Comunicação na internet e a violação do direito à privacidade: uma análise avaliativa das políticas e termos de uso na internet

COMMUNICATION ON THE INTERNET AND VIOLATION OF THE RIGHT TO PRIVACY: AN EVALUATIVE ANALYSIS OF POLICIES AND TERMS OF USE ON THE INTERNET

Magali do Nascimento Cunha

Pesquisadora e coordenadora do Grupo de Pesquisa Comunicação e Religião da Sociedade Brasileira de Estudos Interdisciplinares em Comunicação (INTERCOM). Doutora em Ciências da Comunicação pela Escola de Comunicação e Artes da Universidade de São Paulo.

E-mail: magali.ncunha@gmail.br

Alessandra Lourenço Simões

Professora dos cursos de Engenharia e Tecnologia da Informação na Universidade Metodista de São Paulo. e Especialista em Segurança da Informação.

E-mail: alessandra.simoes@metodista.br

Recebido em 14 de dezembro de 2017. Aprovado em 23 de abril de 2018.

Resumo

A comunicação na internet trouxe rapidez e acessibilidade, ultrapassando fronteiras geográficas, porém trouxe a possibilidade de monitoração e coleta de dados dos usuários. Orientado por revisão bibliográfica, este trabalho tem como objetivo abordar questões do direito à comunicação e à privacidade, através de análise avaliativa das políticas de privacidade dos dez maiores aplicativos de redes sociais on-line, no que diz respeito à coleta de dados pessoais e a forma como são utilizados, buscando trazer os aspectos comuns e as possíveis falhas na comunicação com os usuários.

Palavras-chave: Privacidade. Direito à comunicação. Vigilância.

Abstract

The communication on the Internet brought speed and accessibility, surpassing geographical boundaries, but also brought the possibility of monitoring and collecting data from users. Guided by a bibliographic review, this work aims to address issues of the right to communication and privacy through an evaluative analysis of the privacy policies of the ten largest online social networking applications, especially regarding the collection of personal data and the how they are used, seeking to draw the common aspects and possible failures in communication with the users.

Keywords: Privacy. Right to Communication. Surveillance.

Introdução

As redes sociais sempre desempenharam um papel importante nos processos comunicacionais dos seres humanos e ao longo do tempo foram ganhando cada vez mais força, principalmente com o surgimento da internet (SÁ MARTINO, 2015, p. 55). As redes sociais na internet são espaços virtuais onde fazemos contato e interagimos com pessoas do mundo inteiro sem sair de casa, através de textos, fotos, vídeos, links e outros (GUNELIUS, 2012, p. 127).

Ao mesmo tempo que são plataformas de produção e compartilhamento de conteúdo na internet e possibilitam ao cidadão grande avanço nas comunicações, em que um ambiente foi criado para sua livre expressão e até a organização de mobilizações coletivas, trouxeram também, em contrapartida, a possibilidade de monitoração e vigilância desses usuários. A partir do momento em que a internet é comercializada e a informação passa a ser um bem valioso, empresas e governos do mundo inteiro se interessam pelas possibilidades que essa nova tecnologia oferece, inclusive a de identificar seus usuários, seus gostos e costumes, rastreando-se, assim, os fluxos comunicacionais e interferindo na privacidade dos usuários e, por consequência, na área dos direitos humanos.

Assim como o direito à comunicação, representado pelo direito de liberdade de expressão, o direito à privacidade também é garantido por leis e declarações, como a Declaração Universal dos Direitos Humanos (DUDH), proclamada pela Organização das Nações Unidas (ONU) e a Constituição Federal Brasileira (CF/88). Em tempos de comunicação na internet, esses direitos também são estendidos ao espaço virtual, porém sua violação acontece diariamente, através da vigilância, coleta e monitoração dos dados de navegação ou daqueles publicados espontaneamente pelos usuários, por empresas ou órgãos governamentais, sob diversos pretextos e, muitas vezes, de forma automática. Segundo Paesani (2014, p. 34), o direito à privacidade encontra dificuldades de garantia, principalmente quando parte da própria pessoa a divulgação das suas informações. Porém, conforme Ishitani (2003, p. 1), muitas vezes, os usuários da internet não sabem da coleta dessas informações, nem para que elas são utilizadas, ou não compreenderam corretamente como isso ocorre. Ainda que as afirmações sobre coletas de dados estejam declaradas na política de privacidade ou no termo de uso, que foram aceitos a partir do momento em que um aplicativo foi instalado, a inscrição em uma rede social foi feita, ou ainda a compra em uma loja on-line está prestes a ser efetivada, aparecem sob expressões complicadas e de difícil entendimento.

Diante dos fatores citados, o principal objetivo deste trabalho é compreender as dimensões do direito à privacidade na internet e dos riscos envolvidos na exposição de dados

de usuários durante o processo comunicacional no mundo digital, tais como apresentados nas políticas de privacidade e/ou termos de uso de aplicativos de comunicação digital. A revisão bibliográfica em diversas fontes de pesquisa como livros, periódicos acadêmicos, documentários, dissertações e teses, das áreas de Comunicação Social, Direito e Segurança da Informação, possibilitou o estudo do direito à privacidade nas questões comunicacionais atuais. Através de análise avaliativa das políticas de privacidade e/ou termos de uso de aplicativos de comunicação na internet, buscou-se as características em comum entre elas e o que é comunicado ao usuário em relação aos dados informados, além da análise crítica dos riscos e ameaças à privacidade do usuário na utilização dos meios de internet.

Comunicação, internet e vigilância

A comunicação acompanha o ser humano em sua trajetória evolutiva desde o seu nascimento, primeiro através do choro, seguido pela fala, escrita, depois o surgimento dos primeiros grandes meios de comunicação de massa, como cinema, rádio e televisão, até os dias atuais através da internet, conforme Fedoce (2008, p. 10).

Mas, afinal, o que é a internet? Para a autora Paesani (2014, p. 12), a definição de internet não é clara nem completa, sendo do ponto de vista técnico e de forma simplista definida como uma "rede que liga elevado número de computadores em todo o planeta". Ainda segundo a autora, a grande diferença entre a rede de computadores e a rede telefônica é que cada computador, em sua capacidade de armazenamento, pode conter, possibilitar acessar e fornecer um número vasto de informações, sejam culturais, econômicas, acadêmicas, políticas, pessoais ou sociais, as quais não seria possível obter através do telefone, além de propiciar encontros, troca de opiniões, relacionamentos sociais, entre outros.

Outro ponto importante, que diferencia a internet dos demais meios e que vale ser ressaltado, é que a internet como meio de comunicação também anula a questão da distância física entre as pessoas, conforme cita Paesani (Id., p. 10), além de possibilitar a comunicação de forma instantânea, a todo momento e com várias pessoas ao mesmo tempo. Já para Castells (2013, p. 15), a rede pode ser tratada também como comunicação de massa, "porque processa mensagens de muitos para muitos, com o potencial de alcançar uma multiplicidade de receptores e de se conectar a um número infindável de redes que transmitem informações digitalizadas pela vizinhança ou pelo mundo".

A comunicação livre através das redes sociais on-line

A possibilidade de comunicação, interação e participação no mundo digital ganha um número maior de participantes com a chegada das chamadas redes sociais on-line.

As relações sociais em rede, conforme cita Sá Martino (2015, p. 55) "podem ser entendidas como um tipo de relação entre seres humanos pautada pela flexibilidade de sua estrutura e pela dinâmica entre seus participantes", e apesar de antiga, essa relação ganhou força com o avanço tecnológico e a possibilidade de conectar pessoas através da internet.

Por meio das redes sociais on-line interagimos com pessoas do mundo inteiro sem sair de casa, utilizando recursos de textos, fotos, vídeos, links e outros, conectados a outras pessoas que normalmente compartilham dos mesmos valores, interesses e costumes. Diversos sistemas e aplicativos dessas novas formas de redes sociais, como Facebook, WhatsApp, Youtube, entre outros, surgiram e, diariamente, conquistam cada vez mais usuários .

Com todas essas ferramentas de comunicação ao alcance de pessoas comuns, a rede mundial de computadores não só possibilita a interação social com objetivo de lazer, mas também passa a desempenhar papel importante na participação do cidadão em questões sociais e políticas (CASTELLS, 2003, p. 114). A internet deu voz ao cidadão comum em um meio de divulgação coletiva, como podemos observar nas manifestações ocorridas em 2013 no Brasil, e anteriormente em diversos pontos do mundo, além de protestos de forma anônima no mundo digital. Conforme cita Castells (2013, p. 11), o mundo estava tomado por "aflição econômica, cinismo político, vazio cultural e desesperança pessoal", e as pessoas, desconfiadas do que recebiam como informação dos meios de comunicação de massa, monopolizados, organizaram-se nas redes sociais da internet, em aplicativos nos quais podem expressar sua opinião, chamar a atenção de outros e divulgar o que estava acontecendo, utilizando os recursos disponíveis nessas ferramentas (textos, imagens e vídeos ao vivo). A internet e suas redes sociais on-line tiveram papel importante nessas manifestações, pois possibilitaram despertar o sentimento de indignação de forma coletiva, através da comunicação interativa e em tempo real.

A internet da vigilância

Ao mesmo tempo em que as redes sociais on-line e as plataformas de produção e compartilhamento de conteúdo na internet possibilitaram ao cidadão grande avanço nas comunicações, nas quais um ambiente foi criado para sua livre expressão e até a organização de mobilizações coletivas, veio também, em contrapartida, a possibilidade de monitoração e de vigilância desses usuários.

Fernanda Bruno (2013, p. 125) aborda essa questão quando afirma que as tecnologias que permitem a emissão, o acesso e o compartilhamento da informação, além da possibilidade de anonimato nas relações sociais, são as mesmas que possibilitam a vigilância e identificação de indivíduos no espaço digital. A questão da vigilância torna-se possível a partir do momento em que a internet é comercializada em escala global e a informação

passa a ser um bem valioso. Empresas e governos passam a se interessar pelas possibilidades que a rede mundial de computadores oferece, fazendo com que novos recursos sejam aplicados no desenvolvimento de diversas tecnologias que possibilitam a identificação individual de usuários, a vigilância e a investigação. A partir de interações no mundo digital, as mensagens trocadas pelos usuários são interceptadas, são coletadas informações dispostas em perfis e publicações nas redes sociais on-line, rastreando os fluxos comunicacionais e formando assim grandes bancos de dados (CASTELLS, 2003, p. 142).

O interesse pela monitoração e vigilância dos cidadãos ganha força com a possibilidade de o usuário da internet ser também um possível consumidor, pois assuntos como marca, produto e compra, hábitos, gostos e preferências, também passam a fazer parte do fluxo comunicacional do mundo digital, assim como os governos buscam monitorar seus principais inimigos e ameaças (QUEIROZ, 2002, p. 82).

Para compreendermos melhor, o termo vigilância, segundo o dicionário Michaelis (VIGILÂNCIA, 2017), significa "ato ou efeito de vigiar", "estado de quem vigia, de quem age com atenção e precaução para evitar riscos e perigos". Da mesma forma, verificamos o termo vigiar, que nos remete à "Estar atento a; observar atentamente", "Observar oculta ou secretamente; espreitar", ou ainda "Fazer a verificação de; controlar, fiscalizar" (VIGIAR, 2017).

A vigilância sobre o comportamento de indivíduos e populações inteiras foi objeto de estudo na filosofia com Michel Foucault e relacionada à dimensão do poder em suas múltiplas expressões, sua microfísica. O pensador dedicou-se a estudar as manifestações da vigilância hierárquica e de punições consequentes no período do Iluminismo (final do século 18) até meados do século 20, sendo a vigilância hierárquica.

Foucault (2004, p. 144) indica que o poder produz realidade e a vigilância hierárquica se dá desde o olhar sobre aqueles que são observados e "das pequenas técnicas das vigilâncias múltiplas e entrecruzadas, dos olhares que devem ver sem ser vistos".

Nesse sentido, por meio da vigilância, o poder disciplinar torna-se discreto, permitindo-lhe estar em toda parte e alerta, funcionando de forma permanente e em silêncio. "[O poder] em princípio não deixa nenhuma parte às escuras e controla continuamente os mesmos que estão encarregados de controlar; e absolutamente 'discreto'" (Ibid., p. 148).

Essas bases orientam a perspectiva que alude ao conceito apresentado por Fernanda Bruno (2013, p. 18), que estuda as questões de vigilância e tecnologia, as quais fazem sentido ao objeto de estudo deste trabalho: "uma atividade de vigilância pode ser definida como a observação sistemática e focalizada de indivíduos, populações ou informações relativas a eles, tendo em vista produzir conhecimento e intervir sobre os mesmos, de modo a conduzir suas condutas".

As práticas de vigilância se diversificam e contam com uma grande variedade de ferramentas tecnológicas e a combinação de várias delas para análise. Essas práticas não estão presentes somente nos grandes aplicativos de internet, mas também na nossa rotina nos grandes centros urbanos, em espaços públicos e privados, que aliados aos aplicativos de internet, monitoram a vida de seus usuários. A utilização dessas ferramentas e métodos de captura de dados nem sempre são de conhecimento dos usuários, eles são aceitos para que se possa ter acesso a todas as funcionalidades do site ou aplicativo o qual se deseja utilizar. Conforme Bruno (Ibid., p. 145), "Os métodos de monitoramento vão desde o rastreamento de cliques e a mensuração do tempo dedicado a cada página web até a captura automatizada do que teclamos quando visitamos um site, por exemplo". Se faz necessário ao usuário conhecer essas ferramentas e a maneira como coletam e monitoram seus dados, assim como as possíveis formas de configuração permitidas, inibindo ou diminuindo o acesso a dados os quais não se deseja que se tornem públicos, conhecidos ou divulgados, minimizando assim a monitoração e vigilância, mas não a impedindo totalmente.

A internet e principalmente as redes sociais on-line facilitaram muito os processos de vigilância e de coleta de dados, e de acordo com os relatórios do Departamento de Segurança Doméstica dos Estados Unidos, a rede social Facebook, substitui quase todos os outros programas de coleta de informações da Agência Central de Inteligência (CIA), desde que foi lançado em 2004 (TERMS…, 2013, tradução nossa). Um dos maiores programas de vigilância que o mundo já viu foi revelado em junho de 2013, sob o nome programa *PRISM*, de propriedade da Agência de Segurança Nacional dos Estados Unidos – National Security Agency (NSA). Conforme cita Bruno (2013, p. 10), esse programa "permite que a NSA tenha acesso direto a servidores de grandes empresas da internet, sendo capaz de monitorar comportamentos de seus usuários em escala global". O Governo do Estado de São Paulo também possui um sistema de vigilância de seus cidadãos. Através da Secretaria de Segurança Pública (SSA), o governo de São Paulo anunciou, no primeiro semestre de 2014, o uso de um programa para acessar as informações de usuários da internet, com ou sem as suas autorizações (SOUZA; COSTA, 2015, p. 120). O programa intitulado como *Domain Awareness System* (DAS) – Sistema de Domínio da Consciência –, mais conhecido como *Detecta*, segundo Souza e Costa (Ibid., p. 120), é um sistema de monitoramento criminal, o qual foi desenvolvido através da parceria com a empresa de software americana Microsoft e tem como objetivo realizar associações automáticas entre imagem e dados, os quais ainda estão em fase de implantação.

A questão do direito à comunicação e à privacidade na internet

Com o grande fluxo comunicacional e o compartilhamento de dados pessoais na internet surge a preocupação com direitos garantidos por leis e declarações universais, como por exemplo o direito à comunicação e à privacidade dos cidadãos. Esses privilégios nascem de certas circunstâncias as quais o ser humano passa durante sua jornada evolutiva e o acompanham também no modo de vida em sociedade ao longo de sua história (BOBBIO, 2004, p. 5) e são garantidos a todos os seres humanos desde seu nascimento, independente da cultura, religião, classe social e etnia (MIELKE; MOREIRA; PITA, 2014, p. 13). O reconhecimento dos direitos humanos está ligado diretamente à garantia da paz e da democracia (BOBBIO, 2004, p. 1).

Dentro da gama de direitos inerentes ao homem, se encontra o direito à liberdade de expressão e à comunicação, garantido desde os tempos da Grécia antiga, conforme Mielki, Moreira e Pita (2014, p. 21), de se expressar, transmitir ideias e pensamentos, em quaisquer que sejam os meios, e é resguardado até os dias atuais por constituições federais e declarações universais. Na sociedade atual, a internet e as redes sociais on-line desempenham um importante papel no exercício desse direito, pois dão voz ao cidadão e permitem a interação instantânea entre seus participantes, diferente de outros meios de comunicação em massa (GUARESCHI, 2013, p. 14).

O termo privacidade engloba tudo que está ligado à intimidade do indivíduo, sendo um conjunto de informações, o qual ele pode decidir manter sob sigilo ou comunicar, decidindo também a quem, quando, onde e em que condições (SILVA, 2005, p. 206).

A DUDH cita em seu artigo XII (ONU, 1948, p. 9): "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques".

Já a CF/88 trata da proteção à privacidade através do artigo 5º, incisos X e XII, que dizem, respectivamente:

> São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação.
>
> […] É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL, 1988).

Liliana Minardi Paesani, trata o direito à privacidade como "fundamento a defesa da personalidade humana contra injunções ou intromissões alheias", e salienta a

importância que esse direito vem ganhando "com a expansão das novas técnicas de comunicação, que colocam o homem numa exposição permanente" (PAESANI, 2014, p. 49). Outros autores, como Danilo Duarte de Queiroz (2002, p. 83), também abordam a importância do direito à privacidade tratando-o como o "poder e habilidade de controlar as informações verdadeiras sobre você, que os outros podem vir a saber", cabendo a decisão de comunicar essas informações, a quem, quando, e onde, exclusivamente ao indivíduo, ao qual essas informações pertencem.

Wives (2015, p. 472) cita a importância do direito à privacidade, que beneficia não somente o indivíduo, mas a sociedade como um tudo: "Ao proteger a privacidade de cada um a sociedade ganha como um todo, por garantir que os direitos sejam de fato utilizados, como o direito à liberdade de pensamento, liberdade de expressão, ao livre deslocamento". E segundo Guareschi (2013, p. 89), "não existe liberdade onde não houver a possibilidade de falar e ser ouvido", e que a democracia implica na participação, no direito de falar, expressar sua opinião e manifestar o pensamento.

Violação ao direito à privacidade na internet e suas possíveis consequências

O direito à privacidade, assim como outros direitos fundamentais das pessoas, como a comunicação, tem a capacidade de adaptação a novas realidades tecnológicas, sendo retraído ou expandido conforme o desenvolvimento e mudanças nos setores político, social e governamental, conforme citam Pilati e Olivo (2014, p. 289). Assim, direitos determinados em outros tempos tem sua validade independente da tecnologia a qual se está utilizando.

Fica claro, assim, que não há qualquer diferenciação entre o mundo real e o mundo digital, inclusive nas garantias de direitos. Porém, podemos observar nas últimas décadas que os "avanços da tecnologia não geram somente benefícios, mas também podem prejudicar as pessoas", invadindo as suas privacidades, seus lares e, inclusive, a confidencialidade de suas correspondências, através de novas formas de vigilância a partir do uso da internet (HAMELINK, 2005, p. 111). Paesani (2014, p. 52) aborda esse tema quando cita que "a inserção de mecanismos cada vez mais sofisticados de difusão de informações tem contribuído para um estreitamento crescente do circuito privado, na medida em que possibilita, até a longa distância, a penetração na intimidade da pessoa". Assim, também Castells (2003, p. 140) sugere a possibilidade de violação da privacidade do indivíduo a partir do uso das tecnologias de internet, que "torna possível relacionar indivíduos com processos específicos de comunicação em contextos institucionais específicos", e a partir de então fazer uso de "todas as formas tradicionais de controle político e organizacional".

O resultado da coleta de dados para uso em ações de marketing direcionado, por exemplo, pode ser observado por uma ótica positiva para o consumidor, pois este vai

receber anúncios e promoções mais próximos de seu interesse. Em contrapartida, devemos observar também que dados os quais não se queira que sejam visualizados, por sua particularidade, por serem íntimos, ou que possam gerar roubo e fraude no comércio eletrônico, como dados de cartão de crédito, também estão sendo monitorados, coletados e analisados.

Outro ponto, talvez negativo, sob a ótica do consumidor, é a precificação de um serviço a partir das ações de análise de perfil a partir dos dados coletados, como por exemplo:

> Adquirir dados sobre o perfil biogenético de uma pessoa, bem como dados de consumo, pode ser muito valioso para uma empresa de seguros, entre outras. A combinação de informações sobre pressão alta e compra de bebidas alcoólicas, por exemplo, ajuda a seguradora a definir o nível de risco e também o preço que o cliente deverá pagar por sua apólice. (HAMELINK, 2005, p. 136)

Os aspectos negativos da publicação de "certos hábitos individuais, aparentemente inocentes" e as consequências da sua monitoração dizem respeito a gostos particulares, por exemplo, por doces, que funcionam como "indicadores de tendências que podem ser buscadas ou totalmente rejeitadas pelas empresas" (QUEIROZ, 2002, p. 87).

Ainda na linha de precificação de produtos, Fernanda Bruno (2013, p. 165) cita o caso de uma empresa que presta serviços de consultoria a outras empresas que comercializam seguros de vida. No exemplo, a autora aborda a comercialização de dossiês de clientes ou possíveis clientes, a partir da coleta e análise de dados da internet, onde é possível visualizar os riscos-saúde de cada um e assim categorizar o "bom e o mau cliente".

Conforme Ishitani (2003, p. 12), outro problema observado é a possível tomada de decisão a partir da análise de informações que leva a conclusões incorretas, como por exemplo "alguém pode fazer uma pesquisa sobre o tema Aids e, posteriormente, ter um emprego ou um plano de seguro de vida ou saúde negado", pois a empresa pode concluir que o candidato possa estar contaminado com o vírus.

A vigilância e monitoração também podem interferir na vida de quem deseja fazer uma viagem internacional, conforme exemplo mostrado no documentário *Terms and Conditions May Apply* (TERMS…, 2013). O usuário irlandês de uma rede social escreveu a seguinte frase em seu perfil antes de embarcar "você está livre esta semana para um encontro antes de eu sair e destruir a América?". Quando chegou ao seu destino e passou pelo controle de passaporte, policiais o levaram até uma sala de espera, onde teve sua mala revistada e foi interrogado por cinco horas e questionado sobre sua frase na rede social. Mesmo sua viagem tendo objetivo apenas turístico, a frase postada na rede social não foi interpretada como o turista explicou (farrear, embebedar), e sim como uma ameaça

terrorista, o que resultou na negação de sua entrada nos Estados Unidos, o que provavelmente pode impactar suas viagens para outros destinos internacionais.

O cenário político também pode sofrer consequências a partir da monitoração das redes sociais on-line e da coleta de dados da internet, a partir de propagandas políticas direcionadas:

> No que diz respeito à propaganda política, é possível dizer que ela está cada vez mais segmentarizada em função dos perfis dos eleitores, sendo produzida em função de suas afinidades e preconceitos. Estudos demonstram, por exemplo, que eleitores podem ficar mais sugestionados a votar em determinados candidatos que tenham características faciais semelhantes com as suas próprias. De acordo com os experimentos realizados, a combinação sutil e, praticamente imperceptível, de fotos dos eleitores com fotos dos candidatos (em misturas geradas por computadores) poderia impactar a sua escolha política, especialmente em relação a candidatos desconhecidos. (ANTONIALLI; CRUZ, 2017, p. 11)

Outra importante análise do autor Wives (2015, p. 469), sobre as consequências da monitoração na internet, aborda a questão do exercício da democracia através de outros direitos, pois o Estado democrático garante, além do direito à privacidade, "a liberdade de pensamento e a liberdade de circulação das ideias", como já citado neste trabalho. A violação à privacidade pode ameaçar esses outros direitos, pois inibem e em alguns casos até impedem que ideias contrárias ou divergentes ao governo atual sejam discutidas livremente, cujas consequências podem aniquilar a democracia (Ibid.).

O documentário *Terms and Conditions May Apply* (TERMS…, 2013) também mostra as consequências negativas da monitoração no exercício democrático de manifestação. Cita o exemplo de um professor de antropologia que comandava um grupo de teatro de rua que havia se organizado em redes sociais on-line para realizar uma manifestação. Aproximadamente 50 pessoas que não cometeram nenhum crime foram presas 25 horas antes do casamento real britânico em 2011, apenas porque se organizavam em redes sociais on-line para realizar uma manifestação pacífica.

Em se tratando de consequências globais, Wives aborda o resultado negativo da monitoração realizada por Estados Unidos e Reino Unido em países não democráticos como Irã e Rússia, além da questão do acesso às inovações tecnológicas em países com poucos recursos como o Brasil:

> Os efeitos podem ser ainda maiores; o Irã planeja criar uma internet estatal e se desconectar do restante da internet; a Rússia planeja obrigar a todos os serviços de internet que tenham dados de russos a terem servidores na Rússia, com o pretexto de assim garantir a segurança de seus cidadãos. […] Essas possibilidades são assustadoras, pois reduzem como um todo a

> capacidade da internet de conectar diferentes pessoas ao redor do planeta de maneira igualitária; reduzem também a competitividade ao dividir mercados e obrigar empresas a investir em serviços de hospedagem e servidores caros e ruins em territórios com poucas garantias democráticas. (WIVES, 2015, p. 473)

Já Fernanda Bruno (2013, p. 45) cita a monitoração e vigilância para todos e não mais para suspeitos de crimes, fornecendo provas sem que o crime ocorra, e o perigo de se classificar as pessoas a partir de sua navegação na internet. A autora cita como exemplo a condenação antecipada no caso de uma jovem de 16 anos, filha de imigrantes muçulmanos, residentes no Estados Unidos, que foram convidados a se retirar do país, pois seu perfil de navegação na internet foi classificado como "menina-bomba potencial", por "frequentar o chat de um clérigo islâmico em Londres".

Com isso, temos o contrário da presunção de inocência, apresentada na Declaração Universal de Direitos do Homem, no seu artigo XI, e na CF/88, em seu artigo 5º, inciso LVII: "ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória" (BRASIL, 1988). Somos todos culpados até que se prove contrário!

A política de privacidade como documento legal de violação

A coleta e monitoração de perfis, públicos ou não, e de dados que circulam na internet acontecem sob o resguardo jurídico, ou aparato legal, de que o usuário está ciente do que ocorre com seus dados a partir do aceite das políticas de privacidade e termos de uso, disponibilizados no momento em que se instala o aplicativo ou inicia o uso destes com a criação de um perfil. Muitas vezes não lida, ou lida de forma incompleta, essas políticas são extensas, conforme afirma o diretor e produtor Cullen Hoback (TERMS…, 2013), e se fôssemos ler todas as políticas com as quais concordamos dos aplicativos instalados, levaríamos aproximadamente 180 horas do nosso ano.

Para constatar a afirmação de que muitos usuários não leem as políticas, em 2009 uma empresa britânica colocou algo diferente no seu termo: "Ao concordar com os termos do *website*, você concorda em nos dar uma opção não transferível de reivindicar, agora e para sempre, sua alma imortal" (TERMS…, 2013, tradução nossa). O contrato só vigorou por um dia, mas a empresa "coletou as vidas" de 7 mil usuários. Claro que isto foi uma brincadeira, porém nos leva à reflexão: e se houvesse termos com consequências mais sérias? Fazendo a leitura ou não, o usuário da internet realiza, a partir do aceite, uma troca dos seus "dados pelo privilégio de acesso a *websites*", conforme Castells (2003, p. 143). A maioria das pessoas abre mão de seus direitos à privacidade para ter condições de usar a internet.

Para Danilo Duarte de Queiroz (2002, p. 92), esses documentos podem ser considerados como "contratos de prestação de serviço, contratos estes de adesão", que por consequência estão sujeitos ao direito civil e ao Código de Defesa do Consumidor no Brasil, por exemplo. Esses documentos são elaborados pelas empresas proprietárias de aplicativos de redes sociais ou comercio eletrônico, em que a grande maioria procura declarar aos seus usuários "o modo como realiza a coleta de dados pessoais, o tratamento que é dispensado a tais dados, a possibilidade de compartilhamento com terceiros" (QUEIROZ, 2002, p. 89), entre outros. Também faz parte desses documentos a declaração dos serviços prestados e que para "fazer uso daquele produto ou serviço também se está autorizando o administrador do site a fazer uso de suas informações pessoais da forma como foi disposto na política de privacidade", mesmo que esse condicionamento não esteja tão claro (QUEIROZ, 2002, p. 91). Mesmo sendo tratados como documentos formais e com valor jurídico, vale lembrar que não é possível garantir que os sites estão agindo de acordo com a política de privacidade divulgada e aceita por seus usuários (ISHITANI, 2003, p. 40). O diretor e produtor Cullen Hoback (TERMS…, 2013) aborda em seu documentário, *Terms and Conditions May Apply*, o conteúdo dessas políticas e suas consequências, sendo estas baseadas em histórias reais, criticando o possível desconhecimento do conteúdo das políticas e deixando no ar a seguinte questão: concordamos com termos muito longos. Mas concordamos exatamente com o que?

Análise das políticas de privacidade

Apresentamos aqui uma análise avaliativa das políticas de privacidade dos dez aplicativos mais utilizados por usuários da internet por meio da aplicação de procedimento metodológico apresentado a seguir.

Para compor a amostra com regra de representatividade, foram selecionados os aplicativos Facebook, Whatsapp, Youtube, Instagram, Twitter, Skype, Linkedin, Messenger, Snapchat e Pinterest. A seleção foi baseada em duas pesquisas, sendo a primeira, a *Pesquisa Brasileira de Mídia* (BRASIL, 2015, p. 62), única até o momento que apresenta dados sobre as redes sociais on-line mais utilizadas no Brasil. A segunda pesquisa utilizada é a *Digital in 2017 Global Overview* (KEMP, 2017), publicada em janeiro de 2017, que apresenta as plataformas de redes sociais on-line com maior número de usuários ativos. A partir da primeira pesquisa, selecionamos as redes sociais Facebook, Whatsapp, Youtube, Instagram, Twitter, Skype e Linkedin, as quais também aparecem na lista da segunda pesquisa, mais recente. Para compor as dez políticas, incluímos as redes sociais on-line que aparecem na segunda pesquisa e que são utilizadas mundialmente: Messenger, Snapchat e Pinterest. Foram ignorados aplicativos de blogs que aparecem na

segunda pesquisa, além de aplicativos de uso restrito a alguns países, por entendermos que não representam expressivamente o uso mundial ou específico dos brasileiros.

A análise foi realizada comparando o conteúdo das políticas, validando questões formuladas com base nos tópicos contidos na política de dados do Facebook, o aplicativo citado em primeiro lugar na lista dos dez maiores em número de usuários. Foram utilizados também como fonte de inspiração para a elaboração dos critérios, os tópicos abordados no documentário *Terms and Conditions May Apply*, do diretor e produtor Cullen Hoback, do ano de 2013, cujo foco é a questão da privacidade e as políticas e termos de acordo de uso de serviços na internet. Desta maneira, foi possível correlacionar a comunicação no mundo virtual com a questão da violação à privacidade, além de verificar a maneira como as empresas de serviços na internet comunicam seus usuários a respeito da forma como tratam seus dados, que são disponibilizados nesse ambiente a todo instante.

Como resultado temos o quadro a seguir, o qual resume de forma ilustrativa a análise das políticas de privacidade dos aplicativos estudados, podemos observar que todas se comportam de maneira semelhante.

Quadro 1. Resumo da análise

Questões	Facebook	Whatsapp	Youtube	Instagram	Twitter	Skype	Linkedin	Messenger	Snapchat	Pinterest
Informações que são coletadas								Direcionada às políticas do Facebook		
Destino das informações coletadas										
Compartilhamento das informações com terceiros										
Informações compartilhadas com o governo										
Garantias de não divulgação ou acesso não autorizado às informações coletadas										
Tempo de retenção das informações										
Notificação ao usuário quando há alteração da política										
Data da última atualização										
Menção ao direito à privacidade										
Quais ações podem ser realizadas remotamente										

Fonte: Elaboração das autoras.

Legenda	
	Há a informação e ela é clara, não deixa dúvidas
	Não há informação a respeito
	Há a informação, mas ela não é clara e deixa dúvidas

Em todas as políticas, as informações coletadas são apresentadas, assim como a menção ao compartilhamento com terceiros e com o governo, além da data da última atualização.

Quanto ao direito à privacidade, nenhuma das políticas analisadas faz menção clara a respeito, o que pode aparentar falta de interesse em preservar esse direito.

Outro item não abordado, e de extrema importância, é a possibilidade ao acesso remoto aos dados do usuário. Sua não mensuração, pode deixar dúvidas quanto à existência da possibilidade de acesso ou não e, se é acessado, quem acessa e quais controles de segurança existem. Caso essas informações sejam acessadas remotamente, outras pessoas podem visualizar as informações dos usuários sem sua autorização, podendo, inclusive, ser interceptadas se a conexão remota não tiver padrões mínimos de segurança, como por exemplo o uso de criptografia.

Quanto à notificação ao usuário em caso de alteração na política de privacidade, todas se comportam da mesma maneira, informando que a data de atualização será alterada e que alterações significativas serão comunicadas, porém não esclarecem quais critérios serão utilizados para determinar o que será considerado significativo ou não. Algumas também não esclarecem a maneira como seus usuários serão comunicados, para esse último caso.

O que fica claro é que se o usuário não tiver o hábito de ler de tempos em tempos a política de privacidade do aplicativo em uso, não saberá realmente se houve ou não alteração em seu conteúdo, sendo a continuidade do uso considerada concordância com os termos. No caso do Facebook, Snapchat e Pinterest, não é apresentada a possibilidade de acesso a versões anteriores das políticas, negando-se o acesso ao conteúdo que possivelmente foi atualizado, inserido ou excluído aos seus usuários. Já no Instagram e Twitter, as versões anteriores são apresentadas em inglês.

Com relação ao tempo de retenção, o aplicativo Twitter deixa claro suas condições e o Youtube não apresenta. Os demais aplicativos possuem parágrafos contraditórios, nos quais ora afirmam que excluem quando a conta é desativada ou quando os dados, como fotos, são apagados pelo usuário; ora afirmam que podem reter informações dos usuários por tempo indeterminado. De qualquer forma, não especificam por quanto tempo essas informações serão armazenadas.

No que diz respeito às garantias de não divulgação ou acesso não autorizado às informações coletadas, o aplicativo Youtube apresenta termos claros, enquanto os demais, ou não apresentam nenhuma informação a respeito ou, se apresentam, são imprecisos nos termos utilizados para abordar a questão. Ou seja, não há garantias explícitas de que as informações dos usuários não serão divulgadas ou que existe algum controle de segurança que previna o acesso não autorizado a essas informações.

O destino das informações coletadas não é apresentado pelo aplicativo Facebook, enquanto que nos demais aplicativos, as informações são vagas, sem precisar onde exatamente as informações estão (servidores e localização física destes), pois citam que podem estar em qualquer país onde a empresa tenha sede ou preste serviços.

Em relação ao compartilhamento das informações com órgãos governamentais ou judiciais, a maioria informa que pode compartilhar as informações dos usuários mediante apenas a uma solicitação, acreditando no princípio da boa-fé do solicitante. Esse parágrafo vai de encontro ao direito à privacidade universal, que alega que a quebra de sigilo com o fornecimento de dados e informações pessoais pode ocorrer somente mediante mandado judicial.

Considerações finais

Podemos concluir com este trabalho que a utilização de ferramentas e métodos de captura de dados nem sempre são de conhecimento dos usuários, assim como suas possíveis consequências negativas, como a violação do direito à privacidade, ocorridas a partir da monitoração e vigilância. Como já citado, as políticas e termos de uso dos aplicativos, utilizados como meio de comunicação com os usuários, muitas vezes, não são compreendidos ou lidos na íntegra, por se fazerem confusos e contraditórios. Faz-se necessário ao usuário conhecer essas ferramentas e a maneira como coletam e monitoram seus dados, assim como as possíveis formas de configuração permitidas, inibindo ou diminuindo o acesso a dados os quais não desejam que se tornem públicos, conhecidos ou divulgados, minimizando assim a monitoração e vigilância, mas não a impedindo totalmente.

Os aplicativos são usados, muitas vezes, como o principal meio de comunicação nos dias atuais. Os usuários continuam a fazer uso de aplicativos de rede social, reféns da vida digital, mesmo que não entendam os termos expostos nas políticas e não tenham ciência da violação a direitos, como o da privacidade, que acontece diariamente, bem como aos riscos inerentes a essa violação. Dada a importância do assunto, para os próximos trabalhos, torna-se necessário o desenvolvimento de formas para que a comunicação com os usuários seja mais rápida, clara e precisa, garantindo assim uma conscientização maior quanto às consequências e riscos aos quais estão submetidos ao fazerem uso de tais meios na internet. Além disso, que sejam preservadas as garantias de não violação a direitos estabelecidos pelo Estado democrático, como a privacidade de seus cidadãos, usuários do meio digital, e a liberdade de comunicação, expressão e manifestação, para que a ordem e a paz sejam mantidas.

Referências

ANTONIALLI, Dennys; CRUZ, Francisco Brito. *Privacidade e internet:* desafios para a democracia brasileira. Rio de Janeiro: Centro Edelstein de Pesquisas Sociais, 2017. São Paulo: Fundação Fernando Henrique Cardoso, 2017. 61 p.

BOBBIO, N. *A era dos direitos*. 10ª ed. Rio de Janeiro: Nova Editora, 2004.

BRASIL. Constituição da República Federativa do Brasil, de 5 de outubro de 1988. *Diário Oficial da União*, Poder Legislativo, Brasília, DF, 5 out. 1988. Seção 1, p. 1 Disponível em: <https://bit.ly/1dFiRrW> Acesso em: 21 nov. 2016.

_____. Presidência da República. Secretaria de Comunicação Social. *Pesquisa brasileira de mídia 2015*: hábitos de consumo de mídia pela população brasileira. Brasília, DF: Secom, 2014. p. 47-64. Disponível em: <https://bit.ly/1FAvjZC>. Acesso em: 16 maio 2016.

BRUNO, F. *Máquinas de ver, modos de ser*: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013. 190p.

CASTELLS, M. *A galáxia da internet*: reflexões sobre a internet, os negócios e a sociedade. Tradução Maria Luiza X. de A. Borges. Rio de Janeiro: Paz e Terra, 2003. 243p.

_____. *Redes de indignação e esperança*: movimentos sociais na era da internet. Tradução Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013. 271p.

FEDOCE, R. S. *Comunicação empresarial e novas tecnologias*: realidade e perspectivas. 2008. 82 f. Monografia (Bacharelado em Comunicação Social) – Universidade Federal de Juiz de Fora, Juiz de Fora, 2008. Disponível em: <https://bit.ly/2rI6JDg>. Acesso em: 20 out. 2016.

FOUCAULT, M. *Vigiar e punir*: nascimento da prisão. 14. ed. Petrópolis: Vozes, 2004.

GUARESCHI, P. A. *O direito humano a comunicação*: pela democratização da mídia. Petrópolis: Vozes, 2013. 203p.

GUNELIUS, S. *Marketing nas mídias sociais em 30 minutos*: manual prático para divulgar seus negócios pela internet de modo rápido e gratuito. 1. ed. São Paulo: Cultrix, 2012. 312 p.

HAMELINK, C. J. Direitos humanos para a sociedade da informação. In: MELO, J. M.; SATHLER, L. (Edits.). *Direitos à comunicação na sociedade da informação*. São Bernardo do Campo: Editora Metodista, 2005. p.103-137.

ISHITANI, L. *Uma Arquitetura para Controle de Privacidade na Web*. 2003. 92 f. Tese (Doutorado em Ciências da Computação) – Universidade Federal de Minas Gerais, Belo Horizonte, 2003. Disponível em: <https://bit.ly/2KntKTe>. Acesso em: 24 nov. 2016.

KEMP, S. Digital in 2017 Global Overview. *We Are Social*, New York, 24 jan. 2017. Disponível em: <https://bit.ly/2rvcmGk>. Acesso em: 20 jun. 2017.

MIELKE, A. C.; MOREIRA, D.; PITA, M. *Oficinas formativas*: liberdade de expressão e direito à comunicação. São Paulo: Intervozes, 2014. Disponível em: <https://bit.ly/2KY4nbH>. Acesso em: 8 ago. 2017.

ONU – ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Declaração Universal dos Direitos Humanos*. Assembleia Geral das Nações Unidas, 1948. Disponível em: <https://bit.ly/1CVqinH>. Acesso em: 21 nov. 2016.

PAESANI, L. M. *Direito e internet*: liberdade de informação, privacidade e responsabilidade civil. 7ed. São Paulo: Atlas, 2014. 130p.

PILATI, J. I.; OLIVO, M. V. C. Um novo olhar sobre o direito à privacidade: caso Snowden e pós-modernidade jurídica. *Sequência*, Florianópolis, n. 69, p. 281-300, dez. 2014. Disponível em: <https://bit.ly/2wH9PMV >. Acesso em: 21 fev. 2017.

QUEIROZ, Danilo Duarte de. Privacidade na internet. In: REINALDO FILHO D. (Org.). *Direito da informática:* temas polêmicos. São Paulo: Edipro, 2002. p. 81-96.

SÁ MARTINO, L. M. *Teoria das mídias digitais*: linguagens, ambientes e redes. 2ed. Petrópolis: Vozes, 2015. 291p.

SILVA, J. A. *Curso de direito constitucional positivo*. São Paulo: Malheiros, 2005. 925p.

SOUZA, S. H. C. L.; COSTA, E. G. *Vigiar para punir*: as mídias digitais como ferramenta para prevenir e conter ações criminosas. In: SIMPÓSIO INTERNACIONAL LAVITS, 3., 2015, Rio de Janeiro. *Anais eletrônicos*… Rio de Janeiro: LAVITS, 2015. p.118-131. Disponível em: < http://medialabufrj.net/download/lavits2015-anais/2/4.Resumo57.pdf>. Acesso em: 23 fev. 2017.

TERMS and conditions may apply. Direção: Cullen Hoback. Produção: Cullen Hoback; Nitin Khanna; John Ramos. Intérpretes: Max Schrems; Moby; Mark Zuckerberg e outros. Roteiro: Cullen Hoback. Los Angeles: Hyrax Films; Topiary Productions, 2013. (80 min), son., color.

VIGIAR. In: MICHAELIS Dicionário Brasileiro da Língua Portuguesa. São Paulo: Melhoramentos, 2017. Disponível em: <https://bit.ly/2Ip2s24>. Acesso em: 20 fev. 2017.

VIGILÂNCIA. In: MICHAELIS Dicionário Brasileiro da Língua Portuguesa. São Paulo: Melhoramentos, 2017. Disponível em: <https://bit.ly/2k0nPYQ>. Acesso em: 20 fev. 2017.

WIVES, W. W. *Vigilância e monitoramento*: efeitos micro e macro. In: SIMPÓSIO INTERNACIONAL LAVITS, 3., 2015, Rio de Janeiro. *Anais eletrônicos*… Rio de Janeiro: LAVITS, 2015. p.467-476. Disponível em: <https://bit.ly/2jXGK6H>. Acesso em: 23 ago. 2017.