

PRIVACIDADE NA INTERNET: OS DRAMAS DE UM MUNDO SEM FRONTEIRAS

Gabriel Monteiro de Oliveira

Graduado em Direito pelo Centro Universitário Salesiano de São Paulo, Unidade de Lorena.
E-mail: baiei18@gmail.com

RESUMO

A *internet* trouxe benefícios incontáveis. É graças a ela que as fronteiras parecem não mais existir. Mas, ao mesmo tempo que a agilidade e a liberdade existem como nunca antes visto, a rede mundial de computadores também tem significado uma queda na privacidade de todos os seus usuários. Os dados pessoais passaram a ser uma mercadoria valiosa, capaz de render bilhões de reais às empresas *online* e, assim, com pouca transparência e cada vez mais cidadãos acessando a rede, tem sido difícil garantir um nível mínimo de segurança destas informações pessoais, bem como a privacidade destes usuários. Dentro deste cenário há, ainda, o direito ao esquecimento, cujo gerenciamento vem sendo delegado às empresas de tecnologia, mas que pode representar um choque entre o acesso à informação e o direito à privacidade, algo que deveria ter maior fiscalização de autoridades governamentais e judiciárias, a fim de evitar abusos. O presente trabalho, alinhado ao exposto, visa discutir como o direito à privacidade na internet, um tema que tem cada vez maior relevância para o direito, é tratado atualmente, assim como os reflexos jurídicos deste direito, em especial no que diz respeito ao direito de ser esquecido, estudando, ademais, casos reais apreciados pelo judiciário nacional e internacional.

Palavras-chave: internet, privacidade, direitos fundamentais

INTRODUÇÃO

É praticamente impossível encontrar alguém que não conheça a *internet* no mundo atual. Sua presença é cada vez maior em todos os lugares do globo, e é cada vez mais difícil lembrar-se de fronteiras físicas com o advento da rede mundial de computadores.

A *internet* é parte essencial da vida de tantas pessoas, que muitos sequer pensam em como ela surgiu e se tornou a ferramenta indispensável que é hoje. Mas, com sua expansão, surgem também os problemas naturais da convivência humana, ainda que somente de maneira virtual. E é partir destes conflitos resultantes da convivência na rede que o direito passa a ser

cada vez mais exigido e sua tutela se torna necessária para resolver conflitos e resguardar os cidadãos virtuais.

Neste cenário, o direito à privacidade é um dos que mais vêm sofrendo prejuízos, pois em um mundo que torna a exposição cada vez maior, torna-se ainda mais difícil a preservação da privacidade e a proteção dos dados pessoais armazenados na *internet*. Os serviços digitais, aproveitando-se da democratização do uso da rede mundial de computadores, também encontraram maneiras de obter lucro com o desconhecimento de seus usuários, e os utilizam como mercadoria para vender dados pessoais e oferecer publicidades que, em alguns momentos, beiram à invasão completa de privacidade.

Há, ainda, a situação de que as informações que são colocadas na *internet* possuem um caráter de perpetuidade cada vez maior e são muito mais difíceis de serem removidas de circulação e “esquecidas” do que o seriam em outros tipos de veículos midiáticos. Em uma situação como estas, a quem deve ser dada a responsabilidade para remover – ou não – tais informações? Cabe a governos, através de seu sistema judiciário, decidir todos os casos? Ou as empresas podem ser acionadas para solucionar estes pedidos e decidirem, de maneira unilateral, quem terá direito à remoção desta informação, ou à sua manutenção?

É diante desta realidade que o direito passa a ser importantíssimo, pois é ele, como ferramenta de pacificação social, quem deve trazer as diretrizes bases a serem seguidas para uma convivência saudável e um uso adequado da *internet*. Contudo, muitos governos não possuem interesse imediato em lidar com o assunto, pois seu poder diplomático, bem como seu protagonismo na *internet* tornam irrelevante uma discussão global sobre a rede mundial de computadores. É o caso, por exemplo, dos Estados Unidos, que se aproveitou de brechas para espionar pessoas em todo o mundo, sem respeitar direitos básicos que já existem em outras esferas, mas que a incerteza faz com que, muitas vezes, não sejam utilizados também na esfera virtual.

É esta mesma incerteza, aliada a um desconhecimento ainda existente, que culminaram em decisões exageradas do próprio judiciário brasileiro, que chegou a determinar o bloqueio, por tempo determinado, de um aplicativo de mensagens em todo país.

No presente trabalho, discutiremos a importância da privacidade na *internet*, em especial no conflito de princípios fundamentais que se vislumbra quando se contrapõe o direito de ser esquecido com o direito à informação, e a importância de uma tutela jurídica consciente – e internacional – sobre o assunto para que o uso desta ferramenta que é, atualmente, indispensável para a vida moderna do ser humano seja usada de maneira saudável e sem que exista prejuízo a quem quer que seja.

1. A HISTÓRIA DA INTERNET

Você acorda com um alarme suave, tocando de maneira crescente para que, no melhor momento para isso, você desperte, diminuindo, assim, o cansaço característico de levantar muito cedo pela manhã, isso porque em seu pulso está uma pulseira inteligente, vibrando levemente, que analisou todo o seu sono e percebeu que, para acordar na hora certa e disposto, aquele seria o melhor momento para soar o alarme matinal; pega o celular e, em uma olhada rápida, verifica se foi uma boa noite de sono ou não através de um relatório gerado em um *app* que monitora cada noite de descanso. Finalmente levanta-se e segue para o banheiro, onde sobe em uma balança inteligente que envia para o seu *smartphone* uma informação completa a respeito de seu histórico de peso. Toma seu banho, veste-se e vai tomar o café da manhã, coloca uma cápsula do tamanho de uma pequena noz em um aparelho e, como mágica, uma dose magnífica de cappuccino cai suavemente em sua xícara; abre a geladeira e pega uma maçã, que estão acabando, percebendo isso sua geladeira já atualiza, em seu *smartphone*, a lista de compras da semana para incluir algumas e não te deixar sem frutas. Escova os dentes e saca, novamente, o celular, abrindo o aplicativo de mapas e verificando quanto tempo levará para chegar ao trabalho, percebe que o trânsito não está muito intenso, há tempo para um episódio rápido daquela série de humor que adora; liga a televisão com o próprio *smartphone*, conecta a um streaming de vídeo e inicia o episódio; um pouco depois o celular apita avisando que aquele é o melhor momento para sair de casa com destino ao trabalho e chegar na hora certa. Você vai até o carro, que destrava apenas com sua aproximação, liga apertando um botão, coloca na posição “*drive*” e o deixa sair da garagem sozinho, automaticamente, enquanto se ajeita para ouvir músicas no aplicativo de streaming com uma seleção de músicas para você descobrir naquela semana. No fim do dia do trabalho, você usa o celular para ligar o ar condicionado da sua casa antes mesmo de entrar no carro, pois está quente e você quer chegar em casa e encontrar um clima confortável; ativa a cafeteira para que quando chegar esteja pronto, e quente, mais um cappuccino delicioso como o da manhã. Chegando em casa a porta abre, novamente, apenas com sua aproximação, você pega o cappuccino, abre a geladeira e prepara um lanche, senta diante da TV e continua a série de humor, do ponto onde havia parado antes de sair para o trabalho.

O “conto” acima parece saído direto de uma ficção científica, mas é cada vez mais comum e está cada vez mais próximo da realidade de milhares de pessoas ao redor de todo o mundo; apenas a título de informação cabe dizer que todas as tecnologias nele mencionadas já existem, apesar de algumas ainda encontrarem-se em fases finais de testes, mas a “*internet* das coisas” é uma realidade, apesar de ainda estar em seu início. Mas, para muitos, a história do que nós chamamos hoje de *internet* é desconhecida, e a maioria se surpreenderia em saber que o objetivo inicial da rede mundial de computadores visava um fim completamente diferente do que o se tornou atualmente.

Antes, entretanto, de nos enveredarmos pela história da *internet*, de bom tom faz-se um apanhado geral da evolução surpreendentemente rápida que as comunicações sofreram nos últimos anos.

Não se pode falar em comunicações sem começar pela invenção da imprensa, o princípio do que conhecemos hoje como comunicação “em larga escala”, a imprensa surge com

a tipografia, inventada pelo alemão Johannes Gutenberg em 1445, a primeira a possibilitar uma produção em massa de grandes publicações sem que o custo as tornasse proibitivas¹.

Após, veio a invenção do telefone, que embora não seja uma comunicação em larga escala propriamente dita, merece menção, dado que, quando do surgimento da *internet*, foi através das linhas telefônicas que esta se difundiu pelo mundo. A história do telefone talvez seja a mais conhecida entre todas as que serão citadas aqui, isto é, o nome de Alexander Graham Bell, um imigrante escocês que morava nos Estados Unidos, é conhecido por quase todo o mundo; isto porque foi ele que, em 1875, inventou o telefone, meio sem querer, registrando sua invenção em 7 de março de 1876, quase ao mesmo tempo que o engenheiro Elisha Gray². Contudo a patente de Bell chegou antes e, após longo processo judicial, ele acabou vitorioso. O telefone como inicialmente pensado com certeza manteve suas características, contudo, com o passar do tempo e o avançar da tecnologia, ele se viu unido a diversas outras funcionalidades, vindo a dar origem, em tempos mais recentes, ao *smartphone*, os telefone “inteligentes”, capazes de muito mais do que apenas ligações telefônicas, inclusive – e principalmente – de conectar-se à internet onde quer que se esteja.

Logo em seguida, o próximo passo ao avanço das comunicações foi, sem dúvida, o telégrafo, que tornou a transmissão muito mais ágil, aproximando-se do instantâneo, e este só veio a surgir mais de quatro séculos depois da imprensa, especificamente em 1896 por Guglielmo Marconi, um italiano, que demonstrou, na Inglaterra, o funcionamento de seus aparelhos de emissão e recepção de sinais³. Posteriormente, seguindo a invenção do telégrafo, fazia-se necessária a emissão e recepção de sons mais complexos. Foi somente em 1906 que isso ocorreu, em uma noite de Natal, em Massachussets, nos Estados Unidos, De Forest e Reginald A. Fessenden conseguiram irradiar números de canto e solos de violino⁴. Este meio de comunicação tornou-se importantíssimo, tanto que a famosa máquina Enigma, usada pela Alemanha nazista durante a Segunda Guerra Mundial, usava frequências de rádio para sua comunicação⁵.

¹ CÂMARA, Bira. O nascimento da imprensa, 2009. Disponível em: <<http://jornalivros.com.br/2009/08/o-nascimento-da-imprensa/>>. Acesso em: 30 de out. 2016.

² COSTELLA, Antonio. Comunicação – do grito ao satélite (história dos meios de comunicação). 2ª ed. São Paulo: Mantiqueira, 1984. p. 137.

³ COSTELLA, Antonio. ob. cit. p. 151-152.

⁴ COSTELLA, Antonio. ob. cit. p. 164.

⁵ KRISCHER, Thais Cristine. Um estudo da máquina enigma. Porto Alegre: Graduação em Ciência da Computação da UFRGS, 2012. p. 62. Disponível em <<https://www.lume.ufrgs.br/bitstream/handle/10183/66106/000870987.pdf?sequence=1/>>. Acesso em 30 de out. 2016.

Por fim, antes da *internet*, temos a televisão, surgida na década de 1920, sendo que as primeiras transmissões abertas aconteceram na década de 1930 e, no Brasil, em 1950⁶.

Chegamos, enfim, à história do surgimento da *internet*, a rede mundial de computadores, a maior revolução no que se refere às comunicações, rompendo qualquer fronteira e distância de informações que já existiram. Hoje um acontecimento pode ser transmitido ao outro extremo do globo em tempo real, a ideia de um funcionário trabalhar de sua casa ou de outra cidade, estado ou país deixou de ser algo inimaginável para se tornar cada vez mais comum.

Mas a *internet* surge com um propósito bastante diferente do aspecto que ela tem hoje, uma prova de que algumas invenções são impossíveis de serem contidas.

“A origem da Internet remonta ao ápice da ‘guerra fria’, em meados dos anos 60, nos Estados Unidos, e foi pensada, originalmente, para fins militares.”⁷

Mais do que isso, a *internet* não apenas possuía fins militares, como buscava ser uma forma descentralizada de informações, conectando os computadores norte-americanos em rede, com o intuito de proteger informações sensíveis em caso de um ataque, isto é, como a informação não era concentrada em um só lugar, ao sofrer um ataque militar, as informações continuariam seguras, pois estavam divididas em diversos locais, ainda um projeto rudimentar da internet que conhecemos hoje, ela foi batizada de ARPANET, e foi um método revolucionário de proteger informações⁸. Curiosamente, este método de descentralização veio a se tornar o maior artifício do site de *torrents*⁹ mais famoso da *web*, o lar dos piratas “*piratebay*”¹⁰, que sofre uma perseguição incansável dos mais diversos países, e, em especial, de grandes empresas que buscam resguardar seus direitos autorais, mas, assim como os Estados Unidos imaginaram durante a guerra fria, a descentralização é uma arma muito útil, e o *site* insiste em continuar operando, mesmo sendo retirado do ar sucessivamente.

Posteriormente, esse sistema passou a ser utilizado para fins civis, inicialmente em algumas universidades americanas, sendo utilizado pelos professores e alunos como um canal de divulgação, troca e propagação

⁶ PINTO, Tales Dos Santos. Breve História da televisão; Brasil Escola. Disponível em <<http://brasilecola.uol.com.br/historiag/breve-historia-televisao.htm>>. Acesso em 30 de out. 2016.

⁷ PINHEIRO, Patricia Peck. Direito Digital. 6 ed. rev., atual e ampl. São Paulo: Saraiva, 2016. p. 62.

⁸ PINHEIRO, Patricia Peck. Obra citada, p. 62.

⁹ “*Torrent* é a extensão de arquivos utilizados por um protocolo de transferência do tipo P2P (*Peer to Peer*). Essa transferência acontece da seguinte maneira: os arquivos transferidos são divididos em partes e cada pessoa que tem tal arquivo ajuda a fazer o upload a outros usuários. Isso reduz significativamente o consumo de banda do distribuidor original do arquivo, não sendo necessário que o mesmo fique armazenado em um servidor. Para compartilhar esses arquivos, é necessário usar um programa específico, conhecido como cliente. Ele obtém as informações contidas nos arquivos e se encarrega de toda a comunicação entre os usuários.” PEREIRA, André Luiz. O que é Torrent?; Tecmundo. Disponível em <<http://www.tecmundo.com.br/torrent/166-o-que-e-torrent-.htm>>. Acesso em 03 de nov. 2016.

¹⁰ Por razões morais – e legais – opto por não citar o endereço do *site* neste trabalho.

de conhecimento acadêmico-científico. Esse ambiente menos controlado possibilitou o desenvolvimento da internet nos moldes os quais a conhecemos atualmente.

Entretanto, o grande marco dessa tecnologia se deu em 1987, quando foi convencionada a possibilidade de sua utilização para fins comerciais, passando-se a denominar, então, “Internet”.

Na década de 90, a Internet passou por um processo de expansão sem precedentes. Seu rápido crescimento deve-se a vários de seus recursos e facilidades de acesso e transmissão, que vão desde o correio eletrônico (*e-mail*) até o acesso a banco de dados e informações disponíveis na World Wide Web (WWW), seu espaço multimídia.

Tecnicamente, a Internet consiste na interligação de milhares de dispositivos do mundo inteiro, interconectados mediante protocolos (IP, abreviação de *Internet Protocol*). Ou seja, essa interligação é possível porque utiliza um mesmo padrão de transmissão de dados. A ligação é feita por meio de linhas telefônicas, fibra óptica, satélite, ondas de rádio ou infravermelho. (...).

A interligação física e a uniformização do sistema de transmissão de dados entre as redes, por meio dos protocolos, permitiu, portanto, que a Internet conquistasse maior amplitude no globo¹¹.

Ainda segundo Patricia Peck, em sua obra *Direito Digital*, a velocidade também precisou aumentar, pois os dados passaram a deixar de ser simples para tornarem-se cada vez mais complexos, incluindo áudio e vídeo, e deixando de restringir-se apenas aos computadores para abranger toda uma gama de aparelhos, como TV, telefones celulares, etc., segundo a autora: “Calcula-se que, atualmente, um lar de classe média contenha aproximadamente 200 *chips*, incluindo todos os aparelhos eletrônicos existentes.”; assim como a história que criei no início do capítulo, a própria autora prossegue, em sua obra, no sentido de que “Parece futurismo, mas esse tipo de tecnologia já existe, por exemplo, em equipamentos médicos de ponta, como aqueles utilizados para ressonância magnética.”¹²

Até aqui, falou-se apenas da tecnologia envolvida em toda essa evolução alucinante, mas Patricia Peck abarca a importância do Direito para esta mudança em sua obra, afirmando que:

A complexidade de tal sistema, do ponto de vista jurídico, está nas relações resultantes desta interação, principalmente as relações comerciais. Este ambiente de pessoas conectadas tornou-se extremamente propício para o comércio – aqui surge o conceito de *e-commerce*.

A grande vitrina virtual passa a atrair não apenas empresas, mas também profissionais liberais, *shopping centers*, consumidores, redes de ensino a distância, hospitais, laboratórios, bancos, corretoras e todo aquele interessado em obter uma informação, colocar um produto ou serviço à venda, ou simplesmente buscar entretenimento.

Surtem as comunidades virtuais, os portais horizontais, os portais verticais, os *websites* institucionais, as *homepage* pessoais, os *blogs* e *fotologs*, os metamercados de consumidor-consumidor (C2C), empresa-consumidor (B2C), empresa-empresa (B2B), empresa-empresa-consumidor (B2B2C) – uma verdadeira rede de apatriados.

Todas essas relações entre pessoas e empresas passam a exigir novas regras, princípios, regulamentos, assim como possibilitam a aplicação de antigos princípios que continuam tão atuais para o Direito como o eram em sua origem.

Qual o próximo passo? Não sabemos, mas é importante compreender todo o mecanismo de funcionamento das novas tecnologias de comunicação, entre elas a Internet, bem como sua evolução no futuro cenário de convergência, uma vez que o Direito é resultado do conjunto comportamento e

¹¹ PINHEIRO, Patricia Peck. ob. cit. p. 62-64

¹² PINHEIRO, Patricia Peck. ob. cit. p. 64.

linguagem. Só com essa compreensão é que podemos fazer leis, aplica-las e dar soluções ao caso concreto. É diante de toda essa velocidade de mudanças que nasce o Direito Digital.¹³

Ainda dentro deste cenário em que o Direito é essencial nesta evolução digital, é importante frisarmos a necessidade da discussão a respeito da privacidade, isto porque todo o nosso uso da *internet* gera dados, esses dados são usados para diversos fins, inclusive de mercado, como será explicado mais adiante.

Assim, é essencial que discutamos como a questão da privacidade deve ser abordada e protegida pelo Direito, sem que, entretanto, torne-se um entrave ao desenvolvimento da rede mundial de computadores, pois o Direito não pode tornar-se óbice à evolução digital, mas sim um parceiro, devendo observa-la e resguardar os cidadãos digitais (os quais Patricia Peck chama *e-citizens*), dando caminhos menos obscuros a estes usuários, protegendo, por exemplo, o seu direito a serem “esquecidos”, consubstanciado no Direito ao Esquecimento, que vem sedimentando-se no Direito Europeu, mas sobre o qual o Brasil ainda encontra-se atrasado em legislar, sobre o qual também falaremos no presente trabalho.

2. INTERNET E PRIVACIDADE

O aumento do acesso à internet é um fenômeno global. Cada vez mais pessoas acessam diariamente a rede mundial de computadores. O *Facebook*, maior rede social em atividade, já soma mais de 2 bilhões de usuários¹⁴. Mais de um quarto da população do mundo¹⁵, e aproximadamente dez vezes a população brasileira¹⁶ de acordo com o último censo, tornando-se uma verdadeira “nação digital”.

Com o aumento do número de acessos surgem, por obviedade, situações que passam a requerer a tutela do direito, pois se até mesmo para a patente do telefone houve uma disputa judicial¹⁷, como mostrado no capítulo anterior, certamente a tutela jurídica seria convocada a atuar em um mundo cada vez mais conectado. Entre as necessidades jurídicas advindas de uma nação digital surge, necessariamente, a discussão acerca da privacidade.

¹³ PINHEIRO, Patricia Peck, ob. cit. p. 65.

¹⁴ HIGA, Paulo. Já existem mais de 2 bilhões de usuários no Facebook; Tecnoblog, 2017. Disponível em <<https://tecnoblog.net/217628/facebook-2-bilhoes-usuarios/>>. Acesso em 10 de julho de 2017.

¹⁵ Agência Estado; Estadão, 2013. Disponível em <<http://internacional.estadao.com.br/noticias/geral,onu-populacao-mundial-e-de-7-2-bilhoes-de-pessoas,1042156>>. Acesso em 28 de agosto de 2017.

¹⁶ Conforme dados do IBGE referentes ao Censo de 2016. Disponível em <<http://paises.ibge.gov.br/#/pt/pais/brasil/info/populacao>>. Acesso em 28 de agosto de 2017.

¹⁷ Ver nota de rodapé 2.

A internet representou um verdadeiro novo mundo e, tal qual durante a época das grandes navegações que vieram a conectar o mundo medieval ao continente americano, o descobrimento de uma nova realidade, na qual muitas pessoas se viram fascinadas e imergiram sem refletir as consequências no mundo real de suas ações no mundo digital; afinal, é bastante convidativa a ideia de um universo ao qual se adentra do conforto de sua casa, no qual, acredita-se, ninguém poderá incomoda-lo e onde tudo é possível, sem qualquer reflexo no mundo do “dia-a-dia” assim que se desliga o aparelho.

A verdade, entretanto, mostra-se, vez após outra, diferente. Golpes digitais somam bilhões de reais em prejuízos a milhares de pessoas, causando danos reais através de um mundo que muitas pessoas acreditavam ser “imaginário”. Esta realidade trouxe preocupações a diversos usuários da rede mundial de computadores, elevando, inclusive, o gasto com segurança digital de diversas empresas, que criaram setores inteiros para proteger seus dados de acessos indevidos, inclusive no Brasil¹⁸.

Entre tais preocupações, uma que vem aumentando de intensidade e abrangendo principalmente o “usuário comum” é a privacidade. Fatos recentes aumentaram, ainda mais, esta preocupação, como, por exemplo, o “*whistleblower*” Edward Snowden¹⁹, trazendo à luz informações sobre a espionagem em massa que vinha sendo realizada pela NSA²⁰ e que atingiu pessoas em vários países, inclusive no Brasil²¹, levantando debates inflamados sobre o acesso a dados particulares de cidadãos por governos e empresas, culminando na edição de diversas legislações como, por exemplo, a Lei 12.965, de 23 de abril de 2014, conhecida como “o Marco Civil da Internet”, no Brasil²².

Esta preocupação com a privacidade, apesar do acelerado aumento nos últimos anos, não é nova, na década de 70 já existiam, inclusive, setores em empresas dedicados à proteção da privacidade dos dados, com a criação de cargos de diretoria, como o de CPO, “*Chief Privacy Officer*”, dedicados única e exclusivamente à proteção da privacidade dos dados, segundo a autora Patricia Peck:

¹⁸ SORIMA NETO, João. Investimento em segurança da informação cresce mais no país; O Globo, 2015. Disponível em <<https://oglobo.globo.com/economia/negocios/investimento-em-seguranca-da-informacao-cresce-mais-no-pais-17645471>>. Acesso em 17 de julho de 2017.

¹⁹ Biography.com Editors. Edward Snowden Biography.com. Disponível em <<https://www.biography.com/people/edward-snowden-21262897>>. Acesso em 28 de agosto de 2017.

²⁰ HIGA, Paulo. Governo dos EUA espiona empresas de tecnologia e registros telefônicos da população; Tecnoblog, 2013. Disponível em <<https://tecnoblog.net/132530/governo-eua-prism-espionagem/>>. Acesso em 7 de julho de 2017.

²¹ HIGA, Paulo. EUA espionaram emails e ligações telefônicas de brasileiros; Tecnoblog, 2013. Disponível em <<https://tecnoblog.net/134719/eua-espionagem-brasil-nsa/>>. Acesso em 7 de julho de 2017.

²² PINHEIRO, Patricia Peck. ob. cit. p. 483.

As regulamentações sobre proteção de dados trouxeram a exigência das empresas terem uma pessoa específica com foco na proteção da privacidade dos dados. A este profissional tem se chamado Chief Privacy Officer (CPO). Isso começou primeiro na Europa, nos anos 70, e teve seu aumento depois nos EUA nos anos 90. O primeiro CPO que se tem origem foi criado na Alemanha (Datenschutzbeauftragter). Mas foi depois de 2001 que de fato houve uma consolidação do uso deste profissional nas empresas.

No início, os segmentos que mais demandavam este perfil de executivo eram os relacionados à saúde e ao mercado financeiro, devido a serem indústrias extremamente regulamentadas, com armazenagem de muita informação sensível sobre os indivíduos e com alta exigência de compliance. Como exemplo, temos a exigência da proteção dos registros de prontuários médicos de paciente pela HIPAA - Health Insurance Portability and Accountability Act (lei de 1996). Outro exemplo é a necessidade de proteção de dados financeiros conferidos pelo Fair Credit Reporting Act com o Disposal Rule e Gramm-LeachBliley Act com o Financial Privacy Rule.

(...)

O CPO é responsável por toda a privacidade dos dados de uma organização, bem como por evitar (combater, prevenir, coibir) vazamentos de informação e qualquer utilização inadequada das bases de dados que venham a ferir as regras para os quais foram obtidos ou leis específicas sobre sua guarda (dependendo do segmento em que a empresa esteja atuando)²³.

Certo é, entretanto, que, em um mundo cada vez mais conectado, a segurança da informação, um dos bens mais preciosos em qualquer empresa, vem sofrendo reiterados acréscimos e, corretamente, deve ser um foco de crescente preocupação das empresas, em especial daquelas que lidam com fluxo massivo de dados de cidadãos.

Todos estes acontecimentos colocaram em foco as gigantes de tecnologia, tais como *Google, Facebook, Amazon*, etc., que lidam com imenso fluxo de dados, muitos dos quais de teor bastante particular. Diversos questionamentos sobre o tratamento, manutenção e uso destes dados foi suscitada, em especial porque, na *internet*, a principal fonte de receita de todos os *sites* é com publicidade e, “no produto gratuito, o produto é você”²⁴.

2.1. O usuário enquanto produto

A *internet* trouxe características muito interessantes para empresários, uma das principais é a possibilidade cada vez mais ágil de selar negócios, uma vez que a diferença de tempo entre anúncios, consulta ao produto e aquisição pelo consumidor é cada vez menor. Neste sentido:

A publicidade na Internet é um ensaio para um mundo de convergência entre a rede mundial de computadores e a *TV broadcasting*, que já existe com a TV Interativa em vários países. A publicidade virtual é bem diferente da tradicional veiculada na TV ou nas demais mídias. A particularidade da mídia

²³ PINHEIRO, Patricia Peck. O que é um Chief Privacy Officer (CPO)?, 2017. Disponível em <<https://web.facebook.com/notes/patricia-peck-pinheiro-advogados/o-que-é-um-chief-privacy-officer-cpo/1339648429452444/>>. Acesso em 16 de junho de 2017.

²⁴ HIGA, Paulo. Na VPN gratuita e ilimitada, o produto é você; Tecnoblog, 2016. Disponível em <<https://tecnoblog.net/195305/vpn-gratis-ilimitado-opera/>>. Acesso em 28 de agosto de 2017.

virtual é que, tecnologicamente, é possível finalizar operações comerciais a partir de um simples anúncio. Assim, o objetivo da publicidade – e seu limite – não é apenas a sedução do comprador: uma vez e imediatamente após o momento em que for seduzido, pode ele adquirir o produto com simples toques no *mouse*. A publicidade *online*, portanto, permite chegar até o final da operação, que é a realização da venda efetiva, principalmente nas novas mídias convergentes como a TV Interativa.²⁵

É assim que Patricia Peck inicia sua abordagem em relação às publicidades *online*. Logo em sequência, trazendo o direito para a relação, continua:

Esse tênue limite entre o momento em que termina o anúncio e aquele em que começa a transação comercial tira o sono dos publicitários e traz uma questão jurídica: de quem serão as responsabilidades no caso de propaganda enganosa? O publicitário não é mais aquele sujeito que opera num mundo em que todas as pessoas são absolutamente lindas e saudáveis e os produtos anunciados funcionam perfeitamente bem. Paradoxalmente, passa a ser quase que como o velho e tradicional vendedor de uma loja do mundo real, tendo de manter o convencimento do consumidor até o momento em que este desembolsa o dinheiro, assina o cheque, ou emite-se o comprovante do cartão de crédito/débito – no caso da Internet, até o momento em que o usuário dá o clique definitivo que finaliza a compra. No mundo real, o vendedor, ou a loja, juntamente com o fornecedor ou fabricante, são responsáveis por um produto que não cumpra as atribuições anunciadas; no mundo virtual, chega-se mais uma vez à questão: onde termina a publicidade e onde começa a transação comercial? Quem é o responsável pelo quê?²⁶

A imensa maioria dos portais na *internet* se sustentam, financeiramente, a partir da publicidade; mas o fazem de maneira diferente dos meios de comunicação “comuns”, isto é, somente acessando o sítio existente no anúncio publicitário é que, em geral, o anúncio é cobrado²⁷, e não a mera existência deste anúncio nela, diferente de um *banner* ou anúncio em jornais e revistas que são remunerados apenas pelo espaço, mas nunca pela ida à loja do consumidor. Na rede mundial de computadores, assim como mostrado pela professora Patricia Peck, é cada vez mais difícil definir o ponto publicitário da efetiva transação comercial, isto faz com que a relação seja muito mais interessante para o anunciante, pois há uma probabilidade real de que seu anúncio torne-se receita em alguns *cliques*. Assim, quando um determinado *website* tem um foco muito bem definido, é mais simples planejar qual espécie de produto ou serviço será anunciado, adquirindo maior eficiência com a publicidade. O problema, contudo, surge em relação a *sites* maiores, que tratam de diversos assuntos, em que tal identificação de qual produto ou serviço deve ser anunciado, para atrair maior atenção, passa a ser mais difícil.

²⁵ PINHEIRO, Patricia Peck. Direito Digital. 6 ed. rev., atual e ampl. São Paulo: Saraiva, 2016. p. 412.

²⁶ PINHEIRO, Patricia Peck. ob. cit. p. 412.

²⁷ Apesar de os anúncios publicitários em domínios na internet aceitarem diferentes formas de contratos, é bastante comum o contrato com “custo por clique” em detrimento do contrato por visualizações, porque, em geral, dão mais certeza ao anunciante de que a chance de venda possa ser maior. Apesar disso, os dois métodos existem e são utilizados. Sobre o tema o próprio *Facebook*, em uma área voltada à empresas que desejem anunciar na rede social, dá excelentes explicações sobre as mecânicas dos dois sistemas. Disponível em <<https://pt-br.facebook.com/business/help/214319341922580>>, e <https://pt-br.facebook.com/business/help/683065845109838?helpref=faq_content#> e <https://www.facebook.com/business/help/146070805942156?helpref=faq_content>. Acesso em 29 de agosto de 2017.

Tal realidade traria, em tese, maior dificuldade em se obter receita para estes grandes veículos de comunicação *online*.

Neste cenário, portanto, a situação de serviços como *Facebook*, uma rede social, ou *Google*, o maior indexador de dados da *internet*, ambos possuindo bilhões de acessos semanais em suas páginas²⁸, torna-se bastante peculiar, afinal, pessoas com diferentes interesses acessam a mesma página e teriam, assim, acesso ao mesmo anúncio publicitário, o qual poderia atrair uns, mas não outros.

A fim de solucionar tal problema, estes portais muniram-se da mineração de dados²⁹, com a intenção de compilar um “perfil” próprio de seus usuários, entendendo seus interesses e, assim, exibindo anúncios publicitários direcionados, capazes de atrair maior atenção e, desta forma, aumentar a receita da página, bem como atrair maior atenção de anunciantes. Esta ferramenta não é usada somente por serviços digitais³⁰, mas, certamente, foi intensificada por ela, pois o uso da inteligência artificial³¹ propicia uma mineração de quantias muito maiores de dados, bem como são capazes de gerar leituras ainda mais precisas sobre os usuários.

É óbvio que há uma relação jurídica entre o usuário e o serviço *online*, ainda que não exista transmissão financeira entre um polo e outro, é inegável tal configuração, uma vez que os serviços *onlines* prestam um serviço e são, por esta razão, responsáveis, ainda que esta

²⁸ Top 20: conheça os sites que mais têm acesso em todo o planeta, 2013. Disponível em <<https://canaltech.com.br/curiosidades/top-20-conheca-os-sites-que-mais-tem-acesso-em-todo-o-planeta-6241/>>. Acesso em 28 de agosto de 2017.

²⁹ A mineração de dados é um processo no qual são cruzadas informações a fim de encontrar padrões e identificar gostos, afinidades e outras situações que tornem o sujeito “pesquisado” mais conhecido. É mediante tal processo que as gigantes de tecnologia conseguem criar anúncios publicitários direcionados a cada usuário que acesse o seu serviço. Ao compilar os dados que o usuário inevitavelmente deixa “para trás” durante sua navegação, como uma trilha de pão, passa-se a ter maior conhecimento sobre ele e, assim, maior eficiência nas publicidades que lhe serão mostradas. Sobre “*data mining*” ver <https://docs.oracle.com/cd/B28359_01/datamine.111/b28129/process.htm#CHDFGCIJ>. Acesso em 03 de setembro de 2017.

³⁰ A mineração de dados passou a ser um importante artifício às gigantes de tecnologia, que podem compilar uma quantidade muito maior de dados do que empresas que não atuam diretamente na *internet*. Mas isso não significa que apenas elas utilizem a ferramenta, um exemplo é uma rede varejista norte-americana que, ao minerar os dados de uma consumidora adolescente, descobriu que ela estava grávida antes que ela fizesse o anúncio à sua família, o que era delicado especialmente em virtude de tratar-se de uma adolescente. Esta descoberta fez com que os anúncios enviados à consumidora fossem relacionados à bebês e à maternidade, o que não agradou ao pai da adolescente, que reclamou junto à empresa. Esta se desculpou ao pai, o qual, tempos depois, descobriu sobre a gravidez da filha. Disponível em <<http://olhardigital.uol.com.br/noticia/varejista-norte-americana-descobre-gravidez-de-clientes-com-a-ajuda-de-software/24231>> e <<http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#622fd83034c6>>. Acesso em 27 de outubro de 2016.

³¹ As Inteligências Artificiais estão se tornando cada vez mais avançadas, sendo capazes, por exemplo, de vencer humanos em jogos de altíssima complexidade, Disponível em <<http://g1.globo.com/tecnologia/noticia/alphago-inteligencia-artificial-do-google-vence-desafio-de-go-contra-melhor-jogador-do-mundo.ghtml>>. Acesso em 03 de setembro de 2017. Seu uso pode ser dos mais variados, mas um, sem dúvida, é o de auxiliar na mineração de dados dos usuários *online*, tarefa para a qual a IA é empregada cotidianamente.

prestação ocorra de maneira “gratuita”. Neste sentido de responsabilização, Patricia Peck leciona:

No Código de Defesa do Consumidor, a responsabilidade pela publicidade enganosa é, via de regra, do fornecedor do bem ou serviço (art. 30), já que estes anúncios são veiculados às expensas daquele (art. 10, §2º). Quando, porém, a forma de propaganda permite que em um clique consumidor e fornecedor possam realizar uma operação de compra e venda, o veículo passa a realizar uma verdadeira relação de intermediação, adquirindo responsabilidades semelhantes às de um corretor, integrando, portanto, a cadeia de consumo.³²

Contudo, a maior crítica não vem em relação ao uso de publicidade como fonte de receita por estes portais, mas sim à falta de transparência em como os dados pessoais dos usuários são manipulados, armazenados e utilizados por estes, que muitas vezes não informam, ou dificultam o acesso à informação, como por exemplo por meio de longos contratos que a imensa maioria não lê por, principalmente, ser leiga em matérias jurídicas³³. Tal situação faz com que muitas pessoas consentam com que suas informações sejam comercializadas, sem que sequer saibam que tal possibilidade existe e, em muitos casos, ocorre, uma vez que esta é uma fonte de receita bastante lucrativa para portais da *internet*³⁴.

2.2 A proteção aos dados pessoais

Os dados pessoais dos usuários dos serviços são, atualmente, um dos ativos mais valorizados na *internet*. Por esta razão a privacidade dos usuários anda lado a lado com a proteção a estes dados armazenados nos servidores das empresas. Neste sentido, a já citada Patricia Peck Pinheiro elabora, em sua obra Direito Digital, uma importante posição sobre a proteção aos dados pessoais em um contexto internacional, a qual citamos:

A segurança da informação sempre encontrou uma barreira natural na privacidade. Afinal, se a monitoração e a vigilância são essenciais para prevenção de incidentes na Sociedade Digital, como fica a questão da privacidade neste mundo tão vigiado?
(...)

³² PINHEIRO, Patricia Peck. ob. cit., nota 365, p. 412.

³³ Esta situação gerou, inclusive, a criação de um *site* voltado a facilitar a compreensão dos gigantescos termos de uso que são encontrados na *internet*, o TL;DR, abreviação para “*too long; didn’t read*”, que, em tradução livre, significa “muito longo; não li”. Este serviço resume os contratos e aponta os pontos que devem ser analisados com maior atenção pelos usuários, auxiliando a evitar “golpes digitais” de serviços que se protegem com estes contratos. Disponível em <<https://tldrlegal.com>>. Acesso em 03 de setembro de 2017.

³⁴ De PABLOS, Susana Pérez. Seus dados são vendidos por 7,5 centavos de dólar. El País, 2017. Disponível em <https://brasil.elpais.com/brasil/2017/05/03/tecnologia/1493835469_309268.html?id_externo_rsoc=FB_BR_CM>. Acesso em 16 de setembro de 2017.

Desde o episódio do 11 de setembro de 2001, os EUA vêm sendo acusados por “vigiar” tudo e a todos através das comunicações digitais. De certo modo, este tema foi um dos que alavancaram a própria aprovação do Marco Civil da Internet brasileira em 2014.

A espionagem internacional digital e a violação da privacidade dos usuários da Internet são alguns dos problemas conhecidos da rede no mundo inteiro, mas por enquanto não existe uma instituição que determine até onde governos, serviços de segurança ou empresas podem ir.

Em 2014 ocorreu em Istambul (Turquia) o Fórum Global da Governança na Internet, um dos espaços mais importantes para tentar encontrar maneiras de melhorar o uso da *web*.

Um dos principais desafios é garantir o apoio dos países para a construção de uma internet realmente global e democrática – entre governos autoritários e preocupações com o terrorismo, os passos dos usuários são cada vez mais vigiados, na ausência de regras internacionais sobre a rede.

O Brasil assumiu um papel de protagonista nestas discussões desde que a presidente Dilma Rousseff questionou em 2013 a espionagem internacional realizada pelos EUA e pediu um novo modelo de governança global da Internet, no plenário da ONU.

Logo, o direito de proteger suas informações privadas é um direito que o Brasil reivindica e quer ver ocorrer na Internet. A governança multissetorial é basicamente a garantia da liberdade de expressão, da privacidade dos indivíduos, do respeito aos direitos humanos, uma governança democrática e multissetorial da Internet.

Embora não tenha poder de decisões ou de acordos, o Fórum Global da Governança da Internet tem a vantagem de amplificar as demandas por práticas mais respeitadas na *web*.

Atualmente, há uma comparação entre a discussão sobre a governança global da Internet e às complexas negociações sobre as mudanças climáticas, que já duram décadas e resultaram em avanços tímidos. Da mesma maneira, cada tema relativo à rede é tratado em um fórum específico e não cabe à ONU dizer o que pode ou não um país fazer do ponto de vista de espionagem de cidadãos.

A natureza público-privada, de interesse coletivo da Internet, exige que sua estrutura seja tratada em um âmbito global. Por exemplo, poderia haver um maior esforço legal para dizer que o fato de um cabo ótico no oceano passar por uma determinada cidade ou país não quer dizer que ele possa ser monitorado, da mesma maneira que eu imagino que, quando envio uma carta, as cidades e países por onde a carta passou não abriram a correspondência.

Por certo, a regulamentação sobre a proteção de dados pessoais é um tema extremamente importante no momento atual da Sociedade Digital. Visto que se presta justamente a regular a atividade de tratamento de dados pessoais, que acabaram se tornando verdadeira “moeda” na Internet, além de compor a avaliação dos ativos de empresas digitais.³⁵

Os dados pessoais são, atualmente, um dos maiores ativos de qualquer serviço na *internet*. Como exemplo podemos citar as mais diversas aquisições das gigantes de tecnologia, as quais visam, se não comprar patentes e propriedades intelectuais, certamente o domínio de catálogos completos de dados pessoais de seus usuários³⁶, o que, como visto, é o caminho para anúncios mais eficientes e, conseqüentemente, maior receita financeira advinda da publicidade *online*.

A ausência de políticas públicas sobre o uso dos dados pessoais dos usuários, somado ao fato de cada país possuir legislações diversas e entendimentos próprios sobre o limite da privacidade, faz com que seja bastante difícil uma proteção efetiva sobre a privacidade dos

³⁵ PINHEIRO, Patricia Peck. ob. cit. p. 481-483.

³⁶ A aquisição do *WhatsApp* pelo *Facebook* certamente se enquadra neste caso como um exemplo emblemático, uma vez que o uso do aplicativo de mensagens cresce de maneira intensa, ao possuir dados de seus usuários pode haver mais eficiência na mineração de dados para que os anúncios da rede social sejam cada vez mais rentáveis. Este fato tornou-se claro quando o *Facebook* passou a permitir, por padrão, o compartilhamento de informações do aplicativo com a rede social. Disponível em < <http://www.techtudo.com.br/noticias/noticia/2016/08/whatsapp-comeca-compartilhar-dados-com-facebook-entenda-o-que-muda.html>>. Acesso em 20 de novembro de 2016.

cidadãos digitais. Em especial porque as maiores empresas que utilizam os dados são particulares e, como tais, buscam lucro, muitas vezes não possuindo a mesma preocupação ética com os dados pessoais dos usuários de seus serviços como deveriam.

Fato é, entretanto, que até mesmo alguns órgãos estatais cogitam a possibilidade de utilizar os dados pessoais para aumentar receitas, ou diminuir despesas. A Prefeitura de São Paulo, por exemplo, tem feito estudos para tornar o “Bilhete Único”, cartão que integra metrô, trens e ônibus no município de São Paulo, mais inteligente. O problema que surgiu, entretanto, é que estes estudos esbarraram na privacidade dos usuários do sistema, os quais poderiam ver seus dados, entregues ao governo de boa fé, vendidos, afinal a maioria dos cidadãos acredita que o governo não fará o mesmo uso comercial de suas informações que o fazem outros serviços³⁷.

Ao falarmos de *internet*, tratamos, usualmente, de empresas particulares. E ao discutir privacidade em relação a elas, recorremos a entidades governamentais. A verdade, entretanto, é que não pode ser deixado ao governo criar, sozinho, leis e diretrizes sobre o assunto, sob risco de engessar o sistema digital, que só se tornou o que é hoje graças à sua capacidade única de oferecer uma certa “liberdade” aos seus usuários.

Da mesma maneira que não se pode relegar a gestão digital à governos, deve-se cobrar deles o mesmo cuidado com os dados pessoais de seus cidadãos, se não um cuidado maior, dado que as informações que eles detêm são, sem dúvidas, muito maiores do que as informações que serviços *online* possuem, uma vez que se tratam de dados extremamente mais sensíveis, desde documentos pessoais até registros financeiros. A vida digital trouxe benefícios, os quais devem ser aproveitados para facilitar a vida de todos, tanto do Estado, quanto de sua população, mas a privacidade dos cidadãos e a gestão de seus dados pessoais deve ser tratado como questão de suma importância e possuir a privacidade adequada nas discussões que vierem a implementar maior uso da tecnologia nos dados geridos pelos governos³⁸

³⁷ DANTAS, Tiago; DANTAS, Dimitrius. Doria oferece dados de usuários do Bilhete Único à iniciativa privada, O Globo, 2017. Disponível em < <https://oglobo.globo.com/brasil/doria-oferece-dados-de-usuarios-do-bilhete-unico-iniciativa-privada-20942133>>. Acesso em 03 de setembro de 2017.

³⁸ O governo tem tentando criar ferramentas que facilitem o acesso às informações da população por órgãos governamentais ao mesmo tempo em que facilitam a vida dos cidadãos em possuir suas identidades. Porém ao se informatizar esse conteúdo, é preciso tomar preocupações com relação à privacidade. Sobre o tema, a criação de uma identidade única é, sem dúvida, um importante passo no caminho de se facilitar a vida diária, mas ao se compilar diversos dados em um só sistema, passa a existir maior possibilidade de, com um vazamento, mais dados caírem nas mãos de criminosos e, a partir daí, a possibilidade lesiva deste acesso indevido cresce. Em relação ao assunto, ver < <http://www1.folha.uol.com.br/mercado/2017/05/1887331-identidade-unica-facilitara-dia-a-dia-mas-privacidade-de-dados-sera-desafio.shtml>>. Acesso em 10 de agosto de 2017.

Outra situação que acirrou debates acerca dos dados pessoais dos usuários é o local onde estes são armazenados. A *internet* possibilitou que uma empresa possa existir em determinado país e atuar em outro, diferente. Tal realidade faz com que situações delicadas, em relação à privacidade, possam ocorrer, pois a legislação do país onde se atua poderá ser diferente daquela onde a empresa está sediada. Tal realidade foi, inclusive, objeto de intenso debate quando da discussão legislativa do “Marco Civil da Internet”, pois alguns legisladores queriam que os dados dos brasileiros fossem armazenados localmente, e não no exterior. Até mesmo judicialmente esta discussão aconteceu e causou um embate entre o judiciário e o próprio *Facebook* sobre o acesso aos dados e a sua localização³⁹.

O problema, contudo, em se armazenar as informações localmente é o aumento de custo das empresas, pois isso faria com que elas tivessem de investir em infraestrutura para armazenar todas estas informações, o que poderia tornar o negócio insustentável e, conseqüentemente, interromper o serviço neste país. Um situação como esta não é desejável, por seguir em caminho oposto ao que se deseja atingir com a *internet*, que é um mundo cada vez mais conectado.

Ademais, ao falarmos sobre a proteção de dados pessoais e privacidade, um assunto cuja discussão também tem se tornado de elevada importância é o direito de ver informações pessoais apagadas da rede mundial de computadores, o chamado “direito ao esquecimento”.

3. DIREITO AO ESQUECIMENTO

O Direito ao Esquecimento consiste em uma pessoa ter fatos ligados a si “esquecidos” após um certo lapso temporal em que a existência dessa informação não se faça mais necessária para o restante da sociedade. Tal direito se faz através da não veiculação destes fatos novamente pela mídia ou da desindexação de notícias antigas de buscadores, como o *Google*. Contudo, nas “novas formas de mídias, principalmente a Internet, a propagação rápida da informação cria também outra adversidade: a armazenagem de forma duradoura, dificultando qualquer tipo de esquecimento da informação.”⁴⁰. Isto é, o armazenamento em um caráter quase perpétuo propiciado pela internet faz com que as informações não sejam tão facilmente “esquecidas”,

³⁹ MAIA, Felipe. Dado armazenado no exterior acirra atrito entre Facebook e autoridades. Folha de São Paulo, 2016. Disponível em < http://www1.folha.uol.com.br/mercado/2016/07/1796861-dado-armazenado-no-exterior-acirra-atrito-entre-facebook-e-autoridades.shtml?utm_campaign=website&utm_source=sendgrid.com&utm_medium=email>. Acesso em 10 de outubro de 2016.

⁴⁰ PINHEIRO, Patricia Peck. Direito Digital. 6 ed. rev., atual e ampl. São Paulo: Saraiva, 2016. p. 490.

uma vez que estas encontram-se disponíveis por um período de tempo quase indefinido e cada vez mais acessível a quem quer que seja, tendo em vista a globalização veloz do acesso à internet e ao conhecimento crescente das pessoas em lidar com a ferramenta.

O Direito ao Esquecimento gera, ainda, outro debate acerca do acesso à informação. Tem-se, desta forma, direitos contrapostos, se por um lado deve-se preservar o direito à privacidade e, consequentemente, à dignidade, por outro não se pode ignorar o direito de acesso à informação e à liberdade de expressão por parte dos cidadãos. A União Europeia recentemente decidiu a respeito do Direito ao Esquecimento, aceitando-o como um direito dos cidadãos à privacidade quando informações existentes sobre si forem “incorretas, inadequadas, irrelevantes ou excessivas”⁴¹, sustentando, ainda, que deve ser realizada uma análise de “caso a caso” em que deverá ser levado em conta a relevância da informação para a sociedade e, inclusive, o papel que a pessoa sobre qual a informação trata tem para o público em geral – se é uma pessoa de interesse público ou não, como políticos e afins –, a fim de verificar se trata-se de uma informação passível ou não de ser “esquecida”.

Outro questionamento que se levanta ao se debater a respeito deste direito é a quem recai a análise de quais informações são ou não “incorretas, inadequadas, irrelevantes ou excessivas” e, portanto, a decisão de que elas devem ser “esquecidas”? Não parece sustentável repassar esta incumbência a serviços particulares, como o *Google*, muito menos parece seguro depender única e exclusivamente de uma empresa particular para tal tarefa. Atualmente, na União Europeia⁴², esta função tem sido delegada às empresas particulares em detrimento de órgãos públicos, ainda que esses estejam sujeitos à uma análise posterior pelo Poder Público, o que tem gerado certo receio a respeito da idoneidade e do interesse, bem como na concentração excessiva de decisões a respeito de informações pessoais de cidadãos, que uma organização particular terá ao lidar com os pedidos de Direito ao Esquecimento.

Ademais, mais um problema que advém diz respeito ao caráter cíclico das informações, até quando uma informação deverá ser esquecida? Indefinidamente? Ou deverá haver um outro lapso temporal que poderá remover esta informação do rol de informações a serem esquecidas? Porque se, por exemplo, uma informação a respeito de determinada pessoa que, até aquele momento, não fazia parte da vida pública, mas posteriormente passa a fazer, seja por iniciar participação na vida política ou por qualquer outro motivo, foi esquecida, não significa que esta informação seja irrelevante *ad eternum*, uma vez que este início de participação na vida pública

⁴¹ European Commission: Factsheet on the “Right to be Forgotten” ruling. Disponível em: <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf>.

⁴² Ibidem.

pode fazer com que esta mesma informação passe a ser relevante para a sociedade ainda mais do que o direito desta pessoa à privacidade, devendo, assim, ser reindexada e mantida ao alcance, para acesso dos cidadãos. Como regular uma situação como esta? Deveria haver um novo lapso temporal em que uma reanálise deveria ser feita?⁴³.

Todos estes questionamentos tornam evidente a necessidade de uma discussão acadêmica, que deve ser feita, inclusive, a nível global, dado o caráter internacional da internet. Parece claro que os Estados devem preocupar-se com o tema, mas ao mesmo tempo é necessário um cuidado para não existir um “excesso burocrático” no qual obrigue-se à pessoa interessada em ter sua privacidade preservada, ao invocar o Direito ao Esquecimento, sujeitar-se a um extenuante procedimento judicial para ver seu desejo satisfeito.

Se, por um lado, o Direito ao Esquecimento na internet é dificultoso – dado o caráter cíclico que as informações têm na rede mundial de computadores, por exemplo com o retorno de uma informação antiga após certo período como se fosse recente (em especial o caso das correntes ou dos boatos relacionados a diversos assuntos, por exemplo) – por outro, sua garantia parece coerente com o direito à privacidade, à intimidade e à dignidade da pessoa humana.

Contudo, o direito à informação e à liberdade de expressão, do outro lado da balança, não podem ser ignorados e também devem ser sopesados quando se discute o direito de um indivíduo ao esquecimento. Em uma situação clara de conflito de direitos fundamentais como esta, será que realmente é sensato delegar a função de analisar e decidir às empresas particulares? Se sim, deve haver alguma limitação? E, se não, até que ponto os Estados devem se envolver e de que forma devem fazê-lo?

3.1. Conflito entre o direito à privacidade e o direito ao acesso à informação

A colisão de normas fundamentais é matéria de intenso debate e difícil decisão, no ramo teórico beira a impossibilidade de uma conclusão unânime. Embora alguns pareçam se sobressair diante de outros, como, por exemplo, ocorre com o direito à vida, sem o qual não se poderia exercer nenhum outro direito, outros podem variar de valoração de caso a caso, não sendo coerente – ou sequer adequado – definir um valor específico a um ou a outro sem que existam casos concretos que possam definir a importância de cada princípio em conflito.

⁴³ Blog Harvard, 2014. Righting the right to be forgotten. Disponível em: <<http://blogs.harvard.edu/futureoftheinternet/2014/07/14/righting-the-right-to-be-forgotten/>>.

Sobre o tema, Gilmar Mendes e Paulo Gustavo Branco dizem que “Fala-se em colisão entre direitos fundamentais quando se identifica conflito decorrente do exercício de direitos individuais por diferentes titulares.”⁴⁴, os autores continuam, em relação à uma possível hierarquização de direitos fundamentais:

Questão embaraçosa refere-se ao direito ou bem que há de prevalecer no caso de colisão autêntica. Formulada de maneira explícita: quais seriam as possibilidades de solução em caso de conflito entre a liberdade de opinião e de comunicação ou a liberdade de expressão artística (CF, art. 5º, IX)⁴⁵ e o direito à inviolabilidade da intimidade, da vida privada, da honra e da imagem (CF, art. 5º, X)? (...)

É possível que uma das fórmulas alvitadas para a solução de eventual conflito passe pela tentativa de estabelecimento de uma *hierarquia* entre direitos fundamentais.

Embora não se possa negar que a unidade da Constituição não repugna a identificação de normas de diferentes pesos numa determinada ordem constitucional, é certo que a fixação de rigorosa hierarquia entre diferentes direitos acabaria por desnaturá-los por completo, desfigurando, também, a Constituição como complexo normativo unitário e harmônico. Uma valoração hierárquica diferenciada de direitos individuais somente é admissível em casos especialíssimos.⁴⁶

Assim, percebe-se que a tarefa de definir, em relação ao Direito ao Esquecimento, qual direito fundamental se sobressai, se o direito à privacidade ou à liberdade de expressão e de informação, não é somente árduo, mas, também, perigoso.

Não se faz possível – e sequer coerente – definir de maneira pétreia qual princípio fundamental seria superior, por esta razão, acertadamente, a Comissão Europeia deixou claro que a situação deve ser analisada “caso a caso”, verificando-se o que se sobressai naquela situação específica. Se decidíssemos qual é superior em uma discussão teórica, estar-se-ia sob o risco de atirar ao esquecimento informações relevantíssimas à população, ou, em contrapartida, de escancarar indefinidamente erros que não prejudicam mais ninguém além do agente que os cometeu. Apenas o caso concreto pode nos dar qual direito se sobressai e qual deve ser resguardado em detrimento do outro, razão pela qual, embora discutamos o tema sob um ponto de vista teórico, jamais poderemos nos afastar do debate prático que o direito nos proporciona.

Esta é a razão, inclusive, pela qual se traz exemplos a este debate, a fim de lastrear a ponderação quando diante de casos práticos de conflito entre os direitos em comento. Ou seja, como já se mencionou, se se tem entre os polos da relação, elevado interesse público, como

⁴⁴ MENDES, Gilmar Ferreira, BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 8 ed. rev. e atual. São Paulo: Saraiva, 2013. p. 235.

⁴⁵ Trata-se aqui da Constituição Federal Brasileira.

⁴⁶ MENDES, Gilmar Ferreira, BRANCO, Paulo Gustavo Gonet. ob. cit. p. 237.

quando se tratar de pessoa pública, seja político ou alguém envolvido com diversas pessoas, o direito à privacidade deste indivíduo possivelmente terá valor menor em relevância do que o direito à informação da sociedade. Contudo, mesmo isso não é absoluto, afinal, quando se está diante de uma pessoa pública que quer ver uma informação sobre imagens íntimas suas que vieram à público quando era mais jovem, não haveria qualquer sentido em preponderarmos o direito à informação no presente caso. Qual a relevância desta informação à sociedade? Nenhuma. Agora, qual a relevância de protegermos a privacidade desta pessoa, ainda que pública, nesta situação? Completa.

É exatamente este, inclusive, o entendimento da Suprema Corte brasileira:

No que se refere à tensão entre a liberdade de expressão e de crítica e o direito à honra e à intimidade, existe, no Supremo Tribunal Federal, precedente que reconhece a possibilidade de *diferenciações*, consideradas as diferentes situações desempenhadas pelos eventuais envolvidos. Assim, admite-se, tal como na jurisprudência de outros países, que se estabeleçam critérios diversos para a aferição de possível lesão à honra tendo em vista a maior ou a menor exposição pública das pessoas.⁴⁷

Ou seja, como já citado, nem o direito à privacidade, no excerto melhor exposto como direito à honra, é supremo, nem o direito à liberdade de acesso à informação o é. Ambos devem ser analisados à luz situações concretas, capazes de demonstrar qual prevalecerá sobre o outro em virtude tanto da exposição pública das pessoas do caso, como da informação ali discutida. A obra citada traz, ainda, citação ao julgado no *Habeas Corpus* nº 78.426:

Crime contra a honra e a vida política. É certo que, ao decidir-se pela militância política, o homem público aceita a inevitável ampliação do que a doutrina italiana costuma chamar a *zona di illuminabilità*, resignando-se a uma maior exposição de sua vida e de sua personalidade aos comentários e à valoração do público, em particular, dos seus adversários; mas a tolerância com a liberdade de crítica ao homem público há de ser menor, quando, ainda que situado no campo da vida pública, do militante político, o libelo do adversário ultrapasse a linha dos juízos desprimorosos para a imputação de fatos mais ou menos concretos, sobretudo se invadem ou tangenciam a esfera da criminalidade: por isso, em tese, pode caracterizar o delito contra a honra (...).⁴⁸

Toma-se a liberdade, em relação ao julgado citado, de inserirmos a possibilidade do Direito ao Esquecimento. Por tratar-se de decisão antiga, de 1999, o termo e a discussão deste direito não estavam em voga, mas entende-se plenamente possível e plausível sua anexação a este direito à honra mencionado, uma vez que similares na espécie.

⁴⁷ MENDES, Gilmar Ferreira, BRANCO, Paulo Gustavo Gonet. ob. cit. p. 249.

⁴⁸ HC 78.426, Rel. Min. Sepúlveda Pertence, julgado em 06 de março de 1999, 1ª Turma, DJ de 7 de maio de 1999.

O Ministro Gilmar Mendes e Paulo Gustavo Branco, seguem, em análise da citada decisão, versando que:

Vê-se aqui que também o Supremo Tribunal Federal define tópicos (*topoi*) que hão de balizar o complexo de ponderação, fixando-se que os homens públicos estão submetidos a exposição de sua vida e de sua personalidade e, por conseguinte, estão obrigados a tolerar críticas que, para o homem comum, poderiam significar uma séria lesão à honra. Todavia, essa orientação, segundo o Supremo Tribunal Federal, não outorga ao crítico um *bill* de indenidade, especialmente quando imputa a alguém a prática de atos concretos que resvalam para o âmbito da criminalidade.

(...)

De ver-se, portanto, que a solução para a colisão entre direitos fundamentais dar-se-á à luz da situação concreta trazida ao Tribunal.⁴⁹

Assim, evidente que há necessidade de análise concreta para eventual ponderação entre os direitos conflitantes. Sendo, por isso, impossível falar-se em hierarquização em sentido teórico destes princípios.

Destarte, retoma-se questionamentos já trazidos anteriormente, mas que agora, com maior sustentação, passamos a realizar, uma vez que apenas a presença de casos práticos nos permitiria indagar qual direito sobressai em relação a outro, até que ponto os Estados devem se envolver, ou se abster, e de que forma devem fazê-lo? Será que é mesmo sensato e correto deixar toda esta análise à iniciativa privada?

3.2. A importância de uma postura estatal

Ante o que já foi apresentado, e questionado, acredita-se que os Estados devem sim tomar uma posição, sem, contudo, impor-se de maneira excessiva que possa limitar o avanço e as liberdades que advieram com a internet. Ou seja, deve haver uma parceria entre as empresas particulares e o Poder Público no que se refere ao tratamento do Direito ao Esquecimento.

Globalmente tem avançado a tutela jurídica sobre o tema, em especial na Europa, que decidiu sobre o assunto em 2012. Entretanto, dada a velocidade que a internet possui, os avanços dos Estados encontram-se lentos no tratamento do assunto, sendo que muitos não possuem qualquer legislação sobre ele.

No Brasil a primeira orientação jurídica sobre o Direito ao Esquecimento veio com o Enunciado 531 da VI Jornada de Direito Civil, que diz, *in verbis*, “**A tutela da dignidade da**

⁴⁹ MENDES, Gilmar Ferreira, BRANCO, Paulo Gustavo Gonet. ob. cit. p. 249-250.

pessoa humana na sociedade da informação **inclui o direito ao esquecimento.**” (g.n.), fundamentando no artigo 11 do Código Civil Brasileiro, e sustentando a seguinte justificativa:

Os danos provocados pelas novas tecnologias de informação vêm-se acumulando nos dias atuais. O direito ao esquecimento tem sua origem histórica no campo das condenações criminais. Surge como parcela importante do direito do ex-detento à ressocialização. Não atribui a ninguém o direito de apagar fatos ou reescrever a própria história, mas apenas assegura a possibilidade de discutir o uso que é dado aos fatos pretéritos, mais especificamente o modo e a finalidade com que são lembrados.⁵⁰

No restante do mundo, em igual forma, o Direito ao Esquecimento ainda não possui um tratamento em evidência. São poucos os países que já legislaram sobre o assunto, restando, em geral, apenas decisões dos tribunais sobre o tema, uma vez que a provocação com casos concretos é mais comum, dado que a velocidade de transformação da sociedade é imensamente superior à legislativa.

Como exemplo podemos citar o Chile, no qual o Direito ao Esquecimento surge, também como no Brasil, como um direito de ex-detentos à ressocialização. Não se fala, ainda, em Direito ao Esquecimento no aspecto digital, ou de uma forma mais ampla, estendendo-se às situações mais cotidianas. Apesar de existirem esparsas e raras legislações sobre o tema.

A Europa é, como já mencionado, o principal cenário do debate, mas mesmo lá existem países que ainda não se mobilizaram para discutir e legislar acerca do assunto.

Apesar de existir quem acuse o Direito ao Esquecimento como uma forma de censura⁵¹, acredita-se ser importante uma definição legislativa sobre o tema, a fim de se evitar eventuais abusos e contradições. Inclusive a fim de evitar que seja usado como forma de censura, cerceando o acesso da população a informações imprescindíveis ao debate democrático. Neste sentido, Patricia Peck Pinheiro assevera:

No Brasil e em vários países, já há decisões favoráveis ao “direito ao esquecimento”, ou seja, em plena era da informação, um dos direitos do indivíduo seria o de justamente deixar com que um determinado fato ficasse no passado! Isso porque, em casos excepcionais, este “apagamento” é benéfico para os envolvidos e para toda a sociedade.⁵²

A atuação estatal possui, ainda, relevante importância quando verifica-se que, atualmente, a maior parte da análise sobre os pedidos de Direito ao Esquecimento são direcionados às empresas privadas, como o *Google*, sendo que o procedimento para apuração

⁵⁰ Justificativa do Enunciado 531 da VI Jornada de Direito Civil do Conselho da Justiça Federal Brasileira.

⁵¹ Folha de São Paulo. Reportagem publicada originalmente em 07 de agosto de 2016. Disponível em <<http://www1.folha.uol.com.br/cotidiano/2016/08/1799831-direito-ao-esquecimento-nao-existe-e-e-usado-para-censura-afirma-advogada.shtml>>.

⁵² PINHEIRO, Patricia Peck. ob. cit. p. 493.

do caso e a decisão de remoção ou não do conteúdo acabam competindo única e exclusivamente a estas empresas, sem qualquer participação estatal. Isto é perigoso e passível de gerar imensa instabilidade. Pense-se, por exemplo, uma situação em que o *Google* decida remover um conteúdo que era considerado relevante à população, mas, por interesses particulares desta empresa, percebeu-se melhor a sua desindexação do buscador.

Há visível prejuízo à sociedade que, aliado à ausência de verificação estatal, possivelmente não será descoberto. Quando verifica-se o inverso, ou seja, a negação do Direito ao Esquecimento por parte da empresa particular, há, ao menos, a possibilidade de nos socorrermos ao judiciário, o que poderia sanar eventual arbitrariedade lesiva ao indivíduo. Contudo, como exposto, o mesmo não se pode dizer da informação desindexada indevidamente, que pode, muitas vezes, sequer ser percebida, tornando-se assim, “esquecida” de forma claramente irregular.

É por esta razão que acreditamos relevante e imprescindível uma atuação estatal, legislando sobre o tema e atuando diretamente em sua execução, a fim de evitar censuras e arbitrariedades indevidas. Ressaltamos, porém, que esta atuação governamental não deve, em hipótese alguma, ser feita de forma a burocratizar excessivamente o instituto, sob pena de contribuir à não aplicação do direito, e não o contrário, que é o que se busca. A internet é uma ferramenta ágil e assim deve ser mantida, razão pela qual ao buscarmos uma atuação estatal, esta deve acompanhar essa agilidade da vida *online*, e não o contrário.

Casos recentes trouxeram esse embate entre Estado e empresas particulares a um maior enfoque. Situações de bloqueio do aplicativo de mensagens *WhatsApp*, ou até mesmo a remoção de um serviço completo do ar por infringir direitos autorais mostra que, embora parece ser um território sem lei, à moda faroeste dos filmes norte-americanos, há, claramente, uma disputa por um controle da rede. O problema é que este controle vai, na maioria das vezes, na contramão do direito à privacidade.

4. CASOS CONCRETOS SOBRE A PRIVACIDADE NA INTERNET

É inevitável que quando nos encontramos diante de discussões de privacidade exista um choque entre outros princípios jurídicos. Existem alguns casos marcantes que aconteceram em tempos recentes que inflamaram ainda mais este debate sobre a privacidade e, até mesmo, sobre a interferência governamental na *internet*.

Um destes casos em relação à privacidade suscitou inúmeros questionamentos sobre qual era o tratamento dado pelo *Google* aos dados pessoais armazenados em seus servidores, tratou-se de um caso bastante sensível, envolvendo pedofilia.

Em 2014 o *Google* identificou imagens armazenadas no *Gmail*⁵³ do cidadão norte-americano John Skillern que possuíam conteúdo pedófilo. A empresa, então, alertou o *National Center for Missing and Exploited Children* (NCMEC – Centro Nacional para Crianças Desaparecidas e Exploradas, em tradução livre). A polícia de Houston, Texas, com o acesso a essa informação, obteve um mandado e prendeu o suspeito, verificando, durante o processo, que as imagens existiam, o que fez com que ele fosse sentenciado posteriormente⁵⁴.

Embora esta ação tenha terminado com a prisão de um homem que possuía imagens de abuso infantil, a postura do *Google* deu margem à inúmeras indagações sobre o acesso da empresa ao material pessoal armazenado em seus servidores pelos usuários. Até que ponto a privacidade deveria existir? E a partir de qual situação estar-se-ia cruzando uma linha e violando este direito à privacidade do usuário em manter seus dados pessoais fora do alcance de quem quer que seja? É correto que a empresa tenha acesso aos dados de seus usuários desta maneira?

Há defensores para os dois lados, uns aceitam uma flexibilização da privacidade, conquanto esta possa fazer com que infratores sejam identificados e capturados. Outros, em sentido contrário, acreditam que a privacidade não pode ser invadida desta maneira, ainda que o conteúdo seja ilícito⁵⁵.

A complexidade da situação, entretanto, tem início quando governos pressionam empresas de tecnologia a criarem *backdoors*⁵⁶ para que possam ter acesso às informações de cidadãos que sejam pessoas de interesse.

Um caso recente envolvendo o judiciário brasileiro foi o bloqueio do serviço de mensagens *WhatsApp*, pertencente ao *Facebook*, devido ao fato de esse não entregar

⁵³ Serviço de *e-mails* (endereços eletrônicos) gratuito do *Google* e o segundo mais usado no mundo atualmente <<http://emailclientmarketshare.com>>, inclusive por empresas.

⁵⁴ HAMANN, Renan. Algoritmo da Google ajuda polícia americana a prender pedófilo. *Tecmundo*, 2014. Disponível em <<https://www.tecmundo.com.br/crime-virtual/60067-google-ajuda-policia-americana-prender-pedofilo.htm>>. Acesso em 15 de setembro de 2017.

⁵⁵ PINHEIRO, Patricia Peck. ob. cit. p. 94-108.

⁵⁶ O conceito de *backdoor* é: “O *backdoor* é um recurso utilizado por diversos malwares para garantir acesso remoto ao sistema ou à rede infectada. Para esse fim, os códigos maliciosos podem explorar falhas críticas não documentadas existentes em programas instalados, falhas características de softwares desatualizados ou do *firewall*, para abrir portas do roteador. Alguns *backdoors* podem ser explorados por sites maliciosos, através de vulnerabilidades existentes nos navegadores. As falhas podem garantir acesso completo ou parcial ao sistema por um *cracker*, sendo utilizadas para a instalação de outros malwares ou para o roubo de dados.” Disponível em <<http://www.psafes.com/blog/backdoor/>>. Acesso em 17 de setembro de 2017.

informações sobre uma quadrilha às autoridades que investigavam suas atividades. O *WhatsApp* defendeu-se alegando não ter acesso às informações desejadas, por encontrarem-se criptografadas de uma maneira que nem mesmo a empresa poderia acessar os dados. O judiciário, não aceitando tal postura, determinou o bloqueio do serviço de mensagens em todo o território nacional, o qual permaneceu indisponível a todos os cidadãos brasileiros durante 24 horas⁵⁷, antes de ser reativado após a suspensão da decisão.

Esta não foi a primeira⁵⁸ vez que tal fato ocorreu, bem como não foi a última tentativa de bloqueio do serviço em território nacional⁵⁹. Todas com a mesma intenção, obter dados dos usuários do serviço para uma investigação. Apesar de ser legal esta solicitação de dados por parte do judiciário e, de certa forma, interessante à sociedade a colaboração da empresa com as autoridades, para o fim de capturar infratores. Não deve ser aceita a postura impositiva da maneira como vem sendo feita. O *WhatsApp* se pronunciou a respeito destas solicitações alegando, em todas as vezes, que não tinha acesso aos dados solicitados em virtude do sistema de criptografia que adotava. O que o judiciário queria, entretanto, era que a própria empresa criasse uma maneira de contornar esta segurança para que os dados requisitados fossem disponibilizados às investigações.

Este fato não é restrito ao Brasil e, muito menos, ao *WhatsApp*. A *Apple*, produtora do aparelho celular *iPhone*, travou intensa batalha com as autoridades norte-americanas por recusar-se a desbloquear um aparelho de um suspeito de terrorismo, sob a alegação de que tal situação além de não ser possível em virtude da tecnologia de segurança empregada, feria o direito à privacidade de todos os usuários do sistema da empresa, pois poderia representar risco à segurança das informações caso existisse um meio de se desbloquear um aparelho sem que fosse necessário o uso da senha do usuário para tanto. O *FBI* (órgão de investigação federal norte-americano) exigiu auxílio para que o desbloqueio fosse efetuado, porque o aparelho estava protegido por uma ferramenta da empresa que apaga os dados após muitas tentativas

⁵⁷ HIGA, PAULO. Justiça manda operadoras bloquearem WhatsApp no Brasil por 72 horas. Tecnoblog, 2016. Disponível em <<https://tecnoblog.net/195057/justica-bloqueio-whatsapp-brasil-72-horas/>>. Acesso em 15 de setembro de 2017.

⁵⁸ PRADO, Jean. Justiça manda operadoras bloquearem WhatsApp no Brasil por 48 horas. Tecnoblog, 2015. Disponível em <<https://tecnoblog.net/189494/justica-bloqueio-whatsapp-brasil-48-horas/>>. Acesso em 15 de setembro de 2017.

⁵⁹ HIGA, Paulo. De novo: Justiça determina bloqueio do WhatsApp em todo o Brasil. Tecnoblog, 2016. Disponível em <<https://tecnoblog.net/198626/justica-bloqueio-whatsapp-brasil-de-novo/>>. Acesso em 15 de setembro de 2017.

incorretas de desbloqueio. A justiça norte-americana determinou que a empresa realizasse tal desbloqueio, mas, ainda assim, a *Apple* negou categoricamente este auxílio⁶⁰.

O *FBI* conseguiu, entretanto, acesso ao aparelho, sem informar, contudo, a maneira que utilizou para tal acesso. A *Apple* emitiu um comunicado no qual questionou, mais uma vez, a proteção à privacidade dos dados de seus usuários e solicitando um debate a respeito dos direitos civis e da segurança dos cidadãos, parte do teor do comunicado era:

A Apple acredita profundamente que cidadãos dos EUA e de outras partes do mundo merecem proteção aos seus dados, segurança e privacidade. Sacrificar um desses itens em detrimento de outro só coloca as pessoas e países em grande risco.

Este caso levantou questões que merecem uma discussão nacional sobre nossas liberdades civis e nossa segurança coletiva e privada. A Apple continua comprometida em participar dessa discussão.⁶¹

O grande problema com esta criação de um *backdoor* para que autoridades usem nas investigações é, além de possíveis abusos estatais, que podem facilmente ocorrer, conforme visto com a espionagem realizada pela *NSA* sobre diversos cidadãos em vários países do mundo⁶², é que a criação deste tipo de sistema que permita o acesso aos dados de um aparelho ou serviço não ficará sob exclusividade de governos. A chance de pessoas mal intencionadas, conhecidas popularmente como *hackers* ou *crackers*, se utilizarem destas ferramentas para obter acesso indevido aos dados de outros usuários, utilizando-se para fins próprios e que causam danos, é grande.

Um exemplo desta realidade, inclusive, ocorreu no ano de 2017, quando descobriu-se que diversas brechas em sistemas eram utilizadas pela própria *CIA* (*Central Intelligence Agency* – Agência de Inteligência Central Norte-Americana) para obter acesso remoto aos dados de alvos de espionagem. A agência utilizava-se de vírus, *malwares*, cavalos de troia e afins para explorar vulnerabilidades em diversos sistemas e espionar seus alvos a partir destas falhas. Curiosamente, o sistema de espionagem foi descoberto utilizando as mesmas ferramentas, e as informações foram entregues ao *website WikiLeaks*⁶³, famoso por vazamentos de informações confidenciais de diversas autoridades governamentais ao redor do mundo e cujo fundador, Julian Assange, encontra-se sob asilo do Equador, em uma embaixada deste país em Londres,

⁶⁰ BROWN, John Murray. Após ordem judicial, Apple se recusa a desbloquear iPhone de terrorista. Folha de São Paulo, 17 de fevereiro de 2016. Disponível em <<http://www1.folha.uol.com.br/mundo/2016/02/1740337-apos-ordem-judicial-apple-se-recusa-a-desbloquear-iphone-de-terrorista.shtml>>. Acesso em 15 de setembro de 2017.

⁶¹ PRADO, Jean. *FBI conseguiu acessar os dados de um iPhone sem ajuda da Apple. Estamos perdidos?*. Tecnoblog, 2016. Disponível em <<https://tecnoblog.net/193403/fbi-iphone-criptografia-quebrada/>>. Acesso em 17 de setembro de 2017.

⁶² PINHEIRO, Patricia Peck. ob. cit. p. 96.

⁶³ Disponível em <<https://wikileaks.org>>.

na Inglaterra⁶⁴, este vazamento ficou conhecido como *Vault 7*, sendo o número de documentos obtidos e vazados para o público um verdadeiro recorde⁶⁵.

É por esta razão que a criação proposital de maneiras para contornar a segurança de aparelhos, sistemas e serviços é tão perigosa, pois deixam os usuários vulneráveis a mais pessoas do que aquelas que inicialmente teriam acesso às ferramentas. E é por isso que, ainda que a pressão de governos seja grande para que isso aconteça, este acesso não pode ser concedido, pois os dados pessoais dos cidadãos devem ser preservados. Deve existir um limite para que autoridades governamentais controlem a vida de seus cidadãos e, embora a linha a ser traçada ainda seja discutível, este, em particular, é um ponto no qual ela definitivamente não pode ser atravessada.

O problema, entretanto, reside na força de pressão de governos como o norte-americano, que chegou, inclusive, a retirar do ar um *website* por problemas de infração de direitos autorais e acusações de lavagem de dinheiro. Tal fato demonstraria, por si só, o poder de governos na *internet*; mas este caso em particular vai além, pois o *website* sequer encontrava-se armazenado em servidores nos Estados Unidos da América, mas mesmo assim foi retirado do ar⁶⁶.

Este foi, inclusive, um dos primeiros casos de embate entre governos e serviços digitais, e, sem dúvida, um dos maiores. Foi ele, também, que iniciou, nesta década, os intensos conflitos entre autoridades e tecnologia, os quais vão muito além da discussão sobre privacidade, mas que, não por isso, deixam de ser menos importantes de serem discutidos.

CONSIDERAÇÕES FINAIS

A privacidade é cada vez menor em um mundo tão mais exposto com o advento da *internet* e suas múltiplas formas de comunicação. Tal fato ocorre tanto por culpa dos próprios usuários, que ainda não entenderam os limites entre a vida pessoal e a pública dentro da rede mundial de computadores – em especial em redes sociais –, quanto por culpa das empresas de tecnologia que comercializam os dados de seus usuários na intenção de obter receita e, conseqüentemente, lucro.

⁶⁴ KHATCHADOURIAN, Raffi. Julian Assange, a Man Without a Country. The New Yorker, 2017. Disponível em <<https://www.newyorker.com/magazine/2017/08/21/julian-assange-a-man-without-a-country>>. Acesso em 17 de setembro de 2017.

⁶⁵ ALECRIM, Emerson. Novo vazamento da Wikileaks mostra o enorme poder de espionagem da CIA. Tecnoblog, 2017. Disponível em <<https://tecnoblog.net/210238/wikileaks-vazamento-year-zero/>>. Acesso em 17 de setembro de 2017.

⁶⁶ SILVA, Rafael. Megaupload é desativado depois de operação do FBI. Tecnoblog, 2011. Disponível em <<https://tecnoblog.net/88862/megaupload-desativado-fbi/>>. Acesso em 17 de setembro de 2017.

Tal problema, porém, não pode ser um incentivador para um declínio do uso ou, até mesmo, uma extinção da *internet*, mas sim um propulsor para novas alternativas que tragam maior controle aos usuários e, também, maior proteção aos dados pessoais que não queiram ver expostos.

O acesso à *internet* já foi elevado à condição de direito humano pela ONU, tal realidade deve-se, em muito, pela característica notável desta em ligar pessoas e conhecimentos. O acesso à informação e ao conhecimento propiciado pela *internet* é tão marcante que, atualmente, não se pode dissociar o uso desta ferramenta para pesquisas, seja por trivialidades ou, até mesmo, pesquisas acadêmicas, uma vez que os *database* de universidades de altíssimo renome do mundo inteiro encontram-se totalmente abertos e disponíveis, gratuitamente, para qualquer usuário que as deseje usufruir.

Em contrapartida, como visto, a *internet* também oferece riscos na mesma proporção em que traz confortos. O uso cada vez maior da ferramenta para os mais diversos fins faz com que informações sensíveis sejam armazenadas na rede e nos computadores dos usuários. A própria Declaração de Imposto de Renda brasileira é feita, atualmente, de maneira digital o que facilita o uso e cruzamento dos dados pela Receita Federal Brasileira e diminui custos, mas, também, torna acessível informações de caráter bastante particular de forma muito mais fácil em caso de uma invasão ao dispositivo informático, seja da Receita Federal, seja do contribuinte.

Por esta razão a preocupação com a segurança digital anda lado a lado com a privacidade a ser resguardada na *internet* e é também por esta razão que os governos devem se preocupar com as legislações aplicáveis e, acima de tudo, com o diálogo internacional sobre a governança da *internet*, uma vez que não se pode mais falar da rede mundial de computadores sem que seja levado em conta o fato de que ela é global.

A *internet* auxiliou mudanças de regimes governamentais em países do oriente, por meio da denominada “Primavera Árabe”, unindo os cidadãos insatisfeitos para que pudessem protestar; ela também propiciou uso de dados, que antes seriam de difícil acesso, em pesquisas de locais que jamais poderiam alimentar seus estudos com as últimas descobertas científicas. É na *internet* que se encontra, hoje, o maior volume de notícias, em tempo real, de quase todos os lugares do mundo.

A realidade atual é que, não há mundo, como conhecemos, sem a *internet*. Mas é também por culpa desta realidade que o estudo dos impactos jurídicos desta ferramenta não pode ser ignorado e deve ser suscitado com cada vez mais frequência dentro da academia, do ambiente legislativo, judiciário e, inclusive – e talvez especialmente –, educacional, pois é necessário um contato cada vez maior, e uma conscientização em igual proporção, com a *internet*, o que ela oferece, quais são os seus riscos e como deve ser feito o seu uso saudável e seguro.

Como visto, a *internet* também requer atenção em sua utilização, não podendo mais ser tratada como um mundo completamente à parte do que vivemos, ainda que assim pareça em muitos momentos, a verdade é que a fusão “mundo digital - mundo real” já aconteceu e é um fato indiscutível e inegável no fim da segunda década do século XXI; por esta razão, a *internet* deve ser tratada com a mesma preocupação que mantemos no mundo real, bem como com a mesma seriedade.

Assim, conforme demonstrado, a defesa da privacidade não consegue ser absoluta, pois existirão situações em que outro princípio deverá se sobrepor ao primeiro, como em uma situação de direito à informação perante uma informação que um político ou uma figura pública deseje ver esquecida, mas que é relevante à população. Mas, ainda assim, devem existir mecanismos para que os usuários possam controlar melhor quais informações sobre eles são públicas e, também, quais dados as empresas tem de seus usuários e como ela lida com estas informações. Porque ainda que deva existir uma contrapartida para o uso dos serviços, este comércio de dados pessoais não pode ser indiscriminado, uma vez que tratam-se de pessoas, cujas informações não podem ser tratadas de maneira leviana, devendo ser respeitadas como seres humanos que são.

A *internet* quebrou paradigmas e ainda irá, certamente, ser a protagonista de diversas mudanças que ocorrerão em nosso mundo. Mas não podemos aceitar que seus benefícios ofusquem a necessidade de corrigirmos as falhas que também advieram com ela. É preciso aproveitar os benefícios, mas sem ignorar e deixar de procurar soluções para os malefícios.

REFERÊNCIAS

COSTELLA, Antonio. **Comunicação – do grito ao satélite (história dos meios de comunicação)**. 2ª ed. São Paulo: Mantiqueira, 1984.

MENDES, Gilmar Ferreira, BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 8 ed. rev. e atual. São Paulo: Saraiva, 2013.

PINHEIRO, Patricia Peck. **Direito Digital**. 6 ed. rev., atual e ampl. São Paulo: Saraiva, 2016.

AGÊNCIA ESTADO; Estadão, 2013. Disponível em <<http://internacional.estadao.com.br/noticias/geral,onu-populacao-mundial-e-de-7-2-bilhoes-de-pessoas,1042156>>. Acesso em 28 de agosto de 2017.

ALECRIM, Emerson. **Novo vazamento da Wikileaks mostra o enorme poder de espionagem da CIA**. Tecnoblog, 2017. Disponível em <<https://tecnoblog.net/210238/wikileaks-vazamento-year-zero/>>. Acesso em 17 de setembro de 2017.

BIOGRAPHY.COM EDITORS. **Edward Snowden Biography.com**. Disponível em <<https://www.biography.com/people/edward-snowden-21262897>>. Acesso em 28 de agosto de 2017.

BLOG HARVARD, 2014. **Righting the right to be forgotten**. Disponível em: <<http://blogs.harvard.edu/futureoftheinternet/2014/07/14/righting-the-right-to-be-forgotten/>>.

BROWN, John Murray. **Após ordem judicial, Apple se recusa a desbloquear iPhone de terrorista**. Folha de São Paulo, 17 de fevereiro de 2016. Disponível em <<http://www1.folha.uol.com.br/mundo/2016/02/1740337-apos-ordem-judicial-apple-se-recusa-a-desbloquear-iphone-de-terrorista.shtml>>. Acesso em 15 de setembro de 2017.

CÂMARA, Bira. **O nascimento da imprensa**. 2009. Disponível em: <<http://jornalivros.com.br/2009/08/o-nascimento-da-imprensa/>>. Acesso em: 30 de out. 2016.

CANAL TECH. **Top 20: conheça os sites que mais têm acesso em todo o planeta**. 2013. Disponível em <<https://canaltech.com.br/curiosidades/top-20-conheca-os-sites-que-mais-tem-acesso-em-todo-o-planeta-6241/>>. Acesso em 28 de agosto de 2017.

DANTAS, Tiago; DANTAS, Dimitrius. **Doria oferece dados de usuários do Bilhete Único à iniciativa privada**. O Globo, 2017. Disponível em <<https://oglobo.globo.com/brasil/doria-oferece-dados-de-usuarios-do-bilhete-unico-iniciativa-privada-20942133>>. Acesso em 03 de setembro de 2017.

EUROPEAN COMMISSION: **Factsheet on the “Right to be Forgotten” ruling**. Disponível em: <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf>.

FACEBOOK. Disponível em <<https://pt-br.facebook.com/business/help/214319341922580>>. Acesso em 29 de agosto de 2017.

_____. Disponível em <https://pt-br.facebook.com/business/help/683065845109838?helpref=faq_content#>. Acesso em 29 de agosto de 2017.

_____. Disponível em https://www.facebook.com/business/help/146070805942156?helpref=faq_content. Acesso em 29 de agosto de 2017.

FOLHA DE SÃO PAULO. **Direito ao Esquecimento não existe e é usado para censura.** Reportagem publicada originalmente em 07 de agosto de 2016. Disponível em <http://www1.folha.uol.com.br/cotidiano/2016/08/1799831-direito-ao-esquecimento-nao-existe-e-e-usado-para-censura-afirma-advogada.shtml>.

GLOBO. **AlphaGo, inteligência artificial do Google, vence desafio de go contra melhor jogador do mundo.** 2017. Disponível em <http://g1.globo.com/tecnologia/noticia/alphago-inteligencia-artificial-do-google-vence-desafio-de-go-contr-melhor-jogador-do-mundo.ghtml>. Acesso em 03 de setembro de 2017.

HAMANN, Renan. **Algoritmo da Google ajuda polícia americana a prender pedófilo.** Tecmundo, 2014. Disponível em <https://www.tecmundo.com.br/crime-virtual/60067-google-ajuda-policia-americana-prender-pedofilo.htm>. Acesso em 15 de setembro de 2017.

HIGA, Paulo. **De novo: Justiça determina bloqueio do WhatsApp em todo o Brasil.** Tecnoblog, 2016. Disponível em <https://tecnoblog.net/198626/justica-bloqueio-whatsapp-brasil-de-novo/>. Acesso em 15 de setembro de 2017.

_____. **EUA espionaram emails e ligações telefônicas de brasileiros.** Tecnoblog, 2013. Disponível em <https://tecnoblog.net/134719/eua-espionagem-brasil-nsa/>. Acesso em 7 de julho de 2017.

_____. **Governo dos EUA espiona empresas de tecnologia e registros telefônicos da população.** Tecnoblog, 2013. Disponível em <https://tecnoblog.net/132530/governo-eua-prism-espionagem/>. Acesso em 7 de julho de 2017.

_____. **Já existem mais de 2 bilhões de usuários no Facebook;** Tecnoblog, 2017. Disponível em <https://tecnoblog.net/217628/facebook-2-bilhoes-usuarios/>. Acesso em 10 de julho de 2017.

_____. **Justiça manda operadoras bloquearem WhatsApp no Brasil por 72 horas.** Tecnoblog, 2016. Disponível em <https://tecnoblog.net/195057/justica-bloqueio-whatsapp-brasil-72-horas/>. Acesso em 15 de setembro de 2017.

_____. **Na VPN gratuita e ilimitada, o produto é você.** Tecnoblog, 2016. Disponível em <https://tecnoblog.net/195305/vpn-gratis-ilimitado-opera/>. Acesso em 28 de agosto de 2017.

HILL, Kashmir. **How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did.** 2012. Disponível em <http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#622fd83034c6>. Acesso em 27 de outubro de 2016.

IBGE. **Informações do Censo 2016** Disponível em <http://pais.es.ibge.gov.br/#/pt/pais/brasil/info/populacao>. Acesso em 28 de agosto de 2017.

KHATCHADOURIAN, Raffi. **Julian Assange, a Man Without a Country**. The New Yorker, 2017. Disponível em <<https://www.newyorker.com/magazine/2017/08/21/julian-assange-a-man-without-a-country>>. Acesso em 17 de setembro de 2017.

KRISCHER, Thais Cristine. **Um estudo da máquina enigma**. Porto Alegre: Graduação em Ciência da Computação da UFRGS, 2012. p. 62. Disponível em <<https://www.lume.ufrgs.br/bitstream/handle/10183/66106/000870987.pdf?sequence=1/>>. Acesso em 30 de out. 2016.

LITMUS EMAIL ANALYTICS. **Email Client Market Share**. 2017. Disponível em <<http://emailclientmarketshare.com>>. Acesso em 10 de setembro de 2017.

MAIA, Felipe. **Dado armazenado no exterior acirra atrito entre Facebook e autoridades**. Folha de São Paulo, 2016. Disponível em <http://www1.folha.uol.com.br/mercado/2016/07/1796861-dado-armazenado-no-exterior-acirra-atrito-entre-facebook-e-autoridades.shtml?utm_campaign=website&utm_source=sendgrid.com&utm_medium=email>. Acesso em 10 de outubro de 2016.

OLIVEIRA, Eulina. **Identidade única facilitará dia a dia, mas privacidade de dados será desafio**. 2017. Disponível em <<http://www1.folha.uol.com.br/mercado/2017/05/1887331-identidade-unica-facilitara-dia-a-dia-mas-privacidade-de-dados-sera-desafio.shtml>>. Acesso em 10 de agosto de 2017.

ORACLE. **What is Data Mining?**. Disponível em <https://docs.oracle.com/cd/B28359_01/datamine.111/b28129/process.htm#CHDFGCIJ>. Acesso em 03 de setembro de 2017.

PABLOS, Susana Pérez De. **Seus dados são vendidos por 7,5 centavos de dólar**. El País, 2017. Disponível em <https://brasil.elpais.com/brasil/2017/05/03/tecnologia/1493835469_309268.html?id_externo_rsoc=FB_BR_CM>. Acesso em 16 de setembro de 2017.

PECK, Patricia. **O que é um Chief Privacy Officer (CPO)?**. 2017. Disponível em <<https://web.facebook.com/notes/patricia-peck-pinheiro-advogados/o-que-e-um-chief-privacy-officer-cpo/1339648429452444/>>. Acesso em 16 de junho de 2017.

PEREIRA, André Luiz. **O que é Torrent?**. Tecmundo. Disponível em <<http://www.tecmundo.com.br/torrent/166-o-que-e-torrent-.htm>>. Acesso em 03 de nov. 2016.

PINTO, Tales Dos Santos. **Breve História da televisão**. Brasil Escola. Disponível em <<http://brasilecola.uol.com.br/historiag/breve-historia-televisao.htm>>. Acesso em 30 de out. 2016.

PRADO, Jean. **FBI conseguiu acessar os dados de um iPhone sem ajuda da Apple**. Estamos perdidos?. Tecnoblog, 2016. Disponível em <<https://tecnoblog.net/193403/fbi-iphone-criptografia-quebrada/>>. Acesso em 17 de setembro de 2017.

_____. **Justiça manda operadoras bloquearem WhatsApp no Brasil por 48 horas.** Tecnoblog, 2015. Disponível em <<https://tecnoblog.net/189494/justica-bloqueio-whatsapp-brasil-48-horas/>>. Acesso em 15 de setembro de 2017.

PSAFE. **Backdoor.** Disponível em <<http://www.psafe.com/blog/backdoor/>>. Acesso em 17 de setembro de 2017.

SILVA, Rafael. **Megaupload é desativado depois de operação do FBI.** Tecnoblog, 2011. Disponível em <<https://tecnoblog.net/88862/megaupload-desativado-fbi/>>. Acesso em 17 de setembro de 2017.

SORIMA NETO, João. **Investimento em segurança da informação cresce mais no país.** O Globo, 2015. Disponível em <<https://oglobo.globo.com/economia/negocios/investimento-em-seguranca-da-informacao-cresce-mais-no-pais-17645471>>. Acesso em 17 de julho de 2017.

TOO LONG; DIDN'T READ. Disponível em <<https://tldrlegal.com>>. Acesso em 03 de setembro de 2017.

UOL. **Varejista norte-americana descobre até gravidez de clientes com a ajuda de software.** 2012. Disponível em <<http://olhardigital.uol.com.br/noticia/varejista-norte-americana-descobre-gravidez-de-clientes-com-a-ajuda-de-software/24231>>. Acesso em 27 de outubro de 2016.

VELOSO, Thássius. **WhatsApp começa a compartilhar dados com Facebook; entenda o que muda.** 2016. Disponível em <<http://www.techtudo.com.br/noticias/noticia/2016/08/whatsapp-comeca-compartilhar-dados-com-facebook-entenda-o-que-muda.html>>. Acesso em 20 de novembro de 2016.