REVISTA UCRONÍAS 11
[11-34] DOI: 10.5281/ZENODO.6727100 Nº 5 [enero-junio 2022] ISSN 2684-012X

Ciberfeminismos e tecnologias feministas

Reflexões sobre o anonimato digital e a segurança de dados em uma rede disputada

Flora Carvalho

Universidade Estadual de Campinas (UNICAMP), Brasil
ORCID: https://orcid.org/0000-0003-0707-9105 | floravillascf@gmail.com

Érica Renata de Souza

Universidade Federal de Minas Gerais (UFMG), Brasil
ORCID: https://orcid.org/0000-0003-2195-8237 | erica0407@gmail.com

Palavras-chave:
anonimato | etnografia digital | tecnologias feministas | ciberfeminismo | segurança digital

Recibido: 5 de abril de 2021. Aceptado: 21 de abril de 2022.

RESUMO

Os ambientes virtuais vêm sendo crescentemente utilizados como plataforma para o desenvolvimento e disseminação de ideias, pautas e produções feministas e para denúncias de machismos, misoginias e violências de gênero que ocorrem dentro e fora da internet. Neste contexto, os ciberfeminismos atuam como importantes veiculadores destas ações e são centrais na garantia de modos de denúncias mais seguros às vítimas. Na busca por tal segurança, entra em cena o anonimato, um conceito/ferramenta polêmico e disputado. Neste artigo, em uma articulação de possibilidades metodológicas como a Antropologia Digital (Horst & Miller, 2012), a etnografia multissituada (Marcus, 1995) e perambulação/acompanhamento/imersão nos

[11-34] DOI: 10.5281/ZENODO.6727100
Nº 5 [enero-junio 2022] ISSN 2684-012X

ambientes virtuais (Leitão & Gomes 2018), delineamos algumas das ambiguidades, tensões e discussões que circundam o anonimato digital na arena das disputas políticas e suas implicações na relação com grupos e corpos minorizados, pautas e ações ciberativistas e ciberfeministas, tecnologia feministas, discursos jurídicos e estruturas de poder.

ABSTRACT

Virtual environments are increasingly being used as a platform for the development and dissemination of feminist ideas, guidelines and productions and for denouncing sexism, misogynies and gender violence that occur on and off the internet. In this context, cyberfeminisms act as important carriers of these actions and are central to ensuring safer ways of reporting for the victims. In the search for such security, anonymity comes into play, a controversial and disputed concept / tool. In this article, in an articulation of methodological possibilities such as Digital Anthropology (Horst & Miller, 2012), multisituated ethnography (Marcus, 1995) and wandering / monitoring / immersion in virtual environments (Leitão & Gomes 2018), we outline some of the ambiguities, tensions and compelling that surround digital anonymity in the arena of political disputes and its established in the relationship with minorized groups and bodies; cyberactivist/cyberfeminist actions and agendas; legal speeches; power structures.

KEYWORDS

anonymity | digital ethnography | feminist technologies | cyberfeminism | digital security

INTRODUÇÃO, CONTEXTO E METODOLOGIA

A internet tem sido cada vez mais utilizada, sobretudo nos últimos anos, como plataforma para que mulheres e coletivas[1] feministas exponham e disseminem suas ideias, suas pautas, suas produções e, por outro lado, denunciem o machismo, a misoginia e as violências de gênero que ocorrem dentro e fora do ambiente virtual. Neste contexto, os ciberfeminismos[2] vêm atuando como importantes veiculadores destas ações, tal como centrais figuras na garantia de que estas denúncias se tornem cada vez mais seguras às vítimas. Como parte da garantia de tal segurança, entra em cena a questão do anonimato, um conceito/ferramenta polêmico e disputado, inclusive dentro do próprio ciberfeminismo. Isto, pois ele "reinventa formas de violência contra grupos e corpos minorizados e, por outro lado, rearranja possibilidades de resistências ciborgues como personagem importante nas lutas ciberfeministas e ciberativistas" (Carvalho, 2019b).

1 O uso do termo "coletivas" no feminino para se referir a grupos feministas e ciberfeministas será empregado ao longo do texto, uma vez que grande parte destes grupos assim se autodenomina.

2 "Os ciberfeminismos são movimentos e práticas múltiplas que tentam articular conjuntamente as agendas de grupos feministas (em sua grande pluralidade) com as agendas ciberativistas contra a vigilância na internet, a favor de políticas de defesa de uma internet aberta, segura e democrática" e se inserem na "constante disputa de terrenos, entre perigos e potenciais que a internet traz especialmente para minorias políticas" (Carvalho, 2019b).

[11-34] DOI: 10.5281/ZENODO.6727100

Nº 5 [enero-junio 2022] ISSN 2684-012X

Sendo assim, ao longo deste artigo[3] pretendemos não apenas delinear algumas das ambiguidades, tensões e discussões que circundam o anonimato digital na arena das disputas políticas, mas também quais as suas implicações na relação com grupos e corpos minorizados, pautas e ações ativistas e ciberengajadas, discursos e meios jurídicos e como esse conceito, ferramenta, prática ou universo do anonimato se insere dentro das estruturas de poder e controle vigentes.

Para isso, realizamos esta pesquisa nos amparando em uma série de potencialidades teórico-metodológicas que vêm se desenhando nas últimas décadas e que visam tentar dar suporte àquelas e àqueles que desejam fazer pesquisas não apenas através da internet, mas também na/da internet, a partir e em conjunto com ela, considerando os ambientes virtuais –entrelaçados com os *offline* de maneira intrínseca, como defendem Débora Leitão e Laura Gomes (2018)– como espaços e atores essenciais para se compreender as relações socioculturais na atualidade. Esse projeto de certo não é completamente novo, uma vez que já na década de 90 tínhamos autores como Arturo Escobar que já defendia esta aproximação investigativa da antropologia a respeito da cibercultura, como aponta em seu texto "Bem-vindos à Cyberia: notas para uma antropologia da cibercultura":

> O ponto de partida da presente investigação é a crença de que qualquer tecnologia representa uma invenção cultural, no sentido de que ela produz um mundo. Toda tecnologia emerge de condições culturais particulares ao mesmo tempo em que contribui para a criação de novas condições culturais. Os antropólogos podem estar bem preparados para entender estes processos se estiverem abertos à ideia de que a ciência e a tecnologia são campos cruciais para a criação da cultura no mundo contemporâneo. (Escobar, 1994: 22)

E, ainda antes, temos a emblemática obra de Sherry Turke, *The Second Self*, publicada em 1984 e de grande impacto nas ciências sociais brasileiras dos anos 90 para o estudo do tema.

No entanto, como apontam Marko Monteiro e Fabíola Rohden em seu levantamento histórico a respeito das pesquisas de ciência e tecnologia no Brasil, –"Para além da ciência e do *anthropos*: deslocamentos da antropologia da ciência e da tecnologia no Brasil"– na década de 1990 estas aproximações teóricas das ciências sociais e do fazer etnográfico da/na cibercultura se voltavam muito para tentativas de distinção entre online/off-line ou ainda uma utilização da internet como meio –mediação técnica– e não como sujeito de pesquisa. Por outro lado, nas últimas décadas –principalmente devido a influência de autoras e autores como Latour, Haraway, Stengers– este tipo de investimento etnográfico "perdeu espaço para debates em torno de redes heterogêneas e em função da incorporação de outras perspectivas mesmo nas investigações sobre a cibercultura" (Monteiro & Rohden, 2019). É, portanto, neste contexto mais atual e vertiginosamente crescente em número e complexidade de trabalhos que se encontra a discussão deste artigo.

3 Este artigo é parte revisada e alterada da monografia intitulada "Encriptando denúncias, revelando opressões: A internet enquanto plataforma para denúncias de violência de gênero em tempos de feminismos ciborgues" (Carvalho, 2019c), defendida pele primeire autore em 27/05/2019, no curso de Antropologia da Universidade Federal de Minas Gerais, orientada por Érica Renata de Souza, coautora deste artigo.

[11-34] DOI: 10.5281/ZENODO.6727100
Nº 5 [enero-junio 2022] ISSN 2684-012X

Sendo assim, este artigo pretende a explorar os universos ciborgues (Haraway, 1985) que se desenvolvem com a internet e suas tecnologias do anonimato, pensando seus atores e redes sociotécnicas[4] (Latour, 2012) através de um conjunto de métodos de pesquisa, como: a Antropologia online (Lewgoy, 2009; Amaral 2010; Rüdiger, 2011; Polivanov 2014) ou Antropologia Digital (Horst e Miller, 2012), que se faz em tentativas de delinear as reconfigurações geradas nesta atual era, cada vez mais explicitamente ciborguiana de novos corpos, vivências corporais, interpretações e configurações das interseccionalidades e formas de resistência a partir de um manejo e adaptação da observação participante no ciberespaço, como grupos de *Facebook*, *lives*, fóruns de discussão *online*, sites e aplicativos, etc.; a etnografia multissituada (Marcus, 1995), que tem como objetivos atingir e abordar temáticas multidisciplinares e de alcance globalizado (daí sua importância em contextos de internet onde as fronteiras físicas e sociopolíticas dos "estados nacionais" não se aplicam) e pretende, dessa maneira, seguir "etnograficamente a 'circulação' de atores, objetos e discursos por múltiplos pontos do globo" (Cesarino, 2014: 22) através da articulação de diferentes fontes; e ainda as perambulação/acompanhamento/imersão nos ambientes virtuais (Leitão & Gomes 2018), que propõem entender o ciberespaço enquanto ambiente cartográfico e etnográfico no qual se caminha, participa, observa e imerge, possibilitando o acesso e a geração de formas estendidas e ressignificadas de ambientes e do próprio método etnográfico.

Desta forma, com base nessas metodologias, realizamos um levantamento bibliográfico sobre o histórico jurídico, político e social a respeito de anonimato digital, em especial no contexto brasileiro, a partir de mapeamento e pesquisas sistemáticas no Google, no Google Acadêmico e no TOR.[5] Além disso, em campo realizado de agosto de 2018 a fevereiro de 2019, realizamos também uma etnografia virtual dos sites, organizações e coletivas que tratam de anonimato nas redes, ciberativismo, arquitetura da internet, segurança e governança na internet, e também das polêmicas envolvendo liberdade de expressão e crimes virtuais, privacidade e vazamento/comercialização de dados, e hacktivismo e criptografia nas redes. E, por fim, contactamos também algumas dessas páginas e coletivas e realizamos três entrevistas com participantes e organizadoras destas redes: uma participante da organização Intervozes, uma pesquisadora da Rede Transfeminista de Segurança Digital[6] e Ada uma das coordenadoras de projetos da Safernet[7].

AS HASHTAGS E OS PERIGOS DO NÃO-ANONIMATO

Dentro do contexto de denúncias virtuais, especialmente aquelas voltadas para questões de gênero, um dos movimentos de maior alcance se constituiu especialmente em 2015 com as hashtags de denúncia, como #meuamigosecreto, #meuprimeiroassedio e #chegadefiufiu,[8] que se configuraram como extremamente im-

4 "Bruno Latour (1994) define a estrutura das redes sociotécnicas, na qual o ser humano seria mais um nó numa estrutura não-linear, sempre aberta a novos componentes. A produção contemporânea de 'coletivos híbridos' (Latour, 1994) sugere um modelo de redes como um espaço fértil para viabilizar a produção e a circulação de conhecimento e as novas configurações sociais que emergem na atualidade" (Medeiros & Ventura, 2008).

5 Um software de navegação e pesquisa anônima que protege/não coleta os dados de IP des internautas.

6 Preservando o anonimato da entrevistada, substituímos seu nome pelo pseudônimo Katherine, em homenagem a Katherine Johnson.

7 Preservando o anonimato da entrevistada, substituímos seu nome pelo pseudônimo Ada, em homenagem a Ada Lovelace.

8 "Fiufiu" é uma onomatopeia que remete ao som feito por um tipo específico de assobio utilizado, especialmente por homens, para assediar mulheres em espaços públicos.

[11-34] DOI: 10.5281/ZENODO.6727100
Nº 5 [enero-junio 2022] ISSN 2684-012X

portantes para os movimentos feministas e ciberfeministas brasileiros. Por outro lado, estas hashtags também carregam consigo alguns problemas e problemáticas. A principal problemática das denúncias em redes sociais é que as denunciantes utilizam de seus perfis pessoais, no *Twitter* e no *Facebook*, para apontar as violências que tinham sofreram. Ao mesmo tempo, ao esconderem o nome de seus agressores, operou-se uma lógica de anonimato inversa, na qual as vítimas estavam expostas e os agressores, acobertados. Apesar disso, como pude constatar com inúmeras entrevistas que fizemos ao longo da pesquisa, muitos homens se reconheceram nas postagens e várias mulheres foram perseguidas ou sofreram sérias retaliações por conta de suas denúncias.

No caso das denúncias contra motoristas de aplicativos de transporte, outra modalidade de denúncia nas redes sociais que vêm crescendo bastante nos últimos anos, os casos de retaliações são ainda mais comuns, uma vez que as postagens não deixam dúvida a respeito de quem são os assediadores e abusadores. Em um dos casos relatados, por exemplo, após a denúncia feita no *Facebook*, a vítima começou a ser perseguida por amigos e familiares do denunciado, que lhe mandaram mensagens e comentaram em suas postagens coisas como "vamo [sic] raspar o cabelo dessa mina", além do fato de ter entrado em contato e ameaçado de registrar um B.O.[9] contra ela por calúnia. Portanto, as redes sociais se configuram como ambiente potente, mas pouco seguro para que sirva de espaço para denúncias, não apenas por conta dos riscos de retaliações.

Desta forma, é preciso que encontremos, urgentemente, formas de denunciar na internet e publicizar violências que sejam mais seguras para as vítimas e para as mulheres e pessoas LGBTQIA+ como um todo. Como propôs Katherine, uma das entrevistadas de nossa pesquisa, é urgente a necessidade de os feminismos e ciberfeminismos encontrarem "outras maneiras de denunciar, outras formas de acolher essas denúncias, outros trabalhos de rede que não sejam expositivos pra essas pessoas, de forma que a gente consiga não silenciar essas pessoas e, pelo contrário, acolher e tentar formar essa rede de apoio" (Katherine, 2019). Assim, tais mecanismos poderiam manter os ganhos e objetivos bem-sucedidos das hashtags, mas gerando estes ganhos a partir de práticas que evitem as perseguições e retaliações que a exposição de dados pode causar.

ESCAVANDO CÓDIGOS CIBORGUES: ANONIMATO, PRIVACIDADE E AS MATERIALIDADES DA WEB

No sentido de buscar estas formas outras de se denunciar protegendo os corpos, dados e a própria integridade de mulheres, o anonimato surge como figura central. Associado a ele, e como mecanismo de sua garantia, a criptografia e a encriptação também devem e estão sendo debatidas e utilizadas enquanto ferramentas essenciais. No que diz respeito às denúncias, a criptografia ganha especial importância, pois "tem o condão de reconfigurar arranjos de poder, já que ela possibilita que comunicações e informações sejam ou não disponíveis e para quais pessoas" (Saraiva, 2017: online). Desta forma, para tentar delinear as possibilidades de uma resistência feminista que se proponha ciberativista e conectada às discussões de segurança na internet, é preciso também contextualizar a discussão a respeito de anonimato na rede e os conceitos e práticas que a circulam e constroem, como as noções de privacidade, de liberdade de expressão, de vigilância e de antivigilância no ciberespaço.

9 Boletim de ocorrência policial.

[11-34] DOI: 10.5281/ZENODO.6727100
Nº 5 [enero-junio 2022] ISSN 2684-012X

O anonimato recebeu ao longo do tempo uma série de diferentes definições, mas usualmente é tido como "a condição na qual o nome de uma pessoa é desconhecido", "não-identificável, não-localizável" (Tashiro, 2015: 3), ou ainda na qual a comunicação se encontra não-identificada (Silveira, 2009: 115). A possibilidade de anonimato na internet insere-se ainda dentro de dois outros patamares ou horizontes sociotecnológicos. O primeiro deles é a própria sociedade de controle, definida por Gilles Deleuze (1992) enquanto modo de funcionamento do poder pós-sociedades disciplinares, de maneira que "funcionam não mais por confinamento, mas por controle contínuo e comunicação instantânea" (Deleuze, 1990: 220).

Esta mesma sociedade de controle se vê hoje configurada e reconfigurada também pelas novas tecnologias de rede que possibilitam uma vigilância constante de todos os rastros físicos e digitais deixados pelos indivíduos interagentes nas redes. Além disso, se insere também na rede cibernética – marcada pela multi-interação entre humanos, e entre humanos e máquinas (Silveira, 2009) – chamada de sociedade de informação (Castells, 2000), em que estas possibilidades de vigilância contínua se apresentam não apenas enquanto possibilidades, mas enquanto realidades, em processos de mercantilização de dados pessoais,[10] militarização das redes[11] e rastreamentos geolocalizados de rastros digitais deixados através de nossos IPs ao navegarmos na internet e ao portarmos aparelhos móveis enquanto extensões de nossos corpos e identidades.

> [...] com o desenvolvimento de uma economia baseada em dados, passamos a fornecer importantes informações a nosso respeito em troca de serviços, Wi-Fi públicas ou descontos em medicamentos. Nos últimos anos, nossos dados [...] foram facilmente coletados e processados por diversas empresas e muitas vezes transferidos a terceiros inadvertidamente, isto é, não conhecíamos nem o rosto do nosso negociante. [Sendo assim] na era do capitalismo de vigilância, casos como a possibilidade de discriminação por dados de reconhecimento facial são publicizados pela mídia brasileira e investigados pelo Ministério Público, assim como a coleta e transferência não autorizada a terceiros de dados pessoais por redes de farmácia. (Arvigo et. al., 2018)

Desta forma, o ciberativismo, em especial grupos hackers, tem bancado uma discussão (com cada vez mais apoio da sociedade civil e de grupos de especialistas em tecnologia) pela diminuição da circulação e transmissão de dados pessoais na rede através das tecnologias de criptografia (*Coding Rights*, online). Tal como aponta Donna Haraway, o ciborgue "mapeia nossa realidade social e corporal" (Haraway, 1985: 37) e, sendo assim, a internet muitas vezes opera também no sentido de construir esses mapas de dados e vigilâncias dess usuáries, informações estas que não apenas criam redes de interações múltiplas dentro dos meios virtuais, mas também servem a interesses distintos e verticais em termos de relações de poder.

10 É o caso, por exemplo, de aplicativos de monitoramento dos ciclos menstruais como Glow, Clue e MyCalendar que, como contam pesquisadoras da *Coding Rights*, operam sob a lógica do "chupadados" e "funcionam como laboratórios para a observação de padrões fisiológicos e comportamentais" (VARON, FELIZI, online), compartilhando/vendendo os dados de suas usuárias, usuários e usuáries para uma série de instituições externas como institutos de pesquisa, agências de marketing, a Google Analitcs, jornalistas, plataformas de mídias sociais, dentre muitos outros.

11 Este fenômeno foi denunciado por Edward Snowden, que apontou (e vazou documentos comprovando) em 2013 que Instituições como a CIA e NSA têm sistemas de vigilância e monitoramentos detalhados dos perfis e dados pessoais disponíveis (ou rastreáveis) des usuáries na internet e de seus usos e práticas a partir dela (*Coding rights*, online).

[11-34] DOI: 10.5281/ZENODO.6727100
Nº 5 [enero-junio 2022] ISSN 2684-012X

Neste sentido, tal como defende Sérgio Amadeu da Silveira (2009), o anonimato, apesar de criado dentro destes dois sistemas sociotécnicos descritos, é também seu maior inimigo e transgressor. Isto porque a modernidade criou e estabilizou a ideia de indivíduo enquanto ser de direitos e deveres individuais que estão ancoradas na ideia de uma identidade una e aparente. Sendo assim,

> como bem apontou Zygmunt Bauman, a modernidade tinha um especial horror à indefinição, à incerteza e à ausência de controle. Nesse contexto, o anonimato foi considerado um fator de incerteza em um mundo que clamava por identidades precisas e centradas. (Silveira, 2009: 122)

Desta forma, o controle é oposto ao anonimato, irrastreável e incerto, mas por outro lado, é também possibilitado pela mesma arquitetura de rede que cria a vigilância no ciberespaço. De toda forma, é exatamente por esta posição de ambiguidade incômoda que o anonimato se mostra como arma potente. Além desta, o anonimato, tal como a própria internet, é marcado por uma série de outras ambiguidades e tensões, inclusive jurídicas, principalmente no que tange à dificuldade de gerar algum tipo de regulação nas redes se lidamos com usuáries anônimes.

Além disso, é preciso estar atento ao fato de que o Brasil atual se encontra sob a égide de um governo autoritário, conservador e avesso aos direitos de minorias, tal como ao direito de liberdade de expressão e de crítica. Desta forma, as comunicações anônimas, possibilitadas pelas tecnologias do anonimato, são também neste contexto ferramentas indispensáveis para a sobrevivência de movimentos sociais, de correntes e militantes feministas e LGBTs, e para a defesa de direitos fundamentais, como a privacidade.

ANONIMATO, PRIVACIDADE E LIBERDADE DE EXPRESSÃO NA ESFERA JURÍDICA

A área que até então mais desenvolveu a discussão a respeito do anonimato foi o Direito, na tentativa de desenvolvimento de leis que consigam contemplar o direito ao anonimato –e os direitos a ele associados– e a regulação de atividades na rede, simultaneamente. Juridicamente, o direito ao anonimato foi/é historicamente conjugado ao direito à privacidade. Este, por sua vez, é garantido em lei no Brasil pela Constituição Federal de 1988, no Artigo 5, inciso X e também previsto na Declaração de Direitos Humanos, no Artigo 12, que diz que temos "o direito a manter um domínio a nossa volta, que inclui tudo o que é parte de nós, como nosso corpo, lar, propriedade, pensamentos, sentimentos, segredos e identidade" (Tashiro, 2015: 3). Além disso, neste artigo, o direito à privacidade abarca ainda dentro de si as dimensões do "direito a ser deixado em paz; a limitação de acesso; o controle sobre a informação; o sigilo" (Tashiro, 2015: 3).

Sendo assim, privacidade e autonomia[12] no controle dos próprios dados figuram como direitos fundamentais e ferramentas essenciais para garantia da cidadania das pessoas em uma sociedade. Neste sentido, os direitos ao sigilo e ao controle de informações, presentes na Declaração de Direitos Humanos, nos parecem especialmente centrais ao discutirmos as possibilidades de denúncias anônimas na internet, uma

12 Aqui é importante reforçar que esta autonomia nunca é completa, principalmente pois não somos indivíduos unos fora das relações e porque estas mesmas relações e identidades são constantemente controladas por uma série de forças externas, tais como o Mercado, a Mídia, o Governo, dentre outras. Desta forma, "nenhum ser humano é totalmente autônomo e o limite da liberdade humana se dá no contexto de suas relações com o mundo externo e interno" (Cohen; Gobbeti, 2004: 48).

[11-34] DOI: 10.5281/ZENODO.6727100
Nº 5 [enero-junio 2022] ISSN 2684-012X

vez que descrevem a autoridade dos indivíduos e grupos de salvaguardarem suas identidades em prol de sua segurança. Ao mesmo tempo, aponta a possibilidade de utilizarem esta salvaguarda para gerarem denúncias que garantam processos de cura, de mapeamento de risco para outros membros desses grupos e de gerarem processos de retaliação pelas violências sofridas, sem o risco de serem, por sua vez, retaliados por isso. No que diz respeito à internet e à privacidade e proteção de dados, o debate é mais recente e ainda passa por uma série de discussões e tensões políticas. Até 2018, no Brasil, "a proteção dos dados se apresentava de forma fracionada e esparsa, sendo um grande problema para que o Brasil estivesse integrado nos padrões internacionais de proteção de dados" (Brandão & Oliveira, 2018: 28). No entanto, a exemplo da nova Regulação europeia, a GDPR (*General Data Protection Regulation*), no primeiro semestre de 2018, foi aprovado o Projeto de Lei da Câmara (PLC) N° 53/2018, mais conhecido como "Lei Geral de Proteção de Dados", que tem como objetivo regular os usos de dados de usuáries na internet e protegê-los de usos mercadológicos e de vigilância pública, sem o seu conhecimento e consentimento. "Dessa forma, o Brasil se afasta do modelo de regulamentação setorizada, protege os usuários, ganha segurança jurídica" (Brandão & Oliveira, 2018: 31). Embora não seja voltada para a discussão a respeito do anonimato, a LGPD é um marco histórico na luta pela privacidade na internet e garante aos usuáries um maior controle e segurança a respeito de seus rastros digitais, além de inaugurar no país uma discussão que, se encaminhada com o devido cuidado, pode nos levar para o caminho de conquistar politicamente os direitos a um anonimato seguro e responsável no país.

Entretanto, as possibilidades de navegações anônimas no país são ainda circundadas por uma série de problemáticas, especialmente no que diz respeito a esta intersecção com o Direito. A primeira delas é que, além da privacidade, existe ainda um outro conceito intimamente conectado ao de anonimidade, que é o de liberdade de expressão. O anonimato e a criptografia são defendidos mundialmente por ciberativistas e órgãos internacionais, assim como pela própria ONU (*Coding rights*, online), enquanto ferramentas centrais na garantia da liberdade de pensamento, de expressão e de crítica, mas também porque, em contraste com outros países democráticos, estes conceitos estão colocados juntos na própria Constituição Brasileira, de forma paradoxal.

> Parece estranho, entretanto, falar de direito ao anonimato quando a Constituição Federal de 1998, em seu artigo 5º, IV, expressa que "é livre a manifestação do pensamento, sendo vedado o anonimato". A mesma vedação também aparece no texto da antiga na antiga Lei de Imprensa [27], em seu artigo 7º. (Tashiro, 2015: 9)

Neste sentido, a liberdade de expressão é garantida em lei, mas o anonimato, não, o que se dá especialmente pelo fato de que a comunicação anônima dificulta as regulações dos sujeitos por parte do Estado e a responsabilização de quem cria, expõe ou compartilha informações e conteúdos. "Cria-se uma espécie valorização da liberdade de expressão, mas de concomitante pânico moral quando ela é feita de forma irrastreável" (Carvalho, 2019c).

William Tashiro (2015) demonstra como o Direito encontra-se em constante dificuldade para regular o ciberespaço na era atual da internet, em virtude de sua descentralização espaço-temporal. Surge, portanto, um questionamento central: "como devemos articular os direitos e deveres do cidadão com a regulação da Internet? Existe espaço para o anonimato na Internet?" (Tashiro, 2015: 2). Algumas leis, como a Lei Azeredo e o Marco Civil, tentaram nos últimos anos delinear alguma forma de regulação, sendo que a

[11-34] DOI: 10.5281/ZENODO.6727100
Nº 5 [enero-junio 2022] ISSN 2684-012X

primeira "restringe a liberdade em favor da regulação, e o segundo tem a neutralidade de rede como princípio disciplinador da Internet" (Tashiro, 2015: 9). Ainda assim, não dão conta das atividades anônimas possibilitadas pelas novas tecnologias digitais. Ao buscar explicar as motivações da vedação do anonimato na Constituição, Tashiro argumenta que ela se dá para tentar impedir os abusos ou excessos no exercício da liberdade de manifestação de pensamento e a não-possibilidade de responsabilização nas esferas civil e penal. O autor escreve ainda que isto se torna mais sério e necessário ao tratarmos de denúncias anônimas, que podem ser feitas com base em má-fé e de forma falsa, e diante da possibilidade de "abuso contra o patrimônio moral das pessoas através de acusações ou imputações infundadas, com o objetivo de minar a imagem pública e a honra de um indivíduo ou organização" (Tashiro, 2015: 11). A vedação do anonimato está, portanto, inerentemente associada a uma preocupação com o "excesso de liberdade de expressão", a não possibilidade de responsabilização de possíveis crimes, ofensas e falsas denúncias.

É preciso frisar que de fato esta não é uma questão com respostas fáceis e, sim, um fenômeno complexo cujas repercussões são múltiplas. Ao tratarmos de crimes cibernéticos anônimos e ofensas na internet, é preciso ter em mente que os grupos mais atingidos são compostos por corpos minorizados, principalmente mulheres, LGBTs e pessoas negras. Por outro lado, é difícil pensar em outras formas –que não o anonimato– de, por exemplo, se denunciar, uma vez que em países como o Brasil: a polícia não traz segurança; as vítimas mulheres são responsabilizadas pelas agressões, abusos e assédios que sofrem dentro e fora da internet; e não existem políticas de enfrentamento ao machismo, a cultura do estupro; havendo, inclusive, uma lógica punitivista para as mulheres denunciantes. Ademais, tal como demonstra Clark (2009), existem mecanismos de verificação –chamados de "subspaces[13]"– das informações e denúncias difundidas em plataformas anônimas na internet, como "mecanismos de reputação, de denúncia colaborativa e pelas redes de confiança", ou seja, os "instrumentos interativos de busca e enquete da comunicação distribuída tornam o anonimato reputável (Antoun, 2008: 17)" (apud Silveira, 2009: 127).

Além disso, existe ainda uma série de "reinterpretações oportunas", feitas juridicamente sobre a própria vedação ao anonimato. Isso, pois este mesmo recurso vedado à população em geral é utilizado diariamente por instituições tais como o Disque Denúncias (por telefone e, inclusive, *online* no Estado de São Paulo) (Schincariol, 2016, online). "O Supremo Tribunal Federal tem farta jurisprudência entendendo que, nestes casos, a denúncia anônima serve para deflagrar a investigação policial, não havendo que se falar em nulidade automática da investigação iniciada por uma denúncia anônima" (Schincariol, 2016, online). É importante salientar que este tipo de "denúncia anônima" não concretiza de fato o pretendido anonimato, uma vez que não há sistemas de criptografia e encriptação forte, e, portanto, os envolvidos e os IPs dos denunciantes se tornam rastreáveis. Além disso, estes mecanismos admitem a possibilidade de enviar fotos, áudios e cópias de documentos que, se não passarem por uma limpa de dados, são acompanhados das informações dos aparelhos que retiraram, armazenaram e enviaram estes arquivos. Portanto, tal como ressalta Fernando Schincariol (2016), o Estado só permite os anonimatos que parecem ser a ele oportunos ou controláveis pelo próprio Estado e nunca a comunicação ou denúncia anônima que é feita autonomamente.

13 "It is a common misconception that you cannot trust anonymous information. This is not necessarily true, using digital signatures people can create a secure anonymous pseudonym which, in time, people can learn to trust. Freenet incorporates a mechanism called 'subspaces' to facilitate this" (FREENET, 2002, online).

[11-34] DOI: 10.5281/ZENODO.6727100 Nº 5 [enero-junio 2022] ISSN 2684-012X

> Há uma grande inversão de valores aqui. O Estado Democrático de Direito permite a investigação penal a partir da denúncia anônima, mas proíbe a manifestação do pensamento, o discurso anônimo. O Estado pode te investigar e punir a partir de uma denúncia anônima mas você não pode, anonimamente, exercer o direito de crítica. (Schincariol, 2016, online)

AGENDA CIBERATIVISTA E ANONIMATO

Outra agenda importante neste contexto de disputas a respeito do anonimato que vem se desenrolando nas últimas décadas é a de ciberativistas cujos objetivos são, em especial, a luta pelo respeito da comunicação anônima e da privacidade de dados.

Os precursores deste movimento são conhecidos como *cypherpunks* que "defendem o uso da criptografia como fio condutor de transformações sociais e políticas, acreditam que a privacidade é necessária na era digital, e que ela deve ser conquistada (e não esperada) por meio da criptografia" (Tashiro, 2015: 4). Defendem, portanto, um forte sistema criptográfico que se utiliza da arquitetura da internet e das possibilidades que esta oferece, para gerar possibilidades de navegação, comunicação e ativismo político menos vigiadas, mais autônomas e mais protegidas. Alguns dos *cypherpunks* mais conhecidos são Jacob Appelbaum e Julian Assange, pois foram figuras centrais no desenvolvimento de algumas das tecnologias de anonimato mais difundidas: o TOR e o WikiLeaks, respectivamente. O TOR é

> um *software* que impede a chamada análise de tráfico, uma forma de vigilância que ameaça a liberdade e a privacidade na rede [...] e que distribui a comunicação através de uma rede de voluntários transmissores ao redor do mundo (TOR, 2009), impedindo o monitoramento da conexão, dos sites acessados e evitando que se descubra a localização física dos interagentes. (Silveira, 2009: 121)

Permite, portanto, "usar a Internet através de servidores *proxy* ou de redes voluntárias de 'desidentificação'" (*Coding rights*, online). O TOR, portanto, é ferramenta importante na organização de movimentos sociais, garantia de "direitos humanos" e direitos de grupos minorizados como, por exemplo, a possibilidade de se encontrar informações, remédios e tratamentos para realização de abortos seguros em países (como o Brasil) em que a prática é proibida, como destacou Isabela Bagueiros (2018) em palestra dada no evento anual da CryptoRave em São Paulo em 2018. De toda forma, é sabido o papel da internet na relação de busca de informações e recursos para o aborto, como abordado na pesquisa de Silva (2018). Nesta mesma senda, é importante destacar que o TOR também funciona como uma das principais ferramentas indicadas para a produção de denúncias anônimas nas plataformas mapeadas na minha pesquisa e que serão descritas mais à frente. O TOR adquiriu um nível de relevância e disseminação internacional, e gerou um desconforto tão grande nas organizações governamentais, midiáticas e nas oligarquias de comunicações privadas, que fez com que se construísse o imaginário da chamada *DeepWeb* ou *DarkWeb* em torno de si, enquanto um espaço ilegal e perigoso arquitetado para facilitar atos ilegais e monstruosidades violentas, tais como o tráfico de crianças, órgãos e a pedofilia infantil. Já o *WikiLeaks* é uma organização/plataforma fundada em 2006 por Julian Assange, com base nos princípios de transparência política dos governos e no uso das redes virtuais para garantir tal transparência, ainda que de maneiras não-ortodoxas. Desta forma, o *WikiLeaks* atua a partir do vazamento e compartilhamento de documentos e informações sensíveis que tenham impacto político na população.

[11-34] DOI: 10.5281/ZENODO.6727100
Nº 5 [enero-junio 2022] ISSN 2684-012X

Outro personagem importante no histórico de militância em defesa dos direitos de segurança e privacidade na internet foi o grupo hacktivista *Anonymous*, que teve sua origem em fóruns anônimos virtuais, em 2003, e se caracteriza como uma organização anárquica, anônima, descentralizada e com atuação "global e sempre a favor da liberdade de expressão e da pirataria" (Tashiro, 2015: 5), em defesa do uso das tecnologias digitais e virtuais em favor da luta política e da descentralização da informação.

É importante destacar, ainda, que a militância pelo direito à privacidade na internet, liderada por *cypherpunks*, ainda se centrava quase que exclusivamente em torno de um conceito de liberdades e direitos individuais (reiterando uma lógica moderna de indivíduo que é, por excelência, fundamentada no arquétipo de homens brancos, heterossexuais e de classes econômicas dominantes) e abordava muito pouco a defesa de direitos coletivos. Nesta mesma senda, um importante fato a ser pontuado é que estes grupos de militantes eram compostos, em sua maioria, por pessoas de categorias hegemônicas e privilegiadas (inclusive no acesso aos dispositivos e discussões a respeito desses temas); chegaram a defender, aliás, pautas contra o direito de minorias, como, por exemplo, a não recriminação de atividades discriminatórias, em prol desta teórica "liberdade individual" (May, 2000).

CONTROLE E RESISTÊNCIA COMO PRODUTOS DO MESMO SISTEMA

Outra figura central nas discussões a respeito das possibilidades, ambiguidades e riscos da internet, especialmente no aspecto jurídico deste debate, é Lawrence Lessig, professor de Direito em Harvard, que apresenta em seu livro "Code 2.0" (2006) uma teoria histórica a respeito da regulação da Internet. Lessig defende que o ciberespaço, muitas vezes visto enquanto espaço descentralizado e feito enquanto ambiente libertário, é, na verdade, uma plataforma que, se bem regulada, tem potencial para ser mais restritiva do que as regulações estatais, uma vez que possui um mecanismo único denominado "código". "Sua teoria sobre a regulação ou 'regulabilidade' da Internet veio para explicar as grandes lacunas entre o Direito tradicional e o ambiente do ciberespaço, mas, no final das contas, é aplicável a um escopo muito maior" (Do Carmo & Gonçalves, 2018: 13). Desta forma, Lessig defende que o Direito se aproprie das ferramentas presentes na própria arquitetura da rede para utilizá-las em prol de uma maior regulabilidade. Neste sentido, demonstra como a internet, ao invés de um "paraíso sem regras", já tem as atividades que nela operam restringidas por quatro forças reguladoras, "que se influenciam mutuamente" (Do Carmo & Gonçalves, 2018: 3): o Direito; o Mercado; as Normas Sociais e culturais; e a Arquitetura. Lessig dá especial atenção à arquitetura, pois é nela que se inserem as possibilidades de regulação dos códigos e, portanto, a unicidade que a Internet permite à regulação. No entanto, Paloma Rocillo do Carmo e Pedro Vilela Gonçalves (2018) defendem que o objetivo de Lessig com esta explanação não seria o de aumentar a vigilância e o fim da privacidade des usuáries, mas apenas propor que o Direito se aproprie destas ferramentas, pois senão esta lacuna será, e já está sendo ocupada pelo mercado e pelas normas sociais, que as sujeitam às suas regras, muitas vezes pouco democráticas. Lessig argumenta, ainda, que

> embora pareça inicialmente um ambiente libertário, a Internet é por natureza um dos ambientes mais controláveis criados pela humanidade. [...] nem o controle nem a liberdade são inerentes à Internet, mas opções feitas pelos desenvolvedores de seus códigos e portanto sempre sujeitos à mudanças. (Do Carmo & Gonçalves, 2018: 13)

[11-34] DOI: 10.5281/ZENODO.6727100
Nº 5 [enero-junio 2022] ISSN 2684-012X

No entanto, é preciso ainda destacar que embora o intuito de propor uma regulação responsável à internet (mesmo princípio que operou na formação de leis como a GDPR e a LGPD), posicionamentos como este podem e são utilizados muitas vezes para o combate ou a fragilização do anonimato, uma vez que este se mostra resistente e transgressor das regulações impostas, inclusive, pelos códigos.

Para entender melhor como isso funciona na prática, é preciso adentrar a materialidade que compõe a Internet e seu funcionamento e explorar sua arquitetura e as formas pelas quais essa materialidade vem moldando relações, corpos e vivências no mundo da Sociedade de Informação, tal como vem redefinindo as próprias militâncias e lutas feministas virtuais. Neste sentido, Haraway foi uma das primeiras a nos atentar para a vigente necessidade de se explorar as materialidades e corporificações dos corpos e corpos/máquinas, a começar pela própria defesa da fidelidade do ciborgue ao materialismo (Haraway, 1985: 39), e retomando até mesmo autoras mais clássicas da Antropologia, como Mary Douglas que, segundo a Haraway, nos ajuda "a ter consciência sobre quão fundamental é a imagística corporal para a visão de mundo e, desta forma, para a linguagem política" (Haraway, 1985: 84).

A ARQUITETURA DA INTERNET E A MATERIALIDADE DA REDE

Para começar a escavar as edificações de tal materialidade é interessante partir de uma pergunta feita no texto "Redes cibernéticas e as tecnologias do anonimato" (2009), no qual o autor Sérgio Amadeu da Silveira questiona se existiriam "organizadores da internet?". Segundo Silveira, a resposta a esta questão estaria nos protocolos, os principais responsáveis por organizar as atividades e comunicações feitas através da internet, uma vez que se configuram como conjuntos de regras e convenções dadas pelos algoritmos (códigos programados) que determinam o que é ou não possível dentro da internet. Sendo assim, eles têm papel fundamental em delimitar interações e comportamentos na rede, na medida em que ditam as regras de como a navegação dentro desse mundo pode ou não se dar. "Enquanto a arquitetura do mundo real é baseada nas leis da física, na Internet, é baseada no código" (Do Carmo & Gonçalves, 2018: 14). Os protocolos são, portanto, importantes elementos da Arquitetura da Internet, assim como o que se convencionou chamar de "topologia de rede" –dividida em topologia física e lógica– que é, por sua vez, o "arranjo físico e lógico" (Silveira, 2009: 119) que constitui a materialidade da nuvem. Esta materialidade é composta por uma série de elementos físicos, tais como computadores, cabos, roteadores, switches, concentradores que também têm papel fundamental nas delimitações de possibilidades e impossibilidades das interações e comunicações por computador e na rede. Neste sentido, como aponta o antropólogo Jair de Souza Ramos (2015), a partir da massificação de computadores pessoais e smartphones, estes dispositivos e a chamada "nuvem" passaram a funcionar como terminais de informação e instrumentos de conexão e circulação de informações, práticas e relações.

Voltando, portanto, à arquitetura da rede, composta por estes diferentes elementos dos protocolos e da topologia de rede, ela é responsável por condicionar os acessos que os internautas têm na internet (Tashiro, 2015) e, inclusive, por identificar, mapear e armazenar estes acessos e de onde eles vêm. É neste sentido que Lessig afirma que a Rede "poderia ser projetada para revelar quem alguém é, onde está e o que está fazendo. E se fosse assim projetado, então a Rede poderia se tornar, como argumentaremos ao longo desta parte, o espaço mais regulável que o homem já conheceu"[14] (Lessig, 2006: 53, *apud* Tashiro, 2015: 23). Des-

14 "The Net could be designed to reveal who someone is, where they are, and what they're doing. And if it were so designed, then the Net could become, as I will argue throughout this part, the most regulable space that man has ever known" (Lessig 2006: 53, *apud* Tashiro, 2015).

[11-34] DOI: 10.5281/ZENODO.6727100 Nº 5 [enero-junio 2022] ISSN 2684-012X

ta forma, é possível perceber como esta materialidade da arquitetura da internet tem elementos compartilhados com outras formas de materialidades, mas tem também especificidades que a tornam mais fluida e constantemente manipulável por quem detenha tal conhecimento. Jair Ramos (2015) também descreve esta ambiguidade ao dizer que as materialidades reinventadas do ciberespaço mantêm continuidades, mas também inserem novidades nas maneiras de sociabilidade. Desta forma, a rede mundial de computadores e dispositivos móveis, que dá base para a Internet, e as redes de relações e informação geradas no ciberespaço fazem parte e se inserem no processo histórico indicado por Foucault de formação de cadeias de conexão e circulação de mercadorias, tributos, trabalho e autoridade, como atualizações desse processo, mas ao mesmo tempo inspiradas por ele (de forma que também operam estes fluxos de relações, pessoas, objetos e poder).

Este complexo sistema que compõe a rede cibernética se configura enquanto uma rede de relações e de poder que é descentralizada, mas não horizontal (Ugarte, 2008; Silveira, 2009). Isto parece ocorrer por uma série de motivos. O primeiro deles é que –uma vez que as pretensas barreiras entre mundo off-line e on-line não existem de fato ou estão cada vez mais borradas– as relações estabelecidas na internet e a partir dela seguem operando de acordo com os sistemas e estruturas de poder verticais, coloniais e hierarquizados que existem fora da internet e com as dualidades forjadas que os compõem (como homens-mulheres, ricos-pobres, negros/indígenas-brancos, norte global-sul global, etc.). Outro motivo para essa verticalidade das relações e estruturas da rede cibernética é também o fato de que ela se organiza de acordo com um "sistema de localização de nomes de domínios extremamente hierarquizado, o *Domain Name System*"[15] (Silveira, 2009: 116), que é, por sua vez, controlado por monopólios de grandes operadoras de comunicação. Desta forma, tal como afirma Pierre Mounier, "a Internet como 'espaço público', como 'bem comum' do qual ninguém pode legitimamente querer se apoderar [...] é apenas uma das visões possíveis da comunicação dos computadores em rede" (Mounier, 2006, *apud* Silveira, 2009: 2). Esta mesma estrutura parece, paradoxalmente, propícia tanto ao controle quanto ao não-controle (Silveira, 2009): o primeiro através da utilização das ferramentas da topologia da rede e de seus protocolos para rastreamento e acompanhamento desse *Domain Name System*, que mantém registrados os [16] (identidades virtuais) e atividades (rastros virtuais dessas identidades) feitas na rede; o segundo através da possibilidades das tecnologias de anonimato, como a criptografia e plataformas como o TOR, que desvinculam os endereços de IP de suas identidades civis ou fecham, através de chaves (criptográficas), os acessos a essas identidades e seus rastros.

> No mesmo sentido, Fernanda Bruno escreveu que "as mesmas tecnologias que possibilitaram o anonimato nas trocas sociais e comunicacionais mostram-se eficientes instrumentos de identificação. A vigilância se confunde hoje com a própria paisagem do ciberespaço". (Bruno, 2006: 154, *apud* Silveira, 2009: 130)

15 "O DNS funciona como uma grande tabela que indica um nome em letras e sua correspondência em endereço IP (em números) [...] Assim, os servidores de DNS são como telefonistas da Internet, associando um número mais difícil de se recordar a um nome mais facilmente memorizado" (Do Carmo y Gonçalves, 2018: 6).

16 "Dentro da rede, os dispositivos se comunicam por meio de um IP (*Internet Protocol*). O IP tem duas principais funções: servir de identificação de um dispositivo na rede –números separados em quatro casas (os roteadores TPLink, por exemplo, tem o IP 192.168.1.1)– e dividir as informações em partes (pacotes). Pode-se dizer que pacotes IP são partes de uma informação, e que cada parte está etiquetada com os endereços de origem e destino" (Do Carmo y Gonçalves, 2018: 6).

[11-34] DOI: 10.5281/ZENODO.6727100
Nº 5 [enero-junio 2022] ISSN 2684-012X

Haraway (1985) é outra autora que, ainda antes da expansão da internet, já falava a respeito de como a arquitetura dos sistemas que não têm nada que "naturalmente" diga como devam ser planejados e, portanto, essa arquitetura pode ser utilizada de formas plurais e disputadas.

Neste sentido, a criptografia entra como ferramenta central na possibilidade de utilização da arquitetura da internet para se garantir anonimato e privacidade. "A comunicação anônima dos interagentes é o atenuante ou o antídoto ao controle totalizante engendrado pelo diagrama que regula e opera em toda a organização da rede" (Silveira, 2009: 118). Desta forma, a criptografia pode ser exemplificada da seguinte maneira: tem-se uma informação que é como um objeto guardado dentro de uma casa e, para protegê-la, coloca-se uma fechadura, passível de ser aberta apenas por quem tem a chave daquela tranca.[17] Isto significa que ela opera como uma ferramenta de ocultar e codificar dados e informações, deixando-as ininteligíveis para quem não tem acesso a uma chave para decifrá-las e, portanto, decodificá-las (em geral, os destinatários da mensagem). Nascidas e originalmente utilizadas apenas por governos em situação de guerra (Loureiro, 2014), as práticas de encriptação hoje são bastante difundidas para diversos grupos da sociedade civil,[18] transgredindo, portanto, seus objetivos iniciais (militaristas e colonizadores).

Como não poderia deixar de ser, por sua absoluta relevância enquanto mecanismo anti-controle na internet, a criptografia tem sido alvo de uma série de disputas políticas ao redor do mundo e, inclusive, no nosso país. É o caso, por exemplo, dos bloqueios no *Whatsapp* que foram ordenados pela Justiça Federal nos últimos anos no Brasil, após o aplicativo se recusar a decodificar seu sistema de criptografia (de ponta-a-ponta), para a investigação de crimes, argumentando que não apenas uma ação destas quebraria a confiança des usuáries no sigilo da empresa, mas também porque, segundo eles, é quase impossível decodificar este tipo de criptografia.

ANONIMATO E DIREITOS HUMANOS

Um importante acontecimento que marcou esse histórico de disputas políticas foi o relatório escrito pelo Alto Comissário da ONU, David Kaye, em maio de 2015, cujo objetivo central era defender que "a criptografia e o anonimato permitem que os indivíduos exerçam seus direitos à liberdade de opinião e expressão na era digital e, como tal, merecem uma forte proteção" (Kalia, 2016, online). Kaye defende ainda a centralidade de tecnologias do anonimato para a continuidade do trabalho de jornalistas e ativistas e cita, inclusive, a importância de plataformas como o TOR para a garantia de comunicações e ativismos políticos mais seguros e a busca de informações menos controlada (Plaza, 2015). Em relação à possibilidade de militantes feministas poderem utilizar destas duas ferramentas para exercer seus ativismos na rede sem perseguição e para que mulheres possam denunciar seus casos de violência de gênero sem retaliações, o relatório ressalta:

17 É importante ainda dizer que existem o que se chama de "*backdoors*" ou "porta dos fundos" que são mecanismos de acesso excepcional em criptografias não tão fortes, através dos quais se consegue acessar a informação sem a chave.

18 Ainda assim, é preciso ressaltar que, mesmo em processo de expansão, por enquanto esta é uma prática restrita a certos grupos que têm acesso financeiro e social a este tipo de discussão e aprendizado deste conhecimento, e também aparato tecnológico para tal.

[11-34] DOI: 10.5281/ZENODO.6727100 Nº 5 [enero-junio 2022] ISSN 2684-012X

> • Discurso anônimo é necessário para defensores dos direitos humanos, jornalistas e manifestantes.
> • Proibições do uso individual de tecnologia de criptografia constituem uma restrição desproporcional ao direito à liberdade de expressão.
> • Proibições do anonimato on-line e obrigatoriedade do uso de nome real ou do registro de um chip de celular vão além do permitido pela lei internacional. (ARTIGO 19, 2015: online)

Neste sentido, destaca ainda como as tentativas dos Estados de enfraquecimento e proibição do anonimato na rede seriam formas de atentado aos direitos e liberdades individuais, e aos próprios direitos humanos, e que, ao contrário, os Estados "deveriam protegê-lo e não restringir as tecnologias que o proporcionam" (ARTIGO 19, 2015, online). Thomas Hughes,[19] ao comentar a respeito do relatório aponta ainda como o anonimato e a criptografia são condições fundamentais para que possam existir delações e denúncias de ilegalidades, sem que as e os denunciantes sejam por isso perseguidas(os) de alguma forma.

O relator, no entanto, não foi o primeiro a defender este tipo de posição, e outros importantes estudiosos e militantes, não apenas da área de tecnologia, mas também do Direito, da Sociologia e outras, têm refletido a respeito dos impactos e centralidades do direito ao anonimato para garantia de liberdades e direitos humanos essenciais. Um deles, por exemplo, é Ian Clark, hacker e fundador da rede *Freenet*, que defende que

> Você não pode ter liberdade de expressão sem a opção de permanecer anônimo. A maioria da censura é retrospectiva, geralmente é muito mais fácil restringir a liberdade de expressão punindo aqueles que a exercitam depois, em vez de impedi-los de fazer isso em primeiro lugar. (Clark, online)[20]

Outro defensor desta posição é Walter Capanema, que chega a afirmar que "o anonimato, sem dúvida alguma, é um escudo contra a tirania, de onde quer que ela surja" (*Coding rights*, online) e que, portanto, é um importante mecanismo de ação para subversão e resistência às estruturas de poder. Neste sentido também, vem surgindo uma série de campanhas virtuais encabeçadas por importantes coletivas ciberativistas e feministas, como a campanha #ConecteSeusDireitos, do coletivo Intervozes, que visam promover confluências de agendas entre as lutas feministas e antirracistas e os direitos ao anonimato, privacidade e liberdade de expressão.

ANONIMATO E MULHERES: RISCOS E RESISTÊNCIA DE UMA REDE EM DISPUTA

Se anonimato, como procuramos demonstrar até aqui, se encontra neste local de tencionar estruturas de poder e fazer emergir delas, paradoxal e concomitantemente, riscos e resistências para diversos grupos, quando se trata de mulheres –especialmente mulheres cujos corpos, experiências e subjetividades são

19 Diretor-executivo global da ARTIGO 19, uma ONG originalmente inglesa e presente no Brasil desde 2007, que tem como principal objetivo atuar na defesa da liberdade de expressão e descentralização e acesso à informação e ao combate às violações de Direitos neste sentido (ARTIGO 19, s/d, online).

20 "You cannot have freedom of speech without the option to remain anonymous. Most censorship is retrospective, it is generally much easier to curtail free speech by punishing those who exercise it afterward, rather than preventing them from doing it in the first place" (Clark, s/d). Tradução minha.

[11-34] DOI: 10.5281/ZENODO.6727100 Nº 5 [enero-junio 2022] ISSN 2684-012X

transpassados por outras intersecções minorizadas– este aspecto ambíguo do anonimato se faz ainda mais contundente. Isso se torna bastante evidente nas falas das mulheres entrevistadas e de outras militantes ciberfeministas que mostram claramente que se, por um lado, como apontamos,

> As tecnologias de ocultação de identidades vêm servindo enquanto meio para assediar, perseguir e violentar mulheres e suas privacidades, por outro lado, são estas mesmas ferramentas que podem ser utilizadas para a efetuação de militâncias e denúncias seguras. (Carvalho, 2019a)

Além dessa controvérsia, ainda há o importante fato de que nós, mulheres e pessoas LGBTQIA+, somos ensinadas a sentir culpa e vergonha ao sermos assediadas e violentadas, o que faz com que denúncias que não sejam anônimas se tornem ainda mais raras e difíceis, e o anonimato, ainda mais necessário em casos de assédio e abuso. Neste sentido, Ada, uma de nossas entrevistadas[21] ressalta a importância que o anonimato tem na plataforma de denúncias *Safernet:*

> A questão do anonimato ela é fundamental para os procedimentos de denúncia [...]. Porque a gente sabe que denúncias envolvendo violência contra a mulher certamente podem colocar elas em situação de risco, ou podem sofrer algum tipo de retaliação, ou o agressor, na medida em que tome conhecimento de onde partiu a denúncia, isso acabe fazendo com que ele cometa algum ato mais violento contra a mulher. Enfim... e a gente sabe que nessa rede, de onde as mulheres podem denunciar, nem sempre elas são bem recebidas ou os profissionais estão treinados para receber elas bem. Então, de fato, elas também ficam receosas, né? De buscar delegacias, por uma série de razões, a gente sabe que essa é uma rede, um sistema, que ainda precisa melhorar. Então, você ter canais anônimos de denúncia incentiva a denúncia e protege o denunciante. Então, o anonimato é super importante, sim, e pode ser decisivo pra pessoa fazer ou não a denúncia. (Ada, entrevista realizada em 15/04/2019)

Outras duas falas importantes a respeito dessa complexidade gerada pelo anonimato vêm das ativistas Charô Nunes, do Blogueiras Negras, e a jornalista Ana Freitas, do Nexo Jornal, em entrevistas concedidas ao "Boletim Antivigilância" (Freitas, 2016; Nunes, 2016). Elas contam como, apesar de sofrerem reiteradamente ao longo dos anos de ativismo diversas formas de perseguições e ataques virtuais praticadas por perfis anônimos, permanecem defendendo veementemente que a origem destes nunca foi o anonimato e sim o fato de que as estruturas e lógicas machistas que operam *offline* são transpassadas e reconfiguradas para o mundo da internet. Portanto, enquanto estas não estiverem sendo seriamente combatidas não é possível impedi-las de acontecer virtualmente, criminalizando ou perseguindo o anonimato.

> O episódio não me tornou uma defensora de políticas públicas para registrar dados de navegação de usuários da rede. Me conscientizei da necessidade de uma legislação para proteger dados pessoais, como os meus, facilmente acessíveis no banco de dados do Serasa. Me envolvi ainda mais com o feminismo, ciente da necessidade de educar meninos e meninas sobre igualdade de gênero para que nenhuma outra mulher passe pelo que eu passei. (Freitas, 2016, online)

21 Que atuou, à época da entrevista, como uma das coordenadoras de projeto da *Safernet*.

[11-34] DOI: 10.5281/ZENODO.6727100
Nº 5 [enero-junio 2022] ISSN 2684-012X

> Entender a privacidade como causa do discurso de ódio nada mais é que um estratagema para justificar uma censura que não tem como objetivo acabar de fato com as narrativas contra as mulheres negras e outras minorias. Tem mais relação com coibir os direitos à comunicação e ao direito à privacidade. Nesse caso os maiores penalizados seriam aqueles que estão em luta, não seus algozes que se fiam muito mais na impunidade usufruída por quem difunde opiniões de ódio do que na privacidade. (Nunes, 2016, online)

Neste sentido, as violências praticadas no ciberespaço contra mulheres são, sim, reinventadas e reconfiguradas frente às especificidades que este tipo de espaço proporciona, mas são também reflexos das violências estruturais que historicamente moldam as existências de mulheres no mundo fora da internet, especialmente de mulheres negras, indígenas, pobres, trans, lésbicas e pessoas não-binares.

É importante dizer que, ainda que o objetivo aqui seja dar relevância às formas de resistência e apropriação feminista do anonimato, da internet e da criptografia, estas formas de violência não devem ser subestimadas ou relevadas. As violências virtuais feitas contra mulheres são extremamente graves e têm efeitos muito sérios nas vidas dessas mulheres. Além disso, é também este mesmo tipo de atividade misógina, racista e antifeminista na internet que faz muitas mulheres desistirem da militância *online*, vítimas de ameaças e assédio, como aponta a entrevistadora da *Coding Rights*, em entrevista com Charô Nunes, ao destacar as "consequências que vemos da violência na internet contra minorias, que geram de autocensura até mudança na rotina do indivíduo (em caso de ameaças concretas à integridade física da pessoa), ataques à servidores para gerar DoS (em caso de coletivos), etc." (*Coding rights*, 2016, online).

Por fim, é importante destacar como este tipo de reapropriação das lutas pelo direito ao anonimato em prol de direitos coletivos a grupos e minorias políticas, em contraposição aos debates clássicos e ativistas históricos que estavam mais interessados em defesas de direitos individuais e inseridos em contextos e posições de privilégios, vem crescendo e sendo protagonizada por ativistas e coletivas ciberfeministas. Estes movimentos ciberfeministas de formação de redes virtuais resistentes é identificada também como Tecnologia Feminista, que, segundo as autoras Daniela Araújo, Marta Kanashiro e Débora Oliveira (2020), é um conceito/movimento que agrega uma série de discussões, debates e práticas tecnopolíticas, buscando apontar para a não-neutralidade das tecnologias e das redes cibernéticas e pautando a necessidade de se repensar, a partir das experiências, interesses e necessidades de mulheres, pessoas trans e não-binares, a produção, o manejo, o uso e as discussões a respeito das tecnologias de informação e comunicação (TIC). Desta forma, as autoras apontam que as redes sociotécnicas formadas em torno da construção dessa Tecnologia Feminista,

> Diante dos processos de vigilância e concentração de poder e das violências discriminatórias que atravessam a Internet, em muitos espaços sobre tecnologias livres e redes autônomas e comunitárias passou a ser realizado em paralelo o debate sobre o fortalecimento de medidas de segurança. Os temas muitas vezes se fundem e a autonomia se torna condição necessária para a segurança. Nesse sentido, as tecnologias feministas lembram que as medidas de segurança também não são universais e que a construção de espaços seguros passa por uma combinação de subjetividades, corresponsabilidades e cuidado mútuo. (Oliveira et. al., 2020: 21)

[11-34] DOI: 10.5281/ZENODO.6727100 Nº 5 [enero-junio 2022] ISSN 2684-012X

AMBIGUIDADES E NARRATIVAS DISPUTADAS

O que todos esses diversos grupos, discursos e narrativas disputadas acerca do anonimato demonstram, ainda que de diferentes formas, é como este é um fenômeno de ordem complexa e imbricada em uma série de paradoxos ou, como trata Sérgio Amadeu, "tensões dialéticas". Não apenas o anonimato em si, mas os conceitos, práticas e ferramentas a ele relacionados –de privacidade, de liberdade de expressão e a criptografia em si– estão cheios de ambiguidades e, tal como apontam as ciberfeministas a respeito da internet, também são plataformas e mecanismos que permitem e constroem tanto riscos quanto possibilidades de resistências. Quando se trata do debate de anonimato e violências de gênero, por exemplo, lidamos, por um lado, com casos de violências virtuais contra mulheres, com *trolls* e com ameaças dos mais variados tipos, vindas de usuários anônimos e, por outro, nos deparamos com militâncias (ciber)feministas que só são possíveis através do anonimato. O artigo de Oliveira e colegas (2020) também aponta para estas potencialidades ambíguas da internet, especialmente para mulheres, pessoas trans e não-binares e propõem uma visão crítica delas,

> reconhecendo que a internet e as TICs podem assumir tanto um lugar de resistência, como ser aquele onde as violações de direitos, inclusive aquelas baseadas em múltiplas desigualdades como as de gênero, raça, classe, se proliferam e o debate social é restringido. (Oliveira et. al. 2020: 3)

Assim, se por um lado abrimos as portas para todo um novo tipo de violência de gênero que teoricamente se faz através do "anonimato" *online* dos agressores, por outro, as saídas pela criminalização e aumento na vigilância pelo Estado ou pela "carta branca" para a mediação das plataformas como Facebook e Twitter também são muito complicadas. "Esther Dyson, ex-presidente do Internet Corporation for Assigned Names and Numbers (ICANN)2, problematizou tais dificuldades: 'No final, precisamos lidar com o lado sombrio do anonimato em vez de colocar todo ele fora da lei'" (Silveira, 2009: 129).

É o caso, por exemplo, de várias propostas de PL –Projetos de Lei– dentro da CPI-Ciber. Ainda que contasse com o bom intuito de debater e combater os cibercrimes, com destaque para os crimes virtuais contra mulheres, esta CPI tinha como eixo orientador uma associação perigosa e injusta entre privacidade virtual e a garantia de liberdade para crimes e discursos de ódio na rede (*Coding rights*, 2016). Além disso, como apontam Joana Varon e Lucas Teixeira (2016), os próprios movimentos e grupos atingidos pelos crimes e discursos de ódio na internet, como as coletivas ciberfeministas, que discutem estas questões há anos, não foram escutados ao longo da CPI. Desta forma, o resultado desta CPI foi a redação de uma série de PLs, dentre eles, um que permitia a qualquer delegado da Polícia Civil o acesso aos dados cadastrais e aos endereços de IP de usuáries, em caso de investigação de crimes cibernéticos, sem a necessidade de uma autorização dada por um Juiz.[22] Na prática, esse PL daria acesso livre e irrestrito à polícia para rastreamento e localização de qualquer atividade virtual de qualquer usuário da rede, de forma a servir-se politicamente das ambiguidades e riscos que a comunicação virtual utilizada de forma irresponsável pode trazer, para gerar uma rede de vigilância militarizada nunca antes vista na história do país. A CPI foi alvo de uma série

22 "Embora a Comissao tenha retirado o PL do relatório, um outro projeto parecido veio do Senado e tramita na Câmara como PL N° 5074/2016. Este PL permite à delegados de polícia e membros do Ministério Público a requisição, sem ordem judicial, de dados cadastrais (mas não endereços IP)" (Teixeira & Varon, 2016, online).

[11-34] DOI: 10.5281/ZENODO.6727100
Nº 5 [enero-junio 2022] ISSN 2684-012X

de críticas duras, advindas inclusive de organizações feministas como a *Coding Rights*, o Intervozes e o Think Olga, que argumentaram que

> A permissão de qualquer acesso a dados pessoais de cidadãos sem ordem judicial não tem paralelo em legislações de países democráticos. […] Direitos humanos não podem ser fragilizados a pretexto de atender à celeridade de uma investigação, por um procedimento que, na prática, pode significar uma porta aberta a arbitrariedades e a violações de direitos. (Teixeira & Varon, 2016, online)

O mesmo se aplica às plataformas de redes sociais como "mediadoras", pois nenhuma destas instituições tem condições de determinar/investigar que tipo de conteúdo fica ou é retirado da internet e, mesmo que as tivessem, dar este tipo de acesso e poder não deveria ser nosso objetivo. Além do mais, isso abriria portas para perigosas práticas de censura que poderiam, inclusive, ser usadas contra nós mesmos, na eminência de estados conservadores, como temos experienciado. Sem contar que um afrouxamento ainda maior na proteção de dados pelas plataformas abre brechas para que cada vez mais nossos dados sejam vendidos como mercadorias para empresas, e administrados cada vez mais longe de nosso controle, desrespeitando leis e acordos arduamente conquistados, como a GDPR. Tais saídas geram também outras formas de violência, violência inclusive contra as próprias feministas, constantemente alvos de ações de denúncias por parte de machistas, que conseguem assim o bloqueio de suas páginas pelas plataformas e ocorrências correlatas.

Outra perigosa zona de tensão é a correlação entre o direito ao anonimato na internet e o direito à liberdade de expressão irrestrita. Por um lado, esta correlação parece adequada no que diz respeito aos direitos das mulheres de denunciarem e, para além disso, de produzirem conteúdo feminista, sem serem atacadas e perseguidas politicamente por isso. Por outro lado, é também na chave da "liberdade de expressão" que boa parte dos discursos de ódio no Brasil, dentro e fora da internet, tem operado sob a premissa de que falas e práticas desrespeitosas e/ou agressivas contra minorias seriam formas de liberdade de expressão. Portanto, é preciso ter muito cuidado ao defender o anonimato na internet como um direito fundamental e um meio de ajudar a garantir a defesa dos "direitos humanos" e direitos de grupos minorizados, pois, tal como a internet, o anonimato também não é apenas uma ferramenta de lutas libertárias.

É importante pontuar ainda que todas as tensões envoltas nas discussões a respeito desses conceitos e direitos dizem respeito a disputas políticas. Neste sentido, é preciso ter cuidado com três diferentes posicionamentos no que diz respeito à internet: um que afirma que ela é um paraíso democrático onde as hierarquias se desconstroem e as problemáticas sociais não se aplicam; outro, que ela é um risco constante e iminente a todos os grupos; outro, ainda, que a entende como neutra.[23] Entendemos que ela não seja nenhuma das três coisas de maneira isolada, mas talvez as duas primeiras juntas e concomitantes, em constante tensão e disputa, longe de qualquer pretensão de neutralidade, porque essa disputa também é política.

23 Afirmamos aqui esta não-neutralidade destas tecnologias por uma série de motivos. Em primeiro lugar, pois como vemos a partir de discussões já clássicas na Antropologia de teóricas como Donna Haraway, a neutralidade não é alcançável, nem nas construções dos conceitos e coisas, nem em seus usos e apropriações. Também através das teorias de Haraway, é possível afirmar que as tecnologias em si não são neutras, pois são construídas e construtoras por/de seres interseccionados e operam a partir disso.

[11-34] DOI: 10.5281/ZENODO.6727100
Nº 5 [enero-junio 2022] ISSN 2684-012X

CONSIDERAÇÕES FINAIS

Partindo, portanto, de todo este contexto multifacetado e complexo, composto por uma série de tensões ambíguas e práticas disputadas, seria quase irresponsável e reducionista tentar tratar conclusões fechadas a respeito do assunto. Portanto, nos limitamos a fazer algumas considerações do que considero que sejam caminhos possíveis em direção a usos da internet e do anonimato mais seguros, conscientes e engajados.

Primeiramente, acreditamos que há uma necessidade urgente de expandir o debate sobre internet, anonimato e segurança para dentro dos outros feminismos, que não apenas o ciberfeminismo, e para dentro de outros públicos, que não predominantemente brancos/jovens/classe média. Isto, pois de muito pouco adianta permanecermos em bolhas de discussão dentro dos ciberativismos, dos ciberfeminismos e, até mesmo, dentro da Academia, enquanto as empresas e Estados utilizam da falta de expansão destas discussões para atingir outras populações com políticas de vigilância e comércio de dados dessas pessoas.

> Sendo assim, ainda que o anonimato de fato esteja envolto em uma série de tensões ambíguas e paradoxais, é preciso aprofundarmos nas discussões de seus usos para possíveis resistências, tal como nas possibilidades de construção de redes anônimas responsáveis e politicamente posicionadas em favor de minorias políticas. (Carvalho, 2019a)

Desta forma, expandir as práticas de criptografia –e programação– para grupos outros que não aqueles hegemônicos que atualmente dominam o conhecimento dessa técnica e linguagem se mostra como possibilidade importante. Além disso, ampliar o debate de segurança de dados na concepção de formas outras de se fazer campanhas de engajamento em lutas pela proteção aos direitos de grupos minorizados se mostra também como ponto crucial na concepção de uma internet e uma sociedade mais inclusiva e menos vigiada.

Por fim, pensando que a internet é um espaço de constante disputa e tensão e o anonimato vêm sendo utilizado por grupos distintos cujos interesses reverberam na manutenção e/ou resistência às relações de poder e estruturas de controle, é preciso se apropriar dele de maneira que não seja utilizado para dar continuidade e novas caras às violações de nossos corpos e vivências. É importante também que, tal como destacam as ciberfeministas, estejamos atentos para as ferramentas e características únicas que a internet dispõe para a reinvenção das próprias ações feministas (para além de utilizá-la como potencial para disseminar conteúdos feministas): o alcance ampliado, a possibilidade de anonimização das identidades, a possibilidade de hackeamento de estruturas virtuais de órgãos de poder verticais, a existência de plataformas em que se possa denunciar e alertar outras mulheres (colaborando na prevenção de sua segurança), a ampliação da possibilidade de compartilhamento e agregação de pautas e grupos que não estejam fisicamente localizados no mesmo espaço, dentre muitas outras. É preciso reconhecer os riscos, fragilidades e problemas que tecnologias como a internet trazem, mas é preciso também (visto que estas mesmas tecnologias, na prática, só se expandem no mundo) reconhecer seus potenciais de enfrentamento às mesmas estruturas de poder que nos vigiam e punem através delas.

Por fim, tal como Adriana Silva Barbosa e outras colegas, acreditamos também que outra possível saída para este impasse a respeito das ambiguidades e riscos que a internet e o anonimato trazem para grupos marginalizados é

[11-34] DOI: 10.5281/ZENODO.6727100
Nº 5 [enero-junio 2022] ISSN 2684-012X

> o estabelecimento de campanhas educativas de conscientização dos internautas que contemplem, ao mesmo tempo, conhecimento sobre a internet, as implicações positivas e negativas de seu uso, aspectos referentes à privacidade, princípios éticos e bioéticos das relações humanas, dentre outros aspectos que contribuam para o uso mais consciente da internet. (Silva Barbora et. al., 2014: 120)

REFERÊNCIAS BIBLIOGRÁFICAS

Amaral, A. (2010). Etnografia e pesquisa em cibercultura: limites e insuficiências metodológicas. *Revista USP*, *1*(86), 122-135.

ARTIGO 19. (2015). *Criptografia e anonimato são essenciais para liberdade de expressão.* Recuperado de https://artigo19.org/blog/2015/06/01/criptografia-e-anonimato-sao-essenciais-para-liberdade-de-expressao/ (Visitado em: 20/01/2019)

Arvigo, M.; De Souza, G.; Ferro, A.; Sobral, M. (2018). *Dados à vista! O descobrimento da privacidade*. Recuperado de http://irisbh.com.br/dados-a-vista-o-descobrimento-da-privacidade/ (Visitado em: 08/01/2020).

BAGUEIROS, I. (2018). *Tor: resistir à distopia da vigilância sem fronteiras.* Recuperado de https://www.facebook.com/cryptorave/videos/2215187895375333/ (Visitado em: 20/01/2019).

Brandão, L. C. y Oliveira, D. T. (2018). *Privacidade e Proteção de Dados.* Apostila do Minicurso Fundamentos do Direito e Novas Tecnologias, Universidade Federal de Minas Gerais, Belo Horizonte.

Carvalho, F. V. (2019a). *Anonimato digital: riscos e resistências ciborgues de uma rede em disputa*. Recuperado de https://geict.wordpress.com/2019/12/09/anonimato-digital/. (Visitado em: 08/01/2021)

Carvalho, F. V. (2019b). *Riscos e resistências para mulheres na internet – Possibilidades práticas do ciberfeminismo na era digital*. Recuperado de http://irisbh.com.br/riscos-e-resistencias-para-mulheres-na-internet-possibilidades-praticas-do-ciberfeminismo-na-era-digital/. (Visitado em: 08/01/2021)

Carvalho, F. V. (2019c). *Encriptando denúncias, revelando opressões: A internet enquanto plataforma para denúncias de violência de gênero em tempos de feminismos ciborgues*. Monografia apresentada ao Curso de Antropologia, Universidade Federal de Minas Gerais, Belo Horizonte, 158p.

Cesarino, L. (2014). Antropologia multissituada e a questão da escala. reflexões com base no estudo da cooperação Sul-Sul brasileira. *Horizontes Antropológicos*, *1*(41), 19-50.

Clark, I. (s/f). *The Philosophy behind Freenet.* Recuperado de https://freenetproject.org/pages/about.html (Visitado em: 20/01/2019).

Castells, M. (1999). *A era da informação: economia, sociedade e cultura.* São Paulo: Paz e Terra.

[11-34] DOI: 10.5281/ZENODO.6727100
Nº 5 [enero-junio 2022] ISSN 2684-012X

Coding Rights (s/f). Recuperado de https://cpiciber.codingrights.org/anonimato/#onu-protecao-a-privacidade-a-criptografia-e-ao-anonimato (Visitado em: 20/01/2019)

Coding Rights (2016). *Internet e a voz das mulheres negras.* Recuperado de https://antivigilancia.org/pt/2016/09/entrevista-charo-nunes/ (Visitado em: 01/09/2018).

Coding Rights (2016). *Paradoxos da militância feminista online e offline*. Recuperado de https://antivigilancia.org/pt/2016/09/entrevista-lolaescreva/ (Visitado em: 01/09/2018)

Cohen, C. & Gobbetti, G. (2014). Bioética da vida cotidiana. *Ciência e cultura, 56*(4), 47-49.

Cryptorave (2014). *Tor: resistir à distopia da vigilância sem fronteiras.* Recuperado de https://www.facebook.com/cryptorave/videos/2215187895375333/ (Visitado em: 20/01/2019).

Cunha, T. (2016). *Brasil lidera ranking mundial de assassinatos de transexuais.* Recuperado de http://especiais.correiobraziliense.com.br/brasil-lidera-ranking-mundial-de-assassinatos-de-transexuais (Visitado em: 12/02/2019).

Deleuze, G. (1992). *Conversações.* São Paulo: Editora.

Do Carmo, P. R. & Gonçalves, P. V. (2018). *Inclusão Digital e Governança da Internet.* Apostila do Minicurso Fundamentos do Direito e Novas Tecnologias, Universidade Federal de Minas Gerais, Belo Horizonte.

Felizi, N & Varon, J. *Menstruapps – Como transformar sua menstruação em dinheiro (para os outros)?* Recuperado de https://chupadados.codingrights.org/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros/ (Visitado em: 05/04/2019).

FREENET (2002). *About - What is Freenet?* Recuperado de https://freenetproject.org/pages/about.html (Visitado em: 15/11/2021).

Freitas, A. (2016). *Não há democracia sem garantia de anonimato na internet.* Recuperado de https://antivigilancia.org/pt/2016/09/nao-ha-democracia-sem-anonimato/ (Visitado em: 01/09/2018).

Haraway, D. J. (2009[1985]). O manifesto ciborgue: Ciência, tecnologia e feminismo-socialista no final do século XX. En Tadeu, T., *Antropologia do ciborgue: as vertigens do pós-humano* (pp. 33-118). Belo Horizonte: Autêntica.

Horst, H. A. & Miller, D. (2013). *Digital Anthropology*. Oxfordshire: Taylor & Francis.

Hughes, E. (2007[1993]). *Manifesto Cypherpunk*. Recuperado de https://medium.com/medium-brasil/manifesto-de-um-cypherpunk-3c678c4898c5 (Visitado em: 15/01/2019).

[11-34] DOI: 10.5281/ZENODO.6727100
Nº 5 [enero-junio 2022] ISSN 2684-012X

Kalia, A. (2016). *A criptografia é uma questão de direitos humanos: sua privacidade e liberdade de expressão dependem dela*. Recuperado de http://lerosincopado.blogspot.com/2016/12/a-criptografia-e-uma-questao-de.html (Visitado em: 20/01/2019).

Leitão, D. K. & Gomes, L. G. (2018). Etnografia em ambientes digitais: perambulações, acompanhamentos e imersões. *Antropolítica Revista Contemporânea de Antropologia, 1*(42), 42-65.

Lewgoy, B. (2009). A invenção da (ciber) cultura. Virtualização, aura e práticas etnográficas pós-tradicionais no ciberespaço. *Civitas-Revista de Ciências Sociais*, 9(2), 185-196.

Loureiro, F. O. (2014). *Tópicos de Criptografia para o Ensino Médio.* Dissertação de Mestrado em Matemática, Universidade Estadual no Norte Fluminense Darcy Ribeiro, Rio de Janeiro. Recuperado de http://uenf.br/posgraduacao/matematica/wp-content/uploads/sites/14/2017/09/29082014Flavio-Ornellas-Loureiro.pdf (Visitado em: 28/01/2019).

Marcus, G. (1995). Ethnography in/of the world system: the emergence of multisited ethnography. *Annual Review of Anthropology*, *1*(24), 95-117.

May, T. C. (1994). *The Cyphernomicon: Cypherpunks FAQ and More. – cypherpunks.* Recuperado de https://cpunks.wordpress.com/cypherpunks-faq/ (Visitado em: 14/03/2019).

Nunes, C. (2016). *Internet e a voz das mulheres negras.* Recuperado de https://antivigilancia.org/pt/2016/09/entrevista-charo-nunes/ (Visitado em: 01/09/2018).

Plaza, W. R. (2015). *ONU propõe que a criptografia e o anonimato na internet seja um direito.* Recuperado de https://www.hardware.com.br/noticias/2015-05/onu-propoe-que-criptografia-anonimato-na-internet-seja-um-direito.html (Visitado em: 20/01/2019).

Polivanov, B. (2014). Etnografia virtual, netnografia ou apenas etnografia? Implicações dos conceitos. *Esferas, 1*(3), 61-71.

Ramos, J. (2015). Subjetivação e poder no ciberespaço. Da experimentação à convergência identitária na era das redes sociais. *Vivência: revista de antropologia, 1*(45), 57-75.

Rohden, F. & Monteiro, M. (2019). Para além da ciência e do anthropos: deslocamentos da antropologia da ciência e da tecnologia no Brasil. *Bib: revista brasileira de informação bibliográfica em ciências sociais. 1*(89), 1-33.

Rüdiger, F. (2011). Sherry Turkle, percurso e desafios da etnografia virtual. *Fronteiras-estudos midiáticos, 14*(2), 155-163.

Saraiva, R. et al. (2017). *Dois dedos de prosa sobre criptografia, direitos humanos e o caráter moral do trabalho criptográfico.* Recuperado de irisbh.com.br/pt/blog/dois-dedos-de-prosa-sobre-criptografia-direitos-humanos-e-o-carater-moral-do-trabalho-criptografico/ (Visitado em: 09/01/2019).

[11-34] DOI: 10.5281/ZENODO.6727100
Nº 5 [enero-junio 2022] ISSN 2684-012X

Schincariol, F. (2016). *Liberdade de expressão e anonimato na internet.* Recuperado de https://schincariolfernando.jusbrasil.com.br/artigos/251634616/liberdade-de-expressao-e-anonimato-na-internet. (Visitado em: 20/01/2019).

Silva, A. K. B. (2018). *A experiência de mulheres com o misoprostol no aborto ilegal.* Dissertação de Mestrado, Programa de Pós-Graduação em Medicamentos e Assistência Farmacêutica, Universidade Federal de Minas Gerais, Belo Horizonte.

Silva Barbosa, A. et al. (2014). Relações Humanas e Privacidade na Internet: implicações Bioéticas. *Revista de bioética y derecho*, *1*(30), 109-124.

Silveira, S. A. (2009). Redes cibernéticas e tecnologias do anonimato. *Comunicação & Sociedade, 30*(51), 113-134.

Tashiro, W. (2015). *Direito ao anonimato na internet.* Recuperado de https://williamtashiro.jusbrasil.com.br/artigos/221215593/direito-ao-anonimato-na-internet (Visitado em: 12/02/2019).

Teixeira, L. & Varon, J. (2016). *O caso da CPICiber no Brasil: discurso de ódio e outros crimes cibernéticos como porta de entrada para censura e vigilância.* Recuperado de https://antivigilancia.org/pt/2016/09/cpiciber-discurso-de-odio/ (Visitado em: 20/01/2019).

Ugarte, D. (2008). *O poder das redes.* Porto Alegre: EdiPUCRS.