornalísticas que contavam com fontes anônimas. A maioria das investigações de 15% dos respondentes e todas ou quase todas de 8,33% dos participantes, também contavam com fontes com essa característica. Nenhuma das investigações de 11,67% dos demais jornalistas contava com fontes anônimas e 6,67% preferiram não revelar.

No cenário atual, medidas de contravigilância e prevenção de violações de dados dos jornalistas investigativos não são apenas recomendáveis, mas uma necessidade. Variáveis relacionadas a diferentes atores, incluindo provedores de telecomunicações, empresas de tecnologia da informação e instituições governamentais, devem ser consideradas durante a atuação dos jornalistas investigativos. Os profissionais que adotam medidas mitigatórias buscam proteger as suas fontes em um cenário que impõe riscos e impele o trabalho de apuração de temas sensíveis. Nesse contexto, as possibilidades de intrusão comunicacional e vigilância digital podem ocasionar efeitos que refletem formas de autocensura na abordagem

de temas que envolvem riscos digitais e não utilização das potencialidades comunicacionais do ambiente comunicacional.

4.2.3 Medidas de segurança digital adotadas pelos jornalistas

Como já afirmamos, as tecnologias digitais afetaram de maneira significativa as investigações jornalísticas e a forma como os jornalistas desenvolvem as suas apurações, interagem com as suas fontes e coordenam as suas ações. Paralelamente, os profissionais estão cada vez mais expostos a possibilidades de vigilância digital que apresentam riscos e ameaças específicas que demandam a capacidade de encontrar espaços e ferramentas digitais menos vulneráveis para realizar o seu trabalho.

As percepções gerais dos respondentes sobre práticas específicas de segurança digital perpassam a utilização de *softwares* que permitem navegar na internet anonimamente, como Tor[189] e Tails[190], em seus computadores, tablets ou telefones. 23,33% dos respondentes utilizam essas ferramentas, 35% conhecem, mas acham a utilização desnecessária. É significativo o número de participantes que desconhecem essa possibilidade 41,67%. No que tange à utilização de *softwares* de criptografia de e-mail, 26,67% dos jornalistas fazem uso dessa possibilidade, 23,33% conhecem, mas acham desnecessário utilizar e 50% desconhecem essa forma de diminuição de riscos digitais.

Em relação à utilização de serviços criptografados de nuvem, como o *SpiderOak*[191], apenas 8,33% dos participantes responderam afirmativamente, 30% conhecem essa possibilidade, mas acreditam que a sua utilização seja desnecessária e a ampla maioria (61,67%) desconhece essa possibilidade. Os *plug-ins* de navegação relacionados à privacidade, como *Privacy Badger*[192] ou *DoNotTrackMe*[193], são utilizados por 23,33% dos respondentes, 16,67% conhecem essas possibilidades, mas acham a sua utilização desnecessária, 60% dos participantes desconhecem essas ferramentas.

[189] TOR é um software livre e de código aberto que possibilita comunicação anônima na navegação pela Internet e em atividades online.
[190] Tails é um sistema operacional que pode ser utilizado em diversos computadores a partir de uma memória USB. Tem o objetivo de preservar a privacidade e o anonimato do usuário durante a utilização da internet, para evitar censura. Desta forma, as conexões feitas à internet passam necessariamente pela rede Tor. O usuário pode optar por não deixar rastros no computador que estiver utilizando e usar ferramentas criptográficas em seus arquivos, e-mails e mensagens instantâneas.
[191] É uma ferramenta de colaboração que oferece o serviço de backup e hospedagem de arquivos online que permite aos usuários acessar, sincronizar e compartilhar dados usando um servidor baseado em nuvem.
[192] É uma extensão de navegador gratuita e de código aberto, criada pela *Electronic Frontier*, que bloqueia automaticamente rastreadores invisíveis.
[193] É uma extensão de navegador gratuita usada para bloquear rastreadores na internet. Foi desenvolvida por uma empresa privada que oferece soluções conectadas com a privacidade.

O disco rígido do computador de trabalho de 80% dos respondentes está desprotegido, 30% acham desnecessário utilizar criptografia e 50% não conhecem essa possibilidade. Apenas 20% utilizam essa forma de mitigação de riscos digitais. Mecanismos de pesquisa que melhoram a privacidade, como o *DuckDuckGo* [194] , são utilizados por 21,67% dos participantes, 25% conhecem essa possibilidade, mas acham desnecessário utilizá-la. Mais de 50% dos respondentes indicou desconhecer esse tipo de ferramenta.

Softwares de proteção de senhas são utilizados pela metade dos respondentes, 26,67% deles conhecem esses instrumentos, mas acreditam que eles sejam desnecessários, e 23,33% dos participantes desconhecem essa possibilidade. A criptografia em aplicativos de bate-papo online, como o *CryptoCat*[195], não são conhecidos por 65% dos respondentes, apenas 11,67% utilizam e 23,33% conhecem, no entanto acreditam que seja desnecessário utilizar.

O alto grau de desconhecimento das possibilidades de mitigação de riscos digitais apontado pelos jornalistas investigativos que participaram da *survey* demonstra a necessidade de disseminação dos recursos oferecidos por esse tipo de capacidade para atuação em ambientes digitais nocivos. Mesmo entre os profissionais que conhecem a potencial diminuição de vulnerabilidades, um número significativo demonstra a inexistência da consciência dos riscos e ameaças oferecidos pelo ambiente digital. Os comportamentos e percepções apresentam tendências nos hábitos de segurança digital dos jornalistas e algumas de suas motivações para usar suas próprias abordagens.

Uma das formas mais comuns de exposição a ataques digitais é o uso de redes sem fio públicas em bibliotecas, cafés, durante viagens, etc. Mais de 80% dos participantes indicaram que fizeram esse tipo utilização, outros 16,67% adotam uma postura associada à mitigação de riscos e não utilizam redes públicas. As maneiras de acesso aos conhecimentos relacionados à segurança comunicacional digital são variadas, 45% dos respondentes participaram de eventos de jornalismo, seminários ou webconferências de capacitação. Dois receberam treinamento ou instrução formal na organização de notícias em que trabalham ou trabalharam. Cursos relacionados à segurança digital ou ao jornalismo foram apontados por sete participantes, 40% dos respondentes não receberam treinamento com recomendações sobre como manter seus telefonemas, e-mails ou outras comunicações online seguras.

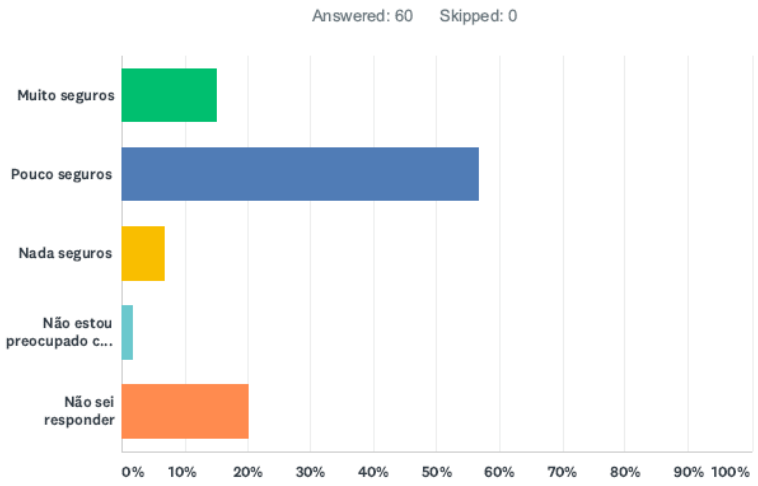
[194] É um buscador que utiliza informações de origem crowdsourcing (colaboração por meio do conhecimento e da participação coletiva) para melhorar a relevância dos resultados, enfatiza a privacidade e não registra as informações do usuário.
[195] É um aplicativo desktop de código aberto destinado a permitir bate-papos criptografados, oferece criptografia ponta a ponta para proteger todas as comunicações com outros usuários da ferramenta de comunicação digital.

O alto número de respondentes que não teve acesso a fontes de conhecimento e informações sobre técnicas de segurança digital pode ser associado ao baixo índice de senso de vulnerabilidade apresentado pelos participantes. O desconhecimento das abordagens e técnicas para proteção e mitigação da vigilância digital nociva enaltece a necessidade de uma cultura de riscos digitais para jornalistas que abordam temas sensíveis.

Durante as entrevistas em profundidade, a falta de acesso a informações e conhecimentos relacionados aos riscos e possibilidades digitais também foram apontados como a principal vulnerabilidade enfrentada pelos jornalistas que abordam temáticas delicadas na atualidade. O aprendizado de práticas digitais seguras e a percepção sobre os possíveis impedimentos impostos pelas possibilidades de intrusão comunicacional e de vigilância digital impõem aos profissionais capacidades que demandam um esforço complementar no trabalho de investigação jornalística, mais do que informados, os profissionais precisam estar dispostos a adotar condutas seguras durante as investigações.

Os níveis de segurança das ações de investigação jornalística estão diretamente conectados com a segurança dos dados e informações que estão nos equipamentos eletrônicos e nas interações dos jornalistas investigativos. No que tange a esta dimensão, a maioria dos participantes apontaram que as suas ferramentas e dados estão pouco seguras (56,67%) ou nada seguras (6,67%), sendo que 20% não sabiam responder. Apenas 15% dos profissionais afirmaram que apresentam níveis muito seguros de preservação das informações digitais. Um dos participantes indicou não estar preocupado com a segurança dos seus dados e informações.

Gráfico 3 – Percepção de segurança dos dispositivos e dados.



Fonte: Elaborado pelo autor, 2019.

Ao mesmo tempo em que os jornalistas entendem a importância de resguardar a segurança de suas fontes e informações digitais, eles são confrontados com a vulnerabilidade de segurança dos seus dispositivos e dados. Profissionais que abordam temas sensíveis precisam buscar preservar suas comunicações com fontes, assim como adotar contramedidas para mitigar potenciais formas de vigilância digital e intrusão comunicacional. A adequação a essas condicionantes e táticas de modulação dependem de uma série de custos, particularmente, ligados à usabilidade e à comodidade durante a utilização de ferramentas ofertadas pelo ambiente digital.

Conforme a maior parte das respostas demonstrou, as necessidades de segurança se aplicam de forma mais aguda em momentos, situações e contextos específicos. Além disso, a possibilidade de acesso às informações e ao aprendizado podem influenciar de maneira singular nas decisões e posturas dos jornalistas investigativos no que diz respeito às medidas de segurança digital. Os custos do uso de estratégias de segurança vão depender do contexto e das necessidades que a investigação jornalística apresentar.

Na maioria das ocasiões, ao lidar com fontes de rotina, os jornalistas investigativos não precisam de estratégias de segurança digital estritas. Entretanto, é essencial que expressem preocupações quanto à confidencialidade de suas formas de comunicação com fontes sensíveis, para não as colocar em risco. De maneira geral, a maioria dos participantes da *survey* apresenta abordagens inconsistentes em relação à segurança digital. Por razões de conveniência e desconhecimento, muitos jornalistas renunciam a medidas de segurança mais abrangentes. Na prática investigativa, as recomendações associadas à preservação e à mitigação de riscos digitais compete com outros aspectos das rotinas jornalísticas, como a velocidade, a facilidade de acesso e as convenções atreladas a utilização de ferramentas digitais amplamente disseminadas.

4.2.4 Indicações de jornalistas vigilantes

Por fim, com base na técnica de amostragem bola de neve, pedimos que os respondentes indicassem jornalistas investigativos (apontando nome e e-mail) que poderiam participar da *survey.* Ao longo dos 30 dias de coleta, recebemos 22 respostas que totalizaram a indicação de 39 contatos. Além disso, requisitamos aos participantes que tivessem mais observações sobre o estudo que deixassem os seus relatos, particularmente exemplos de como a vigilância comunicacional digital e o hackeamento impactaram nos seus trabalhos de investigação jornalística.

Foram registradas sete respostas, três delas eram apenas observações gerais: “Gostaria de receber o resultado desse estudo”; “Nada a acrescentar”; “Achei sensacional este estudo. Vem num momento muito importante para a imprensa de forma geral. E me relatou ferramentas de segurança digital que sequer tinha conhecimento”. Outra era uma sugestão de aprimoramento.

> Poderia perguntar que medidas os repórteres tomam para não terem seus dados (telefones e laptops) furtados quando estão em locais públicos (Congresso Nacional, mesmo salas do Ministério Público, delegacias de polícia, cafés e etc.) e que medidas preventivas tomaram para, em caso de furto dos equipamentos, tornar os conteúdos 1- inacessíveis aos ladrões e 2- acessíveis ao jornalista vítima do furto[196].

Guias de segurança para jornalistas recomendam que sejam utilizadas técnicas de obscurecimento e criptografia de dados para ajudar a gerenciar e proteger dispositivos e informações digitais. Na prática, os jornalistas investigativos apresentaram uma variedade de dúvidas em relação à possibilidade de vigilância digital e como eles podem se resguardar dela. As ferramentas e técnicas de diminuição de riscos possibilitam uma situação mais segura, entretanto podem ser um empecilho no contato com as fontes e com outros profissionais que não estejam dispostos a adotar tais medidas. A modelagem de ameaças e riscos e as práticas de segurança digital devem ser correspondentes aos limites impostos pelos atores e contextos em que as investigações jornalísticas estiverem inseridas. Um dos relatos retrata estes elementos condicionantes.

> Já passei por vários episódios em que desconfiei de espionagem, pois cobria indústrias onde isso é comum: petróleo e mineração. Mais recentemente publiquei reportagem que denunciava grande empresa (de outro ramo) em veículo de grande circulação e meu site foi invadido na mesma ocasião. Então implementei mais segurança nele. Mas ainda assim sinto que somos vigiados e gostaria muito de receber treinamento. Boa sorte na pesquisa[197].

Como já salientamos, formas modernas de vigilância digital possibilitam a coleta, agregação e análise generalizada de dados. Esse potencial pode ser utilizado e se transformar em possibilidades de ataques e intrusão comunicacional contra jornalistas que trabalham com fontes confidenciais e informações sensíveis. O planejamento de abordagens de temáticas desse tipo deve envolver necessariamente a avaliação dos dados que podem ser transmitidos por meio de seus instrumentos, canais de comunicação e potenciais ameaças aos seus dados pessoais. Casos descritos no relato de um dos respondentes demonstram a urgência da tomada de medidas de preservação das informações, por parte dos jornalistas investigativos.

[196] Relato realizado na questão número 39.
[197] Relato realizado na questão número 39.

> Certa vez, uma fonte com quem conversava para uma denúncia me relatou ter sido procurada por um gestor público municipal, que tinha em mãos trechos de nossas conversas por aplicativos de mensagens. Suspendi imediatamente o uso deste serviço em coberturas do tipo. Em outra investigação, fui procurado por um agente de segurança que me informou que partes de uma cobertura em andamento estavam sendo compartilhadas em grupos de WhatsApp de facções criminosas. Neste segundo caso, removemos todo o conteúdo que já estava disponível com identificação e passamos a não assinar e a preservar a imagem dos envolvidos nas matérias[198].

As ameaças e riscos potenciais envolvem cada vez mais o uso de tecnologias digitais de comunicação. Desta forma, se os jornalistas vigilantes tomarem conhecimento das possibilidades de vigilância, em suas diversas formas, podem restringir o acesso aos seus dados, utilizar navegadores mais seguros, ferramentas de criptografia e software de anonimização, dentre outras ações que mitiguem os seus níveis de exposição.

> Outro caso, este extremamente comum, diz respeito a reportagens que impactem de forma direta a categoria de policiais militares do Ceará. Em pelo menos cinco situações, fui alertado de que imagens minhas estavam circulando em grupos de policiais com legenda que me acusava de ser "inimigo" da corporação. Quanto ao tema em geral, a impressão que tenho é de que a maioria dos profissionais está ciente da existência dos riscos de segurança online, mas não se considera um “alvo” em potencial para este tipo de interceptação. Em linguajar bem popular, se acham “peixes pequenos” demais para atrair este tipo de atenção[199].

Conforme indicado não apenas pelos jornalistas vigilantes entrevistados, como também pelos participantes da *survey,* os jornalistas aplicam ferramentas e técnicas de segurança digital seletivas e alinhadas ao contexto em que estão atuando. Como já destacamos, as práticas de segurança digital têm custos que podem ser substanciais e inconvenientes (tempo, esforço e, em algumas ocasiões, investimento financeiro). Elementos e fatores essenciais trabalhados no capítulo 4 devem balizar as escolhas dos jornalistas vigilantes na adoção de ferramentas e técnicas que proporcionem maior nível de segurança.

> Na verdade, ainda é uma preocupação pouco avaliada por jornalistas que atuam nessa área - digo isso de modo geral. Claro, há muitos que se preocupam, mas falo em linhas gerais. Queria ressaltar sobre uma das respostas que produzo material tanto para jornal, como para internet e rádio, pois meu material é aproveitado em todas as plataformas. Penso que deveria ser um tema mais estimulado e difundido, esse da proteção de redes utilizadas por jornalistas de qualquer área de atuação[200].

Aprender e ter acesso aos conhecimentos relacionados às vulnerabilidades e às potencialidades do ecossistema digital são características que foram enaltecidas no decorrer desse estudo. A assimilação dessas informações pode ampliar o entendimento dos

[198] Trecho de relato realizado na questão número 39.
[199] Trecho de relato realizado na questão número 39.
[200] Relato realizado na questão número 39.

profissionais em relação a questões-chave que envolvem a vigilância digital, formas de intrusão comunicacional e os elementos que tangenciam essas problemáticas.

Consequentemente, os profissionais poderão refletir sobre as suas práticas e entender como o contexto que emerge dessas situações afeta os seus cotidianos profissionais. Desta forma, o comportamento dos jornalistas investigativos poderá ser alterado e posturas ligadas à formatação de uma cultura de segurança digital para jornalistas que abordam temas sensíveis seriam mais plausíveis. A partir desse panorama e do problema de pesquisa que orienta este estudo, buscamos apresentar diferentes formas de vigilância digital a que os jornalistas vigilantes estão expostos, motivar medidas e posturas conectadas com a segurança digital dos profissionais e verificar as suas percepções sobre o trabalho de investigação jornalística em ambientes digitais vigiados, intrusivos e nocivos.

Reforçamos a necessidade de preservação de um senso de vulnerabilidade permanente na utilização das ferramentas de comunicação digital. Essa postura exige a consciência de exposição a riscos, ameaças e a possibilidades de ataques digitais por parte dos jornalistas investigativos. A percepção desses elementos trará a noção de avaliação e possibilitará respostas mais eficazes. A necessidade de reflexão e planejamento das ações abrange atitudes elementares, como a proteção dos registros digitais e fontes sensíveis até a visualização das variáveis significativas de infraestrutura da informação, por exemplo, por onde os dados vão passar, quais são os servidores e provedores que serão utilizados.

Cabe ressaltar que parte dos jornalistas investigativos que participaram da pesquisa indicaram a utilização de padrões e técnicas de anonimização de vestígios durante apurações, emprego de criptografia nas comunicações e tráfego na internet por meio de *softwares* que mitigam riscos digitais. Alguns tomam cuidados na interação com fontes, como comunicar-se por meio de telefones descartáveis para dificultar formas de rastreamento e intrusão comunicacional. Outros profissionais renunciam as soluções técnicas, evitam deliberadamente o uso de dispositivos eletrônicos e tecnologias de comunicação digital e utilizam estratégias como por exemplo, encontrar fontes sensíveis pessoalmente. Como esperávamos, os resultados apontam, dentre outros elementos, algumas ações que estão sendo desenvolvidas pelos jornalistas investigativos no ecossistema de comunicação contemporâneo, assim como lacunas e problemáticas que envolvem a vigilância digital, o vazamento de dados e o acesso às novas fontes de informação no ambiente digital.

CONSIDERAÇÕES FINAIS

Nesse espaço de considerações finais, retomamos os principais aspectos desenvolvidos em cada um dos capítulos, o caminho percorrido no estudo e apresentamos uma síntese dos resultados. Basicamente, buscamos verificar entendimentos e transformações culturais que estão provocando revisões e adaptações nas práticas jornalísticas e oferecemos proposições, particularmente relacionadas ao processo de apuração e checagem na investigação jornalística de temas sensíveis.

Até aqui, a tese teve quatro capítulos. No primeiro, caracterizamos o conceito de vigilância em paralelo aos aspectos do jornalismo investigativo transpassado pelo ambiente digital, apresentamos as motivações e os desafios relacionados com a atividade jornalística em um contexto de vigilância digital massiva. Também indicamos a necessidade de adoção de uma cultura de segurança digital para jornalistas a partir de medidas de contravigilância.

No segundo capítulo, verificamos as particularidades da relação entre o jornalismo e a vigilância e, conforme um dos nossos objetivos específicos, discutimos os seus entornos, buscando perceber elementos de tensão entre o papel de vigilante que os jornalistas exercem na sociedade e o fato de que os próprios jornalistas estão sendo vigiados. Além disso, apresentamos uma noção de "jornalismo vigilante" que evidencia algumas características particulares da rotina dos profissionais que desenvolvem investigações perpassadas por ferramentas ofertadas pelo ambiente digital.

O terceiro capítulo tratou do mapeamento de relatórios de entidades representativas (nacionais e internacionais) que registram a incidência de ataques digitais, que são abordados como uma modalidade de risco profissional. Abordamos vulnerabilidades, ameaças e capacidades digitais. Formulamos uma equação simplificada para situações de exposição e vulnerabilidade iminentes, com base teórica e estrutural no "Manual de Proteção para Defensores de Direitos Humanos". A equação envolve três elementos: riscos digitais = ameaças digitais x vulnerabilidades digitais/capacidades digitais. Também tratamos de elementos essenciais da segurança digital para jornalistas, apontando um conjunto de ferramentas e possibilidades que podem ser exploradas pelos profissionais.

No quarto capítulo, evidenciamos os resultados alcançados nas entrevistas em profundidade e na *survey* aplicada no âmbito de jornalistas que tratam de temas sensíveis. Descrevemos detalhes das etapas que abordam elementos relacionados a métodos adotados em investigações jornalísticas no ambiente digital, percepção de riscos digitais por parte dos jornalistas investigativos, identificação das principais capacidades, vulnerabilidades e

ameaças digitais. Nessa etapa, avaliamos os dados coletados e detalhes do percurso metodológico adotado.

Utilizamos um conjunto de métodos e técnicas de pesquisa para verificar os elementos que formatam e tangenciam o que apontamos como proposição central deste estudo: o contexto atual de vigilância comunicacional em meios digitais exige dos jornalistas investigativos um senso permanente de sua vulnerabilidade e a adoção de uma cultura de segurança digital. A partir de quatro etapas distintas que contemplaram o desenvolvimento de uma pesquisa exploratória e revisão bibliográfica sobre questões elementares dos temas centrais do estudo, mapeamento de casos concretos e ações jornalísticas relacionadas com formas de vigilância digital, verificação de registros indicados em relatórios de agressões e ataques a jornalistas, entrevistas em profundidade com seis jornalistas vigilantes e aplicação de uma *survey* que contou com a participação de 78 jornalistas investigativos ligados à abordagem de assuntos sensíveis, apontamos práticas jornalísticas relevantes em matéria de vigilância de formas digitais de comunicação, aspectos negligenciados pelos profissionais, identificação de ferramentas e condutas para minimização da intrusão comunicacional, vulnerabilidades e potencialidades presentes nas investigações jornalísticas contemporâneas.

Dentre os principais resultados apresentados ao longo do estudo, indicamos aspectos contextuais e detalhes das intersecções entre práticas de jornalismo investigativo e formas de vigilância no ecossistema digital. Abordamos ações e condutas jornalísticas, *leaks* como fontes de dados e apuração, noções técnicas ligadas à internet, ferramentas de segurança digital para jornalistas. Com base na premissa de que o aumento da capacidade de vigilância comunicacional de governos e de corporações transnacionais vem modificando drasticamente o jornalismo investigativo, empregamos uma noção de jornalismo vigilante baseada em métodos (possibilidades/necessidades) e limitações (vulnerabilidades) associados à investigação jornalística contemporânea e ao contexto digital em que ela está inserida.

Balizados pelos relatos e indicações de jornalistas investigativos, demonstramos as principais mudanças na investigação jornalística no ambiente digital e a necessidade de apropriação de novos métodos associados com as possibilidades e vulnerabilidades do jornalismo investigativo diante da potencial vigilância nas comunicações digitais. A *survey* evidenciou regularidades e diferenças nas percepções sobre as possibilidades de vigilância digital contemporânea, apontando elementos ligados aos métodos adotados em investigações jornalísticas no ambiente digital, verificação de indícios conexos a consciência de riscos digitais, identificação de possíveis capacidades (utilização de ferramentas de segurança

atrelados com a comunicação digital), vulnerabilidades (como são realizados os contatos com as fontes) e ameaças (como são tratados os dados e informações sensíveis).

Verificamos como jornalistas vigilantes que desenvolvem investigações jornalísticas sobre temas sensíveis enfrentam as possibilidades de intervenção relacionadas à vigilância das comunicações, à interceptação, o armazenamento de dados pessoais e o monitoramento de ações jornalísticas no ecossistema digital. Esses elementos serviram de base para a discussão do problema de pesquisa: diante da vigilância digital massiva realizada por governos e corporações, quais são as principais vulnerabilidades e potencialidades do jornalismo investigativo brasileiro?

De maneira geral, dentre as inúmeras vulnerabilidades apontadas no estudo, destacam-se o desconhecimento sobre as possibilidades de vigilância, a desinformação sobre as formas de mitigação de riscos, a exposição digital voluntária e involuntária dos profissionais e de suas investigações. Como potencialidades, foram evidenciadas as possibilidades de compartilhamento de informações e colaboração, a facilidade de acesso a distintas formas de comunicação digital e a disponibilização de bancos de dados que subsidiam a apuração dos profissionais.

Ao mesmo tempo em que os jornalistas vigilantes percebem que os seus dados estão expostos, eles destacam a necessidade essencial de preservar essas informações, suas comunicações e fontes. Esses aspectos estão alinhados aos pressupostos da pesquisa que consideram que a investigação jornalística transpassada pelas possibilidades tecnológicas pode ser limitada por ferramentas de vigilância comunicacional. As ferramentas de comunicação digital facilitam a projeção de ações ligadas ao jornalismo, ativismo, hacktivismo e, ao mesmo tempo, fazem emergir a urgência da proteção das comunicações e fontes dos jornalistas.

Outro pressuposto que apontamos indica a desproporção entre a capacidade de vigilância do Estado e de grandes corporações transnacionais em relação ao jornalismo, o que gera consequências nocivas à democracia. A ampla maioria dos participantes da pesquisa expressou preocupação com a possibilidade de vigilância das comunicações digitais. Esse aspecto aponta que inúmeros jornalistas vigilantes estão percebendo que suas ações investigativas podem estar sendo vigiadas. Essa percepção pode se desdobrar em formas de cerceamento e constrangimento com consequências significativas nas abordagens e na revelação de informações de interesse público.

Em um ecossistema digital que impõe formas de vigilância onipresentes, as consequências políticas podem ter grande alcance e impacto. Nesse cenário, a vigilância

digital não é um fator remoto, mas uma realidade que afeta diretamente o trabalho de jornalistas, particularmente os que abordam temas sensíveis. As comunicações e ferramentas digitais são cada vez mais importantes para a apuração jornalística e a segurança digital se apresenta como uma necessidade urgente e crucial para os profissionais.

A potencial interceptação, intrusão e vigilância por parte de governos, corporações e criminosos que apresentamos nesse estudo demonstram uma paisagem crítica para atuação dos jornalistas vigilantes. Com base nesse contexto, defendemos a necessidade de estímulos e convenções relacionadas à formatação de uma cultura de riscos digitais para jornalistas. Uma constatação importante desse estudo é a ratificação dessa percepção apresentada pela ampla maioria dos sujeitos de pesquisa.

Abordamos também diferentes tipos de vigilância e suas intersecções com o jornalismo investigativo, como a vigilância digital odienta que trata das ameaças e constrangimentos que emergem das possibilidades comunicacionais e interativas disponibilizadas pelo ambiente digital. Essa prática afeta os jornalistas e consequentemente o trabalho que desenvolvem. Esses episódios apresentam potenciais desdobramentos danosos e consequências nocivas que estão sendo desconsideradas ou precariamente delineadas. Evidenciamos a necessidade premente de consideração, alerta e tipificação de ataques digitais relacionados ao jornalismo. No cenário atual, essa modalidade de ataque pode ser considerada uma forma de violência, limitação e controle da atividade jornalística.

Os resultados demonstram a necessidade da adoção de medidas de contravigilância que podem neutralizar e combater à vigilância por meio do ativismo baseado em pressupostos conectados com a liberdade de informação. Ações de antivigilância consideram princípios democráticos de responsabilidade e transparência. Esses movimentos disruptivos buscam romper a vigilância nociva por meio de mudanças políticas e ações de neutralização, em um sistema dinâmico que inclui e antecipa o comportamento de agentes de vigilância.

As entrevistas em profundidade fortaleceram e ratificaram a importância e a singularidade dos aspectos que tratam das limitações das investigações jornalísticas impostas pela vigilância digital, particularmente pelas formas de intrusão comunicacional do ambiente digital e a urgência da proteção das comunicações digitais de jornalistas que abordam temas sensíveis. Também atenderam ao objetivo principal deste estudo, examinando ações que envolvem o jornalismo investigativo, apontando potencialidades e vulnerabilidades do ecossistema digital.

Em linha com o objetivo principal, sinalizamos as principais dificuldades e ações que facilitam o tratamento e o aproveitamento das possibilidades abertas pelo ecossistema digital,

especialmente no que diz respeito aos grandes vazamentos e a interação de *whistleblowers*, fontes que subsidiam e originam investigações jornalísticas. Os dados da pesquisa apontam indícios e motivações para o estabelecimento de possibilidades associadas a um senso de vulnerabilidade permanente e a condutas mais adequadas para as situações de risco apresentadas pelos espaços digitais.

As informações coletadas apresentam também práticas jornalísticas relevantes relacionadas às possibilidades de vigilância das comunicações digitais e alguns aspectos negligenciados pelos profissionais. Também são identificadas algumas ferramentas e posturas que podem minimizar formas de intrusão comunicacional e vulnerabilidades presentes nas investigações jornalísticas da atualidade.

Para praticamente todos os participantes da pesquisa, as ferramentas tecnológicas digitais são muito importantes para o jornalismo investigativo. Esse indicativo ratifica que o ambiente digital é um elemento central no cotidiano desses profissionais e na atuação durante investigações jornalísticas.

Um número significativo de jornalistas vigilantes que participaram da *survey* está preocupado com segurança digital, mais de 96%. Combinado com a percepção sobre a possibilidade de ser vigiado digitalmente, que sempre está presente para a ampla maioria dos respondentes, podemos afirmar que as problemáticas relacionadas às possibilidades de vigilância digital e intrusão comunicacional são significativas no universo de profissionais avaliados. Esse é um fator importante que está alinhado à percepção dos jornalistas que participaram das entrevistas em profundidade.

Diante desses dados, podemos afirmar que, de maneira geral, os jornalistas investigativos apresentam um nível significativo de preocupação e entendem que suas ações investigativas podem estar sendo vigiadas. Também constatamos a presença de um baixo índice de políticas de proteção de comunicações e informações no ambiente digital no local de trabalho dos jornalistas, menos de 20% afirmaram que têm acesso a informações dessa natureza.

Os dados demonstram que de alguma maneira os avanços tecnológicos das últimas décadas fizeram com que os jornalistas se preocupassem mais com segurança digital. As respostas a respeito da possibilidade de vigilância nos espaços digitais estão conectadas com a percepção geral apresentada na etapa de entrevistas em profundidade, assim como o sentimento de necessidade de intensificação dos cuidados com a privacidade das fontes e das pessoas mencionadas em investigações sensíveis.

No que tange às providências e às atitudes a respeito da própria proteção em relação às possibilidades de vigilância comunicacional digital, as medidas de prevenção de riscos digitais são adotadas em situações pontuais, no entanto um número significativo de profissionais apontou sempre estar munido delas. Em relação ao nível de preocupação sobre as formas de vigilância empregadas no ambiente digital, a grande maioria dos respondentes se diz preocupado ou muito preocupado com o contexto de atuação dos jornalistas.

Mais de 80% dos participantes afirmam estar preocupados com as possibilidades de vigilância em relação a diferentes vulnerabilidades presentes no trabalho de investigação jornalística, como o sigilo das fontes e informações sensíveis. Neste momento, a pesquisa aponta que a vigilância comunicacional digital tem afetado as condutas dos jornalistas no Brasil. Mais da metade dos participantes acredita que o governo brasileiro possivelmente coleta os seus dados e mais de 20% deles têm certeza disso.

Um número significativo de respondentes demonstra que os problemas decorrentes das vulnerabilidades comunicacionais já afetam o trabalho de inúmeros jornalistas investigativos. Na opinião da ampla maioria dos participantes, a preservação dos seus dados pessoais é muito importante para que desempenhem o trabalho de investigação jornalística. Como já ressaltamos, o campo do jornalismo investigativo enfrenta inúmeros desafios ligados à segurança digital que demandam esforços para proteção de dados e informações confidenciais. As dimensões de vulnerabilidade alcançaram também a esfera pessoal e a privacidade dos profissionais.

Mais de 50% dos participantes adotam medidas de segurança para preservar os seus dados pessoais em algumas ocasiões e 40% têm medidas de mitigação de riscos digitais permanentes. As respostas apontam que a segurança digital está se tornando uma questão crucial para os jornalistas investigativos e, consequentemente, em um contexto histórico mais amplo, a segurança da informação jornalística pode ser fomentada por medidas de aculturação de um grupo específico do segmento profissional.

A maioria dos respondentes faz uso pontual de ferramentas de criptografia e outras formas de segurança digital. No que tange às estratégias para proteção das fontes, a maioria dos respondentes sempre adota medidas para resguardar as suas identidades. As formas de contato que habitualmente são adotadas nas interações com fontes que têm informações sensíveis variam bastante, no entanto a maior parte dos participantes apontou o contato pessoal como estratégia predominante. Mais da metade utiliza aplicativos de mensagem para realizar esses contatos, o que, como demonstramos, significa que esses profissionais estão sujeitos a ataques digitais. Os jornalistas descreveram outras formas de interação com as

fontes, por exemplo, utilização de e-mail, sistemas criptografados, chave PGP e contatos via Deep Web.

Alguns respondentes adotam medidas preventivas durante investigações jornalísticas que abordam temas sensíveis, como desligar o celular durante o contato com as fontes, porém um número significativo de jornalistas nunca faz isso. Em relação ao uso de criptografia para se comunicar com fontes por meios digitais, mais da metade dos respondentes indicaram a utilização em algumas oportunidades ou relataram que sempre utilizam essa possibilidade.

As percepções gerais dos respondentes sobre práticas específicas de segurança digital perpassam a utilização de *softwares,* como Tor e Tails que permitem navegar na internet anonimamente. Grande parte dos participantes conhecem ferramentas de mitigação de riscos digitais, mas acham a utilização desnecessária. Também é significativo o número de participantes que desconhecem essas possibilidades. O disco rígido do computador de trabalho de 80% dos respondentes está desprotegido. Em relação aos mecanismos de pesquisa que melhoram a privacidade, mais de 50% dos respondentes indicou desconhecer essa possibilidade. *Softwares* de proteção de senhas são utilizados pela metade dos respondentes e mais de 20% dos participantes desconhecem essa possibilidade. A criptografia em aplicativos de bate-papo online não é conhecida por 65% dos respondentes.

O alto grau de desconhecimento das possibilidades de mitigação de riscos digitais apontados pelos jornalistas investigativos que participaram da *survey* demonstra a necessidade de disseminação dos recursos oferecidos por esse tipo de capacidade para atuação em ambientes digitais nocivos. Dentre os profissionais que conhecem a possibilidade de diminuição de vulnerabilidades, um número significativo demonstra a inexistência de preocupação com riscos e ameaças oferecidos pelo ambiente digital. O uso de redes sem fio públicas é comum entre os participantes, mais de 80% indicaram que fizeram esse tipo utilização.

Chama a atenção o alto número de respondentes que não teve acesso a fontes de conhecimento e informações sobre técnicas de segurança digital. O desconhecimento das abordagens e técnicas para proteção e mitigação da vigilância digital nociva enaltece a necessidade de uma cultura de riscos digitais para jornalistas que abordam temas sensíveis. Como já mencionamos, os jornalistas vigilantes apontaram que a falta de acesso às informações e aos conhecimentos relacionados aos riscos e às possibilidades digitais é a principal vulnerabilidade enfrentada pelos jornalistas na atualidade.

O aprendizado de práticas digitais seguras e a percepção sobre os possíveis impedimentos impostos pelas possibilidades de intrusão comunicacional e de vigilância

digital impõem aos profissionais capacidades que demandam um esforço complementar no trabalho de investigação jornalística. Mais do que informados, os profissionais precisam estar dispostos a adotar condutas seguras durante as investigações.

No que diz respeito aos níveis de segurança dos dados e informações que estão nos equipamentos eletrônicos e nas interações dos jornalistas investigativos, a maioria dos participantes apontou que as suas ferramentas e dados estão pouco seguras ou nada seguras. Apenas 9 dos 60 profissionais afirmaram que apresentam níveis muito seguros de preservação das informações digitais. A maior parte dos participantes demonstrou que as necessidades de segurança se aplicam de forma mais aguda em momentos, situações e contextos específicos.

A possibilidade de acesso às informações e ao aprendizado podem influenciar de maneira singular nas decisões e posturas dos jornalistas investigativos em relação às medidas de segurança digital. Como já indicamos, os custos do uso de estratégias de segurança vão depender do contexto e das necessidades que a investigação jornalística apresentar. Por razões de conveniência e desconhecimento, muitos jornalistas renunciam a medidas de segurança mais abrangentes. Na prática investigativa, as recomendações associadas à preservação e à mitigação de riscos digitais compete com outros aspectos das rotinas jornalísticas, como a velocidade, a facilidade de acesso e as convenções atreladas à utilização de ferramentas digitais amplamente disseminadas.

Uma das principais limitações que encontramos na pesquisa está relacionada à definição dos parâmetros da amostragem. Nosso parâmetro inicial foi avaliar o número de associados da Associação Brasileira de Jornalismo Investigativo (Abraji) que conta com cerca de 320 sócios. Logo percebemos que o perfil desses sujeitos era heterogêneo, pois nem todos eram jornalistas que estavam atuando em investigações (pesquisadores, estudantes, jornalistas que atuavam em outras áreas, entre outros). Diante disso, definimos que adotaríamos uma estratégia não probabilística que apontaria tendências e percepções que não seriam generalizadas, e que se concentrassem apenas nas práticas de jornalistas investigativos.

Cabe ressaltar que o quadro de participações nas duas etapas finais da pesquisa preencheram as nossas expectativas. Para as entrevistas em profundidade, tínhamos previsto a realização de, no mínimo, três entrevistas (número sugerido pela banca de qualificação) e acabamos realizando seis devido às condições favoráveis de logística e disponibilidade dos profissionais. Convidar os jornalistas de maneira personalizada, por diferentes canais de comunicação digital, foi uma estratégia bem sucedida. Para a *survey,* previámos a participação de, no mínimo, 50 jornalistas investigativos. Ao longo dos 30 dias de coleta, alcançamos 78 participantes.

Escolher a interação e a abordagem mais acertada a ser utilizada nas conversas presenciais e no formulário de pesquisa com os jornalistas vigilantes também foi um desafio. A principal limitação nessa dimensão está ligada ao fato de que alguns jornalistas não se sentirem à vontade para falar das suas estratégias de segurança digital e terem dúvidas sobre como abordar temas como vigilância digital e intrusão comunicacional. Nessa perspectiva, não falar sobre temas relacionados à segurança digital também pode ser considerada uma medida de prevenção e proteção de estratégias e exposição a riscos.

Aspectos como desinformação e despreocupação sobre temas relacionados à segurança digital também apresentaram-se como limitações em alguns momentos. Temas sensíveis atrelados à segurança nacional também dificultaram o detalhamento das medidas de vigilância digital que já estão sendo adotadas no âmbito governamental no Brasil. Mesmo assim, conseguimos apontar indícios e situações de risco, ameaças e vulnerabilidades atreladas à vigilância digital no contexto brasileiro.

A dinâmica de evolução tecnológica constante e imediata também apresentou-se como uma limitação do estudo. As atualizações diárias das ferramentas de segurança digital exigem uma verificação regular das formas de mitigação de riscos, ameaças e ataques digitais. Essa condição reforça a necessidade de um senso de vulnerabilidade permanente por parte dos jornalistas investigativos que apontamos nesta pesquisa.

Estamos diante de significativas mudanças de procedimentos, de hábitos e de interferências que afetam diferentes dimensões do trabalho dos jornalistas vigilantes. Novas tecnologias que captam demandas já existentes na sociedade, necessidades preenchidas por recursos tecnológicos e as ferramentas comunicacionais contemporâneas estão determinando um período histórico sem precedentes para o jornalismo investigativo e os elementos que podem desencadear mudanças no comportamento dos profissionais. Novos estudos podem apontar respostas e constatações a esse respeito.

Conforme destacamos, um contexto vigiado gera o que pode ser classificado de liberdade parcial e essa constatação implica formas de opressão e constrangimento. Desempenhar o jornalismo investigativo nessas condições significa sujeitar-se e correr o risco de não explorar o potencial que o jornalismo vigilante tem em relação ao desenvolvimento da sociedade e da democracia.

REFERÊNCIAS

ABERT, **Violações à liberdade de expressão**, 2018. Disponível em: https://www.abert.org.br/web/images/Biblioteca/Liberdade/abert_relatorio_anual_2018_final_web.pdf. Acesso em: 06 out. 2019.

ABRAJI, **Como lidar com assédio contra jornalistas nas redes**, 2018. Disponível em: http://abraji.org.br/publicacoes/cartilha-como-lidar-com-assedio-contra-jornalistas-nas-redes. Acesso em: 17 nov. 2019.

AMERICAN CIVIL LIBERTIES UNION; HUMAN RIGHTS WATCH. "**With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy"**, 2014. Disponível em: https://www.aclu.org/report/liberty-monitor-all-how-large-scale-us-surveillance-harming-journ. Acesso em: 12 ago. 2018.

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: 06 out. 2019.

ARTIGO 19, **Violação à liberdade de expressão**, 2015. Disponível em: https://artigo19.org/?p=8022. Acesso em: 16 nov. 2019.

ARTIGO 19, **Violação à liberdade de expressão**, 2017. Disponível em: https://artigo19.org/?p=13739 Acesso em: 06 out. 2019.

ASSANGE, Julian. **Cypherpunks: liberdade e o futuro da internet**. São Paulo: Boitempo, 2013.

ATAMAN, Bora; ÇOBAN, Barış. Counter-surveillance and alternative new media in Turkey**.** Information, **Communication & Society**. v. 21, n. 7, Londres. p. 1014-1029. 2018. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/1369118X.2018.1451908. Acesso em: 19 jan. 2020.

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

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

BELL, Emily. Facebook is eating the world. 07/03/2016. **Columbia Journalism Review**. Disponível em: http://migre.me/tcvFv. Acesso em: 08 jul. 2018.

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

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

BELL, Emily *et al*. A imprensa nas plataformas: como o Vale do Silício reestruturou o jornalismo**. Revista de jornalismo ESPM/CJR**. São Paulo: ESPM, JUL-DEZ, 2017. Disponível em: https://academiccommons.columbia.edu/doi/10.7916/D8D79PWH. Acesso em: 30 set. 2018.

BENETTI, Márcia; LAGO, Cláudia. **Metodologia de pesquisa em jornalismo**. Petrópolis: Vozes, 2007.

BENNETT, Lucy. *et al*. Journalism, citizenship and surveillance. **Digital Journalism**, 2017. p. 256-261. Disponível em: https://www.tandfonline.com/doi/full/10.1080/21670811.2016.1266134. Acesso em: 28 ago. 2018.

BENTHAM, Jeremy. **El Panoptico**. Madrid: Las Ediciones de La Piqueta, 1979.

BERNSTEIN, Carl. WOODWARD, Bob. **Todos os homens do presidente**. Livraria Francisco Alves Editora S.A, 1978.

BEZERRA, Arthur Coelho. Vigilância e cultura algorítmica no novo regime global de mediação da informação. **Perspectivas em Ciência da Informação**, v.22, n.4, out-dez, 2017. p. 68-81. Disponível em: http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/2936. Acesso em: 19 jan. 2020.

BRADSHAW, P. Chiling Effect: Regional journalists' source protection and information security. **Digital Journalism**, 2016.

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

BRIGADAS INTERNACIONAIS DE PAZ (PBI); OFICINA EM WASHINGTON PARA ASSUNTOS LATINOAMERICANOS (WOLA), **Cambiando el curso de la impunidad.** Disponível em: https://www.wola.org/wp-content/uploads/2019/03/SPN_WOLA-PBI-2019.pdf. Acesso em: 17 nov. 2018.

BRUNO, Fernanda. Mapas de crime: vigilância distribuída e participação na cibercultura. **Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação | E-compós**, Brasília, v.12, n.2, mai-ago, 2009. Disponível em: https://academiccommons.columbia.edu/doi/10.7916/D8D79PWH. Acesso em: 30 set. 2018.

BRUNO, Fernanda. **Máquinas de ver, Modos de ser: Vigilância, tecnologia e subjetividade.** Porto Alegre: Editora Sulina, 2013.

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

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

CASTELLS, Manuel. **Redes de indignação e esperança:** Movimentos sociais na era da internet. Rio de Janeiro, RJ: Zahar, 2013.

CHRISTOFOLETTI, Rogério; OLIVEIRA, Cândida de. Jornalismo pós-wikileaks: Deontologia em tempos de vazamentos globais de informação. **Contemporânea: comunicação e cultura**, vol.09, n.02, agosto de 2011. P. 231-245. Disponível em: https://portalseer.ufba.br/index.php/contemporaneaposcom/article/view/5072. Acesso em: 30 set. 2018.

CHRISTOFOLETTI, Rogério. Privacidade e Regulamentação do Marco Civil da internet: registros e preocupações. **Revista ECO PÓS**. v. 18, n. 3, Rio de Janeiro. p. 213-229. 2015. Disponível em: https://revistas.ufrj.br/index.php/eco_pos/article/view/2150. Acesso em: 11 mar. 2016.

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

CHRISTOFOLETTI, Rogério; TORRES, Ricardo J. Jornalistas expostos e vulneráveis: ataques digitais como modalidade de risco profissional. **Revista Famecos**, Porto Alegre, v. 25, n. 3, setembro, outubro, novembro e dezembro de 2018: ID29210.

CHRISTOFOLETTI, Rogério. Percepções de jornalistas brasileiros sobre privacidade. **Matrizes**. v. 13, n. 2, São Paulo. p. 179-197. 2019. Disponível em: https://objethos.files.wordpress.com/2019/09/document.pdf. Acesso em: 19 jan. 2020.

CNMP, **Violência contra comunicadores no Brasil: um retrato da apuração nos últimos 20 anos**, 2019. Disponível em: http://www.cnmp.mp.br/portal/images/Publicacoes/documentos/2019/Violencia-contra-comunicadores-no-Brasil-VERSAO-FINAL-.pdf. Acesso em: 06 out. 2019.

COMMITTEE FOR JOURNALIST PROTECTION. **Seguridad de la información**. Manual de Seguridad para Periodistas, 2012. Disponível em: https://www.cpj.org/es/2012/04/seguridad-de-la-informacin.php. Acesso em: 06 out. 2019.

CONSTANTARAS, Eva. Lessons Learned From A Collaboration Without Borders in Latin America. **MEDIASHIFT**. 10 jan. 2013. Disponível em: http://mediashift.org/2013/01/lessons-learned-from-a-collaboration-without-borders-in-latin-america010/. Acesso em: 12 ago. 2018.

COLEMAN, Gabriella. How has the fight for anonymity and privacy advanced since Snowden's whistle-blowing?, **Media, Culture & Society**. 2019. Disponível em: https://journals.sagepub.com/doi/abs/10.1177/0163443719843867.Acesso em: 19 jan. 2020.

CORREIA, João Carlos. **O admirável Mundo das Notícias: Teorias e Métodos**. Covilhã: UBI, LabCom, 2011.

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: 06 out. 2019.

DEUZE, Mark. WITSCHGE, Tamara. O Que o Jornalismo está se Tornando. **Parágrafo**. v.4, n.2. São Paulo. p. 8-21. jul./dez, 2016. Disponível em: http://revistaseletronicas.fiamfaam.br/index.php/recicofi/article/view/478.Acesso em: 19 ago. 2018.

DÍAZ, M. **Agresiones 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: 06 out. 2019.

DUTRA, Luma Poletti. Direito à informação em pauta: os usos da lei de acesso por jornalistas. UNB, 2015. **Dissertação.** Disponível em: https://repositorio.unb.br/handle/10482/17909. Acesso em: 31 de mar. 2019.

EGUREN, Enrique. **Manual de Proteção para Defensores de Direitos Humanos**, Front Line, 2005. Disponível em: http://www.dhnet.org.br/dados/manuais/a_pdf/manual_frontline_defensores_dh.pdf. Acesso em: 06 out. 2019.

ELLSBERG, Daniel. **SECRETS: A Memoir of Vietnam and the Pentagon Papers.** Londres: Penguin Books, 2003.

EVANGELISTA, Rafael de Almeida. Capitalismo de vigilância no Sul Global: por uma perspectiva situada. **5o Simposio Internacional LAVITS - Vigilancia, Democracia y Privacidad en América Latina: Vulnerabilidades y resistências**, 2017. Chile, p. 243-253. Disponível em: http://lavits.org/wp-content/uploads/2018/04/08-Rafael-Evangelista.pdfAcesso em: 19 jan. 2020.

FENAJ, **Violência contra jornalistas e liberdade de imprensa no Brasi**l, 2018. Disponível em: http://fenaj.org.br/wp-content/uploads/2019/01/relatorio_fenaj_2018.pdf. Acesso em: 06 out. 2019.

FENAJ, **Violência contra jornalistas e liberdade de imprensa no Brasi**l, 2019. Disponível em: https://fenaj.org.br/wp-content/uploads/2020/01/relatorio_fenaj_2019.pdf. Acesso em: 19 jan. 2020.

FERNANDEZ, N.; MANCINI, P. **CryptoPeriodismo**. Manual Ilustrado Para Periodistas. Disponível em: http://cryptoperiodismo.org. Acesso em: 06 de out. 2019.

FORTES, Leandro. **Jornalismo Investigativo**. São Paulo: Editora Contexto, 2005.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**. Tradução: Raquel Ramalhete. Petrópolis - RJ, Vozes, 1987.

FUCHS, Christian. Como podemos definir vigilância?. **Matrizes**. Ano 5, nº 1. São Paulo. p. 109-136. jul./dez, 2011. Disponível em: https://www.revistas.usp.br/matrizes/article/download/38311/41154.Acesso em: 11 mar. 2016.

FUCHS, C.; TROTTIER, D. Internet Surveillance after Snowden: A Critical Empirical Study of Computer Experts' Attitudes on Commercial and State Surveillance of the Internet and

Social Media post-Edward Snowden. **Journal of Information, Communication & Ethics in Society.** p. 1-38. 2016. Disponível em: http://migre.me/v6nqA. Acesso em: 29 set. 2016.

FUNDACIÓN PARA LA LIBERTAD DE PRENSA. **Manual Antiespías: herramientas para la protección digital de periodistas**, 2015. Disponível em: https://www.flip.org.co/images/Documentos/manual-antiespias.pdf. Acesso em: 06 out. 2019.

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

GREENWALD, Glenn. O estado de vigilância. *In:* BELL, Emily *et al.* (org.). **Journalism After Snowden: The Future of Free Press in the Surveillance State.** New York: Columbia University Press, 2017.

GREENBERG, A. **This machine kills secrets**. New York: Dutton, 2012.

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

GÓMEZ, Karla Patricia Martínez. Periodismo digital y hacktivismo: el caso de anonymous en México análisis comparativo de la cobertura de la operación cartel em cuatro medios mexicanos. **Tese**. Universidad Autónoma del Estado de México, 2017. Disponível em: http://ri.uaemex.mx/bitstream/handle/20.500.11799/66675/Periodismo-Digital-y-Hacktivismo-split-merge.pdf?sequence=3&isAllowed=y. Acesso em: 16 nov. 2019.

GOODMAN, L. Snowball Sampling**. Annals of Mathematical Statistics**, 32, p. 148-170, 1961.

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: 06 out. 2019.

HEIKKILÄ, Heikki. Privacy under surveillance: Towards a conceptual analysis of the price of connection. **Northern Lights**, v. 16, 2018. p. 59–74. Disponível em: https://www.researchgate.net/publication/326977143_Privacy_under_surveillance_Towards_a_conceptual_analysis_of_the_price_of_connection. Acesso em: 19 jan. 2020.

HANSON, Nils. HUNTER, Mark Lee. **A Investigação a partir de Histórias: Um Manual para Jornalistas Investigativos**. Montevideo: UNESCO, 2013. Disponível em: unesdoc.unesco.org/images/0022/002264/226456POR.pdf. Acesso em: 30 set. 2018.

HARDING, Luke. **Os arquivos Snowden.** A história secreta do homem mais procurado do mundo. Rio de Janeiro: Leya, 2014.

HENRICHSEN, Jennifer R. BETZ, Michelle, LISOSKY. Joanne. **Cómo desarollar la seguridad digital para el periodismo.** Unesco, 2016. Disponível em: proledi.ucr.ac.cr/wp-content/uploads/2018/10/Seguridad-digital-para-el-periodismo.pdf. Acesso em: 17 nov. 2019.

INTERNATIONAL CENTER FOR JOURNALISTS. **The State of Technology in Global Newsrooms. 2017**. Disponível em: http://www.icfj.org/sites/default/files/ICFJTechSurveyFINAL.pdf. Acesso em: 08 jul. 2018.

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

KANASHIRO, Marta M. Apresentação: vigiar e resistir: a constituição de práticas e saberes em torno da informação. **Ciência e Cultura**, v. 68 n. 1, São Paulo jan./mar. 2016. p. 20-24. Disponível em: http://cienciaecultura.bvs.br/scielo.php?script=sci_arttext&pid=S0009-67252016000100010. Acesso em: 19 ago. 2018.

KARAM, Francisco José Castilho. **Jornalismo, ética e liberdade**. 4. ed. São Paulo: Summus, 2014.

KONOW-LUND, Maria. Negotiating Roles and Routines in Collaborative Investigative Journalism. **Media and Communication**, v. 7 n. 4, Lisboa, 2019. p. 103-111. Disponível em: https://www.cogitatiopress.com/mediaandcommunication/article/view/2401.Acesso em: 19 jan. 2020.

KOVACH, Bill; ROSENSTIEL, Tom. **The Elements of Journalism: What Newspeople Should Know and the Public Should Expect**. 3. ed. Nova York: Crown Publishers, 2014.

LEE, Micah; HEINRICHS, Randi. Entrevista: How to protect the truth? Challenges of cybersecurity, investigative journalism and whistleblowing in times of surveillance capitalism. **Ephemera**, v. 19 n. 4, San Francisco, nov. 2019. p. 807-824. Disponível em: http://www.ephemerajournal.org/issue/ethico-politics-whistleblowingmediated%C2%A0truth-telling-digital-cultures. Acesso em: 19 jan. 2020.

LEIGH, David. Conclusion: A Golden Age for Investigative Journalism?. *In*: Investigative Journalism: A Survival Guide, Londres: Palgrave Macmillan, 2019, p. 197-208.

LYON, David. **Surveillance after Snowden.** New York: Polity Press, 2015.

LYON, David. As apostas de Snowden desafios para entendimento de vigilância hoje. **Ciência e Cultura**, v. 68 n. 1, São Paulo jan./mar. 2016. p. 25-34. Disponível em: http://cienciaecultura.bvs.br/scielo.php?script=sci_arttext&pid=S0009-67252016000100011. Acesso em: 19 ago. 2018.

LYON, David. Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity. **International Journal of Communication**, Vol. 11, 2017, pp. 824-842. Disponível em: ijoc.org/index.php/ijoc/article/view/5527. Acesso em: 08 jul. 2018.

LYON, David. **The Culture of Surveillance: Watching as a Way of Life**. New York: Polity Press, 2018.

MAIA, Rousiley C. M. Mídia e diferentes dimensões da Accountability. **E-compós- Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação**, 2006. Disponível em: http://www.e-compos.org.br/e-compos/article/view/113. Acesso em: 30 set. 2018.

MANN, Steve. “Sousveillance”: Inverse Surveillance in Multimedia Imaging. **Anais da 12ª conferência internacional anual da ACM sobre multimedia.** Nova York, EUA, outubro de 2004, p. 620-627. Disponível em: https://dl.acm.org/citation.cfm?id=1027673. Acesso em: 16 nov. 2019.

MARCET. José María Caminos. **Periodismo de investigación: teoría y práctica**. Madrid: Síntesis, 1997.

MARÍN, Vicente Serrano. **Fraudebook: lo que la red social hace con nuestras vidas**. Madrid: Plaza y Valdés, 2016.

MARX, Gary T. A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. **Journal of Social Issues**, v. 59. mai. 2003. Disponível em: http://web.mit.edu/gtmarx/www/tack.html. Acesso em: 13 mar. 2016.

MARX, Gary T. Surveillance Studies. **International Encyclopedia of the Social & Behavioral Sciences**, 2ª Ed. v. 23. 2015, p. 733–741. Disponível em: http://web.mit.edu/gtmarx/www/surv_studies.pdf. Acesso em: 19 ago. 2018.

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

MAYER-SCHOENBERGER, V.; CUKIER, K. **Big Data: a revolution that will transform how we live, work, and think**. Londres: John Murray, 2013.

MCGREGOR, Susan E. Digital Security and Source Protection for Journalists. **Columbia University**, 2014. Disponível em: https://academiccommons.columbia.edu/doi/10.7916/D89P3D4M. Acesso em: 06 out. 2019.

MCGREGOR, Susan E; CAINE, Kelly; ROESNER, Franziska. Individual versus Organizational Computer Security and Privacy Concerns in Journalism. **Proceedings on Privacy Enhancing Technologies,** v. 4, pp. 1–18, 2016. Disponível em: https://www.franziroesner.com/pdf/JournoSec-PETS2016.pdf. Acesso em: 10 set. 2019.

MCGREGOR, Susan E; WATKINS, Elizabeth Anne. “Security by Obscurity”: Journalists’ Mental Models of Information Security. **Quieting the Commenters: The Spiral of Silence’s Persistent Effect**, 2016. Disponível em: https://pdfs.semanticscholar.org/4c90/d1233601bdcdf10ac2925869cca26be04647.pdf. Acesso em: 10 set. 2019.

MESQUITA, Lúcia Monteiro. O impacto do Jornalismo Colaborativo no exercício da profissão na atualidade: Análise comparada das plataformas ICIJ, Investigate Europe e Connectas. Universidade de Lisboa, 2019. **Dissertação.** Disponível em: https://www.repository.utl.pt/bitstream/10400.5/17820/1/Dissertacao_Lucia%20Mesquita.pdf. Acesso em: 19 de jan. 2020.

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

MOSCO, Vincent. Economia Política do Jornalismo. *In*: DOURADO, Jacqueline Lima. *et al*. (org.). **Economia Política do Jornalismo: Tendências, Perspectivas e Desenvolvimento Regional**. p. 43-68. Teresina, EDUFPI, 2016.

NASCIMENTO, Solano. **Novos Escribas: O fenômeno do jornalismo sobre investigação no Brasil**. Porto Alegre: Arquipélago Editorial, 2010.

PATERSON, Moira. The Public Privacy Conundrum – Anonymity and the Law in an Era of Mass Surveillance. *In*: LIDBERG, Johan; MULLER, Denis (org.). **In the Name of Security - Secrecy, Surveillance and Journalism**. Melbourne: Anthem Press, 2018, p. 15-32.

PAVLIK, John V. Ubiquidade: O 7º 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: 06 out. 2019.

PEW RESEARCH CENTER. **Investigative journalists and digital security**, 2015. Disponível em: http://www.journalism.org/2015/02/05/investigative-journalists-and-digital-security/. Acesso em: 08 jul. 2018.

PERIS, Manuel. Los ojos del poderoso: Periodismo, Internet y derechos humanos. **Pasajes,** n. 57, p. 56–76, 2019. Disponível em: http://esdeveniments.uv.es/_files/_event/_40314/_editorFiles/file/ponencias/Pasajes57 peris.pdf. Acesso em: 19 jan. 2020.

POSETTI, Julie; The Future of Investigative Journalism in an Era of Surveillance and Digital Privacy Erosion. *In*: O. Hahn; F. Stalph (Orgs.), Digital Investigative Journalism, Reino Unido: Univerisidade de Oxford, 2018, p. 249-261.

RAMONET. Ignacio. "Vivimos bajo el control de una especie de Imperio de la Vigilancia". **Cuba Debate: Contra el Terrorismo Mediático**. 20 fev. 2017. Disponível em: http://migre.me/wtLXo. Acesso em: 21 abr 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: 06 out. 2019.

REPÓRTERES SEM FRONTEIRAS. **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: 08 jul. 2018.

REPÓRTERES SEM FRONTEIRAS. **Guia Segurança Digital**, 2019. Disponível em: guia_seg_digital_rsf.pdf. Acesso em: 17 nov. 2019.

REYES. Gerardo. **Periodismo de investigación**. México: Trillas, 1996.

RUBY, F.; GOGGIN, G.; KEANE, J. Comparative Silence still? Journalism, academia, and the Five Eyes of Edward Snowden (2016). **Digital Journalism**. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/21670811.2016.1254568. Acesso em: 06 out. 2019.

RUSBRIDGER, Alan. Journalism after Snowden. *In*: BELL, Emily *et al*. (org.). **Journalism After Snowden: The Future of Free Press in the Surveillance State.** New York: Columbia University Press, 2017.

RUSSELL. Adrienne. WAISBORD. Silvio. The Snowden Revelations and the Networked Fourth Estate. **International Journal of Communication**, 2017, 858–878. Disponível em: http://ijoc.org/index.php/ijoc/article/view/5526/1935. Acesso em: 12 ago. 2018.

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

SHELTON, Martin L. The Role of Corporate and Government Surveillance in Shifting Journalistic Information Security Practices. **Tese.** University of California, 2015. Disponível em: https://mshelt.onl/p/shelton_2015.pdf. Acesso em: 06 out. 2019.

SHIRKY, Clay. **A cultura da participação:** Criatividade e generosidade no mundo conectado. Rio de Janeiro: Zahar, 2011.

SHIRKY, Clay. **Lá vem todo mundo:** O poder de organizar sem organizações. Rio de Janeiro: Zahar, 2012.

SHIRKY, Clay. The value of digital data. *In*: BELL, Emily *et al.* (org.). **Journalism After Snowden: The Future of Free Press in the Surveillance State**. New York: Columbia University Press, 2017. Disponível em: http://migre.me/wf7aT. Acesso em: 09 jun. 2017.

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: 06 out. 2019.

SILVEIRA, Sergio Amadeu. AVELINO, Rodolfo. SOUZA, Joyce. A privacidade e o mercado de dados pessoais. **Liinc em Revista**, Rio de Janeiro, v.12, n.2, p. 217-230, nov. 2016. Disponível em: http://revista.ibict.br/liinc/article/view/3719. Acesso em: 19 ago. 2018.

SILVEIRA, Sergio Amadeu. **Tudo sobre tod@s: Redes digitais, privacidade e venda de dados pessoais**. São Paulo: SESC, 2017.

SILVEIRA, Sergio Amadeu. **Vigilância abusiva na web não reduz crimes, apenas restringe liberdade.** Disponível em: https://noticias.uol.com.br/opiniao/coluna/2016/03/14/vigilancia-na-internet-nao-reduz-crimes-apenas-restringe-liberdade.htm. Acesso em: 17 nov. 2019.

SILVEIRA, Sergio Amadeu. A noção de modulação e os sistemas algorítmicos. **Paulus Dossiê**, São Paulo, v.3, n.5, p. 18-26, jan-jul. 2019. Disponível em:

https://fapcom.edu.br/revista-paulus/index.php/revista-paulus/article/view/111. Acesso em: 19 jan. 2020.

SIMON, Joel. Introdução: A Nova Face da Censura. **Committee to Protect Journalists – CPJ**, 2017. Disponível em: https://cpj.org/x/6c36. Acesso em: 28 set. 2018.

SNOWDEN, Edward. Edward Snowden: The World Says No to Surveillance. 04/06/2015. **The New York Times.** Disponível em: https://www.nytimes.com/2015/06/05/opinion/edward-snowden-the-world-says-no-to-surveillance.html. Acesso em: 29 ago. 2018.

SNOWDEN, Edward. **Eterna vigilância**. Tradução: Sandra Martha Dolinsky. São Paulo: Planeta do Brasil, 2019.

SOUSA, Jorge Pedro. **Uma história breve do jornalismo no Ocidente**, BOCC, 2008. Disponível em: http://migre.me/wLPNL. Acesso em: 09 jun. 2017.

SPANNOS, Chris. Vigilância em massa e "totalitarismo inteligente". 06/03/2017. **Actantes**. Disponível em: http://migre.me/wf5Z6. Acesso em: 19 jun. 2017.

SYED, Nabiha. Liberdade de informação e assimetria da informação. *In*: BELL, Emily *et al.* (org.). **Journalism After Snowden: The Future of Free Press in the Surveillance State.** New York: Columbia University Press, 2017.

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

THOMAS, Ryan J; PERREAULT, Mildred F. A LINEAGE OF LEAKERS? The contingency of collective memory in coverage of contemporary leaking cases. **Journalism Practice,** 2017, p. 1-18. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/17512786.2017.1389293?journalCode=rjop20. Acesso em: 19 jan. 2020.

TRAQUINA, Nelson. **Teorias do Jornalismo** - Porque as notícias são como são. 2. ed. Florianópolis: Insular, 2005.

TRAQUINA, Nelson. **Teorias do Jornalismo** Vol. II: a tribo jornalística – uma comunidade interpretativa transnacional. Florianópolis: Insular, 2012.

TRÄSEL, Marcelo Ruschel. Jornalismo guiado por dados: relações da cultura hacker com a cultura jornalística. **E-compós- Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação**, 2013. Disponível em: https://www.academia.edu/3136931/JORNALISMO_GUIADO_POR_DADOS_rela%C3%A7%C3%B5es_da_cultura_hacker_com_a_cultura_jornal%C3%ADstica. Acesso em: 16 nov. 2019.

TRÄSEL, Marcelo Ruschel. Entrevistando planilhas: estudo das crenças e do ethos de um grupo de profissionais de jornalismo guiado por dados no Brasil. **Tese**. PUC-RS, 2014. Disponível em: http://tede2.pucrs.br/tede2/bitstream/tede/4590/1/461784.pdf. Acesso em: 16 nov. 2019.

TORRES, Ricardo J. Jornalistas brasileiros atuam em um contexto de alto risco. **Observatório da Imprensa**, 07 maio 2019. Disponível em: http://observatoriodaimprensa.com.br/violencia/jornalistas-brasileiros-atuam-em-um-contexto-de-alto-risco/. Acesso em: 06 out. 2019.

TSUI, Lokman; LEE, Francis. **Journalism**. How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom, 2019, p. 1–23. Disponível em: https://journals.sagepub.com/doi/full/10.1177/1464884919849418. Acesso em: 06 out. 2019.

UNESCO, **Punir o crime, não a verdade: destaques do relatório de 2018 da Diretora-Geral da UNESCO sobre a segurança dos jornalistas e o perigo da impunidade,** 2019. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000266151_por. Acesso em: 06 out. 2019.

VAN DIJCK, José. Confiamos nos dados? As implicações da datificação para o monitoramento social. **Matrizes,** v.11 - nº 1, jan./abr. 2017, p. 41-61. Disponível em: https://www.revistas.usp.br/matrizes/article/download/131620/127911/. Acesso em: 29 ago. 2018.

VIANA, Natalia. Conheça o PlusD, a Biblioteca de Documentos Diplomáticos do WikiLeaks. **Agência Pública**. 07 abr. 2013. Disponível em: https://apublica.org/especial/wikileaks-plusd/. Acesso em: 13 ago. 2018.

VERDÚ, Francisco José Murcia; RUIZ, María José Ufarte. Mapa de riesgos del periodismo hi-tech. **Hipertext.net,** v.18, mai. 2019, p. 47-55. Disponível em: https://www.raco.cat/index.php/Hipertext/article/view/347464/0. Acesso em: 19 jan. 2020.

ZUAZO, Natalia. **Guerras de internet - Un viaje al centro de la Red para entender cómo afecta tu vida**. Buenos Aires: Debate, 2015.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. **Journal of Information Technology**, 30, p. 75–89, 2015. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754. Acesso em: 29 ago. 2018.

ZUBOFF, Shoshana. **The age of surveillance capitalism – The Fight for a Human Future at the New Frontier of Power**. New York: Public Affairs, 2019.

WAISBORD, Silvio. **Watchdog journalism in South America: News, Accountability, and Democracy.** New York: Columbia University Press, 2000.

WASSERMAN, E. Safeguarding the News in the Era of Disruptive Sources. **Journal of Media Ethics**, 2017, v. 32, nº 2, p.72-85. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/23736992.2017.1294020. Acesso em: 06 out. 2019.

APÊNDICE A – ROTEIRO DAS ENTREVISTAS EM PROFUNDIDADE

Este roteiro faz parte da pesquisa *"JORNALISMO VIGILANTE SOB VIGILÂNCIA NOCIVA: VULNERABILIDADES E POTENCIALIDADES DO JORNALISMO INVESTIGATIVO BRASILEIRO"* que é parte da tese submetida ao Programa de Pós-Graduação em Jornalismo da Universidade Federal de Santa Catarina para a obtenção do título de Doutor em Jornalismo. Orientador: Prof. Dr. Rogério Christofoletti. Coorientador: Prof. Dr. Samuel Pantoja Lima.

Ao elaborar as perguntas, estabelecemos elementos para aferir a percepção dos jornalistas relacionada aos aspectos percebidos, adequados e negligenciados nas investigações jornalísticas realizadas em espaços digitais vigiados. O contexto atual de vigilância comunicacional em meios digitais exige dos jornalistas investigativos um senso permanente de sua vulnerabilidade e a adoção de uma cultura de segurança digital. Diante da vigilância digital massiva realizada por governos e corporações, buscamos clarear quais são as principais vulnerabilidades e potencialidades do jornalismo investigativo brasileiro.

1. Qual é a sua percepção sobre o contexto de vigilância comunicacional nociva de ferramentas digitais utilizadas por jornalistas?

2. Como este contexto afeta as suas ações durante investigações jornalísticas que envolvem temas sensíveis relacionados a segredos, vazamentos, crimes, etc?

3. Na sua opinião, podemos afirmar que o aumento da capacidade de vigilância comunicacional, por parte de governos e de corporações, modificou o jornalismo investigativo?

4. Pode citar casos emblemáticos relacionados a vigilância comunicacional e a segurança digital que ocorreram durante a sua carreira?

5. Você se preocupa com segurança digital? Se sim, desde quando?

6. Você adota estratégias para proteger a identidade de suas fontes? Quais as formas de contato que habitualmente adota com fontes que têm informações sensíveis?

7. Quais as principais estratégias e medidas de segurança digital que você adota durante investigações jornalísticas de temas sensíveis?

8. Quais são as principais vulnerabilidades enfrentadas por jornalistas investigativos que desenvolvem investigações em um contexto de vigilância massiva das comunicações digitais?

9. Na sua opinião, quais são as principais potencialidades do ecossistema de comunicação digital para o trabalho de investigação jornalística?

10. Na sua opinião, os jornalistas investigativos da atualidade estão preparados para lidar com vazamentos e whistleblowers? Você se preparou para isso? Como?

11. Defendemos a necessidade de estímulos e convenções relacionadas com a formatação de uma cultura de riscos digitais para jornalistas. Na sua opinião, esse aspecto é importante para o jornalismo investigativo contemporâneo?

12. Como isso pode ser fomentado entre os jornalistas?

APÊNDICE B – BASES PARA O FORMULÁRIO DA *SURVEY*

Durante a elaboração do roteiro de perguntas do questionário, estabelecemos elementos para aferir a percepção dos jornalistas relacionada aos aspectos percebidos, adequados e negligenciados nas investigações jornalísticas realizadas em espaços digitais vigiados.

Condições de aplicação do questionário:

- Convite personalizado para recrutamento e pedido para indicação de mais um profissional;
- Recrutamento de repórteres que frequentem conferências e eventos relacionados ao jornalismo;
- Recrutamento por e-mail e por ferramentas digitais;
- Possibilidade de realização de entrevistas formais para a pesquisa;
- Em caso de entrevistas formais, utilização de dispositivo de gravação portátil, com conhecimento e anuência do entrevistado.
- Possibilidade de convite para participações pontuais, por meio de canais de comunicação da preferência dos jornalistas (aplicativos de mensagens de texto criptografados, ferramentas criptografadas de bate-papo de áudio e vídeo, telefone pessoal e telefone fixo).
- Questionários com tempo de resposta estimado entre 10 e 15 minutos;
- Anuência com Termo de Consentimento Livre e Esclarecido.

Percepção de jornalistas sobre investigações jornalísticas realizadas em espaços digitais

Termo de Consentimento Livre e Esclarecido:

Este questionário faz parte da pesquisa JORNALISMO VIGILANTE SOB VIGILÂNCIA NOCIVA: VULNERABILIDADES E POTENCIALIDADES DO JORNALISMO INVESTIGATIVO BRASILEIRO que é parte da tese de Doutorado submetida ao Programa de Pós-Graduação em Jornalismo da Universidade Federal de Santa Catarina. Orientador: Prof. Dr. Rogério Christofoletti. Coorientador: Prof. Dr. Samuel Pantoja Lima.

Para participar da pesquisa, basta responder a este questionário. Não vai levar mais que 15 minutos.

Ao responder o questionário, você expressa o seu livre consentimento em participar de forma voluntária, sem qualquer vantagem adicional, podendo desistir a qualquer momento. É garantido o seu anonimato e as informações colhidas serão usadas exclusivamente para fins científicos e acadêmicos.

Para saber mais sobre a pesquisa ou ter acesso aos resultados dela, entre em contato com o pesquisador Ricardo Torres. Sobre o doutorando: http://lattes.cnpq.br/2280827424163795
E-mail: ricardo.torres@ufsc.br
Telefone: (48) 99699-0762
Guarde este Termo de Consentimento.

Questionário

Características pessoais

1- Qual o seu sexo?
   ( ) Feminino
   ( ) Masculino
   ( ) Outro

2- Em que região brasileira você trabalha?
   ( ) Centro oeste
   ( ) Nordeste
   ( ) Norte
   ( ) Sudeste
   ( ) Sul

3- Qual a sua idade?
   ( ) 20 a 25
   ( ) 26 a 30
   ( ) 31 a 35
   ( ) 36 a 40
   ( ) 41 a 45
   ( ) 46 a 50
   ( ) Acima de 50

Características profissionais

4- Quanto tempo você tem de carreira?
   ( ) Mais de 3 anos
   ( ) 6 a 10 anos
   ( ) Mais de 10 anos

5- Em que tipo de mídia você trabalha?

( ) Internet

( ) Jornal

( ) Rádio

( ) Revista

( ) TV

( ) Mais de uma das opções acima

6- Para o jornalismo investigativo, as ferramentas tecnológicas digitais são...

1 – Nada importantes

2 – Pouco importantes

3 – Indiferentes

4 – Importantes

5 – Muito importantes

7- Jornalistas se preocupam com segurança digital?

( ) Sempre

( ) Às vezes

( ) Nunca

( ) Não sei opinar

8- Você se preocupa com a possibilidade de ser vigiado digitalmente?

( ) Sempre

( ) Às vezes

( ) Nunca

( ) Não sei opinar

Aspectos ambientais

9- O local onde você trabalha tem políticas de proteção de comunicações e informações no ambiente digital?

( ) Sim

( ) Não tem

( ) Não tem políticas específicas, mas orienta os jornalistas a lidarem com o tema

( ) Desconheço

( ) Não se aplica, pois não estou vinculado a uma empresa

10- Os avanços tecnológicos das últimas décadas fizeram com que os jornalistas se preocupassem mais com segurança digital.

( ) Concordo totalmente

( ) Concordo parcialmente

( ) Não sei responder

( ) Discordo totalmente

Análise contextual

11- Hoje, no Brasil, os jornalistas enfrentam formas de vigilância eletrônica por governos e corporações;

( ) Concordo totalmente

( ) Concordo parcialmente

( ) Não sei responder

( ) Discordo totalmente

12- Jornalistas sentem necessidade de intensificar cuidados com a privacidade das fontes e pessoas mencionados.

( ) Sempre

( ) Às vezes

( ) Nunca

( ) Não sei opinar

13- Você toma providências ou tem atitudes relacionadas a sua proteção no que diz respeito às possibilidades de vigilância comunicacional digital?

( ) Sempre

( ) Às vezes

( ) Nunca

( ) Não sei

14- Quão preocupado você está em relação às formas de vigilância do ambiente digital?

( ) Muito preocupado

( ) Preocupado

( ) Pouco preocupado

( ) Despreocupado

( ) Não sei

15- Você acha que o governo do Brasil possivelmente coleta ou possivelmente não coleta os seus dados, telefonemas, e-mails ou outras comunicações digitais?

( ) Sim, o governo coleta os meus dados

( ) Provavelmente o governo coleta os meus dados

( ) Não, o governo não coleta os meus dados

( ) Não sei responder

Tratamento da informação

16- A possibilidade de intrusão comunicacional interfere no seu cotidiano de trabalho?

( ) Sempre

( ) Às vezes

( ) Nunca

( ) Não sei opinar

17- Na sua opinião, a preservação dos dados pessoais de um jornalista investigativo é importante para que ele desempenhe o seu trabalho jornalístico?

1 – Nada importante

2 – Pouco importante

3 – Indiferente

4 – Importante

5 – Muito importante

18- Você adota medidas de segurança para preservar os seus dados pessoais?

( ) Sempre

( ) Às vezes

( ) Nunca

( ) Não sei opinar

19- Você faz uso de ferramentas de criptografia e outras formas de segurança digital?

( ) Sempre
( ) Às vezes
( ) Nunca
( ) Não sei opinar

Contato com fontes

20- Você adota estratégias para proteger a identidade de suas fontes?

( ) Sempre
( ) Às vezes
( ) Nunca
( ) Não sei

21- Quais as formas de contato que habitualmente adota com fontes que têm informações sensíveis? (Você pode escolher mais do que uma das opções)

( ) Contato por telefone
( ) Contato por e-mail
( ) Contato por aplicações de mensagem
( ) Contato por redes sociais
( ) Contato pessoalmente
( ) Adoto outras formas de contato (quais?)

22- Você utiliza servidores de e-mail de corporações transnacionais como o Gmail, o Yahoo e a Microsoft?

( ) Sempre
( ) Às vezes
( ) Nunca
( ) Não sei

23- Em investigações jornalísticas, você já utilizou contas de e-mail "falsas" ou participou de fóruns online e salas de bate-papo usando nomes de usuários anônimos?

( ) Sim
( ) Não
( ) Desconheço essa possibilidade
( ) Não sei responder

24- Durante investigações jornalísticas que abordam temas sensíveis, você costuma adotar medidas preventivas, como desligar os seus dispositivos eletrônicos, para se encontrar com as fontes?

( ) Sempre
( ) Às vezes
( ) Nunca
( ) Não sei

25- Você usa criptografia para se comunicar com as suas fontes por meios digitais?

( ) Sempre
( ) Às vezes
( ) Nunca
( ) Não sei

26- Quantas das suas investigações jornalísticas atuais contam com fontes anônimas?

( ) Todas ou quase todas
( ) A maioria das histórias em que trabalho
( ) Algumas histórias em que trabalho
( ) Nenhuma das histórias em que trabalho
( ) Sem resposta

Segurança Digital

27- Você utiliza softwares que permitem navegar na web anonimamente, como Tor ou Tails, em seu computador, tablet ou telefone?

( ) Sim, utilizo
( ) Desconheço essa possibilidade
( ) Conheço essa possibilidade, mas acho desnecessário

28- Você utiliza softwares de criptografia de e-mail, como o PGP?

( ) Sim, utilizo
( ) Desconheço essa possibilidade
( ) Conheço essa possibilidade, mas acho desnecessário

29- Você utiliza serviços de nuvem criptografados, como o SpiderOak?

( ) Sim, utilizo

( ) Desconheço essa possibilidade

( ) Conheço essa possibilidade, mas acho desnecessário

30- Você utiliza plug-ins de navegação relacionados à privacidade, como PrivacyBadger ou DoNotTrackMe?

( ) Sim, utilizo

( ) Desconheço essa possibilidade

( ) Conheço essa possibilidade, mas acho desnecessário

31- Você utiliza criptografia no disco rígido do seu computador de trabalho?

( ) Sim, utilizo

( ) Desconheço essa possibilidade

( ) Conheço essa possibilidade, mas acho desnecessário

32- Você utiliza mecanismos de pesquisa que melhoram a privacidade, como o DuckDuckGo?

( ) Sim, utilizo

( ) Desconheço essa possibilidade

( ) Conheço essa possibilidade, mas acho desnecessário

33- Você utiliza softwares de proteção de senhas?

( ) Sim, utilizo

( ) Desconheço essa possibilidade

( ) Conheço essa possibilidade, mas acho desnecessário

34- Você utiliza softwares de criptografia de bate-papo online, como o CryptoCat?

( ) Sim, utilizo

( ) Desconheço essa possibilidade

( ) Conheço essa possibilidade, mas acho desnecessário

35- Você já usou redes sem fio públicas, por exemplo, em uma biblioteca, café ou enquanto viajava?

( ) Sim

( ) Não
( ) Sem resposta

36- Você recebeu treinamento ou instrução formal de qualquer uma das seguintes fontes, com recomendações sobre como manter seus telefonemas, e-mails ou outras comunicações online seguras?
( ) Eventos de jornalismo, seminários ou webconferências
( ) Organização de notícias em que você trabalha ou trabalhou no passado
( ) Cursos relacionados à segurança digital ou ao jornalismo
( ) Não recebi treinamento

37- Qual o nível de segurança dos dados e informações que estão em seus equipamentos eletrônicos e no ambiente digital?
( ) Muito seguros
( ) Pouco seguros
( ) Nada seguros
( ) Não estou preocupado com a segurança dos meus dados e informações
( ) Não sei responder

38- Para esta pesquisa alcançar o maior número de participantes, peço que indique 2 colegas jornalistas investigativos. Cite nome e e-mail:

39- Se tiver mais observações sobre este estudo, fique à vontade para deixá-las abaixo. Estou particularmente interessado em exemplos de como a vigilância comunicacional digital e o hackeamento impactaram no seu trabalho de investigação jornalística.

Obrigado por dedicar o seu tempo para essa pesquisa!
Suas respostas são muito importantes para o estudo.
Um relatório completo com os principais resultados estará disponível nos próximos meses.
Clique no botão abaixo para garantir que suas respostas sejam enviadas e incluídas neste estudo.

APÊNDICE C – ENTREVISTAS EM PROFUNDIDADE NA ÍNTEGRA (EDITADAS)

Sujeito 1 (S1)

P1- Para iniciar, a gente quer entender um pouco a tua percepção pessoal mesmo. Sobre esse contexto de uma possível vigilância comunicacional, que a gente chama de vigilância comunicacional nociva de ferramentas digitais utilizadas por jornalistas. O que você acha a respeito deste tema? Tem alguma opinião a respeito?

S1 - Esse é um tema novo, eu acho até para o jornalismo. Evidentemente que os cuidados digitais já têm um tempo, mas acho que nunca esteve tão em voga quanto hoje, esses ataques hackers que a gente têm visto e a questão da operação Lava Jato e tudo mais faz a gente pensar muito nessa questão. Realmente eu confesso que era um pouco ingênuo, até um tempo atrás, em relação a esses cuidados durante o nosso trabalho de investigação, de não estarmos sendo vigiados. Recentemente eu até coloquei uma fita na frente da câmera do meu notebook, porque pode haver uma invasão, enfim a gente trabalha com temas sensíveis que interessam muito a criminosos. Criminosos de vários tipos, do colarinho branco até criminosos mais barra pesada, vamos dizer assim. Então, assim, eu acho que hoje, mais do que nunca, o jornalista precisa estar atento à questão da vulnerabilidade das mídias digitais, dos meios digitais, eu acho que tem sido uma preocupação minha de uns meses para cá. Eu tive apurando, por exemplo, o caso Marielle (Franco) e tomei algumas precauções de segurança que antes eu não havia tomado em outros casos de apuração. Como, por exemplo, o uso de um celular, não meu, mas o celular da empresa exclusivamente para aquela apuração, para entrar em contato com as fontes mais sensíveis sabe, banda podre da polícia, enfim milicianos, etc. Porque a gente sabe que dá para rastrear o celular, se você dá um contato para uma pessoa, se não sabe o que aquela pessoa pode fazer com o teu número. Dá para rastrear, se você é um policial, se tem acesso a antenas de comunicação, pode rastrear os passos daquela pessoa, onde ela mora, o que ela faz. Pela primeira vez, eu tive muito cuidado mesmo, assim, nesse preparo contra uma eventual espionagem contra mim, porque a gente está acostumado a espionar os outros, no bom sentido, investigar os outros, mas ser investigado é algo bastante complicado.

P2- Partindo dessa perspectiva de uma possibilidade de intrusão comunicacional por parte do governo, corporações ou de grupos específicos. Como esse contexto afeta as suas ações durante investigações jornalísticas que envolvem temas sensíveis?

S1 – Afeta, por exemplo, tem fonte que é tão sensível, que a gente vai contatar, que a gente encontra com ela fisicamente em algum lugar, eu deixo o meu celular na redação ou em casa. Eu vou sem celular, porque mesmo o celular parado, você sabe que ele é rastreável, justamente para que não saibam com quem eu estou falando, onde estou me encontrando, com quem, etc. Esse é um cuidado que a gente precisa ter cada vez mais. É uma coisa que até um tempo atrás nem se falava nisso, há dez anos atrás não se tinha essa discussão e hoje está se tendo. O jornalismo caminha, cada vez mais, para o uso de ferramentas digitais e, por isso, a gente está sujeito também ao reverso, a quem nos vigia usar essas ferramentas como contrainfomação, contravigilância.

P3 - Na sua opinião, podemos afirmar que o aumento da capacidade de vigilância comunicacional, por parte de governos e corporações, modificou o jornalismo investigativo como um todo?

S1 - Não acredito que mudou, as ferramentas do jornalismo ainda são as mesmas clássicas, a entrevista, a coleta de dados, o telefone juntamente ao WhatsApp, enfim, o que seja. Acho que os elementos da reportagem, eles continuam os mesmos. Agora, claro, as grandes corporações, o Estado, de um modo geral, avançou muito nesse trabalho. Por exemplo, quando a gente trabalha com assuntos que envolvem altas autoridades, a gente está sujeito a ser investigado. Então, assim, realmente é algo que passou-se a se pensar nos últimos anos, a partir do WikiLeaks, a partir, por exemplo, do caso do escândalo da NSA que o Glenn Greenwald que revelou. Quer dizer, como que essas agências de inteligência do governo, a gente tem a Abin no Brasil, atuam. Esse jogo é muito pesado. Eu tenho fontes na Abin, até agora essas fontes sempre me trataram com muito respeito, eu não acredito que tenham feito algum tipo de malefício a mim, mas é uma coisa que você fica atento. Tem que ficar atento, a gente não sabe o que vai na cabeça do Estado e lutar contra o poder do Estado, para um jornalista, é ingrato, é altamente constrangedor e pode ter uma consequência mais séria.

P4a - Em relação à tua experiência pessoal, pode citar casos emblemáticos relacionados à vigilância comunicacional ou à segurança digital que ocorreram durante a sua carreira que te afetaram de alguma maneira?

S1 - Não. Até hoje não, sinceramente, até hoje não, nunca houve nenhum episódio.

P4b - Houve algum caso em que você teve que adotar alguma estratégia específica?

S1 - Nesse caso da Marielle sim, mas eu não descobri nenhuma vigilância contra mim, se houve, eu não sei. Mas adotei muitas medidas preventivas, como eu nunca tinha adotado. Como essa questão, por exemplo, do não uso do meu celular pessoal para ouvir certas fontes, para pessoa não ter o meu número e fazer mau uso daquela informação. Então usei o número da empresa, no final da apuração, esse número foi descartado, acabou.

P5a - Pode se dizer, então, que você se preocupa com segurança digital?

S1 – Sim, me preocupo. Hoje me preocupo.

P5b - Desde quando?

S1 – Olha, eu acho que desde o ano passado, 2018 para 2019. E o caso Marielle é muito emblemático, ali, eu aumentei essa vigilância.

P5c - Pode se dizer, então, que esse caso modificou um pouco a sua conduta?

S1 - Sim, modificou. O caso Marielle sim.

P6a - Em relação à outra dimensão que a tese aborda, isto é, as medidas de proteção das fontes. Você provavelmente deve adotar medidas para proteger as fontes. Quais são as formas de contato que habitualmente adota com fontes que têm informações sensíveis?

S1 - Sempre encontros pessoais face a face, em locais públicos, shopping, por exemplo, praça de alimentação de shopping é um clássico. Para segurança da fonte e minha também, em muitos casos, eu conheço a fonte e confio nela, há casos em que estou vendo a fonte pela primeira vez. Então, assim, eu lido com narcotráfico, eu lido com temas muito sensíveis. Então sempre em locais públicos e sempre pessoalmente.

P6b - Não perpassa por ferramentas digitais?

S1 - Às vezes WhatsApp.

P7c - Correio eletrônico?

S1 - Mais raro, a preferência é sempre pelo WhatsApp, principalmente pela criptografia.

P7a – Bom, isso aqui é um pouco redundante também, mas se tu puder detalhar de alguma maneira quais são as principais estratégias e medidas de segurança digital que você adota durante a investigações jornalísticas de temas sensíveis?

S1 - Este do celular é interessante, eu acho. Não usar o meu celular pessoal para entrar em contato com determinadas fontes, que não são todas, mas algumas fontes que eu julgo mais de risco para mim.

P7b - Quanto aos dispositivos eletrônicos, você tem algum tipo de cuidado?

S1 - Sim, tenho. Por exemplo, não especificamente dispositivos eletrônicos, mas redes sociais, eu tenho cuidados. Um deles é nunca postar fotos da minha família. Eu não costumo postar fotos da minha família em rede social, só minhas, por conta do meu trabalho sensível. É uma forma, eu creio, de preservar a família.

P8a - Na sua opinião, quais são as principais vulnerabilidades enfrentadas por jornalistas que desenvolvem investigações jornalísticas em um contexto de possível vigilância massiva das comunicações digitais? Quais as principais vulnerabilidades que esse contexto apresenta?

S1 – Olha, eu acho que a comunicação é a principal delas. O WhatsApp, por exemplo, se alguém eventualmente conseguir quebrar a criptografia de uma conversa de WhatsApp, eu sei que é possível já fazer isso, isso seria altamente danoso para gente, vai estar exposto muita coisa que eu não quero que esteja exposto.

P8b - Estariam vulneráveis?

S1 - Muito vulneráveis. E-mail também não é (seguro). Eu evito e-mail justamente por isso, porque ele é mais frágil do ponto de vista de segurança digital, muito mais frágil, mas a preferência é sempre o WhatsApp, justamente por isso. O Telegram não é uma boa opção, nunca usei o Telegram e não é mais uma opção. Tem uma estratégia que eu aprendi com o crime, mas nunca usei. Que é por e-mail, sem enviar o e-mail, quer dizer você salva no rascunho, uma outra pessoa tem a senha, ela entra no rascunho e vê o e-mail. Como não há transmissão, não é possível a interceptação, mas eu nunca usei isso. É curioso, não é de agora que se usa isso, é antigo já.

P9a - O trabalho também aborda uma dimensão de potencialidades. Nesse sentido, na sua opinião, quais são as principais potencialidades que o ecossistema de comunicação digital apresenta para o trabalho de investigação jornalística?

S1 – É extremamente importante, é vital. Hoje, você tem acesso a inúmeras bases de dados digitais que, poxa, hoje seria impensável fazer jornalismo investigativo sem acesso a sistemas

digitais, especialmente base de dados que, para a gente, é muito importante, *Panama Papers*, por exemplo, fundamental.

P9b – O grande potencial, então, são as bases de dados?

S1 - Especialmente, eu diria as bases de dados, públicas ou não.

P10a - A gente também aborda na tese a questão de grandes vazamentos, grandes volumes de informações. Nesse sentido, tem uma pergunta que é a seguinte: na sua opinião, os jornalistas investigativos da atualidade estão preparados para lidar com vazamentos e com os vazadores?

S1 - Pois é, esse caso da Vaza Jato é um caso muito interessante. Cara, eu acho que, assim, já aconteceu comigo, eu já usei um hacker para publicar reportagem, isso já tem uns 15 anos. Evidentemente, o uso da tecnologia digital era muito incipiente em 2004, na época, eu investiguei com a ajuda desse hacker um esquema de roubo de senhas bancárias, uso de Cavalo de Troia. Na época, isso era uma novidade ainda, hoje mal se usa isso, aqueles programas espiões que você baixa sem querer e eles pegam a sua senha. Era um megaesquema em Santa Catarina, era chefiado por lá, mas eu estava no interior de São Paulo e tinha um braço no interior de São Paulo, eu divulguei isso e até ganhei um prêmio nesse caso.

P10b - Como ficou conhecido esse caso?

S1 – Cara, depois teve uma operação da PF contra esses caras, no ano seguinte, inclusive da PF de Florianópolis, mas eu não me lembro. Eu vou lembrar depois eu te passo, é um caso que me marcou bastante. Assim, foi a primeira vez que eu lidei com tecnologia digital para uma reportagem.

P10c - Isso em?

S1 – 2004, no começo de 2004. Então, assim, é polêmico isso, porque o hacker é um criminoso, um criminoso como um assaltante, com a diferença que ele é um criminoso digital. Há que se tomar muito cuidado com a fronteira ética nesse tipo de situação. O hacker vaza milhões de dados sobre conversas, anos de conversa no WhatsApp ou no Telegram, o que fazer com esse material? É uma dúvida que eu tenho, se isso acontecesse comigo, eu teria noites sem dormir, com certeza. É justamente nesse entrave ético, nesse debate ético de publicar ou não. Evidentemente que há um interesse público no caso da Vaza Jato, mas eu teria algumas reflexões de outra ordem, justamente porque tudo indica, pelo menos, que teria partido de um hacker, mas eu concordo que é algo muito polêmico e não há uma resposta pronta para isso, acho que tem que ser bem debatido pelo jornalismo esse tipo de situação.

P10d - É um processo em andamento?

S1 - É um processo em andamento, eu acho, e o caso da Vaza Jato é muito emblemático disso, é um caso fantástico para se discutir isso.

P10e - No seu caso, você se considera preparado para trabalhar com isso?

S1 – Não, tecnologicamente, eu não sou um jornalista expert em tecnologia, não sou, mas como eu te falei no começo, os fundamentos da reportagem, eles são os mesmos, só se muda,

às vezes, o ambiente, digital ou analógico pessoal. Então, assim, se acontecesse comigo, eu usaria os mesmos filtros como repórter de uma matéria, outro tipo de matéria.

P10f - Como se preparou para isso?

S1 - A minha experiência profissional, o jornalismo continua com as mesmas balizas éticas e de prática. Então, assim, eu sofreria muito para tomar essa decisão, mas é importante, é legal que se tenha esse debate, eu acho importante.

P11 - Na tese, a gente defende a necessidade de estímulos e convenções relacionados com a formatação de uma cultura de riscos digitais para jornalistas. Na sua opinião, esse aspecto é importante para o jornalismo investigativo contemporâneo?

S1 - É extremamente importante, você não sabe que você está sujeito a ser grampeado também, ter suas conversas hackeadas. Como a gente já conversou, nós, jornalistas investigativos, lidamos com fontes muito sensíveis, muito sensíveis. Qualquer vazamento de uma conversa pode colocar em risco a vida do jornalista e da fonte também. Isso é muito sério, tem que ser levado muito em consideração e eu acho que o jornalismo não está preparado para esse tipo de ato criminoso contra si mesmo. O jornalismo, de um modo geral, e eu me incluo nisso, não está suficientemente preparado para lidar com uma invasão desse tipo, por exemplo. Não, não está.

P12 - Nesse sentido, como uma cultura de riscos digitais pode ser fomentada entre os jornalistas?

S1 - Eu acho que já começou isso um pouco, a Abraji tem feito alguns treinamentos nesse sentido que é muito importante, mas acho que muitos, no jornalismo, não levam isso muito a sério ainda, infelizmente, precisam levar. Eu acho que esse caso da Vaza Jato também coloca essa perspectiva, quer dizer, até que ponto eu posso estar sendo hackeado. As pessoas estão mais conscientes desse problema hoje do que há cinco anos atrás.

P13 - A gente chegou ao fim. Tem mais alguma coisa em relação ao tema que você gostaria de ressaltar?

S1 – Não, acredito que não, do meu ponto de vista, a gente abordou tudo que tinha que falar sobre isso. Espero ter ajudado.

Sujeito 2 (S2)

P1a - A entrevista trata da pesquisa que estou fazendo relacionada à vigilância e ao jornalismo investigativo. Vigilância Comunicacional em meios digitais. Então, para iniciar, a primeira pergunta é: Qual é a sua percepção sobre o contexto de vigilância comunicacional que a gente chama, na tese, de vigilância comunicacional nociva em ferramentas digitais utilizadas por jornalistas?

S2 - Se entendi bem, se diz tipo *stalking*[201], esse tipo de coisa.

[201] *Stalking* é um tipo de perseguição persistente, uma forma de violência, na qual sujeitos invadem repetidamente a privacidade das vítimas, empregando táticas de perseguição, por meios diversos (mídias sociais, ligações

P1b - Possibilidade de intrusão comunicacional por parte de governos e organizações?

S2 - Isso é cada vez mais real e a gente não sabe. Porque antigamente pegar um grampo telefônico era muito mais linear, agora com um celular você tem mil maneiras de entrar por um aplicativo ou você pode entrar no sistema operacional, pode ativar a câmera sem saber que também está ativado, então a coisa mudou muito. E hoje em dia é praticamente irrastreável você saber se está acontecendo.

P2 - Como este contexto afeta as suas ações durante investigações jornalísticas que envolvem temas sensíveis, como segredos, vazamentos, crimes?

S2 - Bom, aqui também a gente tem que ter claro o cuidado com fontes e com informação sensíveis. Então a gente costuma usar a criptografia para a comunicação entre nós e aplicativos que a gente considera mais seguros, mas nada é cem por cento seguro.

P3 - Na sua opinião, a gente pode afirmar que o aumento da capacidade de vigilância comunicacional, por parte do governo e de corporações, modificou o jornalismo investigativo como um todo?

S2 - Eu acho que isso talvez ainda não, porque talvez isso ainda não esteja devidamente esclarecido entre os profissionais. De que isso é realmente uma coisa que a gente têm que prestar atenção e nem entre autoridades públicas. Eu acho que pouca gente ainda presta atenção do que deveria prestar em relação a isso.

P4 - Pode citar um caso emblemático relacionado à vigilância comunicacional ou à segurança comunicacional que ocorreu durante a sua carreira?

S2 – Alguns casos. No caso X, claro que a gente reforçou protocolos, mas a gente já têm protocolos de segurança no veículo X. Então a gente já tem protocolos de comunicação e gestão de dados. A gente se preocupa muito com isso, até pela natureza do site. Desde uso de VPN[202] para navegação, até GPG[203], já é uma coisa incorporada a nossa rotina.

P5a - Você se preocupa com segurança digital?

S2 - Sim.

P5b - Desde quando?

S2 - Cara, acho que há uns 10 anos já. Já dei curso sobre isso também, já dei curso sobre TOR[204], sobre navegação anônima, sobre VeraCrypt[205], sobre arquivos criptografados, já é uma coisa que me interessa há bastante tempo.

---

telefônicas, envio de mensagens por SMS, correio eletrônico, publicação de fatos ou boatos em sites da Internet, também conhecido como *cyberstalking*).

[202] VPN significa Virtual Private Network ou Rede Virtual Privada.

[203] GPG é uma criptografia assimétrica que emprega um par de chaves para alcançar seu objetivo (uma chave pública e uma chave privada). É um software livre alternativo ao conjunto de softwares criptográficos PGP.

[204] TOR é um software livre e de código aberto que possibilita comunicação anônima na navegação pela Internet e em atividades online.

[205] VeraCrypt é um programa que realiza criptografia em arquivos e discos do computador. Cria arquivos ocultos e protegidos dentro do sistema operacional, no HD e em dispositivos externos como pendrives.

P5c - Desde quando você é jornalista investigativo?

S2 - Sou jornalista desde 97, 98 e aí 2008, 2009, 2010, o tempo que eu morei na Itália, eu fiz uma especialização em jornalismo investigativo.

P5d - Praticamente desde que você trabalha com isto, se preocupar com segurança digital, é isso?

S2 - Sim, exato.

P6 - Você adota estratégias para proteger a identidade de suas fontes? Quais as formas de contato que habitualmente adota com fontes que têm informações sensíveis?

S2 - Cara, a gente faz o contato conforme a fonte se sente mais confortável ou a gente indica para ela maneiras de se contatar que ela não corra o risco de ser rastreada, então, por isso, não posso dizer quais são.

P7 - Mais alguma estratégia ou medida de segurança digital que você adota durante investigações de temas sensíveis?

S2 - Não, acho que era basicamente isso.

P8 - Na sua opinião, quais são as principais vulnerabilidades enfrentadas pelos jornalistas que desenvolvem investigações jornalísticas sobre temas sensíveis em um contexto de vigilância massiva das comunicações digitais?

S2 - É desconhecimento, é não achar que isso é importante, basicamente isso.

P9 - Na sua opinião, quais são as principais potencialidades do ecossistema de comunicação digital para o trabalho de investigação jornalística?

S2 - Ajuda um monte, né cara, principalmente pesquisa, documentação, dados públicos que são uma coisa incrível que eles têm hoje em dia, banco de dados, isso aí mudou bastante hoje em dia. É possível fazer jornalismo com fontes abertas de uma maneira que não se fazia antes, as coisas estão mais transparentes.

P10a - Na sua opinião, os jornalistas investigativos da atualidade estão preparados para lidar com vazamentos e *whistleblowers*? Você se preparou para isso?

S2 - Cara, eu acho que sim, já tem um histórico, muita gente já lidou com isso, tem bastante casos já, né. Claro que não todos, porque também não são todos os jornalistas que trabalham com esse tipo de material, mas já tem um aprendizado de como lidar com esse tipo de material, inclusive fazendo parcerias e tal. Acho que tem bastante massa crítica.

P10b - Como se preparou para isso?

S2 - Cara, experiências, principalmente a maneira como você lida com as fontes. Tem uma lógica que é muito precisa. Assim, a lógica da proteção de fontes é a mesma lógica da proteção de documentos, a mesma lógica que você vai usar para todas as coisas, então, acho que é um pouco isso.

P11 - Na tese, a gente defende a necessidade de estímulos e convenções relacionados com a formatação de uma cultura de riscos digitais para jornalistas. Na sua opinião, esse aspecto é importante para o jornalismo investigativo contemporâneo?

S2 – Então, acho que é, por isso que eu falei antes que o grande problema é a desinformação, acho que as pessoas ainda não estão aculturadas sobre isso. Não se dão conta da importância, a pessoa acha que tem que só guardar arquivos em uma pasta com criptografia se é uma coisa ultrassensível, e não, às vezes você precisa proteger uma coisa que parece banal, mas que se cai nas mãos erradas e é descontextualizada aquilo pode virar tragédia.

P12 - Nessa direção, então, como isso poderia ser fomentado entre os jornalistas?

S2 - Eu acho que tem que ter que juntar mais educação, principalmente de universidades e cursos, com as redações isso é uma coisa que não acontece. As redações, elas não treinam os jornalistas. Quando o jornalista vai fazer curso é muito mais uma coisa do jornalista. Ele vai pra fora, fica um ano fora ou vai fazer alguma coisa que ele se interessou, mas seria legal se as redações fomentassem isso, levassem gente lá para dentro para fazer treinamento, para falar com as pessoas, para explicar. Isso é uma coisa que eu vejo acontecer pouco, seria legal se acontecesse mais.

P13a - Só uma última pergunta em relação a Vaza Jato. O que você acha que a Vaza Jato significa para o jornalismo investigativo?

S2 – Cara, eu acho que ela significa até mais para o jornalismo independente, significa mostrar que é possível fazer jornalismo de alto nível em um outro formato, de um outro jeito, com uma outra visão, com outra identidade, outra linguagem, em uma outra perspectiva do que é o jornalismo e de como ele tem que ser feito. Sem achar que é o único modo que é possível, sem desmerecer todos os outros, mas saindo do senso comum, tentando buscar outras narrativas, outra linguagem, atingir as pessoas de uma outra maneira.

P13b - Um caso paradigmático, aconteceria sem as possibilidades oferecidas pelo ecossistema digital?

S2 - Acho que não. Com certeza não.

P13c - Acha que o caso é paradigmático para o jornalismo?

S2 - Acho que sim, sem dúvida. Espero que seja, porque vai ser bom para todo mundo.

Sujeito 3 (S3)

P1 - Para tentar entender um pouco sobre a sua percepção contextual em relação a essas problemáticas. Qual é a sua percepção sobre o contexto de vigilância comunicacional de ferramentas utilizadas por jornalistas? Na pesquisa, a gente aborda como uma questão nociva, por parte de governos e corporações.

S3 - Eu acho que a essência do repórter é o trabalho solitário, por mais que às vezes esteja trabalhando em equipe, mas a essência é essa relação dele com o seu objeto de apuração e,

nesse sentido, não é de agora, ele vai querer se preservar. Ele não vai querer que aquilo passe para ninguém. Então a essência dele é essa relação única e exclusiva com a fonte dele, com o objeto. Está intrínseco no repórter esse drama, mais que uma preocupação, é o temor da apuração dele ser compartilhada por outros, a informação ser compartilhada por outros, antes dele dar corpo a essa informação, antes dele ter o controle dessa informação e da forma que ele quer que ela passe. No caso específico que eu posso falar mais um pouquinho, assim do nosso contexto, o contexto jornalístico brasileiro, nós temos uma imprensa de pouca duração. É uma imprensa que surge, de fato, ali no final do século 19. Esse jornalismo, um jornalismo mais diferenciado, fora dessa pauta pública, ele vai se consolidar ao longo do século 20. Esse é um século de muita instabilidade, especialmente para o jornalista, e mais recentemente nós passamos, só nesse século 20, por pelo menos três momentos autoritários: Benazi, o Vargas e depois a ditadura. E vem a redemocratização que é uma democracia incipiente. Então o repórter de investigação, ele, mais do que nunca, é ele e mais ele. Você não tem empresas assim, por mais que estejam consolidadas, você não tem nenhuma empresa que vai garantir uma segurança absoluta no desenvolvimento do repórter, até aonde ele queira chegar. A segurança dele, eu estou falando de segurança física mesmo, passa a ser de responsabilidade dele. Por mais que às vezes a gente fale que as grandes empresas têm uma estrutura etc., em momentos decisivos, o máximo é eles colocarem um advogado lá, um burocrata, ou faz aquela cena toda de estamos juntos etc., mas no final do dia, ele vai para casa dele sozinho. É a mesma coisa as formas de ele tentar preservar o material que ele está recolhendo. Então, não é de hoje, isso é uma conjuntura histórica, o repórter brasileiro, ele sempre foi um bicho, um ser que atuou de forma muito solitária nesse campo de preservação de sua integridade e da integridade do seu material. Você teve, assim, eu estou falando do contexto histórico, acho que você teve, assim, nos anos 70 e 80, os cursos jornalismo, você teve o jornalismo, ele se tornou mais sofisticado, bem mais e por mais que as pessoas achem que o jornalismo esteja degringolando, mas ele foi forçado a uma situação nova, com a Constituição de 88, com a definição do Ministério Público, ele tem que concorrer com outros órgãos. Então tem a questão do Judiciário, ele tem que ser mais sofisticado na sua apuração. A fábrica de processos se torna muito pesada e vêm as novas tecnologias. Com essas novas tecnologias, as empresas mal estão preparadas para absorver novos leitores, essa nova demanda que surge e que está nas redes sociais, tudo maluco e os jornais não conseguem abocanhar essa turma. Que dirá garantir uma formação, uma capacitação para esse profissional estar adaptado a uma esfera, um jogo político de poder que não é mais aquele jogo que você tinha em Brasília até recentemente. Até os anos 90, os arapongas da Abin que ficavam ali e faziam suas gravações. Hoje não, hoje você tem uma plataforma digital toda conectada com possibilidade de entrada aqui e acolá. Então, você está em um jogo muito diferente, muito mais sofisticado. Não é uma crítica, é uma avaliação, uma constatação real, as empresas estão em um desafio de abocanhar novos leitores e essa questão, eu acho que ela passa longe da realidade dos grandes jornais, que dirá dos jornais das capitais do interior, que tiveram até uma explosão de novos veículos. Então essa discussão da questão da segurança, da proteção, da possibilidade do repórter, eu falo da estrutura que permite esse cara atuar de uma forma menos vulnerável. Você teve uma explosão do jornalismo nos últimos anos, uma explosão para o bem. Hoje você tem blogs, se você olhar os blogs espalhados pelo interior do Brasil é fantástico, rádios comunitárias, você tem nas periferias, parece que elas não têm uma conexão com esse jornalismo mais tradicional ou mesmo com esses grupos formadores de opinião, com as universidade, mas você vai em qualquer cidadezinha hoje, você já têm dois, três meninos que estão ali, tem um emprego na prefeitura, ele tem não sei o quê, mas ele está ali com um blog dele, ele está com o jornalzinho policial, ele está na rádio falando as coisas. Então houve uma explosão assim, houve o fim do coronel eletrônico, aquela coisa do Sarney, que todo o político tinha uma rádio e controlava, essa figura, ela desmoronou pelo Brasil a fora. Só que o fim do coronel

eletrônico significou também o fim do escudo do coronel para essa galera. Então você, aí não é papo, não é tese, o que está morrendo de blogueiro no interior do Brasil, radialista, é uma coisa assustadora. Porque o cara, por um lado, não tem a formação do processo de edição, então se rolou um negócio na prefeitura, qualquer escandalozinho, ele divulga. Ele não tem o conhecimento realmente do processo de edição, mas também ele está muito mais vulnerável a essas forças políticas e essa banda podre de polícia, especialmente as chamadas milícias, ao tráfico, esse pequeno, tráfico das cidades médias. Esse menino pega um celular e liga para o cara que ele acha que matou e deixa o rastro dele, manda um 'zap', entra no grupo, para querer saber. Ele vai fazer uma apuração e dá as caras lá, vai no bar, pergunta a todo mundo, sem base nenhuma. Então ele fica exposto e aí os números são assustadores, aí ele morre, aí ele não consegue fazer, ele é ofuscado, ele é perseguido, é um problema sério.

P2a - A partir desse cenário de uma potencial vigilância, principalmente por parte do governo, principalmente nesse espectro digital, essa questão digital e a possibilidade de inserção de corporações e do próprio governo nas investigações, esse contexto, na sua opinião, afeta as suas ações durante investigações jornalísticas que envolvem temas sensíveis relacionados a segredos, vazamentos, crimes, etc?

S3 - Você fala, assim, da questão de eu poder ser investigado?

P2b - Na apuração, durante a apuração, você tem uma potencial vigilância digital, no teu celular, nos teus dispositivos eletrônicos?

S3 - O que está ocorrendo, assim, tudo que é questão eletrônica, celular ou meio remoto não dá para fazer nada, assim, no máximo uma conversa chama outra e tal. E-mail, essas coisas todas, as conversas têm que ser pessoais e mesmo fora de algum lugar. Que eu cobri muito palácio, eu cobri 10 anos o Palácio do Planalto, setorista. Então a gente conversava muito com os militares, com o pessoal da área de segurança, Abin, gente que precisava passar, gente que contava as coisas. Então, a partir daí, eu pessoalmente por experiência própria sempre tive como meta entrevistar as pessoas pessoalmente, sem gravação, esse tipo de coisa, então eu sempre fui assim. Depois com essa coisa de rede social isso não me afetou muito, porque eu já tinha essa prática. Eu fiz também um trabalho, trabalhei muito com militares da ditadura e foi por experiência própria, esses caras, por exemplo, o *personagem* por exemplo, que é o cara que me passava muita informação, ele chegava fazendo barulho ou se não eu ia para a uma cidadezinha e ele me levava em uma caixa de som em um bar, para ter muito ruído para ser uma porcaria a gravação e ali a gente conversava e só ali que ele falava, nos momentos mais finais do trabalho, ele escrevia no papel, eu perguntava, ele escrevia no papel, mostrava o papel, eu olhava, ele colocava no bolso, para não criar prova. Esse é um jornalismo das antigas, porque o jornalismo hoje, você trabalha com uma gama de informações, uma gama de fontes e não dá para uma matéria, não dá para você ter um encontro em um lugar ermo de uma cidade com todo mundo porque, às vezes, o cara está no Nepal, nos Estados Unidos, então mudou. Aí também é os limites da conversa. Eu estou falando tudo isso porque eu não conheço nada seguro e eu não sei o que é seguro. Eu não tenho essa informação do que vai ser seguro para a minha conversa, então, o que eu faço são métodos, por exemplo, se eu tenho uma história para apurar, eu converso com a pessoa até X, eu conto para pessoa uma certa parte.

P2c - Você tem alguns cuidados, isso desde sempre?

S3 - O que estou falando hoje, é que hoje você está pagando um jornalista com muito mais informações e bancos de dados muito maiores. Então é mais complicado e tem uma outra questão que eu vejo em Brasília, é que a Abin, ela ficou obsoleta nesse cenário todo. O que eu vejo hoje são grupos privados de lobby, é uma gente, até o jornalismo cedeu muita gente para esses grupos, que teria um potencial maior e menos engessado do que o próprio governo. Com essa questão de redes, isso ficou muito claro na campanha (eleitoral), essa turma passou a atuar em redes também, você não consegue pegar a digital de ninguém, é um que tá ligado ao outro e assim eles fazem na questão vão sondando. Teve uma queda muito grande das grandes casas de lobby, deu uma esvaziada, mas tem muito mais, outros escritórios, tem muito mais profissionais capacitados nesses grupos, assim de assessorias hoje do que da imprensa.

P2d - Com múltiplos interesses?

S3 - Gente que trabalha, nem múltiplos interesses. Múltiplos interesses têm a imprensa, você, em um jornal, pode ter mil interesses, mas esses grupos têm interesses bem definidos, gente ligada ao sistema financeiro, especialmente sistema financeiro. Então essa gente tem um controle muito grande das redações até porque essas redações são enxugadas. Esse é um problema muito grave que eu vejo, eles têm um acompanhamento não apenas do clipping, mas de redes, de monitoramento de redes sociais.

P2e - No aspecto de vigilância?

S3 - A impressão que eu tenho é que o número deles é maior do que o número de repórteres, aí que está o problema. Se você contar quantos repórteres têm nas redações das sucursais de Brasília, é menos do que dos jornalistas que trabalham nos grupos de lobby, no Congresso.

P3 - Na sua opinião, podemos afirmar que o aumento da vigilância modificou o jornalismo investigativo como um todo?

S3 - Sim, porque isso não é só o aumento da vigilância, mas o aumento da sua capacidade de atuação, porque hoje se o cara escrever uma matéria no interior da Amazônia, que está tendo um surto, horas depois o secretário de segurança lá da fronteira do municipiozinho vai entrar no Facebook dele, para desmentir essa matéria, o conceito de lugares inóspitos acabou. Então essa vigilância de governo e autoridades locais em relação a qualquer coisa que você escreve hoje em uma rede social, o ministro tal já está sabendo, porque está todo mundo já conectado, então a coisa é muito mais direta, o controle é muito mais, e o controle das redes sociais, especialmente desse governo que está aí, um governo que tem o seu exército de rede social, ele só aumenta não é.

P4 - Pode citar algum caso emblemático relacionado à vigilância comunicacional ou que envolva segurança digital que ocorreu durante a sua carreira? Alguma coisa que te afetou.

S3 – Não, nunca tive, graças a Deus. O que rola muito assim é informações, relatórios, assim, sabe, de repórteres, repórter conversou com fulano e sicrano. Isso acaba vindo para o jornal, para tentar melindrar a matéria, isso é muito comum. Esse repórter é ligado a coisa tal. Mas o que eu queria te falar nessa coisa da vigilância, ela envolve atores improváveis, às vezes as pessoas acham que você está sendo monitorado etc., mas esse monitoramento, ele faz de certa forma, parte de todos os agentes do palácio de um governo. Quem atua no Palácio do Planalto, por exemplo, que é uma casa militar, todos seus atos são registrados por todo mundo

e não é pelo carinha da Abin, é pela assessora de imprensa que conversou com você, é pela secretária tal, essas redes de palácio, elas são muito fechadas, então todo mundo é um agente em potencial e essas informações correm muito rápido, rapidamente. Então os perfis dos repórteres são definidos muito rapidamente e ninguém fala: "tenho um dossiê contra você". Embora role sempre, vez ou outra rola, mas as coisas são mais sutis. A informação que você está procurando de repente é entregue para o seu concorrente, é entregue para o seu amigo de jornal. Essas coisas são muito mais sutis assim, a definição. É tanta piração que uma vez, em um comitê de imprensa do Planalto, teve um colega, eles botaram gente da Abin para acompanhar. Esses caras que se colocam como repórter são todos infiltrados, eles estão ali para registrar tudo. É muito comum o uso de outros profissionais para fazer isso infiltrados. Às vezes eu mal chegava na redação, o chefe já falava: "olha, fulano me ligou, falando que você fez perguntas assim". Mas eu acho que um palácio é sempre um, todo mundo é um ser, ali, de investigação. Aí, outra coisa, essa proliferação de repórter acaba você sendo usado. Tem que ter um controle absoluto de quem está conversando, mas ao mesmo tempo é um novo momento, é o momento do fim dos segredos, são atuações mais públicas, então você tem que ser mais transparente às vezes também.

P5a - Nessa dimensão de segurança digital, em relação à sua atuação, você se diria preocupado com segurança digital nos seus dispositivos?

S3 - Documentos, é até meio ridículo falar, mas eu imprimo tudo, guardar aquela coisa impressa e tento tirar tudo do computador. Às vezes eu coloco no HD externo.

P5b - Você procura evitar digitalizar?

S3 - No máximo, coloco no HD externo, o computador está zeradinho.

P5c - Não deixa de ser uma medida de segurança, tu não salva materiais sensíveis nos teus dispositivos pessoais?

S3 - Não, eu deixo impresso.

P5d - Desde quando você toma essa atitude?

S3 - Desde quando eu fazia o *trabalho X*, quando houve até processo para tomar meus arquivos e eu tive que esconder da justiça os meus arquivos, foi levado, a princípio, para o jornal, todos os arquivos impressos para o jornal, depois levei para o chefe de redação, ele levou todas as caixas para casa dele, a minha casa foi arrombada.

P5e - Para encontrar os materiais?

S3 - Eu não sei, na fase eu não queria saber se era, a porta foi arrombada e fecharam novamente. Foi o seguinte, foi um processo, entraram na justiça para tomar os meus arquivos. Eu tirei da minha casa, em seguida ela foi arrombada. Depois disso, eu coloquei no armário do chefe, daí ele tirou de lá e levou para casa.

P5f - Mas ali tinha algum material digital ou só documentos físicos mesmo?

S3 - Eu tinha muitos pen drives, alguns pen drives, mas era tudo, eu tinha impresso tudo, impressão é importante.

P5g - Então você pode dizer que, naquele momento ali, você começou a visualizar risco, você se sentiu ameaçado?

S3 - Isso ainda é 2010, 2011. No caso, era o tipo de matéria, era um grupo de militares que ficavam atrás dessas informações também. Ali eu tinha um problema, foi terrível, casa arrombada, justiça na porta. Eu passei a não ter mais coisa em casa, a não ter mais documentos em casa. Eu sempre levo para casa de pessoas que, tudo no impresso assim. Agora, assim, nos últimos meses, as minhas matérias não têm esse grau de investigação, mas quando é matéria que é complicada, eu não deixo nos arquivos do jornal, no laptop, zero eu não deixo nada, absolutamente nada. Eu sinto mais confiança em fazer o trabalho em uma *lan house* do que fazer no meu computador. Eu prefiro, a partir dali, eu mando as coisas por e-mails que não são os e-mails que eu uso para as fontes. Os e-mails, assim, o que eu uso como contatos de e-mails, eu tenho e-mails de jornal, os e-mails que vêm aquela porrada de releases, têm os meus pessoais que eu uso com os meus amigos e mando para as fontes e têm um ou dois que eu crio naquele ambiente ali para passar informação e esse eu não trafego.

P6a – Aqui, já entra na dimensão do tratamento com fontes. Você adota estratégias para proteger a identidade de suas fontes? Quais as formas de contato que habitualmente adota com fontes que têm informações sensíveis?

S3 - É muito do momento, muito da pessoa, muito da situação. A receita está um pouco ali na fonte, mas para proteger a pessoa, os ambientes que a gente procura essas pessoas, nunca no ambiente de trabalho delas, nunca em ambiente público. Engraçado, às vezes esses tipos de fonte a gente entra em contato por meio de outras, de outras pessoas, de outras fontes que fazem aquelas interlocuções, mas não saberia te responder não, uma forma assim.

P6b - Dependendo da situação, mas por meios eletrônicos em geral?

S3 - Não, até mesmo porque essas pessoas não passam isso. Geralmente essas fontes mais graúdas, elas nem te entregam pessoalmente, elas mandam te entregar.

P6c - Não há um contato direto?

S3 - Esse tipo de fonte já está preparada. Ela que deixa claro a forma de preservação dela mesma, pelo menos essas fontes de governo. Tem também, porque veja, quando é uma fonte dessa, as coisas são muito integradas, se o cara pegar um dado sigiloso vai deixar rastros, então as quebras de informações, elas ocorrem hoje, no contexto atual, por grupos. O Ministério Público, ele decidiu, foi uma decisão, eu diria, assim, de um colegiado, que vamos vazar isso. Assim é o governo também. Então quando essas informações chegam, elas já chegam com seus escudos, as suas proteções. Tipo assim, por exemplo, se o cara entrar hoje na Receita, pegar uma informação sigilosa, ele vai deixar o código dele ou a matrícula, é difícil esses casos. O que ocorre esses vazamentos hoje, é entendimentos internos de governo, de um ministro, de todo mundo e aí chega essa informação vazada. Eu vejo muita informação vazada nesse sentido. Quando chega para o repórter é porque já houve uma decisão de passar.

P7a - Acho que isso você já respondeu, as estratégias e medidas de segurança digital?

S3 - É o computador, têm essas neuras de alguém pegar as informações com o computador desligado.

P7b - É legal perceber que você tem esse senso de vulnerabilidade, isso tá presente na sua atuação?

S3 - É porque se alguém disser que tem um aplicativo de segurança, é maravilhoso, porque eu desconheço e você se molda, você se molda a essa situação, passa a ser mais reservado.

P8 - Na sua opinião, quais são as principais vulnerabilidades enfrentadas pelos jornalistas que desenvolvem investigações jornalísticas nesse contexto que a gente está falando a possibilidade de estar sendo vigiado?

S3 - Eu acho que é a família, porque o jornal ou a empresa, eles mal dão segurança para o repórter e o repórter não consegue proteger a família. Eu falo vulnerabilidade até de uma rede social. Eu, por exemplo, tive que bloquear minha família inteira, mãe, pai, irmãos, sobrinhos, todo mundo, para evitar as conexões, as pessoas começarem a me rastrear, chegar aqui e compor a minha árvore genealógica, da minha família, para não atingir, porque eles vão nas crianças, é terrível. Chegam nos meus sobrinhos que estão há quilômetros de onde eu trabalho. Nas redes sociais, eu tenho um código interno com a minha família, assim, ninguém curte as minhas coisas, ninguém coloca nada nas minhas coisas e eu também não compartilho informações pessoais com a minha família. Eu já não garanto a minha segurança, vou garantir de alguém. Eu venho também de um estado que, por natureza e por tradição, vive o crime organizado, que é o Espírito Santo. Eu sou de Vitória, então lá é uma coisa de controle absoluto sobre todo mundo, então eu já venho desse contexto de crime organizado. Então, por exemplo, se você trabalhar com polícia, no início, em 2017, na pré-campanha presidencial, eu e um colega levantamos a história do motim da greve da PM do Espírito Santo e ali, por meio da ajuda de um colega, a gente identificou as conexões dos organizadores do motim só por meio das redes sociais. Então a gente viu que quem incentivava eram alguns deputados federais e funcionários dentro desses gabinetes e era o braço do Bolsonaro praticamente, no Espírito Santo. Essa matéria teve muito destaque no jornal na época, ali, para mim, ficou muito claro essa rede toda e ficou claro também como a gente estava vulnerável. Porque, de repente, nas ligações, os caras já falavam: "você tem família", esse tipo de coisa. Essas redes, até de Bolsonaro, são muito complicadas, porque envolvem a banda podre e a banda boa da polícia. Essas pessoas acabam tendo como missão, então todo mundo atua para a defesa do cara, entendeu? São várias frentes, o Bolsonaro, o governo dele é incrível e a figura dele, porque ele nasceu, se desenvolve e se mantém por meio de uma rede. Ele não tem o controle dessa rede, mas o menino está lá na ponta, ele está operando e ele tem essas conexões e faz essas conexões. É nessa área de direitos humanos, jornalismo, meios acadêmicos não é rede. São grupos dispersos, é todo mundo um atacando o outro. A universidade faz um trabalho, o jornalismo faz outro, são redes assim que mal ou bem, com todos os seus problemas, atuam em prol de uma expansão do sistema de cidadania, do sistema democrático. Essa gente não, o Bolsonaro, a vitória dele é a vitória dessa rede e quando essa rede é influente, ela tem um controle absoluto, ela tem uma vigilância, ela tem um foco, se o repórter tal bateu em alguém, logo vem uma manada, ela se aglutina ali, então ela tem muito mais capacidade.

P9 - Agora em relação a potencialidades, na sua opinião, quais são as principais potencialidades do ecossistema de comunicação digital para o trabalho de investigação jornalística?

S3 - É um outro mundo, outra plataforma de comunicação e eu acho que não entra só a questão do jornalismo, mas do setor da comunicação. A demanda por comunicação, que é

algo do ser humano, querer ser informado, está muito mais cheia de possibilidades de interação. Não sei como que o jornalismo entra nisso, se vai entrar. Porque o jornalismo, de certa forma, tem um *know how*, um *know how* produzido ao longo de dois séculos. Não sei como vai ser a sua entrada nessa nova plataforma econômica, nessa nova plataforma de informação, mas a demanda por informação, ela, claro, tem um leque muito maior. O que eu acho é que o jornalismo em si, eu está conversando com cara, ele era da Polícia Federal, estava se aposentando e estava montando uma empresa de inteligência para empresas, porque hoje as empresas passaram daquela fase do juridiquês e entraram nessa coisa da investigação da concorrência de mercado mesmo. Aí ele falou para mim assim, eu estou atuando nessa área, é muito legal, muito interessante, mas às vezes falta pessoas para conectar tantas possibilidades que nós temos, dizer para que serve tantas possibilidades que a gente descobre, aplicativos, possibilidades, muitas ferramentas tecnológicas, mas não tem alguém que conecta isso, articula ou até mesmo busca um cliente para aquilo. As coisas que ele falou, eu falei assim, isso aí cabe ao jornalismo, o jornalismo é justamente essa capacidade de conversar, de dialogar, de entender o que o outro quer, de ouvir e passar para o papel de uma forma mais simples o que o outro já está querendo, você conversa com um, está passando para o papel aquilo que ele falou, mas já pensando na cabeça de um terceiro, então, isso é jornalismo. Esta lacuna aí caberia ao jornalista fazer e hoje o agente da comunicação, eu acho que está passando ao largo do jornalismo em si, das escolas de comunicação, é um cara absolutamente multidisciplinar, "multitudo", com vários conhecimentos.

P10a - Na sua opinião, os jornalistas investigativos da atualidade estão preparados para lidar com vazamentos e com vazadores? Você se preparou para isso?

S3 - Essa discussão veio à tona com o *Panama Papers*, passar o conteúdo das informações na íntegra ou resguardá-las para tratar jornalisticamente, ali houve um embate de duas visões que são absolutamente conflitantes, mas absolutamente corretas. Um repórter que pegou as informações e acha que tem todo o tempo do mundo para preparar o material, a informação que ele quer, isso é da essência do repórter, e do outro, o profissional que acha que o interesse público é maior naquele momento e tem que ser naquele momento, repassar tudo e é igual agora estão questionando o The Intercept. Tem coisas que é do repórter, é do tempo dele. Se o repórter começar a ceder para o "interesse público", ele morre. Ele que deve decidir, se o Gleen achou que deve ser aos pouquinhos, é deles as informações, a fonte passou para eles. As pessoas estão passando vergonha com essa história de dizer que o cara é um criminoso, isso é um absurdo, porque quem é criminoso foi quem tirou dos caras lá, ele passou e não tem essa de ser crime. É tradição do jornalismo publicar o que chegou na mão do repórter, vazou e ponto final. Mas isso não é legal? É tradição, foi assim que a imprensa se consolidou e você pode perguntar para dez, quinze pessoas que não estejam magoadas hoje com a prisão do Lula ou com o impeachment da Dilma, mas a imprensa teve um papel fantástico no processo democrático e ainda tem um papel fantástico e ela a vida inteira vazou documento e não precisou dizer. Não vou nem conversar sobre isso. Isso é da história do jornalismo. Jornalismo é isso. Se querem dizer que o jornalismo não pode existir mais, ok, é uma discussão, ou a gente acha que não precisa mais de jornalismo, o jornalismo não é bom para a sociedade, ok, é um argumento, vamos discutir isso aí, vamos acabar logo com o jornalismo. Mas o [que] você está falando?

P10b - É no sentido de preparo mesmo para lidar com isso e se você se sente preparado para lidar com isso?

S3 - Eu me sinto, o que eu não sinto é as empresas, porque grandes vazamentos sempre tiveram, não é de hoje. Eu já estou há 18 anos em redação de jornal e às vezes cai assim, caiu há uns dois anos aquela lista do Facchin, documentos pra caramba, aí quando você tem uma estrutura, o que acontece, a chefia convoca todo mundo e você faz isso, você faz aquilo, a toda uma estrutura. Hoje, eu vejo enxugamento das empresas, se o repórter chegar hoje falando assim para o chefe, eu achei um arquivo aqui e é fantástico, eu tenho que apurar mil histórias, então vai apurando e quando você tiver uma coisa consolidada você traz para gente. Então quer dizer, o momento atual é muito complicado para isso, mas a imprensa sempre soube lidar e trabalhar isso.

P10c - Como você conseguiu se preparar para lidar com esse tipo de vazamento, esse tipo de volume de informações?

S3 – Primeiro, o conhecimento do repórter em relação ao tema, porque às vezes ele achou o arquivo do INSS. E olha rapaz, é uma coisa comum para caramba repórter chegar em redação de jornal falando: "eu tenho aqui o 'mundo'". O repórter tem que dizer o que é aquilo, porque se não o jornal não vai ter condições de colocar a sua equipe inteira para ficar uma semana, duas semanas, um mês naquilo e não dá em nada, entendeu? Então primeira coisa é o repórter. Eu acho que é muito da formação do repórter, não é um conhecimento específico, se o cara tá apurando muita coisa, sabe que aquilo ali realmente tem informação, ele vai atuar ali, ele não vai nem conversar com o redator dele, ele vai direto no chefão e passa por cima.

P11 - Na tese, a gente defende a necessidade de estímulos e convenções relacionados com a formatação de uma cultura de riscos digitais para jornalistas. Na sua opinião, esse aspecto é importante para o jornalismo investigativo contemporâneo?

S3 - Acho que importante é a formação do repórter. Você tem um novo contexto no jornalismo, na política, no jogo do poder e que a imprensa não está preparada, nem um pouco preparada. Acho que congressos, fóruns de discussões, tem a valorização dessa figura do jornalista investigativo, algo que é muito recente, geralmente falavam, esse aí é policial, esse é delegado, sabe de forma pejorativa por colegas e hoje você já tem esse status dentro das redações, qualquer um, setorista da Polícia Federal, virou repórter investigativo. Então há um status e isso foi bom, mas você não tem uma cultura nas redações de investigação em um novo contexto, isso não tem, não tem recursos para isso, não tem estrutura, não tem capacidade de pensar as coisas. Nós estamos muito ilhados, os jornais brasileiros. Tem essas experiências *Panama Papers*, tem algumas interfaces do Brasil, com aquela turma do IPS no Peru, do jornalista latino americano de investigação, eu já fui em vários eventos deles, mas nós não temos conexão com o jornalismo americano, com o jornalismo europeu, com essa gente toda que está fazendo investigação. Nós não temos também grupos definidos, assim, interessantes, como os órgãos americanos que você têm as relações ali com a imprensa, as nossas relações com a Abin, gente que fica cortando jornal ainda para fazer relatório. Hoje, o mundo global, o crime cibernético, o crime digital, toda essa questão das relações dos crimes organizados, a gente está passando batido por isso. Nós estamos longe desse contexto, desse novo jogo, da forma que está sendo jogado e o Brasil é um país ilhado, nós não temos relações com ninguém.

P12 - Chegamos à última pergunta que tem relação com isso. Essa questão de se preparar para esse novo jogo. Como isso pode ser fomentado entre os jornalistas?

S3 - Eu acho que o jornalismo tem que se abrir para o país. Não adianta ficar reunido em congresso em São Paulo. O que eu acho é que a gente tem que se abrir para outros setores da sociedade brasileira, meio acadêmico, por exemplo, eu escuto muito isso assim, o meio acadêmico está em uma ofensiva contundente e as empresas, a gente vai buscar *know how* lá do New York Times, no El País. Se abre para as universidades e as universidades que se abram também, para esses grupos da área jurídica. Eu acho que o jornalismo se fechou demais, para mim é uma coisa muito cara e às vezes eu não consigo nem explicar. Quando eu olho para a imprensa, olho assim, ele está fazendo um jornalismo legal nas matérias, nos jornais, essas matérias às vezes vão sair na televisão, o jornalismo acompanha o poder e até está acompanhando bem, mas a gente não tem conexões com gente que está pensando um novo momento no mundo. Não tem interfaces, o jornalismo está ilhado com aquelas coisinhas antigas, visões antigas de reportagem e ele não está conectado com os diferentes atores sociais. Então, eu acho que as conexões do jornalismo com a sociedade brasileira é que têm que ser retomadas. É o que está ocorrendo de 2013 para cá, você vai ver muito isso. Então quando se fala essa questão aí, eu acho que os jornalistas têm que buscar parcerias. Porque não adianta ficar discutindo tecnologia, que tecnologia está mudando toda hora. O que eu vejo, não só do jornalismo, eu vejo até do ponto de vista democrático, do sistema democrático. Outra coisa que você fala muito de vigilância e controle, é monitoramento e cobrança em relação aos órgãos públicos de investigação, especialmente o TCE. O grupo de trabalho que o TCE montou para investigar *fake news* não deu em nada, chamaram representantes do FBI, não sei quem da Polícia Federal, colocaram gente do mundo inteiro e não deu em nada. Quer dizer, para que serve a Justiça Eleitoral, então tem que ser discutido imediatamente essa questão das eleições por meio das redes sociais. Eu acho que é muito cobrar desses órgãos a garantia de que os princípios democráticos vão ser respeitados.

Sujeito 4 (S4)

P1 - Qual é a sua percepção sobre o contexto de vigilância comunicacional que a gente chama de vigilância comunicacional nociva de ferramentas utilizadas por jornalistas. O que você entende sobre isso?

S4 - Eu nunca tinha escutado esse conceito de vigilância comunicacional, para ser bem sincera contigo. Eu tomo alguns cuidados, para falar algumas coisas. Coisas básicas, nada demais, por exemplo, o Telegram, agora com a Vaza Jato, ficou complicado, mas quando eu me comunico com meus colegas que estão fazendo coberturas sensíveis eu falo pelo Telegram ou pelo Signal. Ultimamente, eu tenho falado muito mais pelo Signal. Quando eu vou falar com pessoas que estão em situação de ameaça, proteção, fontes em off, fontes de governo, etc.

P2 - Você acha que esse contexto da possibilidade de vigilância das comunicações, tipo de alguém estar vendo ou ouvindo, tanto por parte de governos, quanto de corporações, alguém com possibilidade de interferir, de visualizar as suas comunicações, você acha que isso afeta o seu trabalho no dia a dia de alguma forma, quando você aborda temas sensíveis?

S4 - Sem dúvida nenhuma, porque eu estou falando com pessoas que muitas vezes não querem que outras pessoas escutem ou saibam do que elas estão falando, que não seja eu. Tem uma questão de confiança ai que seria abalada mais séria.

P3 - Na sua opinião, podemos afirmar que o aumento da capacidade de vigilância, por parte dos governos e corporações, modificou o jornalismo como um todo e o jornalismo investigativo em particular?

S4 - Impacta só com maiores cuidados. Não cerceou nada do que a gente já tivesse. Inclusive, eu acho que houve um avanço nos últimos tempos da transparência. No acesso à informação, ficou melhor. Agora com o novo governo, um pouco pior de novo.

P4 - Tem algum caso emblemático relacionado à vigilância ou que envolveu segurança digital no decorrer da sua carreira? Situações em que estava sendo monitorada de alguma forma?

S4 - Não, só a questão das ameaças mesmo. Em rede social, já tive casos de mandar mensagens diretas no Facebook. No Facebook direto, me desqualificando, especialmente quando eu cubro presídios. "Porque bandido bom é bandido morto!", que eu tinha que adotar um bandido, levar o estuprador para cuidar dos meus filhos. Nenhuma ameaça de morte explícita, mas coisas que me fizeram repensar a minha segurança, então, por exemplo, eu tenho um botão de pânico no meu celular. Se eu estiver em uma situação de perigo, eu aciono e três pessoas recebem a localização e começa a gravar automaticamente o meu celular. Eu tenho alguns protocolos de segurança, para fazer coberturas em locais violentos ou situações violentas, sempre ter alguém informado, nunca ir sozinha, ter sempre duas baterias, ter identificação de jornalista, nunca ir disfarçado. Eu tomo alguns cuidados de segurança que são mais físicos do que cibernéticos.

P5 - A gente pode dizer que você se preocupa com a segurança digital? Se sim, desde quando?
S4 - Sim, 2013. Quando começaram as manifestações de 2013, que começou a vir esse ódio contra a imprensa, percebi que ali era o caso de tomar mais cuidado.

P6a - Na dimensão de tratamento com fontes, você adota estratégias para proteger a identidade das suas fontes? Quais as formas de contato que adota com fontes que têm informações sensíveis?

S4 - Por Signal, principalmente. Eu tomo todos os tipos de cuidado para que essa fonte não seja identificada. Nunca, jamais, colocá-la em situação de perigo, mas acho que muito é a confiança mesmo que ela tem comigo e que eu consigo assegurar a ela.

P6b - E o contato na esfera digital?

S4 - Se puder encontrar pessoalmente é muito melhor, mas eu tomo cuidado assim, não identificar onde ela mora, onde ela estuda, não coloco inicial. Nada que possa levar a identificação dela.

P7 - Isso aqui é meio redundante, você até já falou alguma coisa das principais estratégias de segurança digital que você adota durante investigações jornalísticas de temas sensíveis.

S4 - Signal, esse botão de pânico que é muito importante, ter alguém informado de onde eu vou e avisar mais ou menos "eu vou a tal lugar, a tal hora e se não voltar presta atenção" e prefiro não ir sozinha.

P8a - Na tua opinião, quais são as principais vulnerabilidades enfrentadas pelos jornalistas que desenvolvem investigações jornalísticas em um possível contexto de vigilância massiva das comunicações digitais? Quais são as principais vulnerabilidades que esse ecossistema que apresenta essa possibilidade de vigilância, que tipo de vulnerabilidades você consegue identificar para os jornalistas investigativos?

S4 - Você sabe que na época da campanha, lá na redação no "portal X", teve uma menina que fez uma matéria, ela entrou em um grupo de bolsonaristas mulheres, se identificou como jornalista e aí na hora que ela se identificou como jornalista ela foi excluída. No dia seguinte, entraram no WhatsApp dela apagaram todas as mensagens e mandaram para ela "Bolsonaro 17". Morri de medo, eu tenho medo, mas eu acho que eu nunca tive contato com uma coisa assim, nesse nível de ameaça digital. Que alguém vai roubar as coisas que estão aqui [smartphone]. A jornalista x [passou por um ataque digital] me contou, porque liguei pra ela quando aconteceu aquilo, a gente é bem amiga, queria saber se ela estava com medo, ela não estava com medo, porque ela cobre guerra e o psicológico dela é outra coisa. Ela falou [que] apagaram todas as mensagens de WhatsApp, só que ela tinha backup de tudo. Então, uma pessoa que já tem esse cuidado de ter o backup. Tem um negócio daqueles ProtonMail[206] que às vezes eu uso, é um e-mail, que não sei, é muito mais criptografado.

P8b - Uma ferramenta de correio eletrônico?

S4 - Você podia entrevistar esse jornalista argentino, Hugo Alconada, ele trabalha no La Nacion. Eu fiz um Workshop com ele, ele é um cara superacessível. Dá uma olhada nas coberturas que ele faz. Se você mandar um e-mail, ele responde.

P8c - Então só para a gente entender, a principal vulnerabilidade é?

S4 - A falta de conhecimento que a gente têm. Eu acho que a gente tinha que ter, a gente tem zero conhecimento sobre internet, na redação. Então, não tem um cara que cobre a internet. O cara que cobre, cobre superficialmente o Facebook. A gente não sabe nada de *Deep Web*. Então, a gente está muito exposto, de fato. O Alconada, por exemplo, estava contando que lá no La Nacion tem um computador que é só para acessar a *Deep Web*, porque ele (o computador) dura três meses. Então a gente não tem o menor conhecimento disso, se a gente tivesse, a gente teria identificado a chegada das *fake news*, isso é um problema. Uma omissão nossa, a gente não está investindo nisso, acho que seria ótimo.

P9a - Eu também estou trabalhando, além das vulnerabilidades, as potencialidades. Aí eu queria saber a sua opinião sobre isso. Quais são as principais potencialidades do ecossistema de comunicação digital para o trabalho de investigação jornalística?

S4 - Eu não manjo nada disso. Eu não faço investigação por aí.

P9b - Não utiliza esse tipo de instrumento?

S4 - Não conheço. Acho que tem gente aqui, bastante gente conhece. Fala um aí só para saber.

[206] É um serviço de correio eletrônico criptografado.

P9c - Banco de dados, às vezes é citado, "utilizo banco de dados para fazer as minhas investigações". A colaboração, algumas pessoas citam isso com uma grande potencialidade que possibilita a aproximação através da comunicação digital.

S4 - O advento de dispositivos tecnológicos facilita demais a nossa vida. Claro que agora com o negócio da Vaza Jato, imagina quantos jornalistas estão preocupados. Isso que a gente estava falando, o nível de exposição e vulnerabilidade. Quando você tem uma conversa privada de fato, é muito delicado se ela é publicada, publicizada, mas não é o que o Intercept está querendo fazer. Mas os dispositivos tecnológicos facilitaram muito [para] a gente fazer esse tipo de conversa e não ter que telefonar, porque pode ser grampeado. Bancos de dados é óbvio né, e as pesquisas também, acho que as pesquisas de Google Trends[207], isso ajuda também na investigação.

P10a - Na sua opinião, os jornalistas investigativos da atualidade estão preparados para lidar com vazamentos e vazadores? A gente está vivenciando, coincidentemente, um momento que um grande banco de dados está sendo base de ações jornalísticas, os jornalistas estão preparados para lidar com isso?

S4 - Não, mas acho que a gente está aprendendo. E assim, claro, um vazamento dessa dimensão não. O vazamento sempre fez parte do jornalismo, todo mundo trabalha assim. Tem processo que é sigiloso e tal. Claro que você não vai lá fazer um pedido formal disso. Você tem que ter uma fonte boa que fale: "isso aqui te interessa então vou te entregar sob sigilo". Com toda uma série de cuidados que você precisa ter com aquela determinada situação. Então, pequenos vazamentos nesse sentido sim. Grandes vazamentos, acho que a gente está apreendendo agora. Eu estou achando a estratégia do Intercept muito, muito interessante. O *Panama Papers*, claro, era um pool de 360 jornalistas investigativos do mundo inteiro, que elite é essa que tem acesso a isso. E em nenhum momento aquilo vazou. Acho isso um milagre quase, sabe? A coisa do Intercept também acho um milagre, quantas pessoas estão nessa equipe? Não sei, mas se forem 15, cara não contar para ninguém o que tem ali... É muito legal de ver que está funcionando e o jeito que eles estão vazando, na minha opinião, é a melhor estratégia que estão fazendo para proteger o jornalismo que está sendo muito atacado. Então, tanto vazar pílulas, como ter o cuidado máximo para entender o que é o interesse público e não expor o colega, não expor a fonte que está falando uma coisa íntima, que não tem interesse público. Não é como pegar o WikiLakes e largar para os outros ir lá pegarem. E eu acho que tem uma coisa também da rapidez na informação, que o fato de ir pingando ajuda. Então, a gente está mantendo esse tema sempre importante, porque é. Se fosse vazar de uma vez, com um tanto de escândalo que nós estamos nesse momento, isso iria sumir. Então, para mim, é uma estratégia bem inteligente. E o fato de agora ter parceiros que estão vazando também, acho que isso, no ponto de vista da autenticidade, do interesse público, da autenticidade das mensagens, é uma boa sacada. Mas, estamos apreendendo na marra.

P10b - Eu ia te pedir para a gente pensar especificamente sobre isso, como vai se dar? Vai se dar com a experiência? Ele está se dando ainda, é dinâmico e contínuo?

S4 - Acho que sim. Acho que ninguém estava e tinha se preparado especificamente para receber um conteúdo de tanta informação vazada assim. E eu acho surpreendente, o acontecimento jornalístico mais importante dos últimos anos no Brasil. A única coisa capaz

[207] É uma ferramenta que mostra os mais populares termos buscados em um passado recente.

mesmo de fazer uma mudança de paradigma agora do que a gente está vendo sabe, que a gente estava muito numa surdez e de repente vêm essas coisas como um jeito de acabar com essa cegueira, porque não é possível. Claro que se fosse uma ou duas falas, a cegueira ia continuar, que está continuando ainda. Por outro lado, traz uma importância para o jornalismo que a gente estava perdendo. A gente estava sendo muito bombardeado. Não estava funcionando. Nossa credibilidade estava sendo testada demais e, com isso, a gente volta a ter uma importância. Me dá até uma alegria. Que orgulho de ser jornalista.

P11 - Na minha tese, a gente defende que há necessidade de estímulos e convenções relacionadas com a formatação de uma cultura de risco digitais para jornalistas. Na sua opinião, esse aspecto é importante para o jornalismo investigativo contemporâneo?

S4 – Fundamental.

P12a - Dentro dessa perspectiva, como isso pode ser fomentado entre os jornalistas, na sua opinião?

S4 – Cursos, acho que formação sistemática nas redações seria muito importante. Na universidade também é muito importante. E acho que as organizações de jornalismo também tinham que ter cursos específicos para quem quisesse fazer isso. Aqui no congresso (da Abraji) do ano que vem.

P12b - Capacitação de uma maneira geral?

S4 - Sim. E coisas mais profundas também, não só uma capacitação. Uma coisa mais, sabe? Eu adoraria. Eu não entendo nada. Esse negócio de planilha eu não curto, mas acho que é muito importante. Então, eu faria, por exemplo.

Sujeito 5 (S5)

P1a - Para iniciar nossa conversa, qual é a sua percepção sobre o contexto de vigilância comunicacional de ferramentas digitais utilizadas por jornalistas? No estudo, tratamos como vigilância comunicacional nociva.

S5 - Não entendi direito, essa vigilância por parte de quem?

P1b - Corporações e do governo, principalmente.

S5 – Primeiro, eu acho que tem uma vigilância já padrão instalada em qualquer plataforma digital comercial, que é das empresas querendo os seus dados, a princípio, sem distinção de quem você é, então não faz diferença se você é jornalista ou uma pessoa comum. As pessoas querem saber o que você está fazendo, para monetizar isso depois. E aí ainda que a intenção não seja de vigiar é uma instrumentalização que se quisesse ser usada para vigiar, pode ser usada. Então, é muito difícil escapar de qualquer vigilância, de todas as vigilâncias em qualquer espaço digital seja por navegador, redes sociais, enfim. A princípio, no trabalho de jornalismo, como jornalista aqui, no Brasil, hoje, eu não tenho a percepção de que haja algo sistemático de vigilância nem do governo, nem das empresas, mas eu acho que há espaço possível para que isso exista. Eu não me sinto perseguido ou vigiado quando estou fazendo o meu trabalho, mas eu acho que há espaço para que se alguém quisesse conseguisse. Então, em casos de investigações muito sensíveis, o cuidado tem que ser muito grande, desde o começo,

porque se você está só fazendo o seu trabalho do dia a dia, você acaba sendo mais frouxo. E aí ainda que você não se sinta perseguido ou vigiado, você está abrindo portas para que você, de fato, seja. Então, se você está apurando alguma coisa que realmente tem informação que você não pode correr o risco de ser pega ou de ter uma comunicação interceptada, você realmente tem que ter cuidado desde o começo.

P2a - Nesse contexto, você acha que essa possibilidade afeta suas ações durante investigações jornalísticas que envolvem temas sensíveis relacionados a segredos, vazamentos e crimes, você acha que afeta de maneira prática?

S5 - É uma preocupação, sempre que tem alguma informação, alguma investigação que ela é [caracterizada por] temas mais sensíveis, a maneira de comunicação é mais sensível, tem que ter cuidado desde o começo.

P2b - Aí tem mudança na apuração?

S5 - Tem mudança na apuração, tem mudança no meio de comunicação com as pessoas, entre os jornalistas, entre jornalista e fonte, a maneira como você vai buscar informação, principalmente meios de comunicação entre jornalistas, que geralmente essas apurações não são feitas sozinhas, não é? São feitas entre vários jornalistas. Comunicação entre os jornalistas passa por um cuidado muito grande, troca de documentos obviamente e com fontes não precisa nem falar. É diferente.

P3 - Na sua opinião, podemos afirmar que o aumento da capacidade de vigilância comunicacional, por parte de governos e de corporações, modificou o jornalismo investigativo de uma forma geral?

S5 - Sim. Sim, principalmente nos últimos cinco anos. A partir do momento que a internet virou peça central de qualquer investigação que você vai fazer, seja ela baseada em dados digitais ou não. A partir do momento que a internet virou o principal meio de transmissão de informação, mudou tudo, eu acho. As preocupações passaram a ser outras, os problemas passaram a ser outros e aí tudo mudou. As ferramentas mudaram, a forma de comunicar mudou, a forma de passar dados de um lado para o outro mudou. Acho que foi uma transformação, eu não peguei a fase anterior a essa, então eu não sei, eu nunca fiz uma investigação como era feita há 20 anos atrás, mas eu tenho certeza que é bem diferente da maneira como é feita hoje.

P4a - Pode citar casos emblemáticos relacionados à vigilância comunicacional e à segurança digital que ocorreram durante a sua carreira?

S5 - É o que eu posso falar é do *Panama Papers* e outras investigações feitas junto com ICIJ[208]. O ICIJ é um consórcio internacional de jornalistas que desenvolveu um método muito particular de tocar grandes investigações, envolvendo centenas de jornalistas do mundo inteiro. Isso também é uma das coisas que só é possível porque a tecnologia avançou, a internet avançou, as investigações que são feitas hoje seriam impossíveis de serem feitas há 20 anos atrás.

[208] O Consórcio Internacional de Jornalistas Investigativos (ICIJ) foi fundado em 1997 pelo *Center for Public Integrity* e reúne jornalistas de mais de 65 países que buscam investigar delitos internacionais, atos de corrupção, abuso de poder, etc.

P4b - Sobre o caso que, no caso, envolveu a possibilidade de vigilância comunicacional e um protocolo diferente de segurança digital, imagino?

S5 - Com certeza. Eles desenvolveram plataformas próprias com um grau de segurança que não se compara com qualquer outra plataforma aberta na internet para a comunicação interna e para a comunicação com as fontes. Então, mais do que criptografia, eles desenvolveram sistemas internos, para que esses jornalistas tivessem comunicação entre si segura, com várias etapas e várias camadas de segurança, desde o login até a criptografia de arquivo, acesso ao banco de dados, criação de banco de dados próprio, para não ter que depender, várias ações para criar um espaço seguro, para que centenas de jornalistas pudessem trocar informações com segurança, informações sensíveis que não podiam ser divulgadas. Basicamente não usar nenhuma rede estabelecida de comunicação, não usar e-mail tradicional, não usar redes sociais de jeito nenhum para se comunicar sobre a investigação e jamais deixar qualquer contato dos documentos que estão sendo avaliados com qualquer banco de dados público acessível.

P4c - Esse protocolo foi formalizado de alguma maneira entre os jornalistas? E existiu alguma capacitação em relação às fontes também, para que elas soubessem operar as ferramentas?

S5 - Sim, as duas coisas. Todos os jornalistas que fizeram parte das investigações foram treinados nesses sistemas internos e aprenderam a usar, tinha um protocolo muito rígido de comunicação, então não podia conversar sobre as coisas da investigação por meios não desenvolvidos pelo consórcio. Então toda a comunicação era feita em uma plataforma própria. Todos os documentos eram trocados dentro de uma plataforma própria isolada de outras, e aí com as fontes a mesma coisa, exceto as fontes que foram consultadas publicamente, depois que as investigações já estavam com os dados divulgados, quem forneceu as informações, o sigilo nessa relação foi absoluto. Inclusive, a maior parte das fontes que forneceram essas informações não são conhecidas pelos próprios jornalistas que ajudaram a investigar os documentos. Eu, por exemplo, não sei quem é a pessoa que ofereceu os dados lá no começo. Eu tive acesso a todos os dados, mas não tive acesso a essa fonte. Então, foram várias camadas de mediação e segurança para evitar que a informação vazasse. Nos dois casos tanto no *Panama Papers*, quanto no *Paradise Papers* e outras investigações, ninguém sabe quem é a fonte até hoje, exceto quem recebeu lá na ponta.

P5a - Essa pergunta parece ser meio repetitiva, mas só para a gente ratificar isso. Você se preocupa com a segurança digital? Se sim, desde quando?

S5 - Sim, desde que eu comecei a usar, desde o começo do trabalho, como eu já comecei a trabalhar em uma época de jornalismo feito via internet, por meios digitais, eu nunca trabalhei antes dessa fase.

P5b - Quando você começou a atuar no jornalismo investigativo?

S5 - Desde o começo, quando entrei no *"veículo x",* em 2015. Desde que eu entrei, comecei a atuar com isso.

P6a - Você adota estratégias para proteger a identidade de suas fontes? Quais as formas de contato que habitualmente adota com fontes que têm informações sensíveis?

S5 - Sim, óbvio. Aí varia muito a maneira como você vai falar com a pessoa, a maneira como você vai trocar informação e documentos, se for o caso. Varia muito do caso e de que tipo de documento é.

P6b - Como trabalhar essa gradação baixo, médio, alto grau?

S5 - Não, não tem uma classificação formal. Acho que é realmente uma percepção de cada caso, que nível de preocupação aquele caso exige e vai desde de conversa diária com fontes, talvez não tenha uma preocupação muito grande.

P6c - Os teus dispositivos, costuma adotar alguma medida?

S5 - O padrão de sempre, tudo que tem documento, tenho acesso com dois fatores de autenticação, todos os sistemas têm as recomendações básicas de criação de senha, troca de senha sempre. As recomendações básicas de segurança, eu sigo todas as mais normais e alguns casos exigem passos além do que esses, por exemplo, tem fonte que não fala por linha telefônica, porque pode ser grampeado e só faz ligação com WhatsApp, por exemplo, que é criptografado e você não consegue. O WhatsApp eventualmente não vai conseguir fornecer o áudio para ninguém, e não tem como grampear, que é por dados. Esse é o exemplo mais simples. Aí tem fontes que você não se preocupa com isso, porque o assunto que você está falando com ela por telefone não tem nenhum problema, e aí envio de dados, não usar o e-mail pessoal para mandar os dados, eventualmente criar contas de e-mail específicas para tratar de algum assunto. A criptografia de arquivos sempre. Enfim, aí cada caso é um caso, tem caso que realmente não exige esse tipo de preocupação, aí o contato é mais livre.

P6d - Em geral, não tem nada estruturado, um plano?

S5 - Não tem nada formalizado, é claro que, por exemplo, nas investigações da ICJI tinha um baita protocolo. Aí todas as situações eram previstas, mas outras apurações do dia a dia não.

P6e - Esse protocolo está disponível?

S5 – Não, ele é interno, interno para quem fazia parte da investigação. Porque envolvia os sistemas deles, não é uma coisa aberta. Nas outras investigações, investigações do dia a dia é percepção mesmo, você meio que sabe. É claro, está sempre aberto você cometer um erro, deixar uma brecha, mas varia de caso para caso.

P7 - Quais as principais estratégias e medidas de segurança digital que você adota durante investigações jornalísticas de temas sensíveis?

S5 - O principal é muito cuidado com todos os logins e acessos seus, desde a conta de e-mail que você usa publicamente até bloquear celular, desbloquear celular. Enfim, senhas de acesso em geral para qualquer coisa, muito cuidado, sempre trocando, sempre utilizando senhas que não possam ser deduzidas. Envio de arquivos sempre [exige] preocupação de criptografia ou por onde vai enviar o arquivo. Acho que os de sempre são esses e eventualmente a ligação telefônica de não conversar por aplicativos que são abertos ou não usar chat de Gmail, chat do Facebook para tratar de assuntos assim, mas aí são as recomendações de sempre. O padrão é esse.

P8a - Na sua opinião, quais são as principais vulnerabilidades enfrentadas por jornalistas que desenvolvem investigações jornalísticas nesse contexto que a gente está tratando de vigilância massiva das comunicações digitais?

S5 - É sempre a falta de cuidado com essas coisas, seja da parte dos jornalistas, seja da parte da fonte. A vigilância, ela só é feita se você permite. Ela está em todo lugar, em maior ou menor grau e aí o quão você vai deixar ela chegar aos seus dados é uma coisa que depende muito de você, de que níveis de obstáculos que você vai adotar, aí pode chegar a um nível extremo de você não usar um navegador de internet comum, a selecionar o navegador para limpar os cookies do meu histórico de navegação, então têm todos esses níveis e aí a principal vulnerabilidade é que as outras pessoas envolvidas não tomem esse cuidado que você está tomando ou que todo mundo deveria estar tomando.

P8b - Que no caso poderia comprometer?

S5 - Exatamente, exatamente, sempre que tiver, que alguma investigação que a gente, nunca aconteceu, mas se alguma investigação que estivesse fazendo vazasse, ia ser por falha de alguém. A vulnerabilidade é sempre ou ignorância da pessoa, ou o erro, ou a negligência, ou imperícia, a vulnerabilidade maior é sempre a falta de procedimento, de seguir o protocolo de segurança.

P9 - Nessa dimensão, na sua opinião, quais são as principais potencialidades do ecossistema de comunicação digital para o trabalho de investigação jornalística?

S5 - Comunicação, troca de informação, basicamente comunicação. O que fez, o que permitiu um salto incalculável nas possibilidades de investigação jornalística, em relação ao que não existia antes, são os meios de comunicação entre as pessoas. Nesse caso do ICIJ é obvio, você vai colocar 400 jornalistas de 80 países para investigar a mesma coisa sem deixar isso vazar. Era impossível, se não tivessem tecnologias de comunicação e segurança avançadas junto. E aí, claro, tem que ter outras coisas que também melhoram, tipo banco de dados. Hoje em dia, você consegue fazer banco de dados que você não conseguia fazer antigamente, ferramentas de acesso a esses bancos de dados, porque não adianta também se ter todos os dados organizados, se não for fácil e compreensível acessá-los. Assim, o avanço da tecnologia possibilitou ao jornalismo coisas inimagináveis há 20 anos atrás e aí tem todos os problemas que isso traz.

P10a - Outra dimensão que a gente está trabalhando é a questão de vazamentos. Aí a pergunta é a seguinte: Na sua opinião, os jornalistas investigativos da atualidade estão preparados para lidar com vazamentos e vazadores? Você se preparou para isso?

S5 - Quando se diz vazamentos, você diz vazamentos do que está sendo investigado ou os vazamentos de dados para jornalistas?

P10b - Na verdade, quando eu trato de vazamentos, eu trato de grande volume de informações, por exemplo, o caso Snowden ou, agora, o que a gente está acompanhando [Vaza Jato].

S5 - Alguém vazar muitas informações para jornalistas.

P10c - O que a gente está encontrando agora, o WikiLeaks também faz isso, vaza um grande volume de informação, você acha que os jornalistas investigativos atualmente estão preparados para lidar com esses dados e depurar essas informações?

S5 - Acho que existem sim grupos preparados e organizados para isso. O ICIJ talvez seja o exemplo mais evidente no mundo que conseguiu conduzir, o *Panama Papers,* em específico, acho que foi um caso muito paradigmático. Foi a primeira investigação desse tamanho com uma quantidade de dados inacreditável, quase 3 teras de dados brutos. Então, eu acho que esse procedimento mostra que é possível e também abriu caminhos para que novos casos como esse aconteçam no futuro. Até o caso que está saindo agora do *The Intercept* com as conversas é outra prova de que sim, existem, hoje, jornalistas preparados para lidar com isso. Obviamente não são todos, obviamente se aprende muito ao longo do processo, erros podem ser cometidos, mas eu acho que sim, hoje em dia já existe jurisprudência profissional para tratar casos como esse. Aí existem vários casos que são paradigmáticos, que ajudaram a construir essa coisa. O WikiLeaks que foi um pouco diferente, porque ele foi um grande vazamento, só que ele não foi divulgado via jornalismo, os caras divulgaram os documentos brutos. É diferente do que ICIJ fez, por exemplo, eles conseguiram os dados vazados e fizeram um trabalho jornalístico extenso de mais de um ano antes de divulgar as informações. Então são casos diferentes, mas cada um foi criando jurisprudência. A cada caso os jornalistas estão mais preparados, porque você consegue ver o que deu certo e o que deu errado. E acho que esse caso aqui no Brasil, [que] está tendo agora do *The Intercept*, que vai ser importante para isso também, porque é um caso também inédito, de troca de mensagens entre juiz e procuradores da operação mais importante, e como lidar com isso e como publicar o conteúdo. São muitos fatores que têm que ser considerados e também é o caso que eles, com certeza, estão aprendendo à medida que estão desenvolvendo. É muito complexo, um sem número de questões éticas, técnicas, de opinião pública. É um assunto muito nocivo na opinião pública. Para a gente no Brasil muito mais do que foi o *Panama Papers*, por exemplo, embora o *Panama Papers* tenha sido globalmente muito maior, para o Brasil, esse assunto de agora é muito mais nocivo. Tem que considerar tudo isso na hora de publicar. Também é um caso que vai se aprendendo à medida que ele vai se desenrolando. Aí tem a evolução tanto técnica, quanto deontológica da ética, do como divulgar e como falar, como tratar esses dados brutos que você conseguiu ter acesso.

P11 - Dentro da tese, a gente defende a necessidade de estímulos e convenções relacionadas com a formatação de uma cultura de riscos digitais para jornalistas. Na sua opinião, esse aspecto é importante para o jornalismo investigativo contemporâneo?

S5 - Sim. A capacitação para meios digitais é essencial. O trabalho pode ser muito comprometido se a pessoa não tiver conhecimento de algumas coisas, às vezes, bem básicas de segurança digital, sigilo e privacidade. Aí entra tanto as questões éticas, relacionamento com a fonte, quanto às questões técnicas de segurança mesmo. É preciso sim e em um mundo ideal isso seria discutido nas faculdades e na formação básica do jornalista que quer trabalhar com jornalismo investigativo, é base para poder realmente fazer as investigações.

P12 - Dentro dessa perspectiva do que é necessário, como isso pode ser fomentado entre os jornalistas, na sua opinião?

S5 - Acho que um dos jeitos é esse congresso (Congresso Internacional da Abraji). É um ótimo exemplo, que as pessoas vindo aqui para falar sobre esses assuntos conscientizam outras pessoas que eventualmente vão trabalhar com isso também. Formação de jornalistas,

faculdade, curso, capacitação de jornalistas que já estão formados e principalmente fazer desse assunto uma pauta discutida sempre em grupos, entre os jornalistas. E aí pode ser em congresso, pode ser em conversas, enfim, esse assunto tem que estar presente em todos os aspectos da formação dos jornalistas.

P13 - Tem mais alguma coisa que quer falar a respeito do tema?

S5 - Não, acho que é isso.

Sujeito 6

P1a - São 12 perguntas. A primeira é para avaliar a tua percepção sobre o contexto de vigilância comunicacional que a gente chama, na tese, de vigilância comunicacional nociva de ferramentas digitais utilizadas por jornalistas. Qual a tua percepção sobre isso?

S6 - Vigilância por parte de quem, no caso?

P1b - De Governo e corporações, Estados e corporações.

S6 - Eu acho que é tudo muito obscuro. A gente tem muita notícia de fora, de quebra de sigilo e afins, que a gente sabe que acontece tanto por parte de grandes corporações de tecnologia, a pedido de governos, quanto por parte de governos diretamente. Isso, no Brasil, a gente não tem muita informação, a gente sabe que são dispositivos legais que possibilitam que isso seja feito. A gente não tem informação se isso é feito de fato, se é usado de fato, a gente sabe que nos bastidores têm pedidos, por parte do governo, em cima de dispositivo que tem no Marco Civil da Internet, artigo décimo terceiro, incisos segundo e quinto que dispõem sobre isso. É sobre a guarda de dados pessoais por parte de empresas de telefonia, elas têm que armazenar metadados durante o ano. Enfim, esse dado pode ser pedido mediante ordem judicial, a gente não tem como confirmar que isso é de fato feito, mas a gente sabe depois que é feito, mas não necessariamente contra jornalistas. São dados que, enfim, não vão comprometer diretamente uma conversa, mas podem comprometer uma fonte ou algo assim. Já falei que isso é tudo muito obscuro mesmo. São coisas que são muito fáceis de serem feitas, não têm só os jornalistas como alvo, enquanto jornalista, mas talvez como uma pessoa física, só como um bolo no meio de uma multidão. Porque a gente têm muito dispositivo conectado hoje que é extremamente vulnerável, ainda mais em um contexto de AI (Inteligência artificial), a gente tem babá eletrônica em casa que se conecta à internet, mas não tem uma defesa a postos. Acho que a gente está extremamente vulnerável a esse tipo de vigilância. Não é possível dizer o quanto ela é feita em cima do jornalista pela prática da profissão em si, mas dá para dizer que se for feita, o estrago pode ser bastante grande, as consequências podem ser bastante nefastas nesse tipo de caso.

P2a - Em se tratando da sua atuação, como este contexto afeta as suas ações durante investigações jornalísticas que possivelmente envolvam temas sensíveis relacionados a segredos, vazamentos, crimes, etc?

S6 - Eu não atuo muito diretamente nesse tipo de área, não é muito a minha atuação dentro da tecnologia, mas uma coisa que eu faço com frequência é me comunicar com hackers e, para isso, eu tenho que ter uma série de medidas. Alguns eu só consegui conversar pessoalmente até hoje, nunca pude gravar essas conversas. Alguns me permitem anotar porque são pessoas que vão me inscrever o passo a passo para cometer um crime, um crime virtual. Eu aprendi,

por exemplo, a clonar telefone para poder explicar para o leitor como que funciona esse tipo de coisa, assim seria necessário, de fato, saber o passo a passo para clonar? Não, mas eu me sinto muito mais à vontade, eu sinto que vou ter uma forma muito mais, vou ser muito mais didático para o leitor, para explicar como funciona esse processo. Claro que eu não vou dar um tutorial, até porque isso é ilegal. Assim como foi ilegal a pessoa me explicar como que faz isso, mas eu acho que se eu aprender como é que faz, não preciso fazer obviamente, porque isso é um crime, mas ter noção desse passo a passo e, para isso, é uma avaliação caso a caso. Eu sempre defendo que você tem que avaliar tudo caso a caso para você saber e não viver numa paranoia. Tem noções de segurança que você tem que aplicar no seu dia a dia para você pensar em você como alvo genérico, como pessoa física mesmo, não ser alvo de um golpe, não ser alvo de um roubo de identidade. Medidas de segurança básicas que deixam você um pouco menos suscetível a esse tipo de ataque de um criminoso mais ralé que vai usar você para ganhar dinheiro, mesmo como pessoa física. E aí, enquanto jornalista, é a questão de você avaliar caso a caso mesmo com quem você está lidando, quem pode estar interessado naquilo e quais medidas você vai tomar, e também o conhecimento técnico da sua fonte, como eu lido bastante com hacker, isso tende a não ser um problema. É muito mais eu ter que correr atrás e entender como que eu vou fazer para me comunicar com essa pessoa, do que eu ter que ensinar essa pessoa a se comunicar comigo por meio seguro.

P2b - É que as fontes têm um alto nível de conhecimento?

S6 – É, o que eu normalmente vou fazer é entrar em contato com essa pessoa ou com algum conhecido em comum. Algumas vezes já aconteceu de eu ter que acionar esse conhecido em comum e falar: "o teu amigo está me hackeando", avisar ele que sou eu, está de boa, não é treta. E aí a gente vê como que a gente faz. Às vezes a gente conversa por WhatsApp mesmo, dependendo do conteúdo da conversa, às vezes move para algum outro sistema mais seguro. É importante que, assim, normalmente esse intermediário é uma pessoa com quem eu converso com frequência. Então não é uma conversa suspeita, que você simplesmente chega para uma pessoa com quem você nunca conversa e tem aquela conversa uma vez e depois você publica uma coisa. É muito fácil depois com os registros de telefonia ou, enfim, de navegação saber quem foi. Nunca conversou com esse cara, de repente aparece e logo depois a matéria é publicada. Uma pessoa com quem você conversa com frequência, seja um assessor, o assessor de uma empresa ligada a essa pessoa.

P3a - Na sua opinião, podemos afirmar que o aumento da capacidade de vigilância comunicacional, por parte de governos e de corporações, modificou o jornalismo investigativo como um todo?

S6 – Olha, eu acho que está modificando, na verdade. Assim, a gente aprende muito, eu cubro essa área há pouco tempo, na verdade, mas em tempos de informática é bastante, estou há uns três anos. Sempre tive muita relação, uma relação muito próxima com isso, desde criança, mas de trabalho, de atividade profissional têm uns três anos ligado à cibersegurança em si. Enfim, é algo que eu vejo se transformando não só no jornalismo, mas na sociedade, como um todo, e algo [que] assim como privacidade mudou muito com o *Cambridge Analytica*[209], o

[209] A Cambridge Analytica é uma empresa de análise de dados que utiliza comportamentos para direcionar conteúdos. Em 2018, jornalistas do *The New York Times* e *Observer of London*, ligado ao *The Guardian,* revelaram um esquema de coleta, venda e uso indevido de dados de milhões de norte-americanos. As reportagens demonstram como a empresa, fundada em 2013 e conhecida por seus trabalhos nas campanhas pró-Brexit, no Reino Unido, e de Donald Trump, nos EUA, montou perfis, baseados em traços da personalidade, de cerca de 50 milhões de pessoas, com o objetivo de formar opiniões e direcionar votos ao candidato republicano.

escândalo do Facebook, as pessoas passaram de fato a se preocupar com isso e ter interesse nesse tipo de assunto. Acho que agora, com esse trauma, digamos, de supostas mensagens vazadas, envolvendo pessoas de alto escalão do governo, juiz, promotor, eu acho que é algo que gera mais preocupação. Tenho dado palestras agora sobre cibersegurança, por exemplo, que lotou a sala. Tem tido um interesse muito maior. Existem casos em que jornalistas foram atacados no passado e imediatamente depois ofereci treinamentos que [eles] não tinham interesse. Agora, com esse trauma, esse interesse fica maior. Então, eu já tenho ouvido de jornalistas, já da velha guarda, que antes havia muita relutância, que normalmente pessoas mais jovens que estão entrando agora, como já foram criadas nesse meio cibernético, tem um pouco mais de noção de como que isso funciona. As pessoas mais velhas, que estão há mais tempo [que] você, veem o trabalho do tipo, "vou encontrar um 'Garganta Profunda' aí, em um lugar público, vou em um shopping, vou em um parque, que não vai levantar suspeita, para me entregar os documentos", mas logo na sequência está ligando para pessoa. Não adianta nada, mas isso hoje, depois de alguns episódios, também durante as eleições que tiveram alguns ataques a jornalistas, esse interesse começou a crescer, agora depois do episódio da Lava Jato, aí também houve um interesse maior, eu acho que a tendência é que isso aumente.

P3b - Modificação em curso, podemos dizer?

S6 - Modificação em curso sim, acho que a gente tem uma preocupação com o mundo físico muito maior do que a gente tem com o mundo digital, não só os jornalistas, as pessoas como um todo, mas isso, aos poucos, está mudando eles estão percebendo a relevância do mundo digital, que o estrago pode ser tão nefasto quanto no mundo físico.

P4 - Tem um caso emblemático relacionado à vigilância comunicacional ou à segurança digital que ocorreu durante a sua carreira?

S6 - Comigo diretamente, eu já fui hackeado duas vezes entrevistando hackers, uma foi logo que eu comecei nesse mundo, eu queria conversar com alguns hackers, entender como que é o trabalho deles. Isso sem um fim profissional mesmo, só para me preparar, curiosidade de conhecer. Um conhecido fez a ponte com uma pessoa. Por uma coincidência, deve ter acontecido outras vezes que eu não percebi, na verdade, mas, assim, por coincidência eu estava no meu e-mail na hora, comecei a ver e-mails meus sendo abertos, coisa que eu não tinha lido, eu fiquei "ué, o que está acontecendo?", isso [foi] uma enorme coincidência e aí fui entrar, ver quem estava online na minha conta de e-mail e vi que tinha gente online, além de mim. Eu tirava o cara, ele voltava, tirava, ele voltava. Entrei em contato com a pessoa em comum e falei: "bicho, dá um toque no cara aí que enfim". Daí ele falou: "como você entrou em contato com ele do nada, ele está tentando descobrir quem é você e ver que você não é uma ameaça, que não é alguém da PF, relaxa que ele já sai". Depois saiu e eu comecei a adotar medidas de segurança mais estritas. Teve um segundo episódio também, uma pessoa fez a ponte para falar com outro hacker e, nessa hora, ele já me avisou: "ele vai vasculhar toda a sua vida", eu falei: "beleza, eu sei como é". Aí eu sentei para conversar com esse hacker no dia seguinte, a primeira pergunta que eu fiz para ele foi: "e aí o que você descobriu sobre mim?" Ele falou: "cara, eu não tive muito tempo, mas você usa a senha 'tal', né?" Aí eu usava, por sorte, porque eu já tinha tido aquele susto. Hoje já consigo entender qual foi o procedimento que esse hacker adotou para descobrir essa suposta senha. Na hora, eu já inferi

---

Em 2017, o *The Guardian* já demonstrava o interesse da empresa de inteligência britânica em direcionar a população do Reino Unido a adotar uma visão a favor da saída do país da União Europeia. Mais informações em: https://www.nexojornal.com.br/expresso/2018/03/19/O-uso-ilegal-de-dados-do-Facebook-pela-Cambridge-Analytica.-E-o-que-h%C3%A1-de-novo. Acesso em: mar. 2019.

o que ele estava fazendo e que ele estava tentando me intimidar, até então ele não me conhecia, hoje, a gente virou amigo. Ele é um hacker, uma pessoa convertida, ele era um cara, digamos, do lado negro da força e hoje ele trabalha tentando fazer pessoas que assim como ele eram criminosos, não dá para dizer que era criminoso, porque efetivamente ele nunca cometeu nenhum crime, mas ele trabalhava numa área um pouco mais cinzenta. Teve esses dois episódios e também teve um positivo, no caso que eu participei de um evento no qual vários especialistas de segurança foram, tiveram a vida vasculhada, como parte de uma pesquisa, todos voluntários, e tentaram fazer o mesmo comigo e descobriram muito menos de mim do que descobriram de [um] especialista em segurança da informação, acho que foi um episódio, nesse caso, positivo, porque eu tinha tomado várias profilaxias digitais e consegui mitigar esse impacto, mas ainda assim tem coisas que não tem o que fazer.

P5a - Você se preocupado com segurança digital?

S6 - Sim, bastante, o tempo todo.

P5b - Desde quando?

S6 - Eu tive uma preocupação básica desde sempre, por estar sempre no mundo, no meio digital, mas foi nesse ataque que deve ter uns 3 ou 4 anos, está indo para 4 anos, que foi uma coisa um pouco mais assustadora, foi um baque mais forte. A partir daí, foi a escalada mesmo. Foi em 2015, começo de 2016.

P5c - Você se formou quando?

S6 - Eu me formei em 2014.

P5d - A vida inteira esteve imerso?

S6 - Desde criança. Eu era aquela criança que arrumava o computador da vizinhança sabe. O meu primeiro emprego, em 2011, foi de professor de inglês e aí logo, dentro dessa escola mesmo, acabei assumindo funções de marketing, por estar estudando jornalismo e suporte técnico de informática dentro da escola. Sempre tive uma relação muito grande com isso. Comecei a estudar e trabalhar com dados e afins um pouco depois da graduação. Sempre tive muita ligação, muita facilidade com essa área do mundo informatizado.

P6a - Agora vamos falar sobre uma dimensão que a gente trabalha na tese que é o cuidado com fontes. Você adota estratégias para proteger a identidade de suas fontes? Quais as formas de contato que habitualmente adota com fontes que têm informações sensíveis?

S6 - É aquilo que eu mencionei, normalmente, como eu lido bastante com hackers, essa questão do sigilo parte muito deles, eu não preciso nem falar, que eles sabem como isso funciona, sabem muito melhor do que eu, na verdade. Então, assim, eu vou e sigo o que a pessoa pede, eu não preciso evangelizar ninguém, não preciso pregar para convertido. O que era a segunda parte?

P6b - As formas de contato?

S6 - Pessoalmente ou peço para alguma pessoa fazer uma ponte.

P6c - Se for no ecossistema digital, tem alguma estratégia específica?

S6 – É, isso vai depender do grau da treta do que a pessoa está me falando. Pode ser uma mera conversa no WhatsApp ou no Telegram, um chat secreto no Telegram, que vai se autodestruir teoricamente ou aí migrar para um sistema mais escuso. Teve gente que já pediu para entrar em contato comigo por meio de chat de jogo. Nós dois entramos no mesmo jogo ao mesmo tempo, como se estivesse jogando, por lá a gente conversou. Que era para me ensinar como que funcionava um tipo de ataque específico. Aí varia muito e eu procuro, como são pessoas escoladas, eu prefiro deixar esse pessoa à vontade.

P7 - Isso aqui parece redundante também, mas eu acho que a gente pode sintetizar quais são as principais estratégias e medidas de segurança digital que você adota durante investigações jornalísticas de temas sensíveis? No seu caso, que tipo de medidas que você adota recorrentemente?

S6 - Recorrentemente, o uso de senhas mais fortes, não repetir, isso é o básico, uso de autenticação em duas etapas sempre que possível. Tomo cuidado com todas as redes que eu me conecto, na verdade, que eu não me conecto, no geral. É muito, muito raro você me vê conectado ao wi-fi público, por exemplo, ou wi-fi compartilhado, ou wi-fi que eu não conheça. Se eu fizer isso, eu vou adotar medidas de cautela. Eu uso sistemas para proteger o meu telefone, os meus computadores, eu tenho muitas medidas de segurança em prática, eu não uso o mesmo sistema para tudo, dependendo do que eu vou fazer, eu vou usar uma variação do Linux ou uma outra variação do Linux. Uma que vai me oferecer anonimato, uma que vai me oferecer um sistema mais seguro ou Windows para comunicações ou para situações do dia a dia. Assim não vou clicar em links, não vou baixar arquivos, eu vou baixar, eu vou clicar, mas não no meu sistema primário. Então, eu tenho telefones, tenho sistemas só para teste de coisas, assim não vou fazer essas coisas no meu dia a dia, que aí entra uma questão de compartimentalização também. Eu não vou salvar todas as informações em um lugar só quando estou trabalhando com uma coisa um pouco mais complexa ou algo que eu não gostaria que chegasse a público. Criptografia em tudo. O meu telefone é criptografado, o meu computador é criptografado, mas, assim, tem que ter toda uma noção, entender qual é o sistema, o que você está usando, quais são as limitações e quais são os benefícios dele. Porque às vezes você vai ter um custo de usabilidade, vai ser conforme você vai adotando medidas de segurança. Chega o momento que o negócio fica inconveniente, que você pode acabar, você é ser humano, ser displicente com aquilo e deixar algo desligado que, enfim, isso te expõe. Então vale pensar, talvez seja melhor eu baixar um pouco o nível de segurança, mas ter alguma segurança e não usar esse nível mais alto no dia a dia e deixar esse nível mais alto para situações específicas, porque eu sei que vai chegar o momento que vai ser inconveniente, eu vou acabar simplesmente desligando e ficar totalmente descoberto. Então você precisa analisar caso a caso, é importante também, mas no dia a dia, acho que essas são as principais medidas e, claro, bom senso e antena ligada o tempo todo.

P8a - Na sua opinião, quais são as principais vulnerabilidades enfrentadas por jornalistas que desenvolvem investigações jornalísticas em um contexto de vigilância massiva das comunicações?

S6 - Displicência. Você não ter essa noção do ambiente em que você está inserido, você achar que isso é seguro. Enfim, você adotar uma ou outra medida de segurança e ter uma falsa noção de que você está realmente coberto, mas na verdade você não está, porque você não entende realmente como aquilo que você está usando funciona e você não se dá ao trabalho de

perguntar para alguém que realmente entenda. Tem que ter uma preocupação de entender como que aquele protocolo, aquela comunicação que você está fazendo funciona. Como aquela informação sai do seu celular, sai do seu computador, vai para outra pessoa, como e o que pode influenciar nesse meio. Quem pode querer interceptar isso, o que essa pessoa pode fazer com essa informação. Dispositivos legais que podem entrar no meio, então você não ter, de fato, essa preocupação com a sua segurança digital e com a segurança digital da sua fonte.

P8b - Isso é a principal vulnerabilidade?

S6 - Segurança digital, não só pensando em comunicação, nesse caso, comunicação, porque você está se comunicando com uma fonte, mas pensando em segurança digital de empresas, dados que estão guardados em algum lugar, é muito mais difícil você atacar o sistema de uma empresa, do que você atacar uma pessoa. O usuário é sempre o elo mais fraco. A displicência nossa, eu digo displicência, porque eu parto do pressuposto que, no geral, os jornalistas não conhecem essa área, não conhecer não é o problema, isso passa a ser displicência a partir do momento em que você não procura conhecer e entender o ambiente em que você está inserido, para proteger realmente a sua fonte. Entender que essas vulnerabilidades existem e saber quais são. Pode não ter o conhecimento técnico para montar um sistema extremamente seguro, mas você saber que você precisa procurar esse tipo de coisa é importante.

P9 - Tem uma dimensão do trabalho que também trabalha as potencialidades. Aí eu pergunto, na sua opinião, quais são as principais potencialidades do ecossistema de comunicação digital para o trabalho de investigação jornalística?

S6 - Ele é muito bom porque traz muitas seguranças que antes a gente não tinha, apesar de todas essas vulnerabilidades que vêm, também de uma falsa noção de segurança em pontos que ela não existe, mas, por exemplo, é muito mais fácil você interceptar ligações e interceptar comunicação na verdade não ligações, mas SMS, enfim, numa rede 2G do que em uma rede 3G, que é mais fácil do que uma rede 4G, que vai ser mais fácil que uma rede 5G. Então essas coisas vão se atualizando e criam canais seguros. Canal de ligação criptografada. É muito mais fácil você grampear um telefone, do que você grampear uma ligação para um aplicativo de VoIP. Acho que isso traz possibilidades que antes você não tinha tanto para o lado negativo, quanto para o lado positivo.

P10a - Na sua opinião, os jornalistas investigativos da atualidade estão preparados para lidar com vazamentos e com os vazadores?

S6 – Depende, alguns estão. Quem está há mais tempo nesse ramo, alguns estão preparados, têm medidas impostas para isso, mas acho que, no geral, assim, chegar um whistleblower para um jornalista, mesmo que tenha uma característica mais investigativa, todo o jornalista é investigativo por definição, mas que tenha mais essa aura de desvendar grandes mistérios, digamos [que] seja na segurança, enfim. Chegar em uma pessoa qualquer da velha guarda ou da jovem guarda não inserida nesse meio digital talvez tenha uma surpresa negativa. E também no whistleblower, nesses casos, muitas vezes a noção de segurança parte muito mais do whistleblower do que do jornalista, porque não é o jornalista pedindo para alguém tomar essa medida, mas parte dessa pessoa. Existem formas que o jornalista pode ajudar a assegurar o sigilo dessa fonte. Tem um caso, acho que foi no Estados Unidos, se não me engano, que documentos foram vazados e, por padrões de impressão nesses documentos, o governo americano, enfim, o governo responsável, tenho quase certeza que foi o governo americano, por padrões na impressão do papel que foi escaneado e mandado para o jornalista conseguiu

descobrir de qual impressora saiu aquilo. Isso também é algo que é extremamente difícil você esperar que um jornalista esteja preparado, mas também a fonte talvez devesse saber que o lugar onde ela trabalhava, de onde ela estava vazando, que isso seria um problema.

P10b - No seu caso, você se sente preparado? Se sim, como se preparou para isso?

S6 - Acho que, assim, o preparo, você se sentir preparado, acho que é um problema também, porque esse negócio é algo que muda constantemente. O protocolo que hoje é seguro, amanhã pode não ser. Então, você tem que se manter sempre atualizado em relação a essa esfera e descobrir quais são as vulnerabilidades que foram descobertas hoje. Algo que há alguns anos era o estado da arte ou quase estado da arte em segurança, que é o protocolo PGP para criptografia de e-mails, já foi quebrado. Então assim, hoje ele não é tão seguro quanto ele era há alguns anos, amanhã ele vai ser menos seguro do que hoje. Nesse meio tempo surgiram outros protocolos que fazem essa mesma função e são mais seguros. Amanhã também não vão ser. Acho que é sempre um processo de você se preparar e conhecer tecnologias novas, técnicas novas e vulnerabilidades novas também.

P11 - Na tese, a gente defende a necessidade de estímulos e convenções relacionadas com a formação de uma cultura de riscos digitais para jornalistas. Na sua opinião, esse aspecto é importante para o jornalismo investigativo contemporâneo?

S6 - Sim, sim, é importante.

P12 - Nessa perspectiva, como isso pode ser fomentado entre os jornalistas?

S6 - Infelizmente, a gente vai precisar de mais sustos, educação e tempo. Oferecer treinamento, oferecer conscientização, talvez enfiar isso meio que goela abaixo, redações e chefias perceberem que isso é algo que é fundamental, tão fundamental quanto a sua segurança física e fazer com que as pessoas de fato aprendam isso. Não é necessário, novamente, um grande conhecimento técnico, você não precisa virar um especialista em cibersegurança, você não precisa virar um hacker, mas você precisa ter a noção de que essas ferramentas que você usa têm limitações e quais são essas limitações, para que em um caso mais específico você possa procurar ajuda, se for o caso, para lidar com isso. Enfim, tudo passa no fim pela educação mesmo, treinamento.

P13 - Tem mais alguma coisa que a gente não tratou que você gostaria de ressaltar?

S6 - Acho que não, acho que é isso mesmo.

APÊNDICE D – PRINCIPAIS AMEAÇAS, VULNERABILIDADES E CAPACIDADES DIGITAIS PARA JORNALISTAS

Principais ameaças digitais	
Escutas telefônicas sem autorização na redação ou local de trabalho	Ações e estratégias desenvolvidas pelo Estado e por corporações para interferir nas ações dos jornalistas.
Escutas telefônicas sem autorização na casa do jornalista ou em seu telefone celular/smartphone	Ações e estratégias desenvolvidas pelo Estado e por corporações, para interferir nas ações dos jornalistas.
Violação de contas pessoais na internet	Ataques a contas pessoais do jornalista e utilização dos seus dados de maneira nociva.
Furto ou extravio de arquivos ou informações	Exposição de informações e dados sensíveis de maneira involuntária.
Violação ou interceptação de mensagens instantâneas (WhatsApp, Signal ou Telegram)	Forma de intrusão comunicacional que possibilita a intervenção e acesso às interações com contatos e fontes do jornalista.
Violação ou interceptação de e-mail funcional ou pessoal do jornalista	Forma de intrusão comunicacional que possibilita a intervenção e o acesso às interações com contatos e fontes do jornalista.
Coleta de dados de histórico de navegação	Forma de intrusão comunicacional que possibilita visualização de temas e dados pesquisados pelo jornalista.
Violação e invasão de sistemas nas redações	Dados e informações apurados podem ser violados e alterados.
Furto de senhas por meio de phishing [210] *ou pharming*[211]	Visa à obtenção de dados e senhas, de maneira geral, envolvem estratégias de engenharia social.
Instalação e ativação de vírus, malware ou código malicioso para coleta ou destruição de arquivos	Forma de intrusão comunicacional que visa prejudicar investigações jornalísticas.
Monitoramento de navegação em tempo real	Possibilidade de monitoramento e acesso a informações e processo de investigação.
Quebra de criptografia de mensagens ou arquivos	Possibilidade de negligenciamento das mensagens e arquivos de investigações.
Principais vulnerabilidades digitais	
Exposição no ambiente digital	Ocorre pela necessidade de atuação no ambiente digital, para realizar atividades rotineiras ou ocasionais de investigação.
Ferramentas de comunicação digital	Ocorrem pela utilização de aplicações e softwares acessíveis e vulneráveis.
Descuidos de manutenção e/ou não atualização de antivírus ou sistemas de segurança digital	Negligência ou omissão diante de situações de risco que podem facilitar formas de vigilância digital.
Gestão da segurança digital fora do âmbito laboral (família e tempo livre)	Os jornalistas investigativos devem adotar medidas de proteção em seu tempo fora do trabalho (família e tempo livre), pois as relações pessoais também podem se converter em vulnerabilidades.
Principais capacidades digitais	
Capacitação regular para manejar ferramentas de segurança digital	Desenvolver capacidades para explorar as ferramentas de segurança digital e mitigar riscos.
Planos de segurança digital e processos de	Conhecimento, planejamento e apropriação dos

[210] Maneira de obter dados pessoais de usuários, pela utilização combinada de meios técnicos e engenharia social. Ocorre por meio do envio de mensagens eletrônicas que procuram induzir o usuário a fornecer dados pessoais, por meio do acesso a páginas falsas, da instalação de códigos maliciosos projetados para coletar informações sensíveis e do preenchimento de formulários contidos na mensagem.

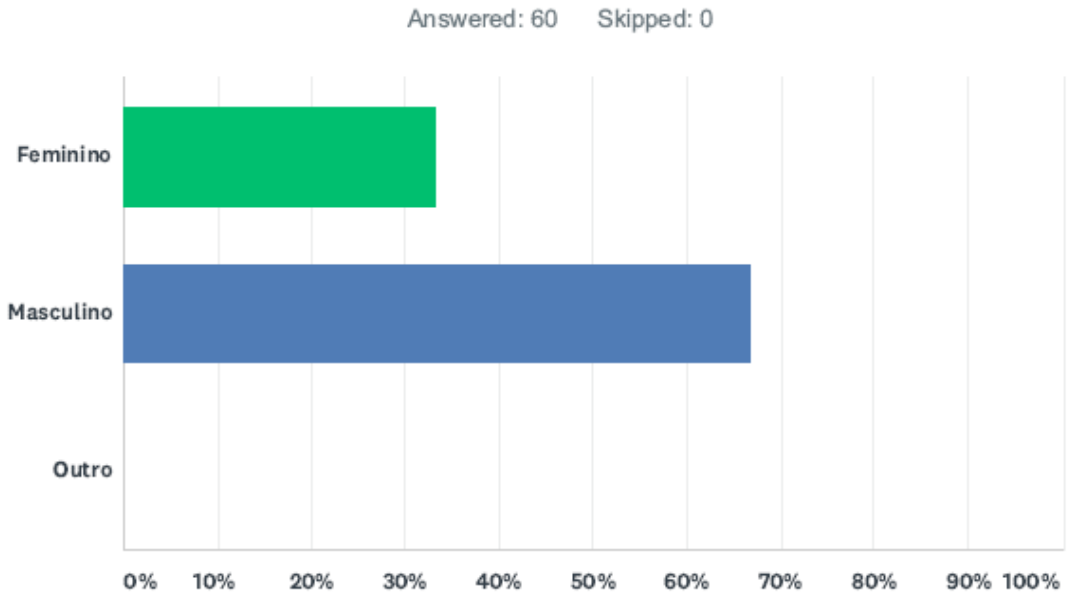
[211] É um tipo específico de phishing que envolve a redireção da navegação do usuário para sites falsos, por meio de alterações no serviço de Domain Name System (DNS). Ocorre quando o acesso a um site legítimo é redirecionado, de forma transparente, para uma página falsa.

investigação	procedimentos de segurança digital.
Habilidade de compreender o contexto e os riscos digitais	Os jornalistas investigativos necessitam de informações precisas de seu contexto de atuação, dos atores envolvidos no processo e de seus interesses.
Capacidade para definir planos de atuação	Os jornalistas investigativos precisam definir e implementar planos de ação com exemplos que envolvam situações de risco.
Capacidade para obter conhecimentos de especialistas em segurança digital	O jornalista investigativo pode recorrer a conselhos e recomendações de especialistas e organizações específicas que possam aumentar a sua capacidade de proteção digital.
Cuidados específicos com fontes que têm informações sensíveis	Adoção de protocolos de segurança digital alinhados aos níveis de risco impostos pela investigação jornalística.
Whistleblower (Vazador)	Estratégias refinadas de contato e manutenção do anonimato das fontes que vazam informações e dados sensíveis. Adequação as possíveis demandas comunicacionais apresentadas pelas fontes.
Cuidados com testemunhas ou vítimas envolvidas na investigação jornalística	Avaliação dos riscos atrelados às vítimas e às testemunhas envolvidas na investigação, por meio de medidas de segurança específicas. Estratégias de reação a possíveis ameaças digitais.
Manter, enviar e receber informação sensível	Os jornalistas investigativos devem ter capacidade de guardar informações sensíveis em formatos seguros, para mitigar as possibilidades de roubo, vírus e demais ataques digitais. Também devem ter protocolos seguros para enviar e receber informações e dados.

APÊNDICE E – GRÁFICOS E TABELAS DA *SURVEY*

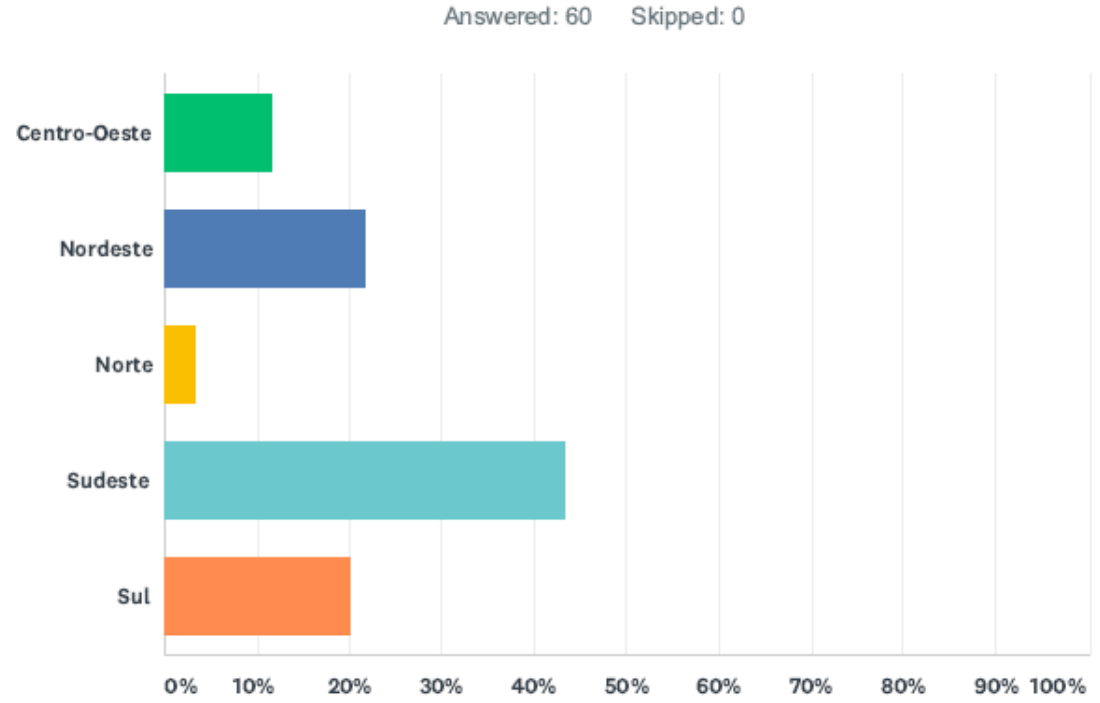
CARACTERÍSTICAS PESSOAIS

Questão 1: Qual o seu sexo?



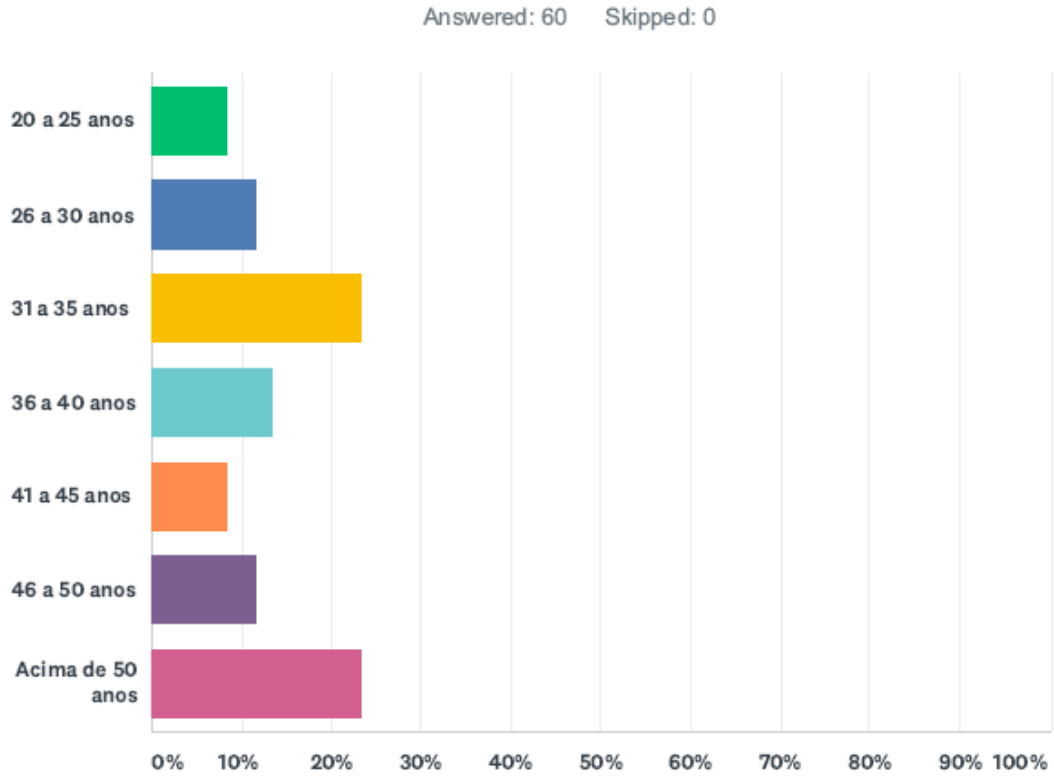
ANSWER CHOICES	RESPONSES	
Feminino	33.33%	20
Masculino	66.67%	40
Outro	0.00%	0
TOTAL		60

Questão 2: Em que região brasileira você trabalha?



ANSWER CHOICES	RESPONSES	
Centro-Oeste	11.67%	7
Nordeste	21.67%	13
Norte	3.33%	2
Sudeste	43.33%	26
Sul	20.00%	12
TOTAL		60

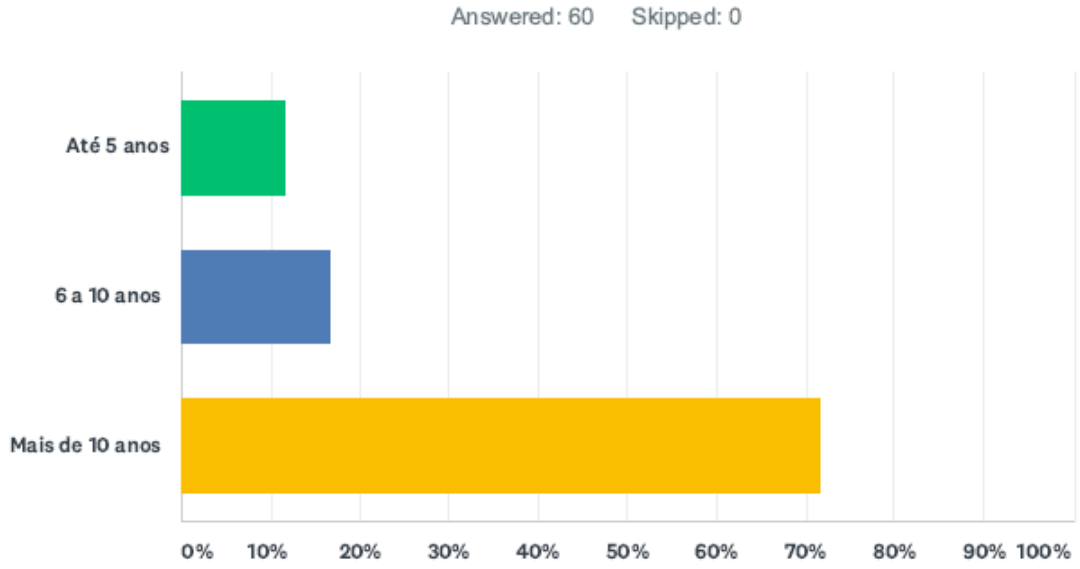
Questão 3: Qual a sua idade?



ANSWER CHOICES	RESPONSES	
20 a 25 anos	8.33%	5
26 a 30 anos	11.67%	7
31 a 35 anos	23.33%	14
36 a 40 anos	13.33%	8
41 a 45 anos	8.33%	5
46 a 50 anos	11.67%	7
Acima de 50 anos	23.33%	14
TOTAL		60

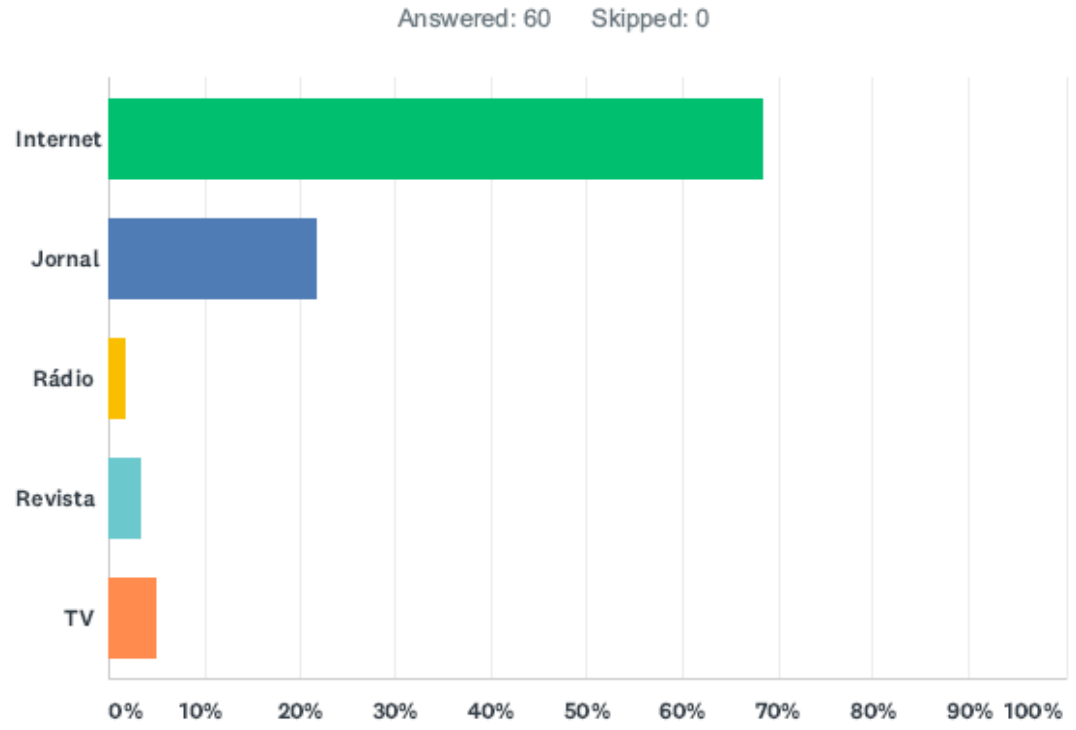
CARACTERÍSTICAS PROFISSIONAIS

Questão 4: Quanto tempo você tem de carreira?



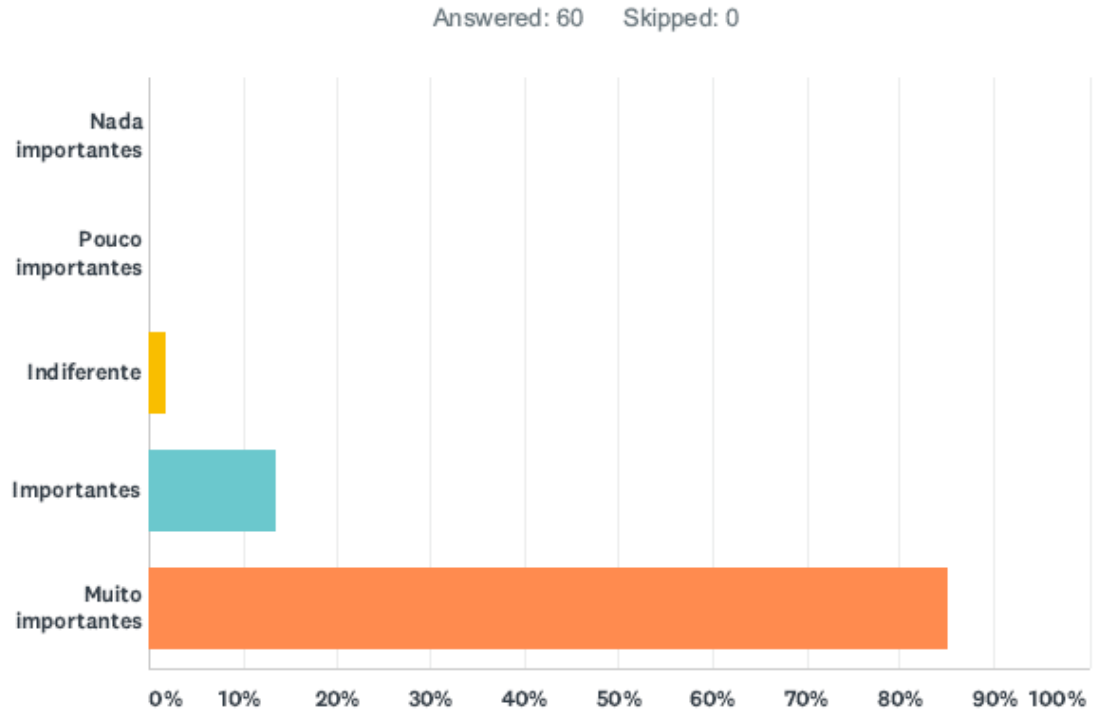
ANSWER CHOICES	RESPONSES	
Até 5 anos	11.67%	7
6 a 10 anos	16.67%	10
Mais de 10 anos	71.67%	43
TOTAL		60

Questão 5: Em que tipo de mídia você trabalha?



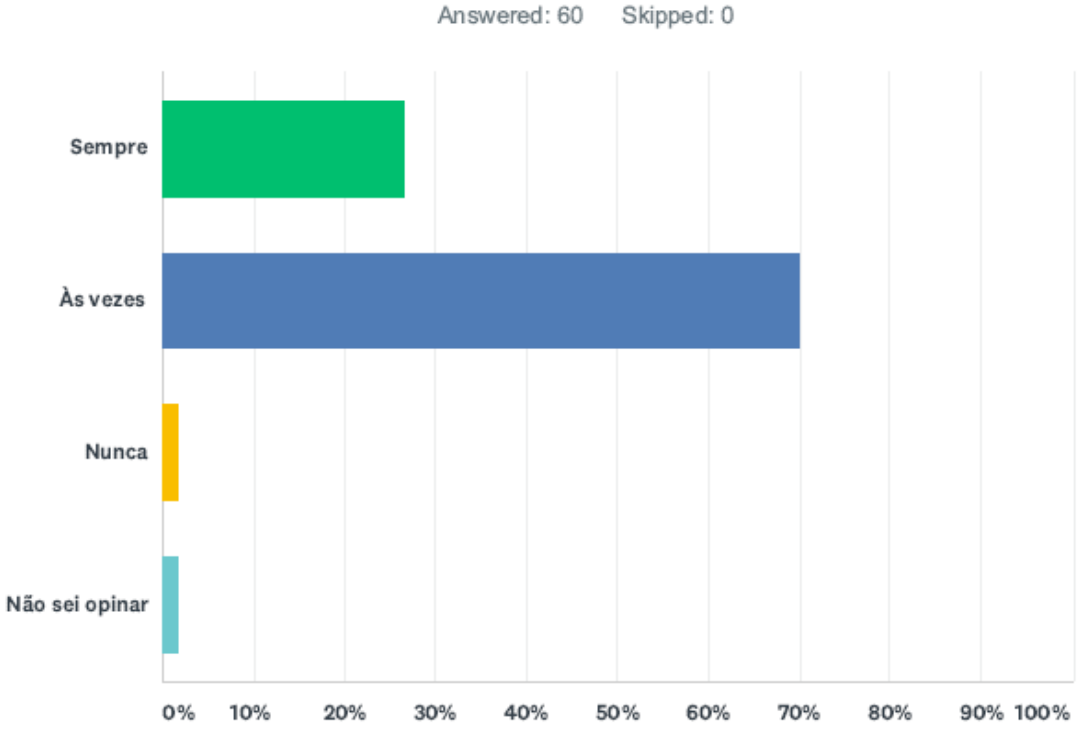
ANSWER CHOICES	RESPONSES	
Internet	68.33%	41
Jornal	21.67%	13
Rádio	1.67%	1
Revista	3.33%	2
TV	5.00%	3
TOTAL		60

Questão 6: Para o jornalismo investigativo, as ferramentas tecnológicas digitais são...



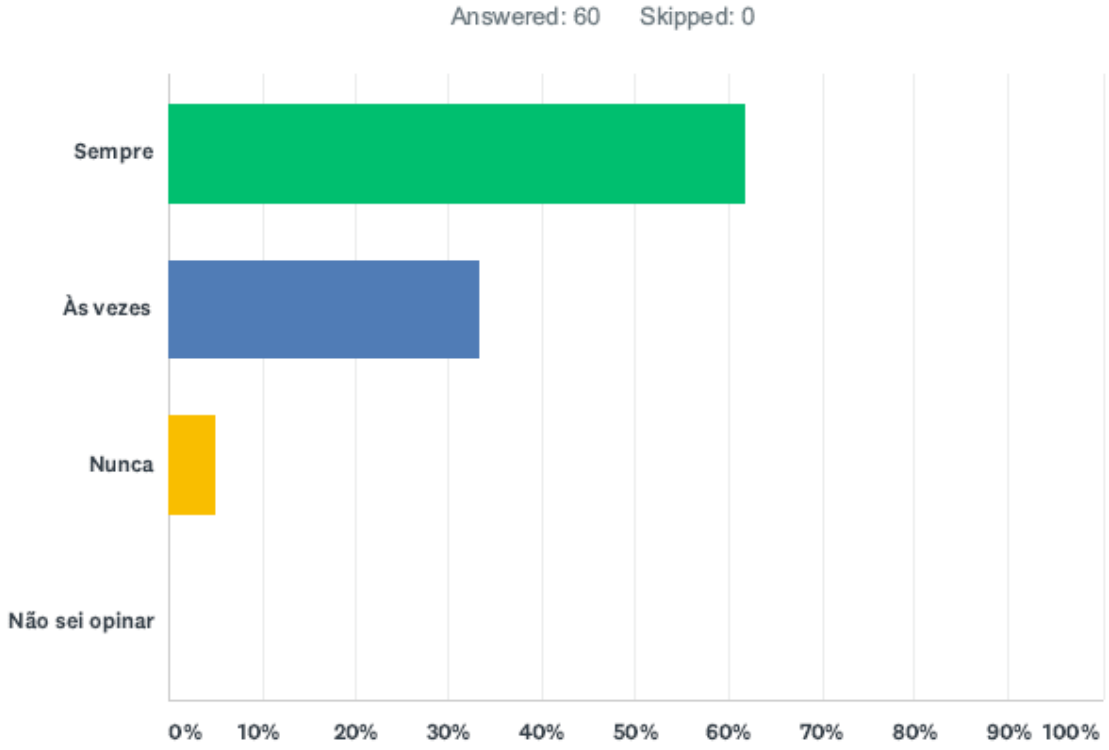
ANSWER CHOICES	RESPONSES	
Nada importantes	0.00%	0
Pouco importantes	0.00%	0
Indiferente	1.67%	1
Importantes	13.33%	8
Muito importantes	85.00%	51
TOTAL		60

Questão 7: Jornalistas se preocupam com segurança digital?



ANSWER CHOICES	RESPONSES	
Sempre	26.67%	16
Às vezes	70.00%	42
Nunca	1.67%	1
Não sei opinar	1.67%	1
TOTAL		60

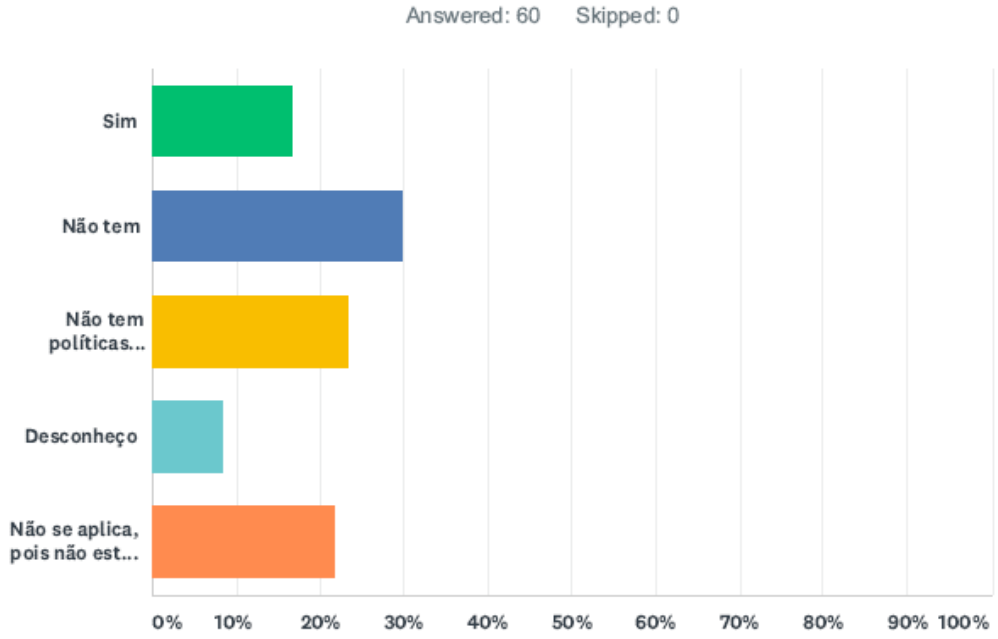
Questão 8: Você se preocupa com a possibilidade de ser vigiado digitalmente?



ANSWER CHOICES	RESPONSES	
Sempre	61.67%	37
Às vezes	33.33%	20
Nunca	5.00%	3
Não sei opinar	0.00%	0
TOTAL		60

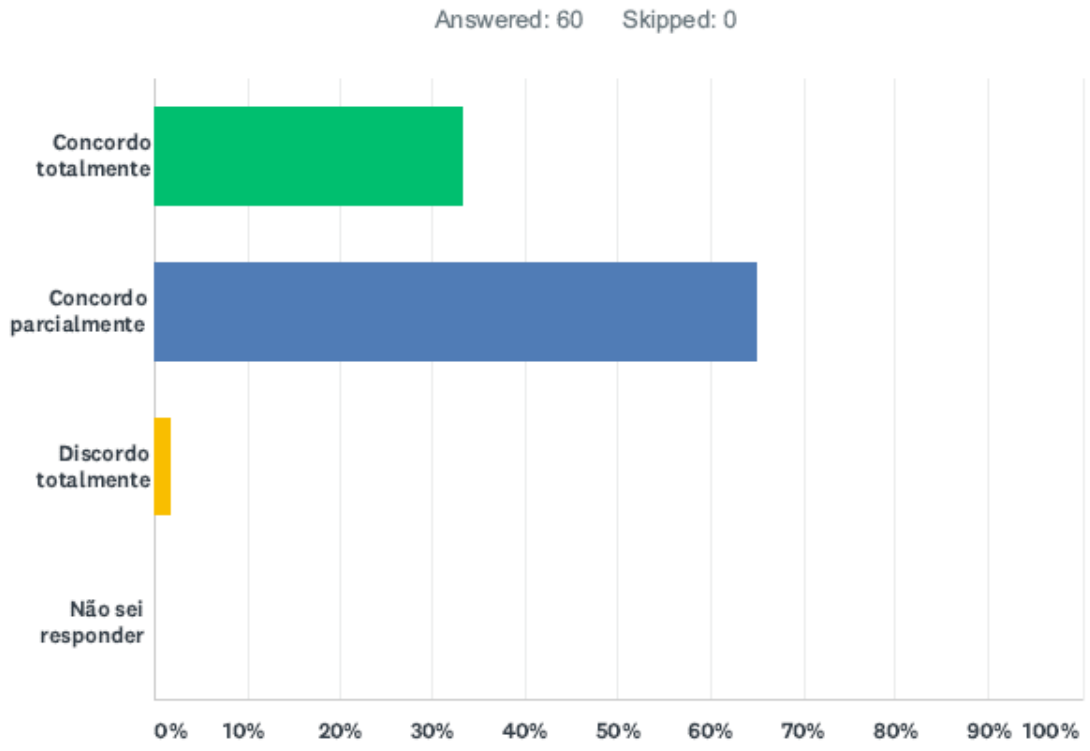
ASPECTOS AMBIENTAIS

Questão 9: No seu local de trabalho, há políticas de proteção de comunicações e informações no ambiente digital?



ANSWER CHOICES	RESPONSES	
Sim	16.67%	10
Não tem	30.00%	18
Não tem políticas específicas, mas orientações para se lidar com o tema	23.33%	14
Desconheço	8.33%	5
Não se aplica, pois não estou vinculado a uma empresa	21.67%	13
TOTAL		60

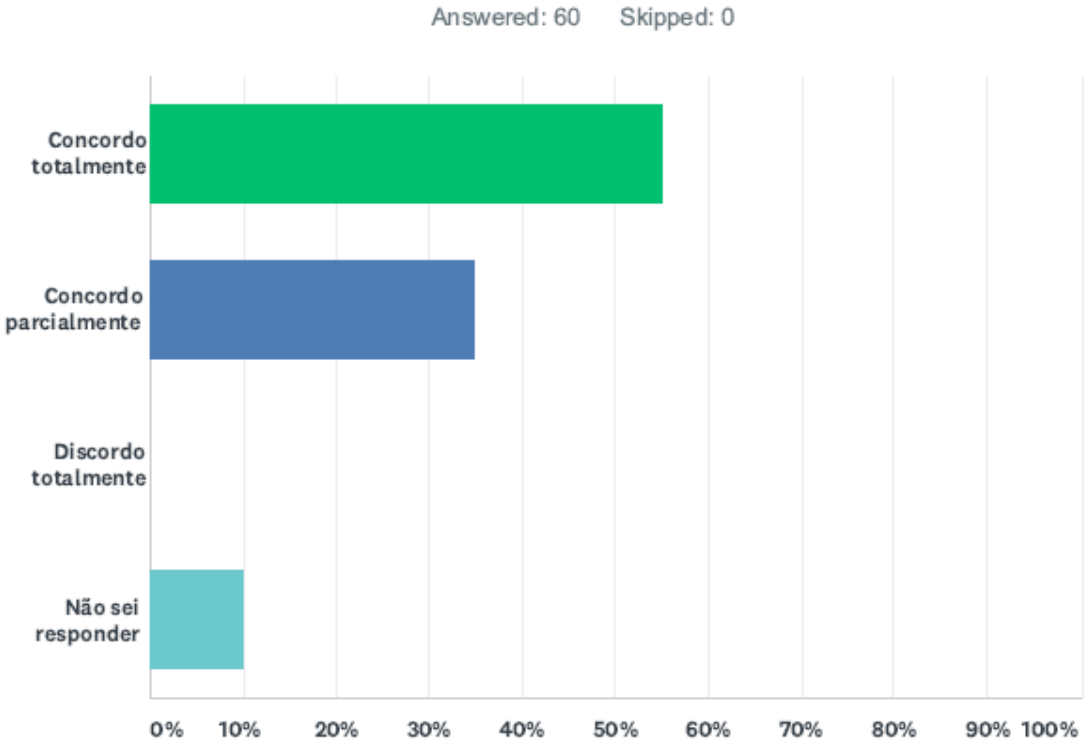
Questão 10: Os avanços tecnológicos das últimas décadas fizeram com que os jornalistas se preocupassem mais com segurança digital.



ANSWER CHOICES	RESPONSES	
Concordo totalmente	33.33%	20
Concordo parcialmente	65.00%	39
Discordo totalmente	1.67%	1
Não sei responder	0.00%	0
TOTAL		60

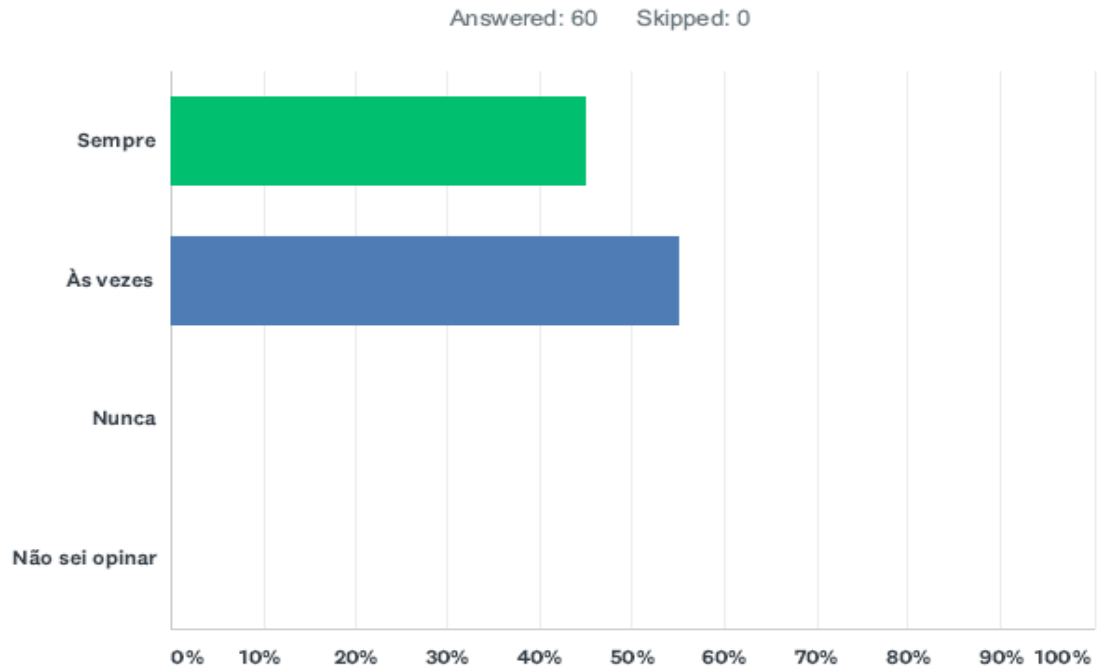
ANÁLISE CONTEXTUAL

Questão 11: Hoje, no Brasil, os jornalistas enfrentam formas de vigilância eletrônica por governos e corporações.



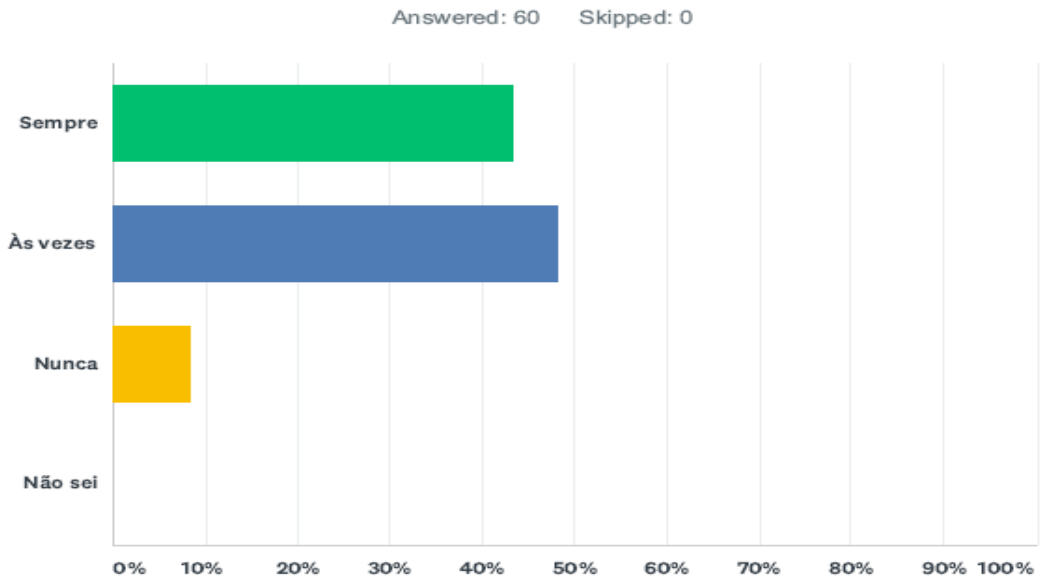
ANSWER CHOICES	RESPONSES	
Concordo totalmente	55.00%	33
Concordo parcialmente	35.00%	21
Discordo totalmente	0.00%	0
Não sei responder	10.00%	6
TOTAL		60

Questão 12: Jornalistas sentem necessidade de intensificar cuidados com a privacidade das fontes e pessoas mencionadas.



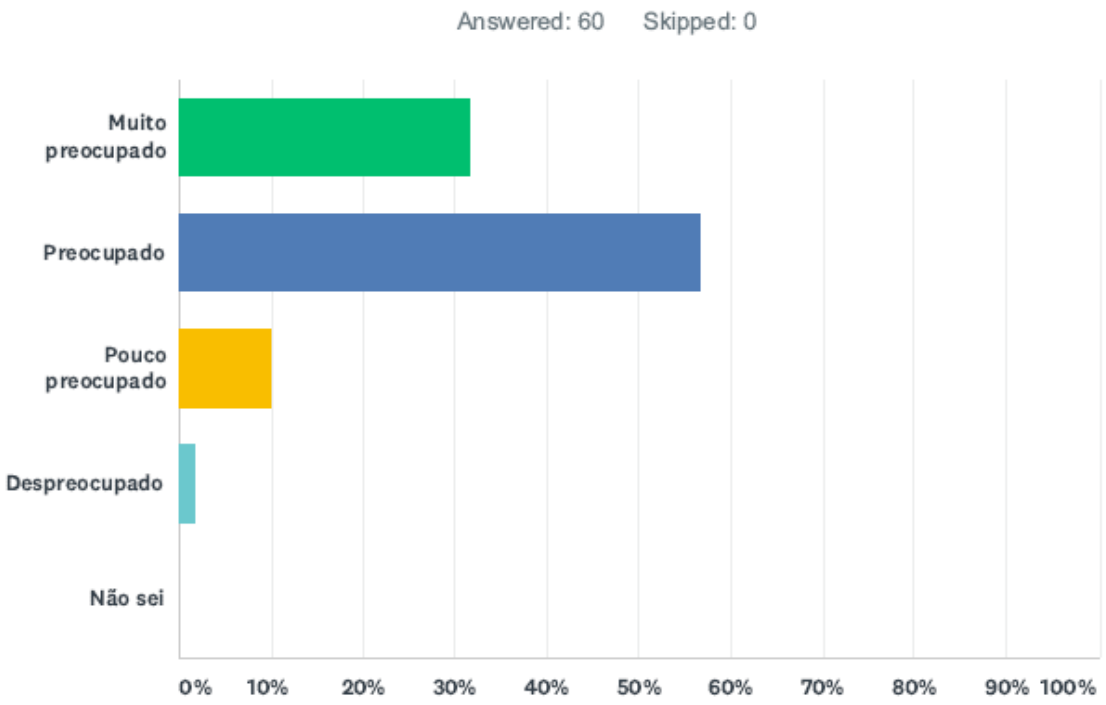
ANSWER CHOICES	RESPONSES	
Sempre	45.00%	27
Às vezes	55.00%	33
Nunca	0.00%	0
Não sei opinar	0.00%	0
TOTAL		60

Questão 13: Você toma providências ou tem atitudes relacionadas a sua proteção no que diz respeito às possibilidades de vigilância comunicacional digital?



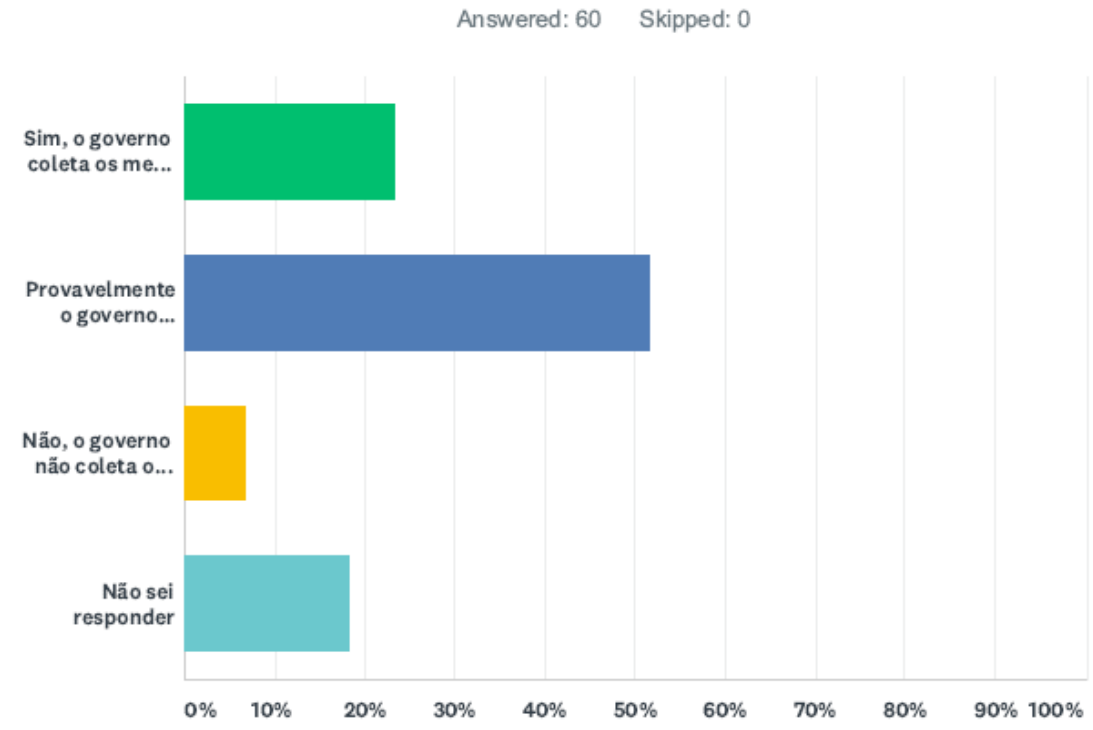
ANSWER CHOICES	RESPONSES	
Sempre	43.33%	26
Às vezes	48.33%	29
Nunca	8.33%	5
Não sei	0.00%	0
TOTAL		60

Questão 14: Quão preocupado você está em relação às formas de vigilância do ambiente digital?



ANSWER CHOICES	RESPONSES	
Muito preocupado	31.67%	19
Preocupado	56.67%	34
Pouco preocupado	10.00%	6
Despreocupado	1.67%	1
Não sei	0.00%	0
TOTAL		60

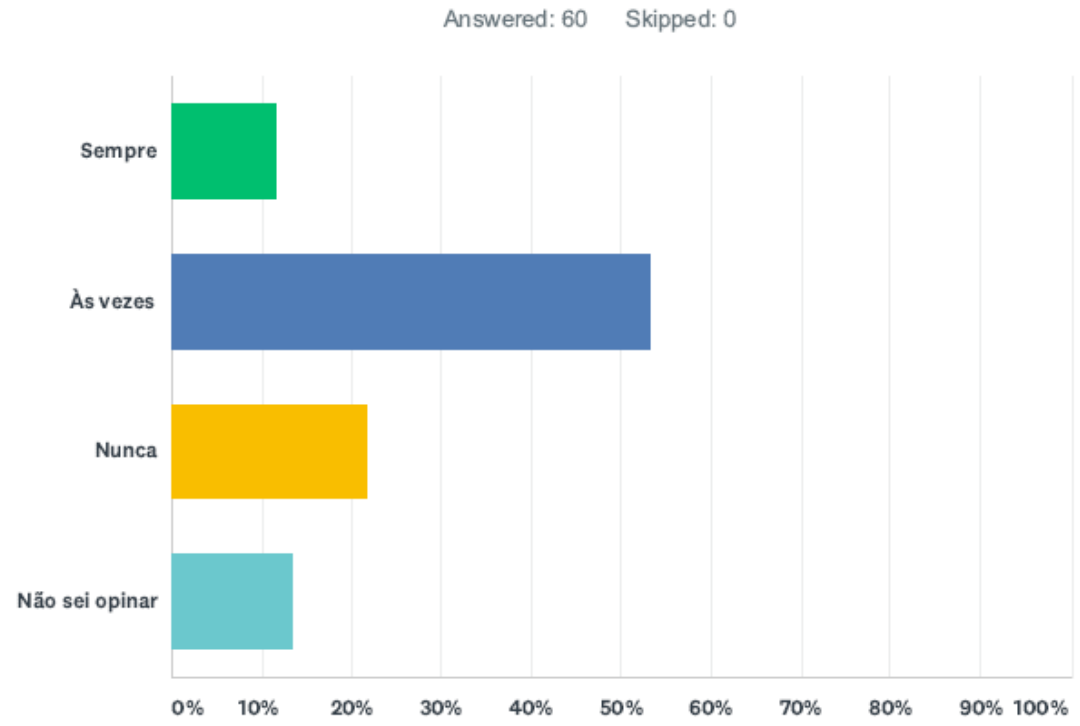
Questão 15: Você acha que o governo do Brasil possivelmente coleta os seus dados, telefonemas, e-mails ou outras comunicações digitais?



ANSWER CHOICES	RESPONSES	
Sim, o governo coleta os meus dados	23.33%	14
Provavelmente o governo coleta os meus dados	51.67%	31
Não, o governo não coleta os meus dados	6.67%	4
Não sei responder	18.33%	11
TOTAL		60

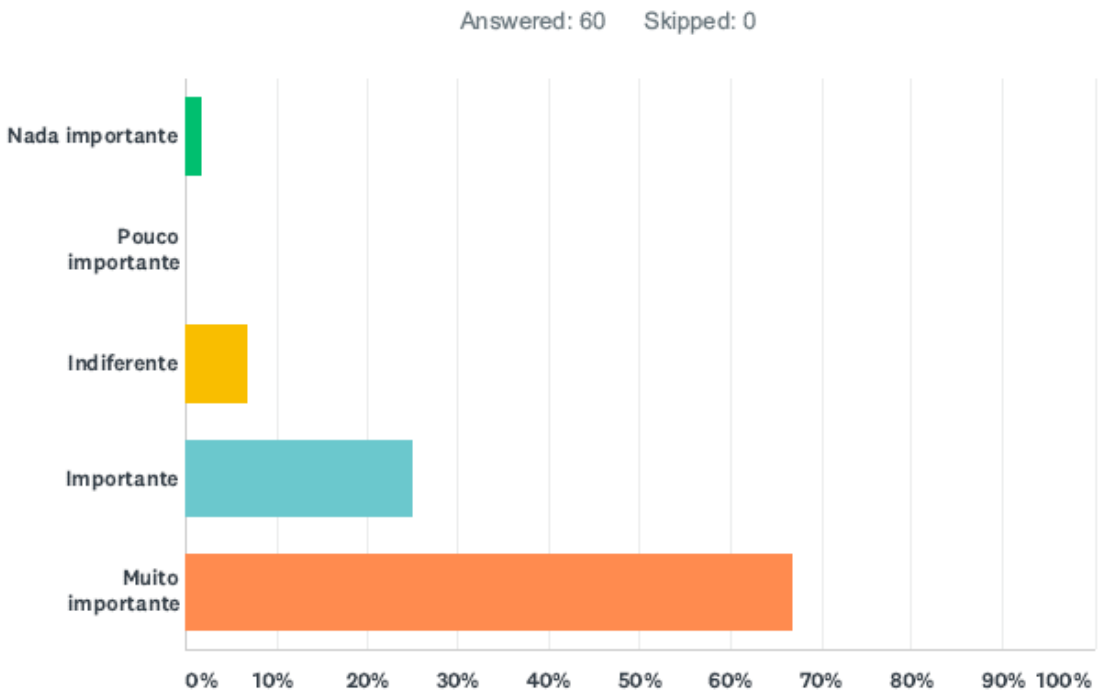
TRATAMENTO DA INFORMAÇÃO

Questão 16: A possibilidade de intrusão comunicacional interfere no seu cotidiano de trabalho?



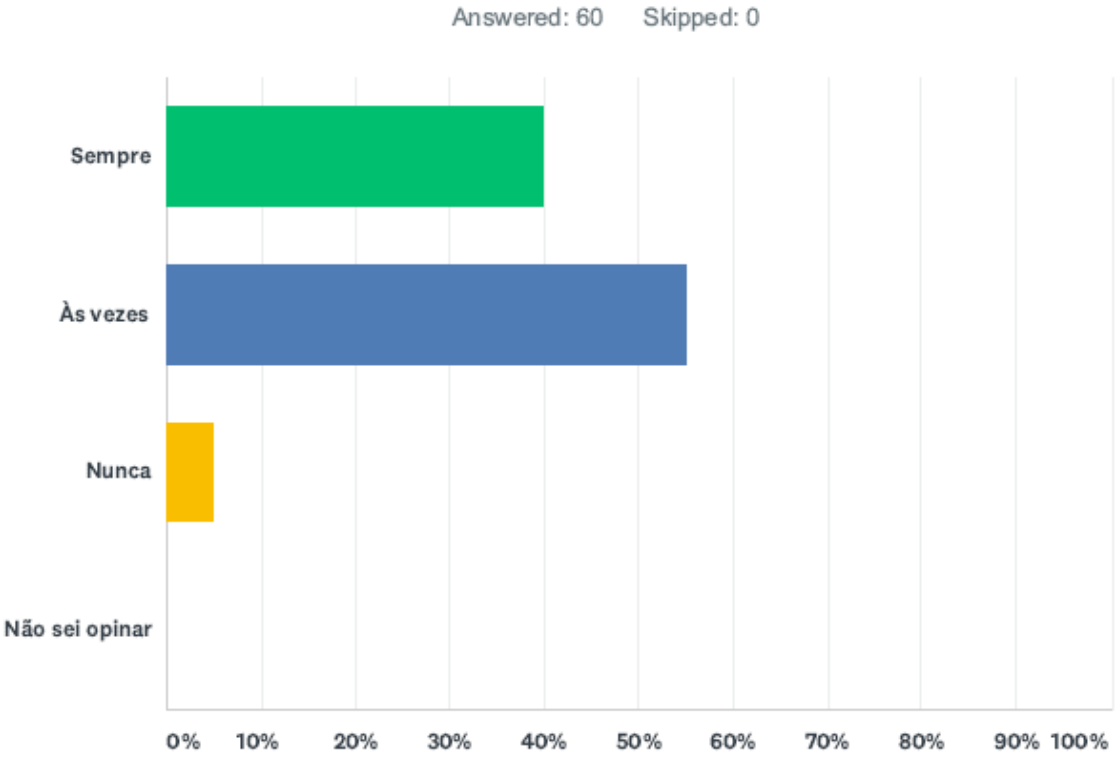
ANSWER CHOICES	RESPONSES	
Sempre	11.67%	7
Às vezes	53.33%	32
Nunca	21.67%	13
Não sei opinar	13.33%	8
TOTAL		60

Questão 17: Na sua opinião, a preservação dos dados pessoais de um jornalista investigativo é importante para que ele desempenhe o seu trabalho jornalístico?



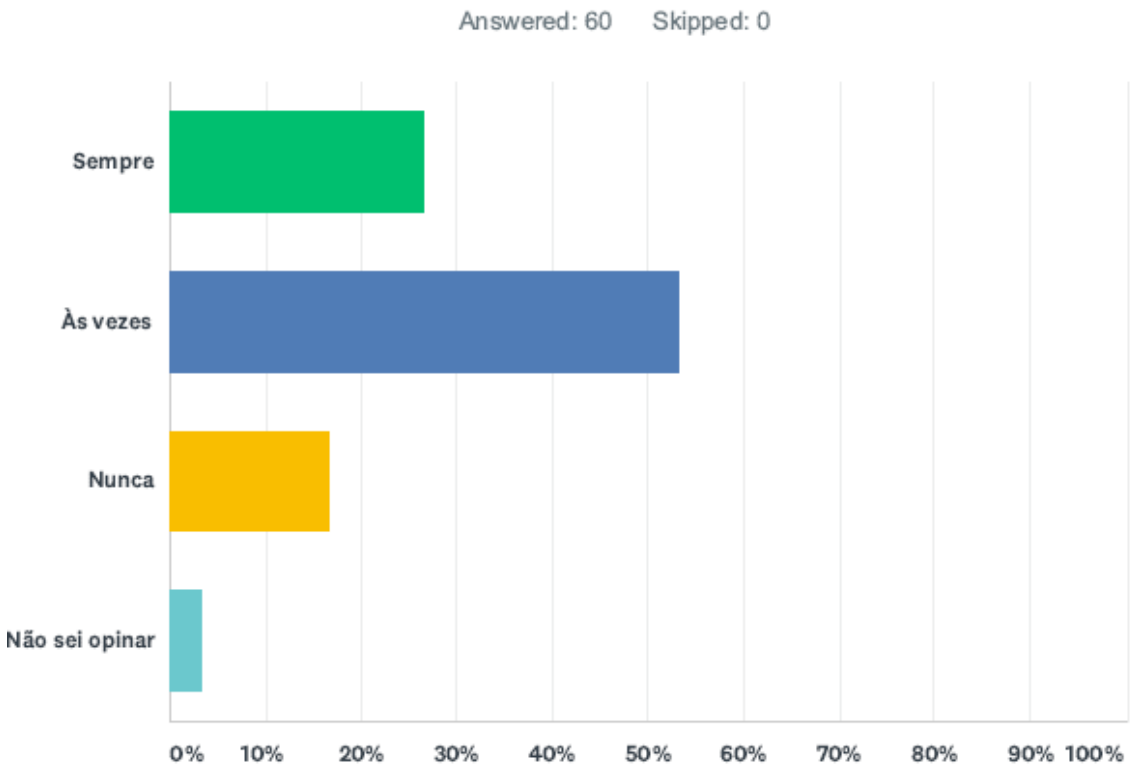
ANSWER CHOICES	RESPONSES	
Nada importante	1.67%	1
Pouco importante	0.00%	0
Indiferente	6.67%	4
Importante	25.00%	15
Muito importante	66.67%	40
TOTAL		60

Questão 18: Você adota medidas de segurança para preservar os seus dados pessoais?



ANSWER CHOICES	RESPONSES	
Sempre	40.00%	24
Às vezes	55.00%	33
Nunca	5.00%	3
Não sei opinar	0.00%	0
TOTAL		60

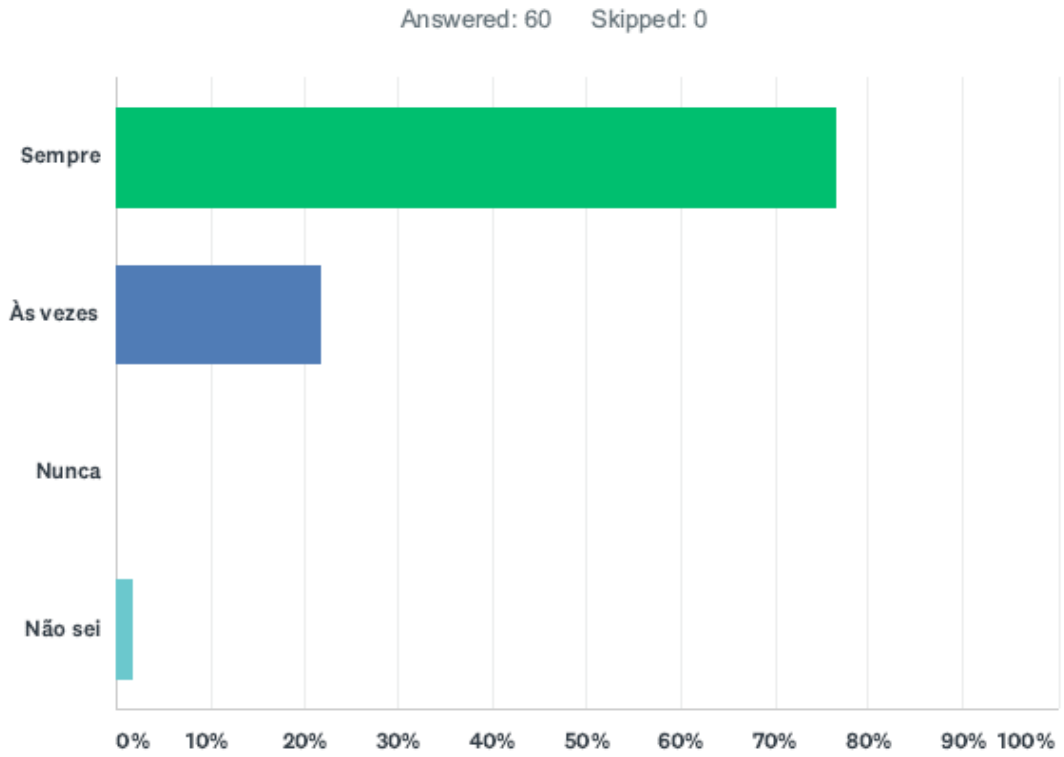
Questão 19: Você faz uso de ferramentas de criptografia e outras formas de segurança digital?



ANSWER CHOICES	RESPONSES	
Sempre	26.67%	16
Às vezes	53.33%	32
Nunca	16.67%	10
Não sei opinar	3.33%	2
TOTAL		60

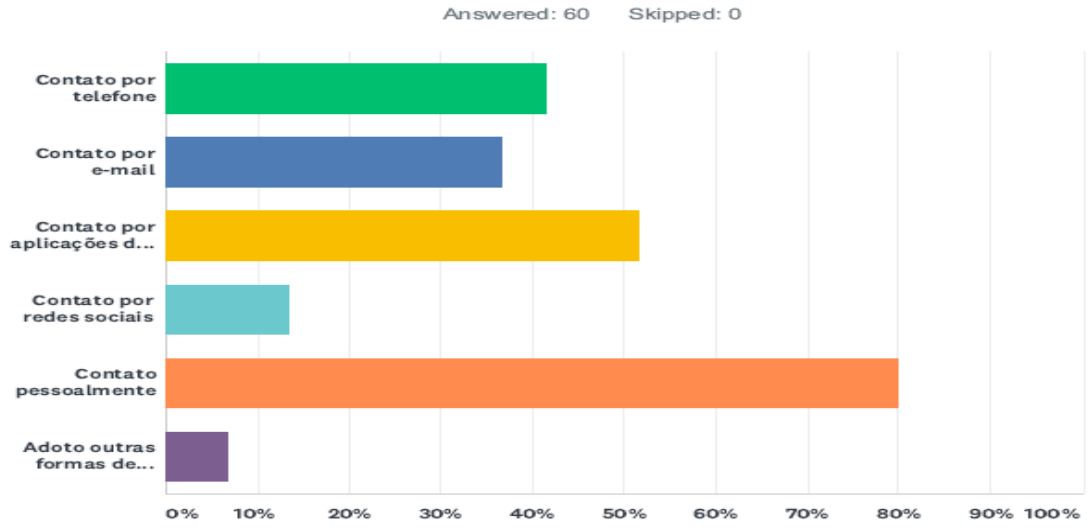
CONTATO COM FONTES

Questão 20: Você adota estratégias para proteger a identidade de suas fontes?



ANSWER CHOICES	RESPONSES	
Sempre	76.67%	46
Às vezes	21.67%	13
Nunca	0.00%	0
Não sei	1.67%	1
TOTAL		60

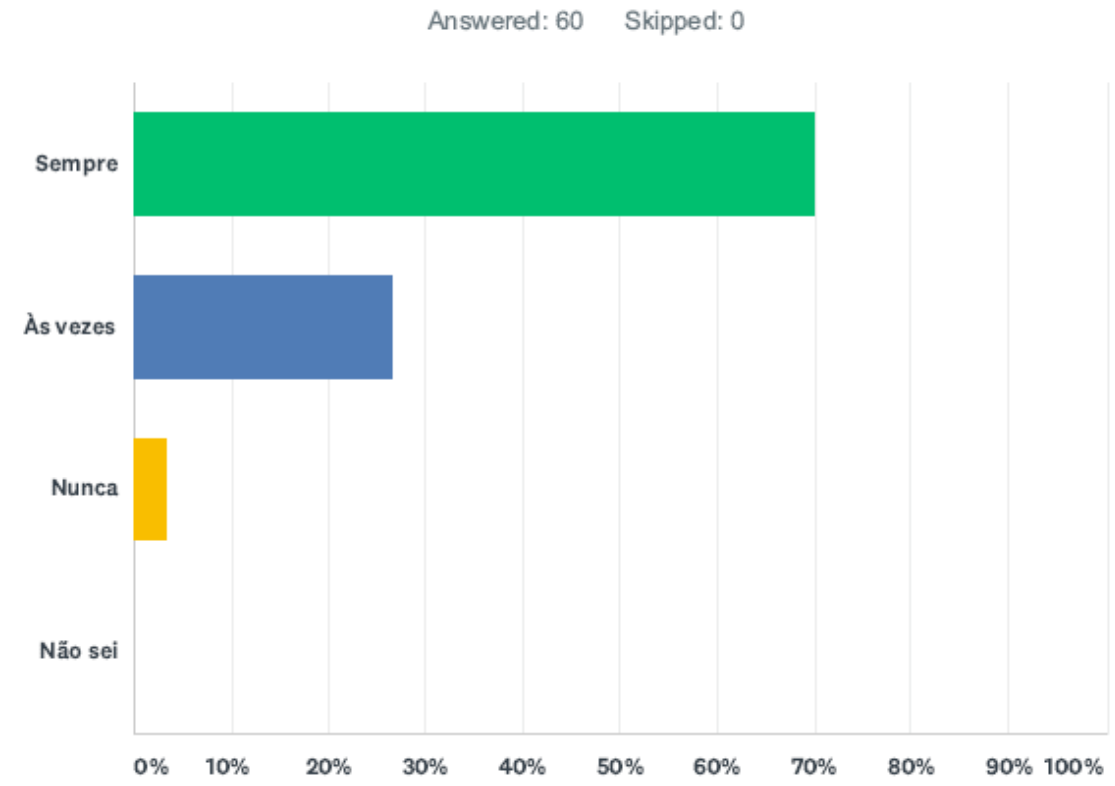
Questão 21: Quais as formas de contato que habitualmente adota com fontes que têm informações sensíveis?(Você pode escolher mais do que uma das opções)



ANSWER CHOICES	RESPONSES	
Contato por telefone	41.67%	25
Contato por e-mail	36.67%	22
Contato por aplicações de mensagem	51.67%	31
Contato por redes sociais	13.33%	8
Contato pessoalmente	80.00%	48
Adoto outras formas de contato (quais?)	6.67%	4
Total Respondents: 60		

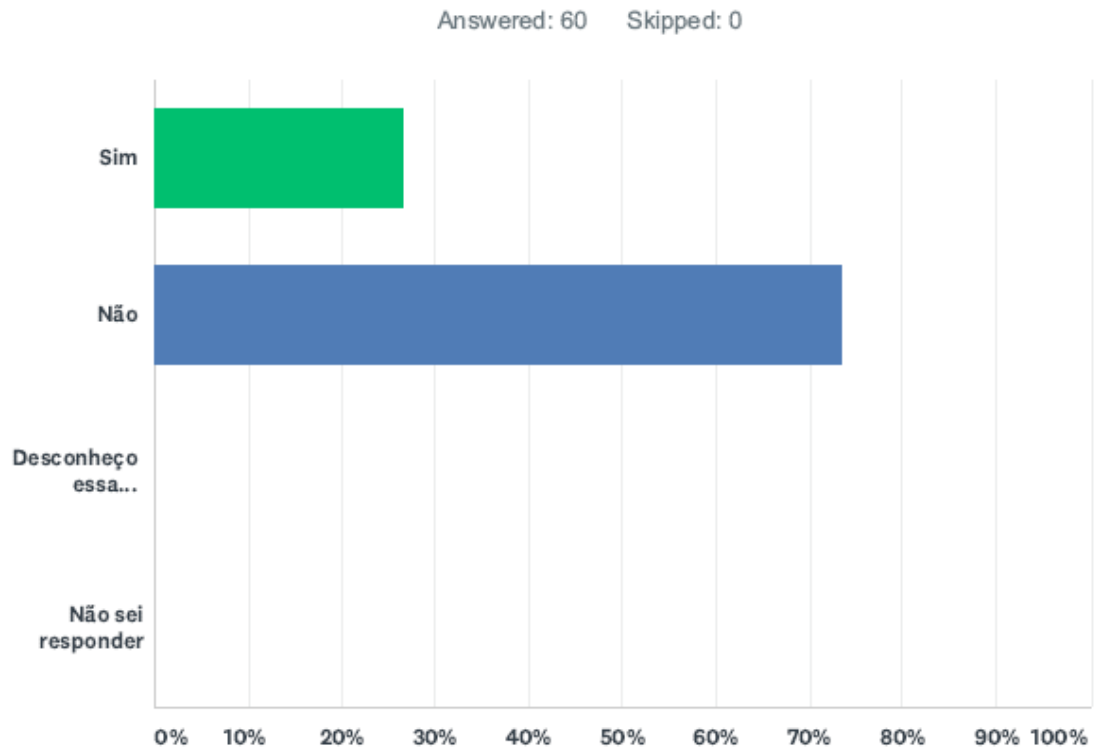
#	ADOTO OUTRAS FORMAS DE CONTATO (QUAIS?)	DATE
1	e-mail criptografo, chave PGP, contatos via deep web	10/11/2019 11:41 AM
2	Sistemas criptografados	10/5/2019 2:25 PM
3	App de mensagens e email criptografados	10/3/2019 12:01 AM
4	No caso do email, utilizo criptografado (geralmente os que dão possibilidade de usar mensagens autodestrutivas, como o protonmail). O trabalho obriga a usar vários emails. No meio deles, há não criptografados e criptografados. No contato com fontes de temas sensíveis, uso o criptografado.	9/25/2019 4:03 PM

Questão 22: Você utiliza serviços de e-mail de corporações como Google/Gmail, Yahoo e Microsoft?



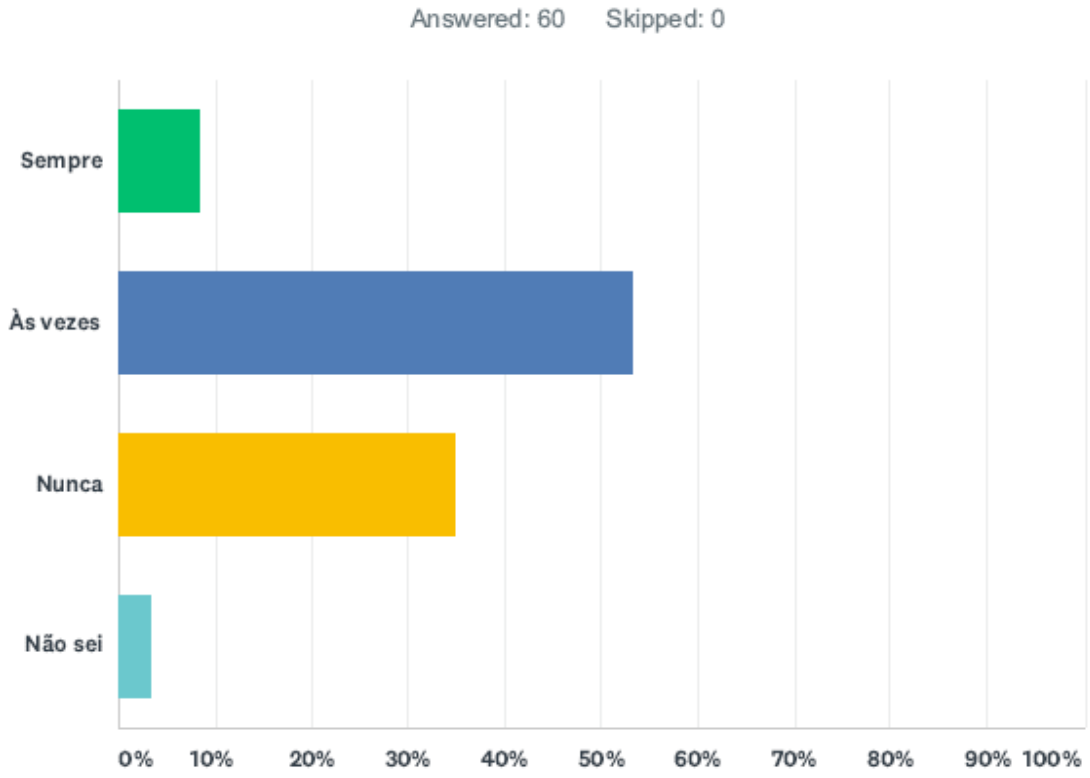
ANSWER CHOICES	RESPONSES	
Sempre	70.00%	42
Às vezes	26.67%	16
Nunca	3.33%	2
Não sei	0.00%	0
TOTAL		60

Questão 23: Em investigações jornalísticas, você já utilizou contas de e-mail “falsas” ou participou de fóruns online e salas de bate-papo usando nomes de usuários anônimos?



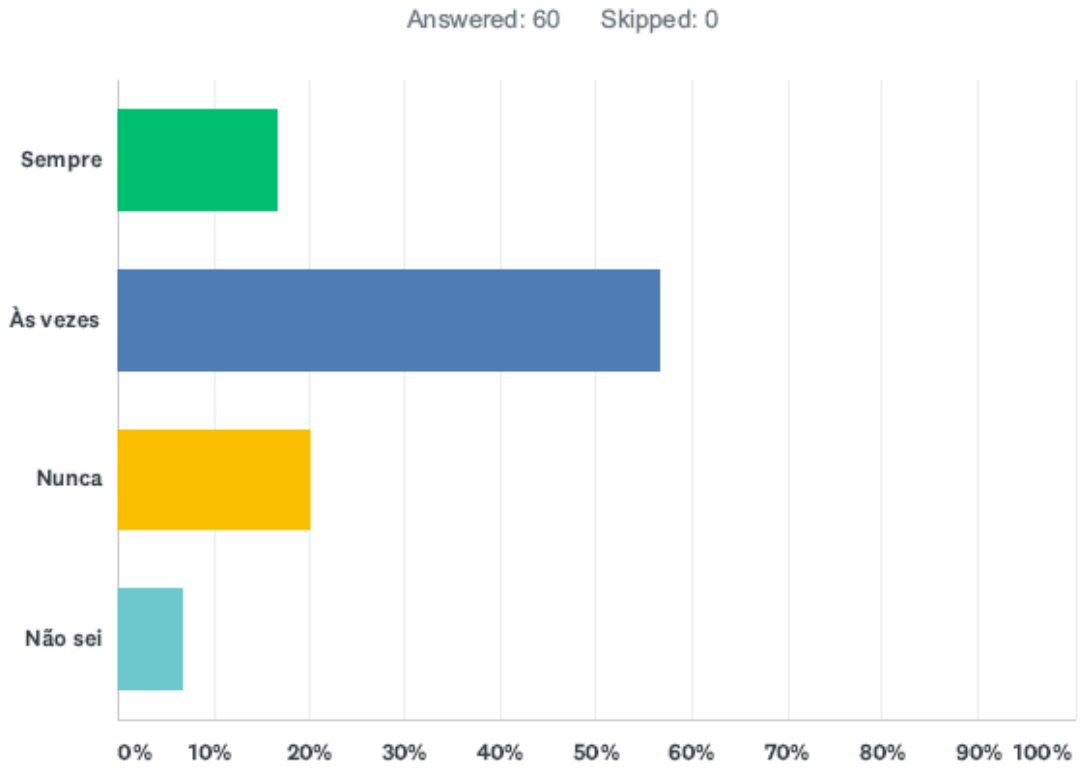
ANSWER CHOICES	RESPONSES	
Sim	26.67%	16
Não	73.33%	44
Desconheço essa possibilidade	0.00%	0
Não sei responder	0.00%	0
TOTAL		60

Questão 24: Durante investigações jornalísticas que abordam temas sensíveis, você costuma adotar medidas preventivas, como desligar os seus dispositivos eletrônicos, para se encontrar com as fontes?



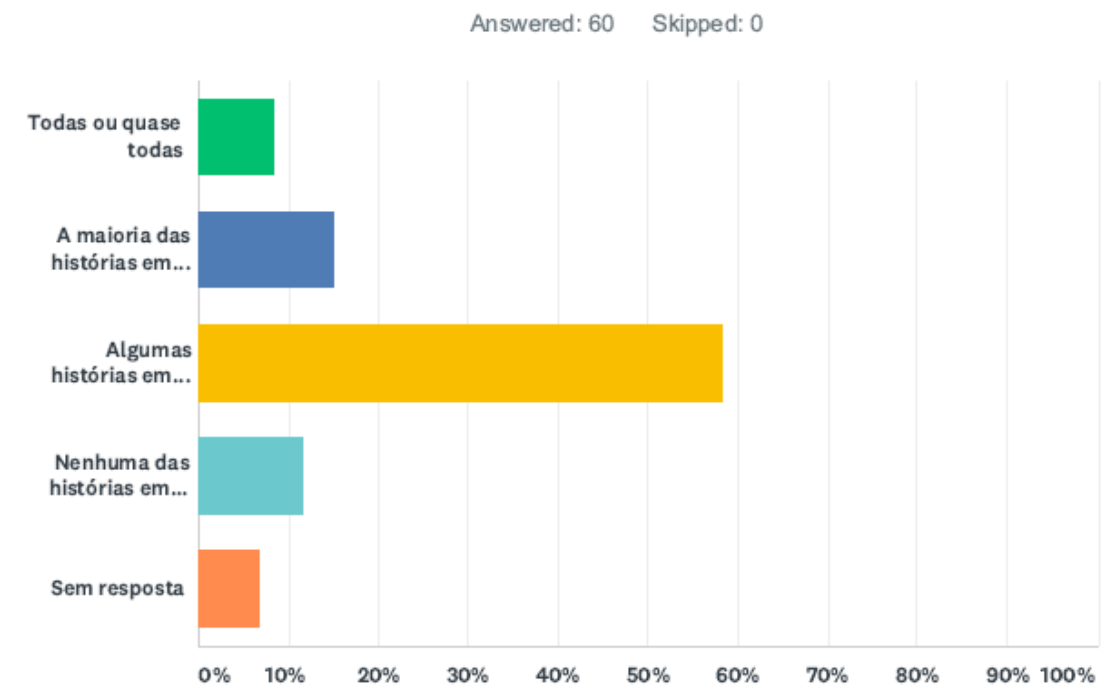
ANSWER CHOICES	RESPONSES	
Sempre	8.33%	5
Às vezes	53.33%	32
Nunca	35.00%	21
Não sei	3.33%	2
TOTAL		60

Questão 25: Você usa criptografia para se comunicar com as suas fontes por meios digitais?



ANSWER CHOICES	RESPONSES	
Sempre	16.67%	10
Às vezes	56.67%	34
Nunca	20.00%	12
Não sei	6.67%	4
TOTAL		60

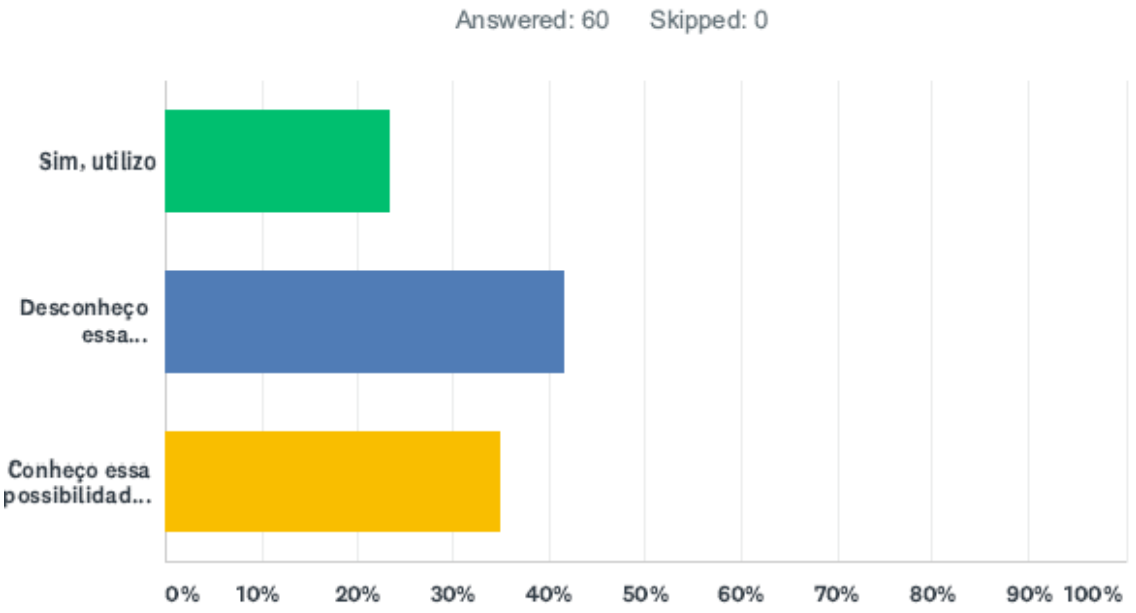
Questão 26: Quantas das suas investigações jornalísticas atuais contam com fontes anônimas?



ANSWER CHOICES	RESPONSES	
Todas ou quase todas	8.33%	5
A maioria das histórias em que trabalho	15.00%	9
Algumas histórias em que trabalho	58.33%	35
Nenhuma das histórias em que trabalho	11.67%	7
Sem resposta	6.67%	4
TOTAL		60

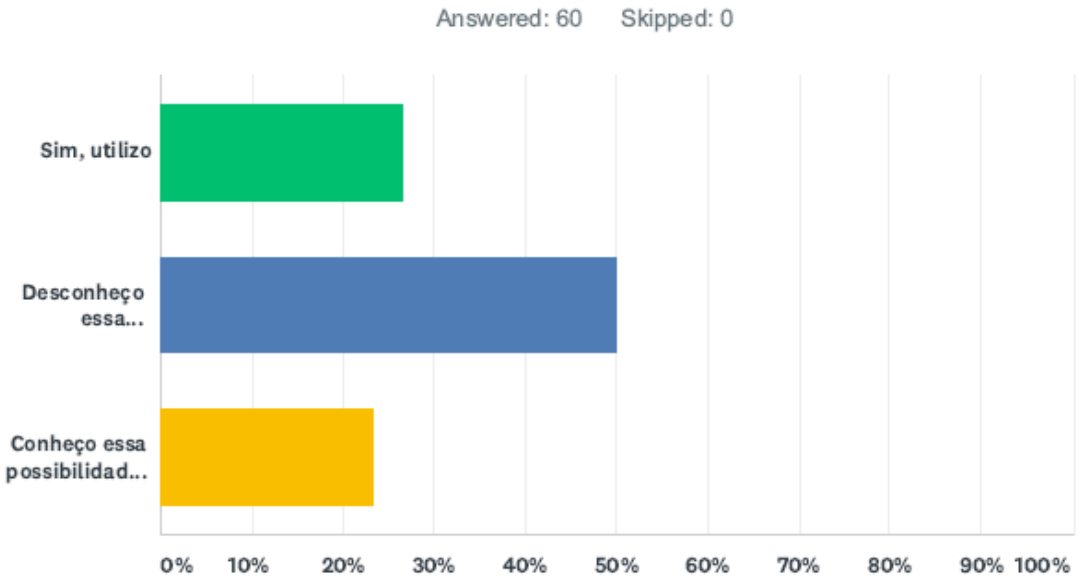
SEGURANÇA DIGITAL

Questão 27: Você utiliza softwares que permitem navegar na web anonimamente, como Tor ou Tails?



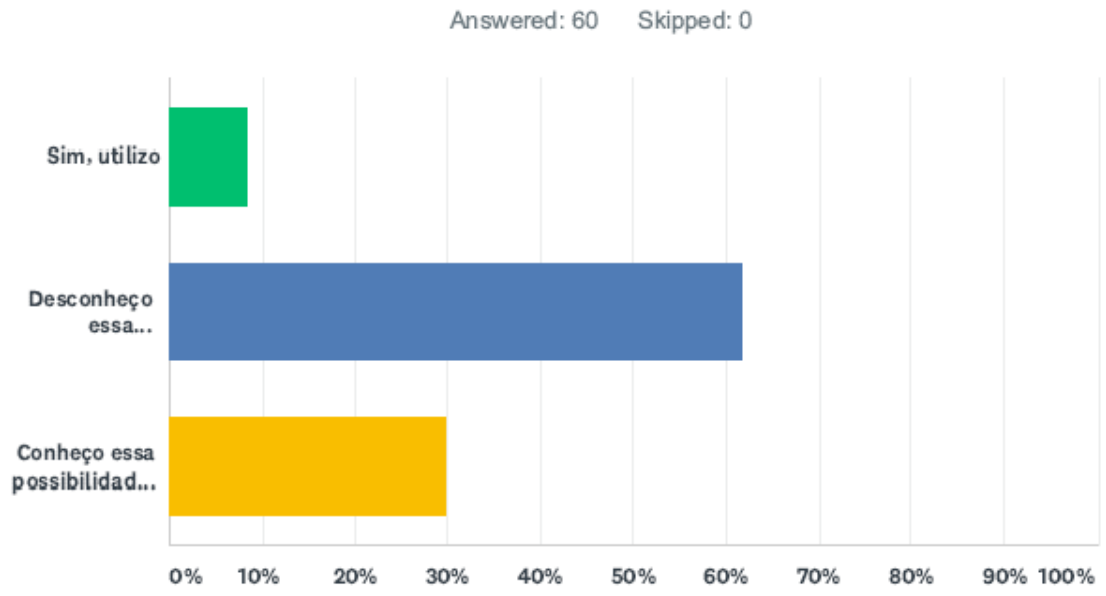
ANSWER CHOICES	RESPONSES	
Sim, utilizo	23.33%	14
Desconheço essa possibilidade	41.67%	25
Conheço essa possibilidade, mas acho desnecessário	35.00%	21
TOTAL		60

Questão 28: Você utiliza softwares de criptografia de e-mail, como o PGP?



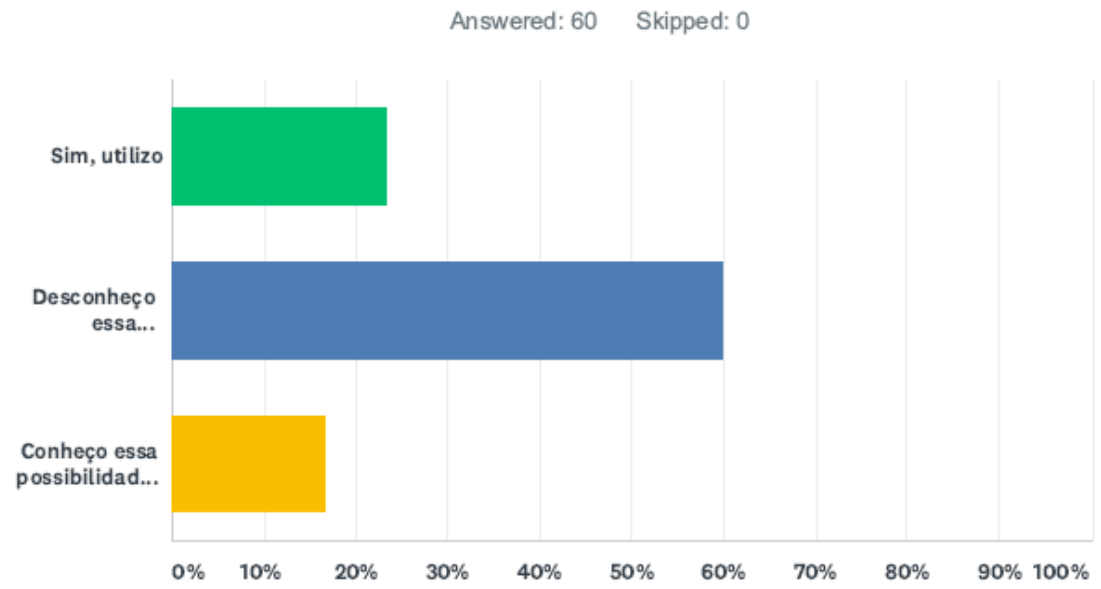
ANSWER CHOICES	RESPONSES	
Sim, utilizo	26.67%	16
Desconheço essa possibilidade	50.00%	30
Conheço essa possibilidade, mas acho desnecessário	23.33%	14
TOTAL		60

Questão 29: Você utiliza serviços de nuvem criptografados como o SpiderOak?



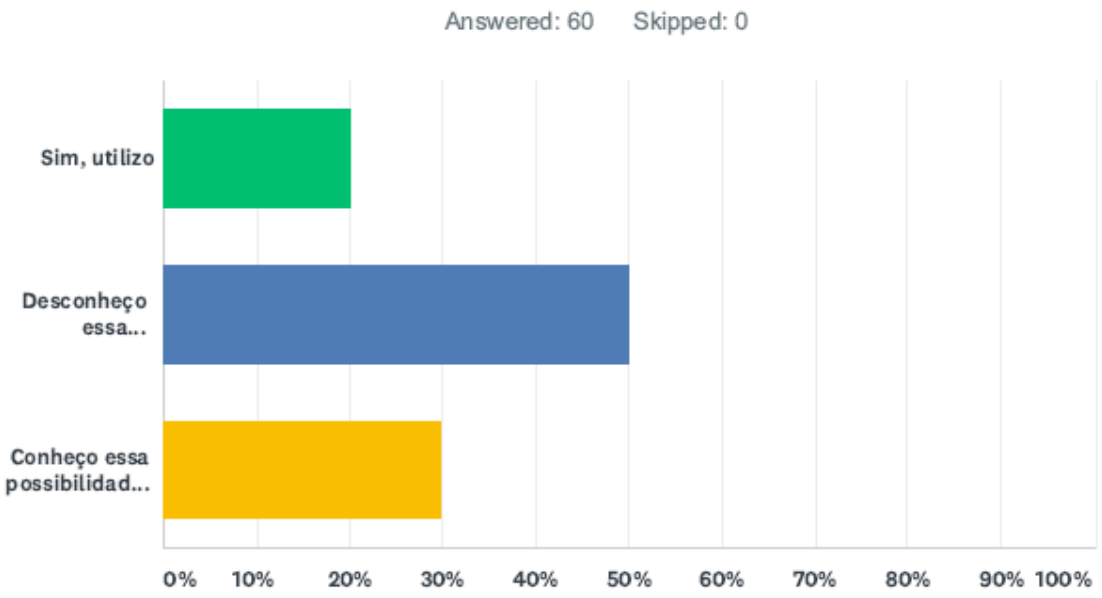
ANSWER CHOICES	RESPONSES	
Sim, utilizo	8.33%	5
Desconheço essa possibilidade	61.67%	37
Conheço essa possibilidade, mas acho desnecessário	30.00%	18
TOTAL		60

Questão 30: Você utiliza plug-ins de navegação relacionados à privacidade, como PrivacyBadger ou DoNotTrackMe?



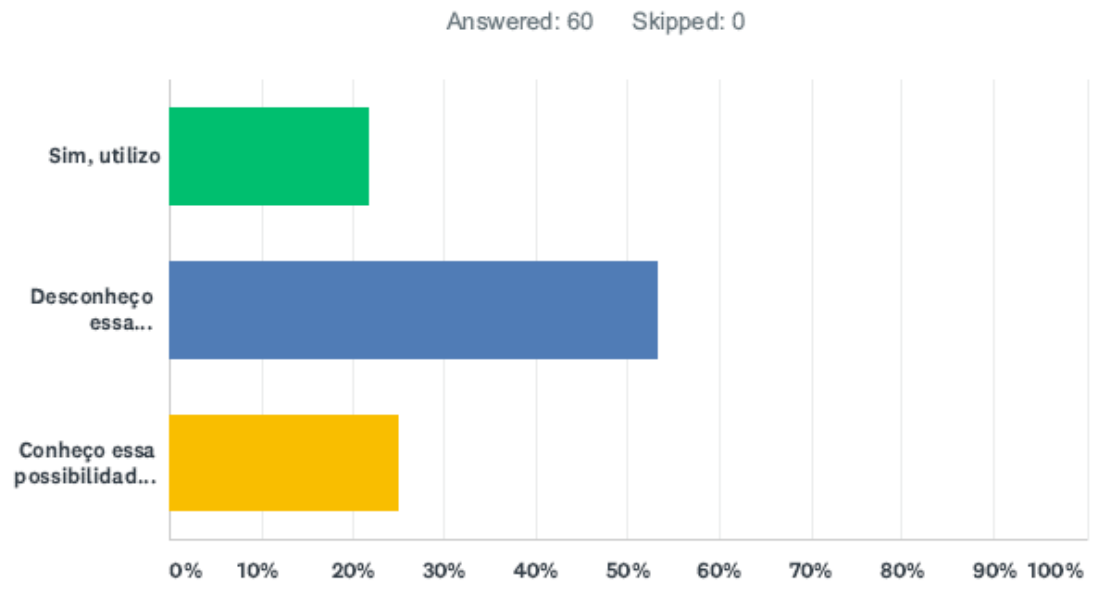
ANSWER CHOICES	RESPONSES	
Sim, utilizo	23.33%	14
Desconheço essa possibilidade	60.00%	36
Conheço essa possibilidade, mas acho desnecessário	16.67%	10
TOTAL		60

Questão 31: Você utiliza criptografia no disco rígido do seu computador de trabalho?



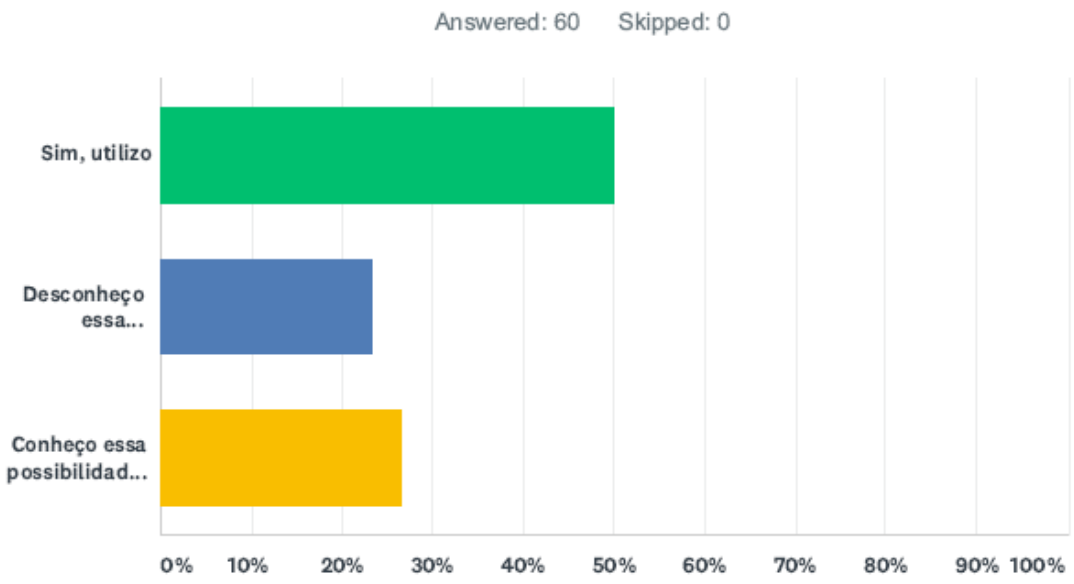
ANSWER CHOICES	RESPONSES	
Sim, utilizo	20.00%	12
Desconheço essa possibilidade	50.00%	30
Conheço essa possibilidade, mas acho desnecessário	30.00%	18
TOTAL		60

Questão 32: Você utiliza mecanismos de pesquisa que melhoram a privacidade, como o DuckDuckGo?



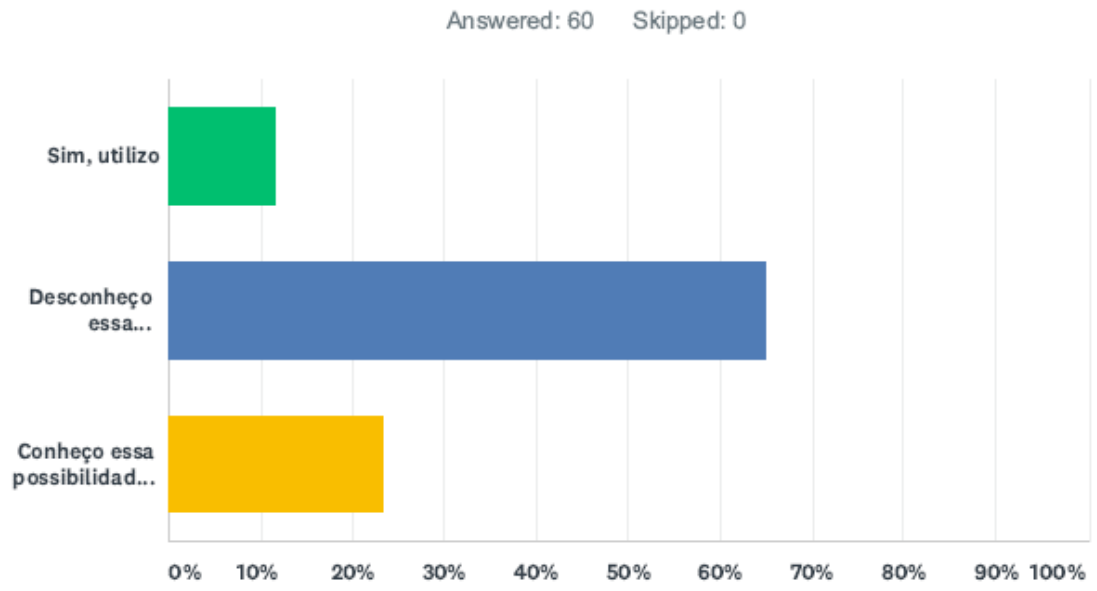
ANSWER CHOICES	RESPONSES	
Sim, utilizo	21.67%	13
Desconheço essa possibilidade	53.33%	32
Conheço essa possibilidade, mas acho desnecessário	25.00%	15
TOTAL		60

Questão 33: Você utiliza softwares de proteção de senhas?



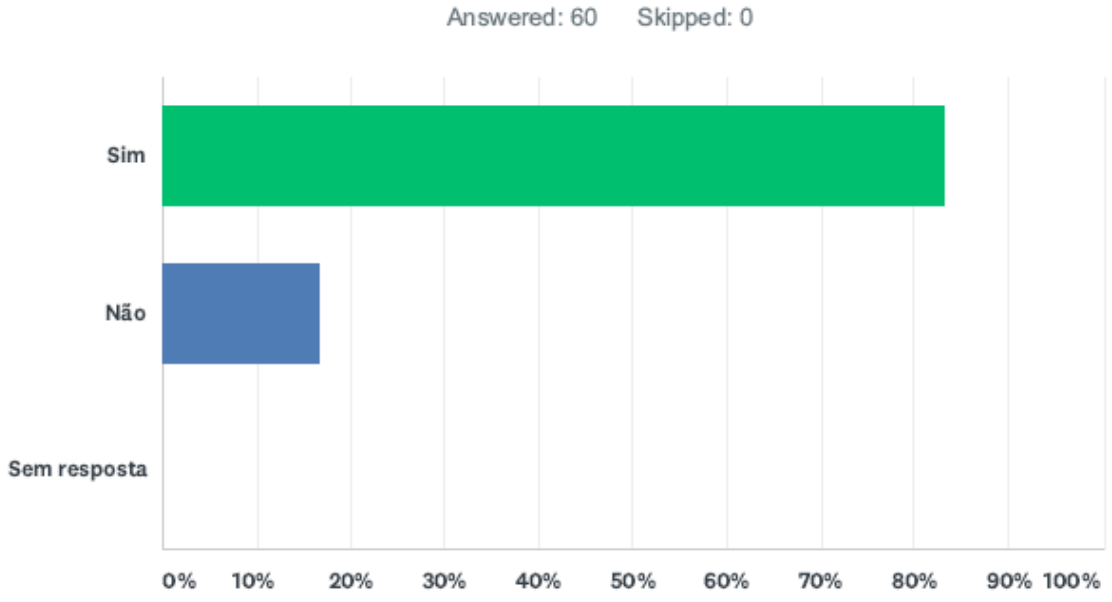
ANSWER CHOICES	RESPONSES	
Sim, utilizo	50.00%	30
Desconheço essa possibilidade	23.33%	14
Conheço essa possibilidade, mas acho desnecessário	26.67%	16
TOTAL		60

Questão 34: Você utiliza softwares de criptografia de bate-papo online, como o CryptoCat?



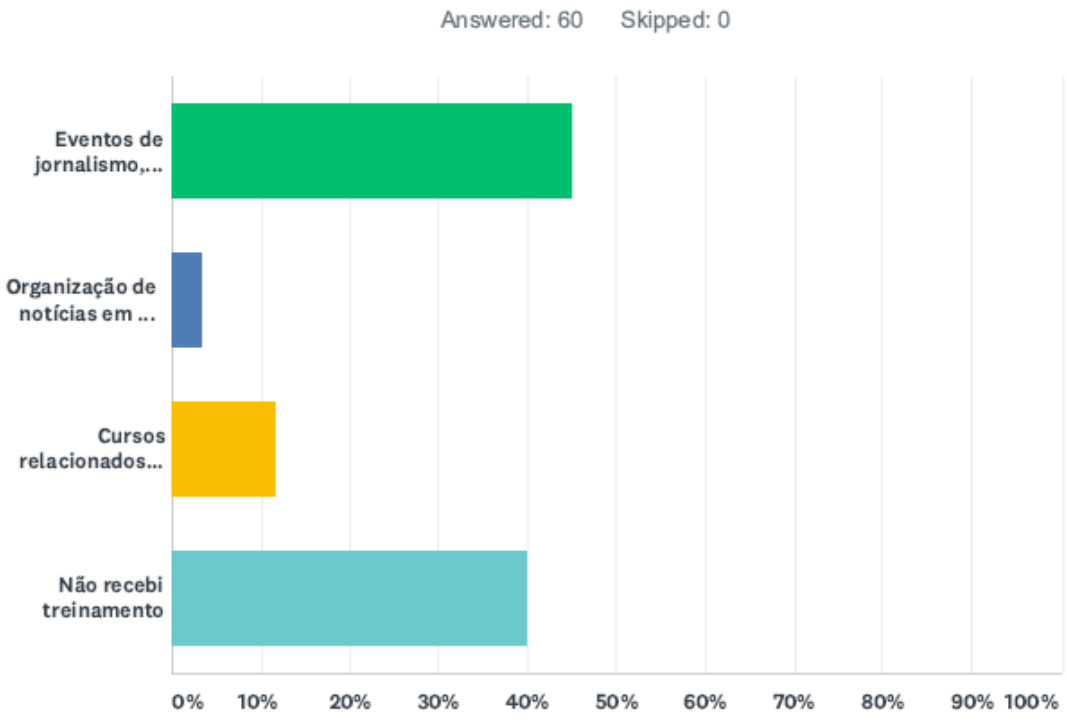
ANSWER CHOICES	RESPONSES	
Sim, utilizo	11.67%	7
Desconheço essa possibilidade	65.00%	39
Conheço essa possibilidade, mas acho desnecessário	23.33%	14
TOTAL		60

Questão 35: Você já usou redes sem fio públicas, por exemplo, em uma biblioteca, café ou enquanto viajava?



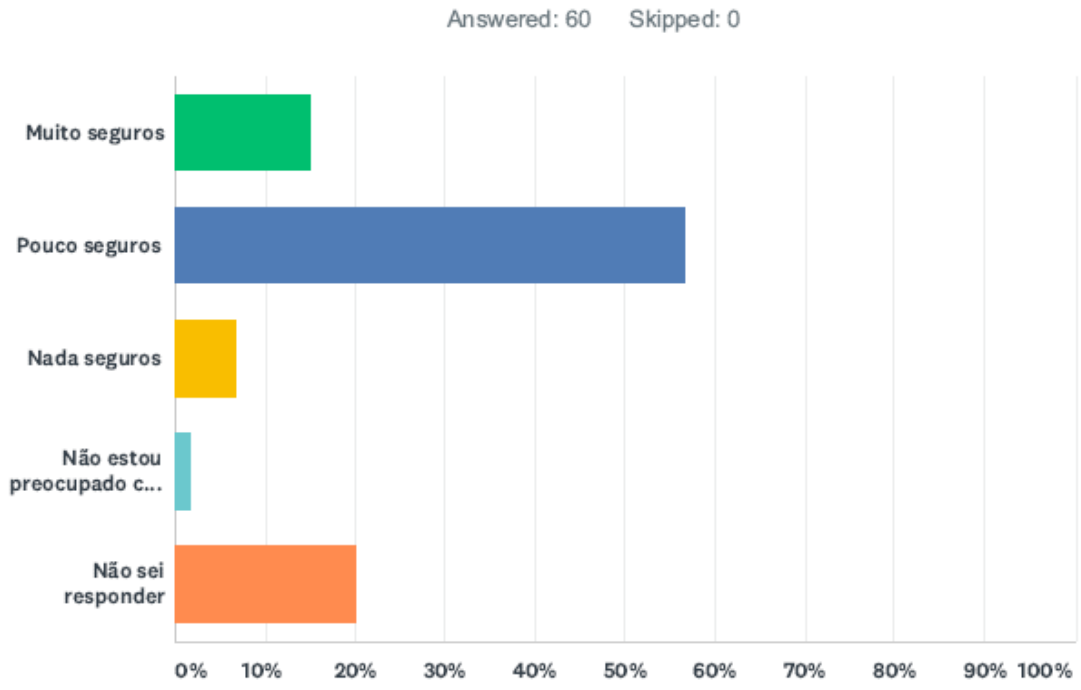
ANSWER CHOICES	RESPONSES	
Sim	83.33%	50
Não	16.67%	10
Sem resposta	0.00%	0
TOTAL		60

Questão 36: Você recebeu treinamento ou instrução formal de qualquer uma das seguintes fontes, com recomendações sobre como manter seus telefonemas, e-mails ou outras comunicações online seguras?



ANSWER CHOICES	RESPONSES	
Eventos de jornalismo, seminários ou webconferências	45.00%	27
Organização de notícias em que você trabalha ou trabalhou no passado	3.33%	2
Cursos relacionados à segurança digital ou ao jornalismo	11.67%	7
Não recebi treinamento	40.00%	24
TOTAL		60

Questão 37: Qual o nível de segurança dos dados e informações que estão em seus equipamentos eletrônicos e no ambiente digital?



ANSWER CHOICES	RESPONSES	
Muito seguros	15.00%	9
Pouco seguros	56.67%	34
Nada seguros	6.67%	4
Não estou preocupado com a segurança dos meus dados e informações	1.67%	1
Não sei responder	20.00%	12
TOTAL		60

APÊNDICE F– MODELO DE TCLE

Termo de Consentimento Livre e Esclarecido (TCLE)

Você está sendo convidado a participar da pesquisa intitulada: "JORNALISMO VIGILANTE SOB VIGILÂNCIA: PRINCIPAIS VULNERABILIDADES E POTENCIALIDADES DO JORNALISMO INVESTIGATIVO BRASILEIRO NO CONTEXTO DE INTRUSÃO COMUNICACIONAL MASSIVA DO SÉCULO XXI". Este questionário faz parte da tese submetida ao Programa de Pós-Graduação em Jornalismo da Universidade Federal de Santa Catarina para a obtenção do Grau de Doutor em Jornalismo. Orientador: Prof. Dr. Rogério Christofoletti. Coorientador: Prof. Dr. Samuel Pantoja Lima.

O contexto atual de vigilância comunicacional em meios digitais exige dos jornalistas investigativos um senso permanente de sua vulnerabilidade e a adoção de uma cultura de segurança digital. Diante da vigilância digital massiva realizada por governos e corporações, quais são as principais vulnerabilidades e potencialidades do jornalismo investigativo brasileiro?

Informações complementares sobre a pesquisa

- *Título da pesquisa:* JORNALISMO VIGILANTE SOB VIGILÂNCIA: PRINCIPAIS VULNERABILIDADES E POTENCIALIDADES DO JORNALISMO INVESTIGATIVO BRASILEIRO NO CONTEXTO DE INTRUSÃO COMUNICACIONAL MASSIVA DO SÉCULO XXI;
- *Nome do pesquisador responsável:* Prof. Dr. Samuel Pantoja Lima;
- *Nome do pesquisador assistente:* Ricardo José Torres;
- *Pesquisa:* Trata-se de tese que será submetida ao Programa de Pós-Graduação em Jornalismo da Universidade Federal de Santa Catarina para a obtenção do Grau de Doutor em Jornalismo;
- *Procedimentos aos quais o participante da pesquisa se sujeitará:* Para participar da pesquisa, o participante responderá a um questionário. A sua participação levará cerca de 20 minutos. Ao responder o questionário, o participante expressará o seu livre consentimento em participar de forma voluntária, sem qualquer vantagem adicional, podendo desistir a qualquer momento. Será garantido o seu anonimato e as informações colhidas serão usadas exclusivamente para fins científicos e acadêmicos.
- *Objetivos da pesquisa:* Geral - Examinar ações que envolvem o jornalismo investigativo, apontando potencialidades e vulnerabilidades do ecossistema digital.

Específicos – Observar a emergência de tensionamentos impostos pela vigilância relacionados ao jornalismo investigativo; Verificar implicações da possibilidade de intrusão comunicacional na atividade jornalística contemporânea;

- *Possíveis riscos e desconfortos decorrentes da pesquisa:* o participante está sujeito a possíveis desconfortos, por exemplo, aborrecimento ou desacordo com o conjunto de questões proposto pela pesquisa;
- *Sigilo das informações do participante:* Garantimos o sigilo das informações fornecidas por todos os participantes da pesquisa, no entanto, alertamos para o risco de quebra de sigilo não intencional.
- *Comitê de Ética em Pesquisa com Seres Humanos – UFSC:* O órgão colegiado interdisciplinar, deliberativo, consultivo e educativo, vinculado à Universidade Federal de Santa Catarina, independente na tomada de decisões, foi criado para defender os interesses dos participantes da pesquisa em sua integridade e dignidade e para contribuir no desenvolvimento da pesquisa dentro de padrões éticos.
- *Endereço físico da CEPSH-UFSC*: Prédio Reitoria II, R: Desembargador Vitor Lima, nº 222, sala 401, Trindade, Florianópolis/SC, CEP 88.040-400, Contato: (48) 3721-6094, cep.propesq@contato.ufsc.br;
- *Garantia de acesso às informações de pesquisa:* É garantido o livre acesso às informações da pesquisa, bem como o participante se retirar da pesquisa sem qualquer prejuízo.
- *Resolução em que a pesquisa está baseada:* Esta pesquisa está baseada na Resolução CNS 510/16, os pesquisadores cumprirão as prerrogativas apresentadas por esta resolução.
- *Garantia de indenização*: Garantimos o reparo ao dano, seja ele material ou imaterial, devidamente comprovado da pesquisa, devendo ser pago de acordo com a legislação vigente (Resolução CNS 466/12, no item IV.3.h.3.). Também garantimos o ressarcimento a possíveis despesas com transporte e alimentação, assegurando ao participante da pesquisa que todos os eventuais gastos dele serão ressarcidos (Resolução 466/12, item IV.3.g e Resolução 510/16, ART. 17, inc. VII).

Para saber mais sobre a pesquisa ou ter acesso aos resultados dela, entre em contato: Ricardo Torres – Programa de Pós-Graduação em Jornalismo (PPGJOR) - UFSC - Florianópolis (SC)

Sobre o pesquisador: http://lattes.cnpq.br/2280827424163795

E-mail: ricardo.torres@ufsc.br

Telefone: (48) 99699-0762

Endereços profissionais dos pesquisadores (responsável e principal): Campus Universitário Reitor João David Ferreira Lima, s/nº, Trindade – Florianópolis – SC

CEP: 88040-900.

Guarde o seu Termo de Consentimento.

Esse TCLE será elaborado em duas vias, rubricadas em todas as suas páginas e assinadas, ao seu término, pelo convidado a participar da pesquisa, ou por seu representante legal, assim como pelo pesquisador responsável, ou pela (s) pessoa (s) por ele delegada (s).

_____ _____

Assinatura pesquisador Assinatura participante

ANEXO A – LIBERAÇÃO DO CEPSH

UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC

PARECER CONSUBSTANCIADO DO CEP

DADOS DA EMENDA

Título da Pesquisa: JORNALISMO VIGILANTE SOB VIGILÂNCIA: PRINCIPAIS VULNERABILIDADES E POTENCIALIDADES DO JORNALISMO INVESTIGATIVO BRASILEIRO NO CONTEXTO DE INTRUSÃO COMUNICACIONAL MASSIVA DO SÉCULO XXI

Pesquisador: SAMUEL PANTOJA LIMA

Área Temática:

Versão: 3

CAAE: 07276819.9.0000.0121

Instituição Proponente: Universidade Federal de Santa Catarina

Patrocinador Principal: Capes Coordenação Aperf Pessoal Nivel Superior

DADOS DO PARECER

Número do Parecer: 3.254.622

Apresentação do Projeto:

Florianópolis, 26 de março de 2019.

EMENDA O projeto JORNALISMO VIGILANTE SOB VIGILÂNCIA: PRINCIPAIS VULNERABILIDADES E POTENCIALIDADES DO JORNALISMO INVESTIGATIVO BRASILEIRO NO CONTEXTO DE INTRUSÃO COMUNICACIONAL MASSIVA DO SÉCULO XXI – CAAE 07276819.9.0000.0121, obteve sua aprovação junto ao CEP UFSC na data de 25 de março de 2019, sob parecer de n. 3.221.359. O objetivo primário da pesquisa é examinar ações que envolvem o jornalismo investigativo apontando potencialidades e vulnerabilidades do ecossistema digital. O protocolo aprovado propõe um percurso metodológico dividido em quatro etapas, sendo que a terceira etapa sofreu alterações.

Nesse sentido, esta emenda tem como objetivo apresentar essa alteração.

Onde se lê: 3ª Etapa – Seleção de casos paradigmáticos relacionados ao jornalismo investigativo (Estudo de casos múltiplos –Vazamentos Snowden – The Intercept (Brasil); Cablegate – Agência Pública (Brasil); Panama Papers –Poder 360 (Brasil). Avaliação por meio de técnicas de análise de conteúdo elencando os aspectos percebidos, adequados e negligenciados nas investigações jornalísticas realizadas em espaços vigiados.

Endereço: Universidade Federal de Santa Catarina, Prédio Reitoria II, R: Desembargador Vitor Lima, nº 222, sala 401
Bairro: Trindade **CEP:** 88.040-400
UF: SC **Município:** FLORIANOPOLIS
Telefone: (48)3721-6094 **E-mail:** cep.propesq@contato.ufsc.br

UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC

Leia-se: 3ª Etapa – Seleção de casos paradigmáticos relacionados ao jornalismo investigativo para realização de entrevistas em profundidade com profissionais envolvidos nos casos (de 3 a 5 entrevistados). Análise dos aspectos percebidos, adequados e negligenciados nas investigações jornalísticas realizadas em espaços vigiados e aferição da percepção dos jornalistas envolvidos nessas situações.

A justificativa para a solicitação de emenda diz respeito ao fato de inclusão de entrevistas em profundidade sugeridas pela banca de qualificação da tese que ocorreu no dia 15 de março de 2019. Os riscos previstos para esta nova etapa são iguais aos apresentados no projeto inicial, nesse sentido, não há necessidade de ampliar as medidas a fim de minimizá-los. Também não há necessidade de alteração do TCLE ou de qualquer outro documento relacionado ao projeto inicial.

Objetivo da Pesquisa:
Já avaliados

Avaliação dos Riscos e Benefícios:
Já avaliados

Comentários e Considerações sobre a Pesquisa:
O CEPSH tomou ciência da emenda proposta pela banca de qualificação e pelo pesquisador.

Considerações sobre os Termos de apresentação obrigatória:
De acordo com a legislação vigente.

Recomendações:
Não se aplica.

Conclusões ou Pendências e Lista de Inadequações:
O CEPSH tomou ciência da emenda proposta pela banca de qualificação e pelo pesquisador e encaminha para aprovação.

Considerações Finais a critério do CEP:

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMAÇÕES_BÁSICAS_1326149_E1.pdf	01/04/2019 12:02:12		Aceito

Endereço: Universidade Federal de Santa Catarina, Prédio Reitoria II, R: Desembargador Vitor Lima, nº 222, sala 401
Bairro: Trindade **CEP:** 88.040-400
UF: SC **Município:** FLORIANOPOLIS
Telefone: (48)3721-6094 **E-mail:** cep.propesq@contato.ufsc.br

UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC

Continuação do Parecer: 3.254.622

Outros	emenda.pdf	01/04/2019 11:59:39	RICARDO JOSE TORRES	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	TCLE.docx	12/03/2019 21:31:19	RICARDO JOSE TORRES	Aceito
Projeto Detalhado / Brochura Investigador	Tese_ricardo_torres.pdf	02/02/2019 10:09:30	RICARDO JOSE TORRES	Aceito
Brochura Pesquisa	Relatorio.pdf	20/01/2019 09:05:35	RICARDO JOSE TORRES	Aceito
Folha de Rosto	Folha_de_Rosto.pdf	20/01/2019 09:03:18	RICARDO JOSE TORRES	Aceito

Situação do Parecer:
Aprovado

Necessita Apreciação da CONEP:
Não

FLORIANOPOLIS, 09 de Abril de 2019

Assinado por:
Maria Luiza Bazzo
(Coordenador(a))

Endereço: Universidade Federal de Santa Catarina, Prédio Reitoria II, R: Desembargador Vitor Lima, nº 222, sala 401
Bairro: Trindade **CEP:** 88.040-400
UF: SC **Município:** FLORIANOPOLIS
Telefone: (48)3721-6094 **E-mail:** cep.propesq@contato.ufsc.br