

Considerações sobre a privacidade na internet

Considerations about privacy on the internet

Patrícia Maurício Carvalho¹

Resumo:

Este artigo retrata o início de uma pesquisa sobre a invasão de privacidade via internet praticada contra usuários por outros usuários, por empresas de internet e até por governos, e ainda sobre os crescentes casos de difamação e calúnia através de redes sociais e aplicativos. O objetivo da pesquisa é fazer um mapeamento da legislação existente e das disputas por leis e regras relativas a este tema, além de observar repercussões desta realidade na grande imprensa. Para isso, acompanhei casos de invasão de privacidade, injúria e difamação ao longo de 2014 no jornal O Globo e, com menor regularidade, em outros veículos; busquei sentenças judiciais sobre o tema; analisei leis e acompanhei embates sobre projetos de lei. Concluo que novos meios tecnológicos exigem novas regulações para que o direito do cidadão possa ser protegido.

Palavras-chave:

Internet; Privacidade; Regulação.

Abstract:

This article portrays the beginning of a research on the invasion of privacy committed against internet users by other users, internet companies and even by governments; and about the increasing cases of libel and slander through social networks and applications. The purpose of the research is to map the existing legislation and disputes over laws and rules relating to this topic. This paper also notes some consequences of this fact in the press. For this, I followed cases of invasion of privacy, libel and defamation over 2014 in the newspaper O Globo and less regularly in other media outlets, sought court rulings on the subject, begun to analyze laws and followed clashes on bills. The conclusion, still preliminary, is that new technology means new regulations so that the citizen's rights be protected.

Keywords:

Internet; Privacy; Regulation.

¹ Mestre e doutora pela Universidade Federal do Rio de Janeiro, docente do departamento de Comunicação da PUC-Rio. E-mail: patriciamauricio@puc-rio.br

1 Introdução

Invasão de privacidade, calúnia e difamação em escala nacional ou mesmo mundial não envolvem mais apenas celebridades. Com a internet, pessoas anônimas também podem ser vítimas, com sérios prejuízos a sua reputação. Aplicativos como o Secret e o Lulu² e comentários na rede social Facebook e no aplicativo WhatsApp são alguns dos principais instrumentos para este tipo de ação. Por isso, a criação e o cumprimento das leis que coíbem este tipo de crime estão na ordem do dia, assim como a palavra privacidade. Este artigo retrata o início de uma pesquisa que busca levantar algumas questões relativas a este fenômeno e fazer um mapeamento da legislação brasileira e das disputas a respeito de privacidade e crimes contra a honra na internet.

Para pesquisar os casos, acompanhei o jornal *O Globo* de janeiro a dezembro de 2014 e, ao escrever este artigo, busquei novamente na versão do jornal na internet os casos noticiados no período. Além disso, de forma mais esporádica, busquei notícias sobre o tema na versão *online* de outros veículos, como a *Folha de S. Paulo*.

A internet chegou ao Brasil em 1991 para servir à comunidade acadêmica, com a instalação da Rede Nacional de Pesquisa em 11 capitais, e veio se disseminando e crescendo em importância na vida dos usuários/cidadãos. Hoje, o acesso por aparelhos celulares e outros dispositivos móveis é cada vez maior. Os internautas brasileiros são agora 51% da população, sendo que 31% dos brasileiros têm celular com internet³ (percentual que só cresce). Esta mobilidade facilita enormemente que os usuários entrem na rede a qualquer momento, curtindo *posts* em redes sociais, comentando e compartilhando o que for de seu interesse. Em meio a essas pessoas com acesso facilitado à rede estão aquelas classificadas por usuários como *haters*, que espalham seu ódio em postagens nas redes sociais, atacando outras pessoas, como veremos através de exemplos a

² Aplicativo que permitia aos usuários compartilhar com os demais opiniões íntimas sobre pessoas com que haviam se relacionado anteriormente, com o objetivo de ajudar a quem estivesse interessado em se relacionar com essas pessoas a decidir se valia a pena.

³ Pesquisa TIC Domicílios, do Cetic.br, órgão ligado ao Comitê Gestor de Internet do Brasil, com dados coletados entre setembro de 2013 e fevereiro de 2014. Informação disponível em: <<http://cetic.br/usuarios/tic/2013/>>. Acesso em: 27/06/2014.

seguir. Pelo alcance da internet e a reprodução que se faz das postagens, o dano causado em geral é bem maior do que o da antiga fofoca boca a boca.

A base para esta pesquisa está em autores que estudaram e/ou estudam a realidade da comunicação brasileira a partir do ponto de vista da economia política da comunicação, e especialmente analisando a construção de leis e os debates de propostas e projetos de leis que se propunham a lidar com esta realidade. Os conflitos entre os grupos de interesse nesse processo são particularmente interessantes para a minha pesquisa. Nesse sentido, Bolaño e Brittos mostram, em seus livros e artigos, que as mudanças no campo da comunicação estão dentro de um contexto.

A economia política da comunicação se interessa pelo estudo da totalidade das relações sociais que formam os campos econômico, político, social e cultural, objetivando compreender a mudança social e a transformação histórica e como ela repercute e se imbrica com o mundo da comunicação em todos os sentidos. (BOLAÑO; BRITTOS, 2007, p. 49).

Ainda do ponto de vista da economia política da comunicação, Dantas (2014) classifica como “convergência dos meios” o processo econômico, político e cultural que está fazendo convergir para um mesmo regime de negócios e de práticas sociais o conjunto da cadeia produtiva da indústria cultural, apoiada em meios eletrônicos de comunicação. De acordo com o autor, as reformas políticas e econômicas neoliberais realizadas no fim do século XX colocaram as comunicações como serviços privados, orientados para o mercado, mudando a orientação anterior de entender as comunicações como um serviço público. O mesmo teria acontecido nos EUA e Europa. Segundo ele, corporações midiáticas globalizadas, a maioria sediada nos EUA, estão presentes em todos os elos da cadeia produtiva: produção, programação, transmissão e distribuição.

No Brasil, as barreiras legais têm servido para os conglomerados nacionais de radiodifusão aberta se defenderem da entrada no mercado audiovisual dos operadores de telecomunicações. Em meio a essas contradições, o Estado é chamado a intervir, seja para desmontar legislações ultrapassadas, seja para assegurar os direitos dos consumidores frente a corporações quase monopolistas, os direitos dos cidadãos por serviços públicos essenciais, os empregos, o desenvolvimento tecnológico-industrial etc. Mas é verdade que, hoje em dia, nos principais países, essa intervenção vem se dando no

sentido de atender principalmente às exigências do mercado. (DANTAS, 2014, p. 38).

Dantas afirma que vivemos hoje uma nova etapa do capitalismo internacional, o “capitalismo mediático-financeiro”, no qual as corporações midiáticas são controladas ou contam com importantes participações de grupos financeiros e fundos de investimentos – incluindo participações em diversas corporações supostamente concorrentes. É sobre esse pano de fundo de novas empresas que surgem com base na internet, especialmente de redes sociais diversas, com atuação mundial e inicialmente sem regulação, temas caros à economia política da comunicação, que as reações dos usuários de redes sociais e aplicativos, dos legisladores e da Justiça se dão.

Veremos mais adiante reflexos desse contexto, por exemplo, na disputa entre a Justiça e o Facebook para identificar difamadores. Além disso, venho acompanhando o trabalho de Ronaldo Lemos (2012) sobre direito e internet e, pontualmente, outros autores que tratam da questão da internet, como alguns citados neste artigo.

2 Aplicativos e redes sociais tornam-se instrumento de *cyberbullying*

As redes sociais, criadas para que os usuários possam compartilhar comentários, fotos e vídeos com amigos, parentes e conhecidos, se tornaram palco da chamada trolagem⁴ e *cyberbullying*. Os casos são inúmeros, já tendo resultado até em suicídio de adolescentes, com repercussão na grande imprensa. Reportagens de novembro de 2013 relatavam que uma adolescente de 16 anos se matou no Piauí após saber que um vídeo em que ela aparecia tendo relações sexuais tinha sido divulgado no aplicativo para *smartphones* Whatsapp. Uma semana depois, outra menina da mesma idade cometeu suicídio no Rio Grande do Sul, depois que um ex-namorado seu publicou no Facebook e no Twitter fotos em que ela aparece com os seios à mostra. O delegado responsável pelo caso afirmou

⁴ Desestabilizar discussões, provocar e enfiar pessoas na internet. Entrar no perfil deixado aberto por outra pessoa em seu computador e fazer-se passar por ela, fazendo comentários inadequados, também é chamado de trolagem.

que os responsáveis seriam enquadrados no artigo 241 A do *Estatuto da Criança e do Adolescente*, que qualifica como crime grave a disseminação de fotos, vídeos ou imagens de crianças ou adolescentes em situação de sexo explícito ou pornográfica (ILHA, 2013).

A psicóloga e psicanalista Beatriz Breves, que dá consultas há 30 anos, lançou em 2014 o livro *A maldade humana: como detonar uma pessoa no Facebook*, com a também psicóloga e psicanalista Virgínia Sampaio. A motivação para o livro não veio de casos que ela tratou no consultório, mas de sua própria experiência como vítima, que ela acredita que tenha tido como causa questões internas de seu condomínio, onde era síndica. O caso de Beatriz também acabou sendo relatado na grande imprensa. Um vizinho postou no Facebook que uma gata cega e idosa tinha sido pisoteada por Beatriz enquanto a mãe dele tentava protegê-la, e a mãe em questão precisara ser medicada. A psicóloga, porém, diz adorar animais e tem em casa gatos e uma cadela. Em entrevista a um repórter do jornal *O Globo*, Beatriz resumiu os ataques, esclarecendo que “os mais pesados” decidiu nem colocar no livro, pois “ninguém aguentaria ler”.

Foram mais de mil postagens em dez dias. Pediam linchamento, prisão, morte: ‘essa bruxa, quando partir pro andar de baixo, vai cair de bunda no tridente’, ‘morte para essa maluca’, ‘tem que morrer, fdp’, ‘MATA DE PORRADA, DIZ O END QUE EU MESMO MATO’⁵. Fui chamada de vadia, monstro, ser hediondo, Lúcifer, demente, maldita, criatura bestial. No fim, já diziam que eu queimava gambá com querosene. [...] Você não sai a mesma. Até ao falar disso a gente se emociona. Imagine um adolescente? Não vai suportar. Ou fica com traumas ou, no extremo, se mata. Sugiro um Disque SOS Violência Internet onde você poderia ligar, ouvir uma voz real, se acalmar e receber apoio social, jurídico e psicológico. A internet é muito rápida e a Justiça é muito lenta. É preciso criar mecanismos mais velozes para impedir os danos. (VENTURA, 2014, p. 6).

Leis existem para punir crimes como esses. Os chamados crimes contra a honra são a injúria, calúnia e difamação. A injúria é quando se ofende a dignidade e o decoro de alguém (em geral, em alguma discussão direta com a pessoa), e a pena para isso é de multa ou um a seis meses de detenção. A calúnia, quando se atribui a alguém, de maneira falsa, a responsabilidade pela prática de um determinado fato definido como crime, tem pena de seis meses a dois anos, mais

⁵ Em maiúsculas no original, o que, no contrato de leitura dos usuários de internet, significa gritos.

multa, e quem divulga a mentira contra alguém que tinha sido dita por outra pessoa incorre na mesma pena, mesmo não tendo sido o autor original da calúnia. A difamação, que consiste em imputar a alguém fato ofensivo a sua reputação, tem pena de três meses a um ano de detenção e multa. E ainda há agravantes que podem elevar a pena em um terço, como o crime ser cometido na presença de várias pessoas, ou por meio que facilite a divulgação da calúnia, da difamação ou da injúria – que é o caso da internet.

Além desses artigos do *Código Penal*, o artigo 5º da *Constituição Federal* afirma, no inciso IV, que é livre a manifestação do pensamento, sendo vedado o anonimato; no inciso V, afirma que é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem; e, no X, que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

O aplicativo Secret, para dispositivos móveis, foi lançado em maio de 2014 com uma ideia original bastante interessante: todos os participantes são anônimos, com suas postagens identificadas apenas por um ícone, e cada um pode postar um problema seu sobre o qual deseja desabafar e, a partir daí, receber conselhos e ajuda. A pessoa poderia abrir totalmente seu coração, já que não é identificada. A ideia foi rapidamente desvirtuada e boa parte das postagens passou a ser falando mal de terceiros, comentadas e disseminadas.

Os problemas trazidos pelo aplicativo repercutiram na grande imprensa. A jornalista Cora Rónai, em sua coluna “Digital” no jornal *O Globo*, relatou algumas postagens de pessoas desesperadas com o Secret:

A maldade e a vulgaridade que tomaram o Secret de assalto não são problema exclusivamente brasileiro. As opiniões na página de download do aplicativo na App Store americana adquirem, com frequência, um tom desesperado:

‘Não baixem o Secret!!!’, implorava, ontem, uma usuária. ‘O bullying virou uma praga, e aplicativos horríveis como esse só fazem estimular a prática!’

‘Leiam isso!’, pedia outro usuário. ‘Este aplicativo seria ótimo para pessoas maduras, mas adolescentes estão postando fotos de garotas peladas e pessoas já querem se suicidar. Este app deve ser tirado de circulação! Sinto muito por quem está curtindo, mas o app está levando muita gente à loucura, não podemos postar nada sem sermos julgados e xingados de nomes horríveis! Lamento, mas cansei de ver

peças dizendo que querem se matar e gente anônima respondendo para irem em frente'. (RÓNAI, 2014, p. 27).

Diante de inúmeras denúncias no Brasil, a Justiça do Espírito Santo atendeu ao pedido do Ministério Público do estado e determinou, em liminar de agosto de 2014, que a Apple e o Google removessem o Secret e o Cryptic, similar da Microsoft, de suas lojas virtuais oficiais e também dos smartphones dos usuários que já os haviam baixado, sob pena de multa de R\$ 20 mil por dia. O Ministério Público alegava que diversas pessoas estavam sendo atacadas em sua honra sem poder se defender, dado o anonimato das postagens. Em sua sentença, o juiz Paulo César de Carvalho, da 5ª Vara Cível de Vitória, utilizou o artigo 5º, inciso IV da *Constituição Federal*:

[...] a liberdade de expressão não constitui um direito absoluto, sendo inúmeras as hipóteses em que o seu exercício entra em conflito com outros direitos fundamentais ou bens jurídicos coletivos constitucionalmente tutelados, que serão equacionados mediante uma ponderação de interesses, de modo a garantir o direito à honra, privacidade, igualdade e dignidade humana e, até mesmo, proteção da infância e adolescência, já que não há qualquer restrição à utilização dos aplicativos indicados na inicial.
Para compatibilizar tais direitos com a liberdade de expressão, sem que haja censura prévia, é que a Constituição adotou o modelo de liberdade com responsabilidade, vedando o anonimato⁶.

O juiz disse ainda que “o inciso X, do mesmo dispositivo, garante que ‘são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito de indenização pelo dano material ou moral decorrente de sua violação’”⁷.

Muitos usuários se consideram seguros ao agir anonimamente contra outras pessoas na internet. A Justiça, como visto, pode quebrar o sigilo e descobrir quem está por trás dos perfis anônimos. Mas há quem faça isso na própria rede. O pesquisador americano Bryan Silley, da Rhino Security, hackeou o Secret e conseguiu descobrir autores de postagens anônimas (E AGORA?, 2014). Ele

⁶ Processo nº 0028553-98.2014.8.08.0024, consultado no site do Tribunal de Justiça do Espírito Santo. Informação disponível em: <http://aplicativos.tjes.jus.br/sistemaspublicos/consulta_12_instancias/ver_decisao_new.cfm>. Acesso em 20/09/2014.

⁷ Idem.

informou sobre a descoberta aos criadores do aplicativo, mas isso mostra o quanto o anonimato na rede é vulnerável mesmo a outros usuários.

O Marco Civil da Internet, debatido por mais de três anos no Congresso Nacional, entrou em vigor em 23 de junho de 2014. Embora ainda seja uma lei relativamente recente, ela já foi usada, por exemplo, no caso de uma estudante da Universidade Presbiteriana Mackenzie, em São Paulo, que sofreu *cyberbullying* em maio de 2014 em dois grupos de conversas do aplicativo Whatsapp. A mãe e advogada da jovem, Adriana Cavassani, contou ao jornal *O Globo* que a filha entrou em depressão e pensou em suicídio (JANSEN, 2014a, p. 29). O caso foi julgado na 8ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo. Em seu voto, o relator, juiz Salles Rossi, explica que a autora da ação pedia a exibição dos endereços IP dos autores de conversas do Whatsapp que apresentavam conteúdo difamatório contra a jovem, além de “montagens de fotografias de cunho pornográfico”. O Facebook tentou alegar que o Whatsapp tinha sede fora do Brasil e que não tinha gerência sobre o aplicativo. O juiz, porém, negou o recurso, explicando que isso não era impedimento para informar os endereços e o teor das conversas dos grupos *Atlética Chorume* e *Lixo Mackenzista* que violavam o direito de personalidade da autora, pois era notória a compra do Whatsapp pelo Facebook, que é “pessoa jurídica que tem representação no país, com registro na JUCESP”. De acordo com o voto do relator, o Facebook:

deve guardar e manter os registros respectivos, propiciando meios para identificação dos usuários e teor de conversas ali inseridas determinação, aliás, que encontra amparo na regra do artigo 13 da Lei 12.965/2014 (conhecida como Marco Civil da Internet), ao dizer que 'Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento'⁸.

⁸ Processo n. 2114774-24.2014.8.26.0000 do TJSP. Informação disponível em: <<http://esaj.tjsp.jus.br/cpo/sg/search.do?jsessionid=93C0C6871239896D8D3A340C15A1A558.cpo1?conversationId=&paginaConsulta=1&localPesquisa.cdLocal=-1&cbPesquisa=NUMPROC&tipoNuProcesso=UNIFICADO&numeroDigitoAnoUnificado=2114774-24.2014&foroNumeroUnificado=0000&dePesquisaNuUnificado=2114774-24.2014.8.26.0000&dePesquisaNuAntigo=>>>. Acesso em 20/10/2014.

3 Leis recentes tratam da invasão de privacidade via internet

A invasão de privacidade também é algo que ocorre cada vez com mais frequência, e acabou gerando a Lei Carolina Dieckmann, batizada assim por causa da grande publicidade na mídia dada a um caso envolvendo a atriz brasileira de mesmo nome. O computador pessoal de Carolina foi invadido por *hackers*, que roubaram fotos em que a atriz aparece nua e as divulgaram na internet. Toda a discussão em torno do caso e o empenho da atriz em conseguir uma punição para quem a atacou acabaram levando à aprovação da lei em curto espaço de tempo. A lei 12.737, de 30 de novembro de 2012, tornou crime invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo. Também tornou crime instalar vulnerabilidades para obter vantagem ilícita. A pena é detenção de três meses a um ano e multa.

No mesmo dia da entrada em vigor da Lei Carolina Dieckmann, começou a vigorar também a chamada Lei Azeredo (Lei 12.735), que ganhou esse apelido por ter como relator o senador Eduardo Azeredo (PSDB-MG). De acordo com esta lei, os órgãos da polícia judiciária estruturarão setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado. A tramitação deste projeto de lei, que começou em 1999, foi cercada de polêmica e acabou sendo atropelada pela Lei Carolina Dieckmann e o Marco Civil da Internet, uma proposta do governo federal.

A proposta original⁹ pretendia incluir no Código Penal Brasileiro ciber-crimes como a disseminação de vírus, o estelionato eletrônico (como o roubo de senhas), a divulgação inadvertida de dados pessoais e a criminalização não só da produção e divulgação de conteúdos que promovem a pedofilia, mas também o armazenamento desses materiais. O projeto também criava regras para identificar e armazenar dados de usuários para potencialmente identificar melhor os suspeitos de incorrer nesses crimes, obrigando provedores a preservar esses registros por três anos e ampliando suas obrigações de fiscalização e denúncia de crimes. [...] O projeto apresentou severa resistência da sociedade civil pelo temor de que seus artigos amplos poderiam

⁹ Da Lei Azeredo.

ameaçar a liberdade de expressão e a privacidade dos usuários – tópicos que ficaram de fora na versão final da lei. (PAGANOTTI, 2014, p. 147-148).

A invasão de privacidade de forma geral é permitida pelos usuários no caso da sua relação com as empresas de internet. Muitas vezes o usuário permite o acesso a seus dados pelo buscador, redes sociais, provedor de internet ou outros, mas de forma geral não há uma reflexão sobre o que essas empresas podem fazer com os dados coletados, ou mesmo exatamente que tipo de dados se está deixando disponível para consulta e até mesmo compartilhamento por parte dessas empresas.

E as possibilidades de invasão de privacidade não param de aumentar. Hoje, a chamada internet das coisas já começa a ser realidade e tem o objetivo de facilitar a vida, mas novidades como a geladeira que faz a lista de compras e se comunica com o supermercado para pedi-la em domicílio podem parecer a máquina a vapor se comparadas à *brainet*. O neurocientista Miguel Nicolelis já prevê, em suas pesquisas, uma ligação homem-máquina tão profunda que você “poderá conversar com uma multidão, fisicamente localizada em qualquer parte do planeta, por meio de uma nova versão da internet (a ‘brainet’), sem a necessidade de digitar ou pronunciar uma única palavra” (2011, p. 25), somente através do pensamento. Vale lembrar que Nicolelis já conseguiu gerar a comunicação por pensamento entre um rato de laboratório no Brasil e outro nos EUA (VICTOR, 2013, p. 44).

No mundo concreto atual, o motorista parado no trânsito das grandes cidades pode usar seu celular com internet para acessar aplicativos que mostram em seu caminho, no mapa, onde o trânsito está parado (em vermelho). A pessoa oferece a sua localização ao aplicativo, que gera um bem comum, a inteligência coletiva do engarrafamento. Porém, o que mais podem fazer com a sua localização? Ou com a sua lista de compras? Ou ainda, num futuro aparentemente remoto, mas já projetado, com o que quer que esteja se passando no seu pensamento? Que grau de controle temos ou teremos sobre a nossa privacidade? Bezerra e Waltz ajudam a refletir sobre o assunto ao definir privacidade e intimidade:

A privacidade e a intimidade são direitos fundamentais presentes na Declaração Universal de Direitos Humanos e na Constituição da República de 1988. A privacidade refere-se a tudo o que o indivíduo não pretende que seja de conhecimento público, reservado apenas aos integrantes do seu círculo de convivência particular, enquanto a intimidade diz respeito única e exclusivamente ao indivíduo. Esses direitos se estendem ao domicílio, à correspondência, às comunicações e aos dados pessoais. (BEZERRA; WALTZ, 2014, p. 162).

Atualmente é preciso de fato se preocupar com a invasão de privacidade feita pelas próprias empresas de internet ou mesmo por governos. Medidas judiciais ou de agências reguladoras são uma constante nesse novo mundo da comunicação, explicitando as disputas de interesses que podem vir a gerar novas leis e regras. Um dos muitos exemplos foi a multa de US\$ 22,5 milhões dada à empresa Google pela Comissão Federal de Comércio (FTC) dos EUA em agosto de 2012. A empresa usou um código de computação conhecido como *cookie* para enganar o Safari nos dispositivos móveis iPhone e iPad, para que, assim, o Google pudesse monitorar usuários que bloqueassem o registro de suas atividades na internet (GOOGLE É, 2014).

Um caso recente mostra como é tênue a fronteira entre o bem e o mal quando se trata de invasão da privacidade do cliente pela empresa de internet – seja ela um provedor, buscador, rede social ou qualquer outra que tenha acesso a seus dados. O Google denunciou à ONG americana Centro Nacional para Crianças Perdidas ou Exploradas que um usuário do Gmail tinha imagens de crianças nuas em seu e-mail. A ONG alertou a polícia de Houston, no Texas, que prendeu o criminoso ao analisar seus dispositivos eletrônicos, cheios de imagens e mensagens sobre pornografia infantil. Ele já tinha uma passagem pela polícia em 1994 por atacar uma criança (JANSEN, 2014b).

Em abril deste ano, o Google havia alterado seus termos de uso, passando a informar que os usuários têm seus conteúdos, inclusive e-mails, analisados automaticamente, para que a empresa possa “fornecer recursos relevantes”. E desde 2008, o Google utiliza sistemas para verificar e combater o compartilhamento de pornografia infantil.

Na União Europeia, após pressão popular, o Tribunal de Justiça ordenou o Google a apagar links de busca que desabonem cidadãos da UE a partir de

informações inconsistentes, não pertinentes ou que deixaram de ser pertinentes com o decorrer do tempo. No primeiro dia em vigor da decisão do tribunal, 26 de junho de 2014, foram feitas mais de 12 mil solicitações de remoção ao Google.

No Brasil, a operadora de telecomunicações Oi foi multada em R\$ 3,5 milhões pelo Ministério da Justiça em julho de 2014. O provedor de internet Velox, da Oi, teria cometido violação ao direito à privacidade e intimidade e publicidade enganosa (CASEMIRO; XAVIER, 2014, p. 28). As investigações começaram em 2010, a partir de denúncias de que a Oi, em parceria com a empresa britânica Phorm, desenvolveu o software Navegador, que mapeava o tráfego de dados do consumidor na internet para compor seu perfil de navegação. Os perfis, segundo o Departamento de Proteção e Defesa do Consumidor do ministério, eram comercializados com anunciantes, agências de publicidade e portais da web para oferta de publicidade direcionada a esses consumidores. O serviço foi suspenso pela Oi, que afirmou que as informações “sensíveis” não eram catalogadas.

Poucos usuários do Facebook sabem que, seguindo um caminho dentro da área Configurações do perfil, é possível saber quais são os dados que a rede social está coletando do usuário, dados que utiliza para vender anúncios direcionados aos interesses daquela pessoa. Para muita gente, descobrir o que é coletado para uso da empresa Facebook pode ser assustador. Não são apenas as postagens de textos, fotografias e vídeo, ou mesmo as conversas reservadas, que são utilizados, mas também de que endereço IP a rede foi acessada pelo usuário a cada momento, o tamanho de roupa que usa, a lista de amizades desfeitas e a fase da vida em que o Facebook acredita que os amigos dele estejam (ARAGÃO, 2014).

O Google também monitora as buscas que os clientes fazem e os locais onde estão para vender anúncios direcionados, conforme se vê na correspondência enviada a empresas que serão possíveis anunciantes:

Seus clientes atuais provavelmente buscam por sua empresa pelo nome [...]. Mas seus futuros clientes pesquisam pelo ramo de atividade do negócio e a cidade de interesse. [...] Sua empresa pode até aparecer, mas não chamará muito a atenção deles. Ao anunciar no Google AdWords, você destaca sua empresa e seu ramo de atividade, além de

ofertas e condições especiais para milhares de consumidores. [...] Os anúncios podem focar em seu bairro e localidade¹⁰.

Esses são apenas alguns exemplos de casos envolvendo a questão da privacidade e as empresas de internet. Mas governos também acessam informações de usuários na rede. O caso mais rumoroso, e que despertou a atenção do mundo para o assunto, foi o das denúncias do ex-administrador de sistemas da CIA Edward Snowden em relação ao governo americano. Em junho de 2013, Snowden começou a vazar para a imprensa documentos sigilosos da Agência Nacional de Segurança (NSA), mostrando que o governo dos Estados Unidos monitora cidadãos e mesmo outros governos de países aliados, como o Brasil e a Alemanha. Apesar de ter tido que se mudar dos EUA para a Rússia para evitar ser preso por conta das denúncias, Snowden afirmou que não se arrependeu de divulgar as informações, dizendo acreditar que sua ação vai ajudar os americanos, que agora têm “o poder de decidir por eles mesmos se estão dispostos a ceder sua privacidade a um estado de vigilância constante” (QUEM É, 2014).

Toda esta discussão que envolve a regulação da alta tecnologia do século XXI tem uma questão de fundo que remete ao filósofo Walter Benjamin, o qual, no contexto pós-I Guerra Mundial, escreveu *Crítica da violência – Crítica do Poder* (1987). A palavra usada por Benjamin em alemão, *gewalt*, serve tanto para violência quanto para poder, e o ensaio é construído a partir desta ambiguidade. Benjamin questiona o que podemos comparar com o nosso ditado “os fins justificam os meios”. Para ele, a questão não é se a violência serve a fins justos ou injustos. Se a pergunta for essa, não se critica a violência pura, e sim se ela foi bem aplicada ou não naquele caso. Deve-se produzir então uma crítica da ordem dos meios.

Existe uma tradição jurídica de sobreposição dos fins aos meios. É direito natural do homem fazer o que ele é capaz de fazer, como usar a violência para conseguir o que quer. Mas para viver em sociedade é preciso renunciar a este direito, e é a partir daí que se cria a ordem política. O direito é um conflito de direitos. Vivemos numa sociedade em que o direito positivo se sobrepõe ao natural, mas sem acabar com ele. Surge então algo que, para Benjamin, é um

¹⁰ Correspondência enviada a empresas em agosto de 2014, incluindo preços e condições.

dogma da sociedade moderna: usando meios ilegítimos podemos atingir fins justos. Para romper com o dogma é preciso separar meios e fins.

O filósofo italiano Giorgio Agamben refletiu sobre esse pensamento de Benjamin em seu livro *Estado de exceção*, no qual questiona o espaço da política hoje e o que fazer diante da nova configuração do poder. Agamben começa citando *Teologia política*, livro de 1922 de Carl Schmitt (teórico do nazismo), em que este formula a teoria do estado de exceção e diz que “soberano é aquele que decide sobre o estado de exceção”. Os nazistas montaram uma teoria para justificar, pelo direito público, o regime ditatorial. Para Agamben, o estado de exceção, que antes era exceção, agora é uma prática essencial mesmo nos países democráticos. O livro do filósofo italiano foi publicado em 2003, bem antes das denúncias de Snowden, mas aquilo que o autor chama de estado de exceção já estava configurado, nos Estados Unidos (sem falar em outros países), com medidas como o Ato Patriótico americano, autorizando prisões por longo tempo e escuta telefônica, depois proibidas pelo Supremo Tribunal dos EUA.

No Brasil, um dos principais pontos do Marco Civil da Internet é a proteção à privacidade. A nova lei obriga todos os serviços de internet (sites ou aplicativos móveis) a deixar claro para seus cidadãos como seus dados pessoais serão coletados e tratados. O fornecimento das informações pessoais coletadas a terceiros fica proibido, “salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei”.

Mas a entrada em vigor do marco civil não encerra o assunto: um novo debate público já está se esboçando. Um ponto que precisa de regulação é a obrigação de todos os provedores de acesso guardarem registros de acesso dos clientes por um ano, e sites e aplicações com fins econômicos, por seis meses. Essa questão já gerou protestos de especialistas e outros interessados no tema, que reclamam que haverá um custo enorme para as empresas e um retrocesso na privacidade.

4 Considerações finais

Com todos os exemplos que vimos acima, e apesar de novas leis já estarem sendo criadas, é preciso continuar debatendo a questão da privacidade e da intimidade na internet, criando instrumentos para que o cidadão possa ser protegido em seus direitos fundamentais. As mudanças tecnológicas estão constantemente criando novos cenários, e estes devem ser regulados pela sociedade através de seus representantes.

O Marco Civil da Internet, a Lei Carolina Dieckmann e as leis contra difamação e calúnia são os principais instrumentos que os cidadãos brasileiros têm à sua disposição para combater ataques à privacidade, à intimidade, à honra e à imagem. A visão romântica da internet como território livre para a liberdade de expressão veio sendo empanada pelo seu uso como terra de ninguém, aberta a qualquer tipo de vandalismo ou *bullying* virtual. Muitos ainda acreditam que se pode fazer qualquer coisa na internet sem punição, e quanto mais divulgação houver sobre as punições, melhor será para a sociedade. E é preciso um profundo debate sobre até que ponto o Estado, em seu dever de proteger os cidadãos, tem o direito de invadir sua privacidade.

REFERÊNCIAS

AGAMBEN, Giorgio. **Estado de exceção**. São Paulo: Boitempo, 2004.

ARAGÃO, Alexandre. Facebook deixa usuário ver todos os passos armazenados pela rede social; leia depoimentos. **Folha de S. Paulo**, 14/07/2014. Disponível em: <<http://www1.folha.uol.com.br/tec/2014/07/1484727-facebook-deixa-usuario-ver-todos-os-passos-armazenados-pela-rede-social.shtml>>. Acesso em: 17/07/2014.

BENJAMIN, Walter. **Obras escolhidas: magia e técnica, arte e política**. São Paulo: Brasiliense, 1987.

BEZERRA, Arthur C.; WALTZ, Igor. Privacidade, neutralidade e inimputabilidade da internet no Brasil: avanços e deficiências no projeto do Marco Civil. **Revista Eptic Online**, v. 16, n. 2, maio/ago. 2014.

BOLAÑO, César R.; BRITTOS, Valério C. **A televisão brasileira na era digital: exclusão, esfera pública e movimentos estruturantes**. São Paulo: Paulus, 2007.

BRASIL. Código Penal. Decreto-lei n. 2.848, de 07 de dezembro de 1940. Capítulo V – Crimes contra a honra. **Portal da Legislação**, Brasília, DF Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm>. Acesso em 30/06/2014.

BRASIL. Lei Azeredo: Lei n. 12.735, de 30 de novembro de 2012. **Portal da Legislação**, Brasília, DF, 03 dez. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 30/06/2014.

BRASIL. Lei Carolina Dieckmann: Lei nº 12.737, de 30 de novembro de 2012. **Portal da Legislação**, Brasília, DF, 03 dez. 2012. Disponível em: <http://legislacao.planalto.gov.br/legisla/legislacao.nsf/Viw_Identificacao/lei%2012.737-2012?OpenDocument>. Acesso em: 30/06/2014.

BRASIL. Marco Civil da Internet: Lei 12.965, de 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 30/06/2014.

CASEMIRO, Luciana; XAVIER, Luiza. Oi é multada em R\$ 3,5 milhões por violação de privacidade. **O Globo**, 24/07/2014.

Constituição federal: Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em 30/6/2014.

DANTAS, Marcos. Da Cofecom ao PNBL: balanço e perspectivas do debate sobre Comunicações no Brasil. In: DANTAS, Marcos; KISCHINHEVSKY, Marcelo. (Orgs.). **Políticas públicas e pluralidade na comunicação e na cultura**. Rio de Janeiro: E-papers Serviços Editoriais, 2014.

E AGORA? Hacker cria forma de burlar anonimato no Secret. **O Globo**, 22/08/2014. Disponível em: <<http://oglobo.globo.com/sociedade/tecnologia/e- agora-hacker-cria-forma-de-burlar-anonimato-no-secret-13695864#ixzz3BQhj9fJs>>. Acesso em: 24/08/2014.

GOOGLE é multado por violar a privacidade de usuários do Safari. Disponível em: <<http://oglobo.globo.com/tecnologia/google-multado-por-violar-privacidade-de-usuarios-do-safari-5742368#ixzz3QxJPorw>>. Acesso em: 30/06/2014.

ILHA, Flávio. Jovem comete suicídio depois de ter fotos íntimas vazadas na internet. **O Globo**, 20/11/2013. Disponível em: <<http://oglobo.globo.com/brasil/jovem-comete-suicidio-depois-de-ter-fotos-intimas-vazadas-na-internet-10831415#ixzz3Bmllb4Fc>>. Acesso em: 26/08/2014.

JANSEN, Thiago. Pedida quebra de sigilo de usuários do WhatsApp que espalharam imagens difamatórias. **O Globo**, 26/09/2014a.

JANSEN, Thiago. Polícia prende pedófilo graças a dica de provedor. **O Globo**, 05/08/2014b, p. 24

LEMOS, Ronaldo. **Futuros possíveis: mídia, cultura, sociedade, direitos**. Porto Alegre: Sulina, 2012.

NICOLELIS, Miguel. **Muito além do nosso eu: a nova neurociência que une cérebro e máquinas – e como ela pode mudar nossas vidas**. São Paulo: Companhia das Letras, 2011.

PAGANOTTI, Ivan. Pressão virtual e regulamentação digital brasileira: análise comparativa entre o marco civil da internet e a Lei Azeredo. **Revista Eptic Online**, v. 16, n. 2, maio/ago. 2014.

QUEM é Edward Snowden, o ex-agente que vazou documentos secretos dos EUA. **Revista Época**, 10/06/2013. Disponível em: <<http://revistaepoca.globo.com/Mundo/noticia/2013/06/quem-e-edward-snowden-o-ex-agente-que-vazou-documentos-de-espionagem-dos-eua.html>>. Acesso em: 20/08/2014.

RÓNAI, Cora. Secret: o fim de uma linda ideia. **O Globo**, 22/08/2014.

VENTURA, Mauro. Duas limonadas e a conta com... Beatriz Breves. **Revista O Globo**, 24/08/2014.

VICTOR, D. Brasileiro liga cérebro de ratos pela internet. **O Globo**, 01/03/2013.

Recebido em: 14.05.2015

Aceito em: 07.08.2015