UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS

FACULDADE NACIONAL DE DIREITO

PROTEÇÃO DA PRIVACIDADE NA INTERNET

ADRAILDO FERMIANO DE SÁ BARRETO

Rio de Janeiro – RJ

2018/1º semestre

ADRAILDO FERMIANO DE SÁ BARRETO

PROTEÇÃO DA PRIVACIDADE NA INTERNET

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. Flávio Alves Martins.**

Rio de Janeiro – RJ

2018/ 1º semestre

CIP - Catalogação na Publicação

B273p

Barreto, Adraildo Fermiano de Sá
Proteção da Privacidade na Internet / Adraildo Fermiano de Sá Barreto. -- Rio de Janeiro, 2018.
71 f.

Orientador: Flávio Alves Martins.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade de Direito, Bacharel em Direito, 2018.

1. Direito à Privacidade. 2. Internet. 3. Redes Sociais. 4. Dados Pessoais. 5. Marco Civil da Internet. I. Martins, Flávio Alves, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a).

ADRAILDO FERMIANO DE SÁ BARRETO

PROTEÇÃO DA PRIVACIDADE NA INTERNET

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. Flávio Alves Martins.**

Data da Aprovação: __/__/____.

Banca Examinadora:

_____
Orientador

_____
Co-orientador (Opcional)

_____
Membro da Banca

_____
Membro da Banca

Rio de Janeiro – RJ

2018/ 1º semestre

Dedico este trabalho, especialmente, aos meus pais, que sempre me acompanham e me apoiam e também a minha grande e insubstituível família.

AGRADECIMENTOS

Aos meus pais, Adraildo Monteiro e Marcia Fermiano, que sempre me ajudaram e me proporcionaram as melhores condições para eu alcançar meus objetivos.

À toda a minha família, por toda confiança que sempre tiveram em mim.

Aos meus amigos, com os quais compartilhei as experiências da faculdade e meus planos para este trabalho.

Aos Professores Guilherme Martins e Flávio Martins, que me orientaram no projeto e na monografia, respectivamente, tornando possível a conclusão deste trabalho.

À Universidade Federal do Rio de Janeiro e, mais especificamente, a Faculdade Nacional de Direito, onde me preparei para a área que sempre desejei.

RESUMO

Com a evolução tecnológica, representada principalmente pelos computadores, pela internet e, mais recentemente os smartphones, o mundo se tornou conectado e todas as pessoas estão diariamente disponibilizando suas informações e vendo as dos outros, de forma a se flexibilizar continuamente o direito á privacidade. Se objetivou avaliar a efetividade da proteção à privacidade e aos dados pessoais nas legislações atuais e nos projetos de lei em tramitação, além de demonstrar a importância da internet no desenvolvimento da personalidade da pessoa humana. Os objetivos foram buscados através de pesquisa bibliográfica e jurisprudencial. Primeiro se buscou demonstrar que apesar de seus problemas específicos, a internet mudou a sociedade, sendo um novo ambiente para a cidadania e para as relações entre as pessoas através das redes sociais. Posteriormente se tratou da proteção à privacidade, amparada pelo Marco Civil da Internet, contra as diversas formas de desrespeitar este direito. Por último, o foco recaiu sobre as diferentes medidas de proteção da privacidade com base na doutrina, na jurisprudência dos tribunais e nos projetos de lei tratando especificamente dos dados pessoais. Conclui-se que apesar da vasta legislação protetiva à privacidade, ainda cabe questionar quanto a efetividade jurídica das escolhas legislativas e a necessidade de uma lei específica sobre os dados pessoais.

Palavras-chave: Direito à Privacidade; Internet; Redes Sociais; Dados Pessoais; Marco Civil da Internet.

ABSTRACT

With the technological evolution, represented mainly by computers, the internet and, more recently, smartphones, the world has become connected and all people are daily making available their information and watching others, in order to continuously flexibilize the right to privacy. The purpose of this study was to evaluate the effectiveness of the protection of privacy and personal data in current legislation and draft legislation, and to demonstrate the importance of the internet in the development of the personality of the human person. The objectives were sought through bibliographical and jurisprudential research. First it was tried to demonstrate that in spite of its specific problems, the internet changed the society, being a new environment for the citizenship and for the relations between the people through the social networks. Subsequently it dealt with the protection of privacy, supported by the Civil Landmark of the Internet, against the various forms of disrespect of this right. Lastly, the focus was on different measures of privacy protection based on doctrine, court case law and draft legislation specifically dealing with personal data. It is concluded that despite the vast legislation about protection of privacy, there is still a question as to the legal effectiveness of legislative choices and the need for a specific law on personal data.

Keywords: Right to Privacy; Internet; Social networks; Personal data; Civil Landmark of the Internet.

SUMÁRIO

INTRODUÇÃO

Os direitos da personalidade estão previstos em onze artigos no Código Civil (artigos 11 a 21) regulando o direito ao próprio corpo, o direito ao nome, o direito à honra, o direito à imagem e o direito à privacidade. Como atributos da personalidade da pessoa humana, as previsões legais têm como objetivo, principalmente, proteger esses direitos no âmbito das relações particulares. O valor que motiva essa proteção é a dignidade da pessoa humana, um dos fundamentos da República Federativa do Brasil, presente no artigo 1º, inciso III da Constituição Federal. Esse mesmo valor sustenta os direitos humanos no plano internacional e os direitos fundamentais, reunidos principalmente no artigo 5º da Constituição Federal. Independente da diferença de nomenclatura, o valor tutelado é o mesmo.

Esses direitos da personalidade eram entendidos como absolutos, imprescritíveis, inalienáveis e indisponíveis, porém esta concepção sofreu uma alteração com a mudança dos costumes sociais, das formas de entretenimento e da evolução tecnológica, com destaque para o surgimento da internet. Essa flexibilização não deve ocorrer de forma que a pessoa humana titular destes direitos dispense integralmente a sua proteção. As características citadas continuam válidas para estes direitos, porém devem ser admitidas as autolimitações voluntárias de seus titulares desde que elas sejam temporárias e se restrinjam aos objetivos pretendidos.

Antes da popularização do telefone, da televisão, do computador e da internet, a vida da pessoa na sociedade se resumia aos locais em que ela estava presente ou as pessoas que ela conhecia. Sua vida diária abrangia sua convivência com a família na residência e no seu bairro, seu local de trabalho e locais de lazer. Suas memórias gradualmente passaram a ser melhor preservadas com as fotos, que eram compartilhadas com as pessoas que faziam parte de seu círculo social, ainda fortemente ligado à proximidade territorial. Havia um relevante controle sobre o que se tornava ou não de conhecimento público, preservando-se o que era privado ou íntimo. Cadastros ainda se prendiam ao formato físico do papel e preenchimento manual, o que dificultava que os dados se difundissem rapidamente. Os espaços para expressar a sua opinião ainda não eram dotados de forma a dar rápida e imediata publicidade.

Com as diversas tecnologias atuais, principalmente, os computadores que estão presentes em diversas residências e estabelecimentos, inclusive podendo ser portáteis (*notebooks*) e os *smartphones* (que são telefones que incorporaram características dos computadores), podemos evidenciar a era da informática onde vivemos. Esses equipamentos são os maiores expoentes da transição para um mundo digital, concentrando trabalho e entretenimento num único lugar.

Para conectar todos os usuários do mundo, a internet é o ambiente que foi criado e se popularizou pela sua falta de controle centralizado. um ambiente democrático que pode ser acessado por qualquer pessoa que puder se conectar. Seja através dos computadores, *smartphones*, *smartwatch*, *smartv,* todos os usuários com acesso à internet podem fazer parte dessa comunidade, participando de discussões, expondo as suas opiniões ou a si mesmo, através dos populares sites de hospedagem de imagens, vídeos e as que sem dúvida recebem o maior destaque, as redes sociais. A vida das pessoas deixou de ser somente o ambiente físico que elas transitam diariamente, a internet também se tornou um ambiente a ser considerado. Não há uma separação rígida entre as relações entre as pessoas no ambiente propriamente real e no ambiente virtual. As pessoas criam suas concepções delas mesmas, seus perfis para interagir com os outros no ambiente virtual.

Nesta situação que se deve analisar como proteger o direito à privacidade quando se tornou natural tornar pública a vida privada. Principalmente, considerando, por exemplo, práticas como o *revenge porn*, a criação de banco de dados e o surgimento dos *crackers,* pessoas com conhecimento de informática que atuam de forma a causar dano e tirar proveito, com atos ilícitos, como o roubo de dados pessoais, com repercussão cível e, até possivelmente, penal. Dentre os problemas que surgiram especificamente com a internet podem ser citados, por exemplo: Códigos Maliciosos (*Malware*), *Spam* e *Cookies*.

Com esta monografia se objetiva: identificar sob que aspectos se permite a flexibilização do direito à privacidade, demonstrar a importância da internet para o desenvolvimento da personalidade da pessoa humana, analisar algumas práticas de violação à privacidade na internet; avaliar a efetividade das soluções atualmente apresentadas pelo direito para os litígios envolvendo o direito à privacidade na internet; e apresentar alguns projetos de lei em tramitação e como eles podem se

adequar as mudanças nas relações sociais e comerciais causadas pela influência diária e constante da internet.

No primeiro capítulo será analisada a criação da internet, como um dos principais destaques da evolução tecnológica e como essa rede mudou a sociedade, se tornando um espaço de exercício da cidadania, de formação da identidade e de relações pessoais nas redes sociais. Outro ponto importante é a formação de banco de dados pessoais cedidos voluntariamente pelos seus titulares e a sua necessária proteção. Também se tratará do surgimento de problemas específicos da internet, tais como os *crackers* e os *malware*.

No segundo capítulo será tratada da proteção do direito à privacidade na internet, junto de seus desdobramentos na proteção dos dados pessoais e o direito ao esquecimento, sendo também fundamental a análise dos dispositivos da Lei nº 12.965/14, o Marco Civil da Internet e de algumas formas de violação a privacidade na internet.

No terceiro capítulo serão buscadas medidas de proteção da privacidade, a partir de uma consulta a doutrina, ao posicionamento dos tribunais de nosso país a partir de alguns acórdãos e uma breve análise de propostas de regulamentação sobre a proteção de dados pessoais, em tramitação no Congresso Nacional, sendo elas o PL 5276/2016, o PLS 330/2013 e o PL 4060/2012.

Busca – se entender como a internet é fundamental para o desenvolvimento do indivíduo e como o direito pode atuar para proteger a privacidade, de forma a concretizar a dignidade da pessoa humana, frente as novas formas de violações de direitos que, algumas vezes, as pessoas não têm consciência de estarem sendo violados ou desconhecem meios de garantir a sua preservação.

1. A MUDANÇA SOCIAL PROMOVIDA PELA INTERNET

1.1. TECNOLOGIA E INTERNET

Atualmente não se consegue estar alheio à tecnologia e desconectado da Internet. Isso se deve à acelerada evolução tecnológica que se iniciou nas últimas décadas.

A evolução dos componentes físicos, os chamados *hardware,* se percebe com o aumento da capacidade de processamento, armazenamento, diminuição dos custos de produção e do preço para o consumidor, além do seu tamanho, tomando formas portáteis que permitem o uso em qualquer lugar.

A evolução dos programas, chamados *software,* permitiu a adoção das mais variadas funcionalidades. Se uma das funções mais triviais era digitar textos, atualmente é possível listar várias em uma quantidade indefinida, como por exemplo, ver filmes, ouvir música, realizar ligações e chamadas em vídeo, fazer compras.

A cada passo dessa evolução se tem o objetivo de atender as necessidades dos usuários que ainda não foram satisfeitas, ou realizá-las de forma mais inovadora e eficiente.

A Internet se trata de uma rede de computadores ligados entre si, que se conectam e se comunicam através de um conjunto de protocolos TCP/IP (*Transmission Control Protocol/ Internet Protocol*). Outra característica é a ausência de fronteiras físicas, o que permite a conexão de usuários de todo o mundo, como mais uma demonstração dos efeitos da globalização. Inexiste um controle centralizado, de forma que não há hierarquias e se permite uma maior liberdade de expressão, garantindo um espaço para os grupos que não podia expor sua mensagem nos meios tradicionais de comunicação, como os jornais, as rádios e a televisão.

Quanto a origem da Internet, em seu momento inicial e de uso restrito, ensina Martins[1]:

> Sua origem remonta aos anos 1960, durante a Guerra Fria, quando o governo norte-americano deu vida ao projeto ARPANET (“*Advanced research projects agency*”), no sentido de uma ligação entre computadores militares e industriais, em

[1]MARTINS, Guilherme Magalhães. **Contratos eletrônicos de consumo**. 3. ed., rev. atual. e ampl. São Paulo: Atlas, 2016.

> 1969, por intermédio da rede telefônica, de modo a prevenir um possível ataque nuclear, inexistindo, em razão de tal preocupação, um centro de controle único a ser destruído. (MARTINS, 2016, p. 25).

A arquitetura descentralizada se baseava em pacotes, de forma que a mensagem se fragmentava no envio e se reconstruía no recebimento. Os padrões TCP/IP foram bem-sucedidos e passaram a ser usados nas universidades e centros de pesquisa.

No final da década de 1980, houve um aumento significativo na velocidade das comunicações, devido as evoluções tecnológicas, utilizando satélites, fibras óticas e cabos. Foi denominada Web 1.0. A partir dos anos 1990, devido ao desenvolvimento de um protótipo da *World Wide We*b pelo cientista Tim Berners-Lee e sua equipe, no CERN ("*European Particle Physics Laboratory*"), chegou-se ao padrão HTML, que consiste em armazenar as informações, de modo que os dados de texto, imagem, som ou vídeo sejam visualizados em um único arquivo conjunto sob o padrão de hipertexto. Essa evolução, junto da crescente popularização dos computadores permitiu que a Internet chegasse a um grupo muito maior de consumidores.

Em 1994, com a segunda geração da Internet, chamada de "*Information Superhighway*" ou super-rodovia da informação, o computador passou a ser multi-função, desempenhando o papel de televisão, rádio, telefone e videofone. Com a Web 2.0, a segunda versão da *World Wide Web*, a Internet se tornou uma plataforma onde os usuários voluntariamente inserem o conteúdo.

Com a Web 3.0 ou Web semântica se busca utilizar a quantidade maciça de informações disponíveis de forma mais precisa para se adequar as necessidades de cada indivíduo, tornando as experiências individualizadas. Com isso, as aplicações precisam se comunicar entre os dispositivos, seja microcomputadores ou telefones móveis.

Com isso se viabiliza a Internet das Coisas. Se trata de uma rede que conecta o *hardware* e o *software* permitindo a conexão com a Internet em qualquer lugar e em qualquer dispositivo, seja computador, celular, carro, televisão. Com isso são produzidos dados sobre o comportamento e preferências do usuário, de forma que as sugestões para ele estejam o mais próximo possível de suas necessidades.

Dentre os métodos de comunicação na Internet, podem ser destacadas as redes sociais virtuais, o *e-mail,* as discussões públicas, os serviços de informação e a comunicação por tempo real.

As redes sociais virtuais são ambientes de interação entre os usuários, que se apresentam através de perfis, que são verdadeiras construções de si mesmos. Nesses ambientes, as pessoas desenvolvem relações sociais num ambiente virtual que não estão totalmente separadas das relações sociais nos ambientes físicos. Segundo Martins[2] (2016, p. 52), "Trata-se de uma manifestação do mundo real onde se desenvolvem novas situações subjetivas existenciais, em grande parte estimuladas pelo meio de comunicação". Nas redes sociais virtuais que melhor será analisada a questão da privacidade, por serem o método de comunicação na Internet mais popular na atualidade e onde se tem desenvolvido o hábito expor voluntariamente a vida privada.

O *e-mail* ou correio eletrônico tem o objetivo de troca de mensagens entre o emitente e o destinatário, a qual passa por diferentes servidores até chegar ao seu destino. É necessária a identificação dos agentes dessa comunicação e a troca não é imediata, nem mesmo há, em regra, a garantia do recebimento ou leitura da mensagem.

As discussões públicas ou *newsgroups* se tratam de fóruns onde os usuários discutem sobre temas específicos. A inclusão pode ser aberta a todos ou pode exigir uma inscrição prévia através de correio eletrônico.

Os serviços de informação permitem a consulta e troca de informações entre computadores à distância, podendo ser os seguintes: protocolos FTP (*File Transfer Protocol*) que permitem obter um arquivo de um computador ligado a Internet e a *World Wide Web* (Teia de Alcance Global) ou WWW que utiliza a linguagem HTML e permite a visualização de hipertextos, os quais são a compactação de documentos com texto, imagem e som. O acesso a esses hipertextos ocorre através dos *links*.

A comunicação em tempo real permite um diálogo entre vários usuários que trocam mensagens digitadas num canal ou sala de conversação. Adotam-se pseudônimos e a comunicação pode vir a se tornar privada, de forma que o conteúdo será restrito a destinatários específicos.

[2]MARTINS, Guilherme Magalhães. **Contratos eletrônicos de consumo**. 3. ed., rev. atual. e ampl. São Paulo: Atlas, 2016.

1.2. INTERNET E CIDADANIA

Mesmo com a expansão do acesso aos computadores e a Internet, isso não ocorreu de forma igualitária. O acesso à tecnologia e ao serviço exigem um investimento que, em regra, não pode ser arcado pelas camadas menos favorecidas da sociedade. Com isso, a exclusão econômica e social se identifica com a exclusão digital.

Os excluídos digitais estão alheios a sociedade de informação. Não tem acesso aos dispositivos tecnológicos e desconhecem como utilizá-los. Com isso é necessária a inclusão digital de forma a garantir-lhes um meio de exercício da sua cidadania dentro do contexto atual da sociedade.

Inclusão digital é ter acesso físico aos dispositivos que acessam a Internet, sendo o mais comum os computadores. Não deve se restringir meramente a um uso de editor de textos ou criação de planilhas. Deve ser ensinado o manuseio dos equipamentos e todas as possibilidades oferecidas pelos programas. Neste ponto sobre a cidadania, se buscaria demonstrar que é possível se informar ao tomar conhecimento do ambiente onde o usuário está inserido, ao mesmo tempo em que pode se expressar, permitindo opinar e participar das alterações promovidas.

Quanto a este aspecto, Batista et alli.[3] trata:

> A literacia digital é, portanto, outro ponto importante a ser vencido pelos governos. O fato da população ter baixa qualificação e condições educacionais empobrecidas, reduz o uso e possibilidades trazidas pela TI e Internet. Vencer o analfabetismo, no que tange, também, seu aspecto digital, é introduzir no mundo da tecnologia uma parte da população que hoje vive na sombra, à mercê daqueles que detém o poder do acesso para produzir informação. (BATISTA et al., 2016, p. 11)

Para o profissional de hoje é necessário ter esse conhecimento, o qual deve ser levado também ao estudante. O acesso a essas tecnologias pode contribuir para novas formas de aprendizado e criação de conhecimento. Também deve ser destacada a possibilidade de ampliação do acesso à educação com a modalidade a

[3] BATISTA, Nadine Victor; BATISTA, Gisele Victor; GOMES, Nicole Victor. A TRANSPARÊNCIA PÚBLICA E OS DESAFIOS DA ACESSIBILIDADE: A INTERNET ENQUANTO INSTRUMENTO DE APROXIMAÇÃO ENTRE ESTADO E CIDADÃO NA ERA DA SOCIEDADE DA INFORMAÇÃO. **V Seminário de Ciências Sociais Aplicadas**, Criciúma, v. 5, n. 5, p.1-17, maio 2016. Disponível em: <http://periodicos.unesc.net/seminariocsa/article/view/2786>. Acesso em: 13 abr. 2018.

distância, que beneficia as pessoas que não podem frequentar uma instituição de ensino, permitindo o estudo através do acesso digital.

Somente com a educação e o acesso aos meios digitais que as pessoas poderão participar de forma mais eficiente do ambiente virtual onde se constrói o interesse público, fruto das discussões sobre a necessidade do bem comum. Vale destacar que na Internet é um meio mais direto de contato entre o Estado e o cidadão. Por essa razão, o debate se torna menos influenciado e mais independente da interferência dos grupos de comunicação que dominam os meios mais tradicionais como a televisão e o rádio.

Nesse ponto traz-se a contribuição de Silva[4], com o seguinte trecho:

> A partir dessas leituras, consideramos surgimento do tripé formado pela comunicação pública, cidadania e democracia que geram um ciclo de interdependência para a eficácia de seu funcionamento. As pessoas precisam ser informadas sobre seus direitos, como buscá-los, discutir em suas comunidades os interesses comuns, mostrar suas necessidades e buscar meios para garantir a igualdade e execução dos direitos. Na comunicação pública, o interesse público e o bem comum devem estar acima de qualquer interesse institucional. E só se conhece as necessidades, o que é esse interesse público por meio de interações com os cidadãos. (SILVA,2016, p. 326).

A comunicação pública deve ser o meio pelo qual se discute a cidadania e o interesse público. Deve ser incentivada a participação do cidadão para que ele contribua para a discussão, justamente pelos assuntos se tratarem de interesse geral. A iniciativa não deve vir somente das instituições governamentais, podem partir também dos próprios cidadãos ou de organizações com relevância social.

Quanto ao cenário brasileiro, Silva[5] conclui:

> Apesar de um processo histórico que também contou com reivindicações sociais, trabalhistas, políticas, o Brasil ainda possui um Estado que, mesmo com as propriedades

[4] SILVA, Vivian Duarte da. COMUNICAÇÃO PÚBLICA NA INTERNET E CIDADANIA. **Ii Interprogramas – Xv Secomunica**: COMUNICADORES E MUTAÇÕES: CENÁRIOS E OPORTUNIDADES, Brasília, p.325-335, set. 2016. Disponível em: <https://portalrevistas.ucb.br/index.php/AIS/article/download/7869/4881>. Acesso em: 14 abr. 2018.

[5] SILVA, Vivian Duarte da. COMUNICAÇÃO PÚBLICA NA INTERNET E CIDADANIA. **Ii Interprogramas – Xv Secomunica**: COMUNICADORES E MUTAÇÕES: CENÁRIOS E OPORTUNIDADES, Brasília, p.325-335, set. 2016. Disponível em: <https://portalrevistas.ucb.br/index.php/AIS/article/download/7869/4881>. Acesso em: 14 abr. 2018.

> interacionais da Internet, centraliza sua comunicação em suas próprias realizações que não mostram a participação e o incentivo à atuação popular. Há indícios sim de informações para o conhecimento cidadão e seus direitos, mas em uma frequência menor do que as apresentações do que faz e do "bom" desempenho do atual governo. Os próprios seguidores da página canalizam suas interações aos assuntos mais destacados e frequentes pelo governo.
>
> Contudo, vê-se que o espaço da comunicação pública existe, a ferramenta de interação, multimídia, ágil, fácil, crescente e promissora também. Mas ainda há um longo caminho para direcionar meio, ferramentas, instrumentos a um exercício de cidadania democrático e, assim, garantir que os direitos estejam acima das realizações e interesses governamentais. (SILVA, 2016, p. 334/335).

Além de viabilizar a participação na elaboração de leis e discussão das matérias pertinentes a sociedade, o governo ao prestar informações cumpre a transparência exigida e, que é melhor exercida atualmente. Com a disposição na Internet, se faz a prestação de contas ao cidadão se permitindo conferir a quantidade e a forma de gasto do dinheiro público, envolvendo os orçamentos, as licitações e os contratos administrativos.

Os seguintes diplomas fazem parte dessa tendência, conforme indicado por Batista et alli.[6]:

> A transparência pública no Brasil começou a ser discutida a nível cotidiano a partir da Lei de Transparência - Lei Complementar 131/2009, bem como com o direito à informação pública pela Lei de Acesso à Informação nº 12.527, de 18 de novembro de 2011. (BATISTA et al, 2016, p. 6).

Somente pelo acesso à informação que será promovida a transparência pública e combatida a corrupção. Essa transparência é exigida das três esferas de governo e de qualquer organismo que receba verba pública.

Apesar desse progresso quanto a disponibilização de informações, deve ser criticada a forma como são apresentadas. Disponibilizar planilhas, dados técnicos,

[6] BATISTA, Nadine Victor; BATISTA, Gisele Victor; GOMES, Nicole Victor. A TRANSPARÊNCIA PÚBLICA E OS DESAFIOS DA ACESSIBILIDADE: A INTERNET ENQUANTO INSTRUMENTO DE APROXIMAÇÃO ENTRE ESTADO E CIDADÃO NA ERA DA SOCIEDADE DA INFORMAÇÃO. **V Seminário de Ciências Sociais Aplicadas**, Criciúma, v. 5, n. 5, p.1-17, maio 2016. Disponível em: <http://periodicos.unesc.net/seminariocsa/article/view/2786>. Acesso em: 13 abr. 2018.

números, informações de contratos não são suficientes para cumprir o objetivo da lei. É necessário, mais uma vez, que o cidadão compreenda as informações que lhe são disponibilizadas.

A efetiva participação do cidadão na sociedade, no nível tecnológico atual, somente ocorrerá através de melhoria da educação, envolvendo a inclusão digital, considerando a necessidade de conhecimento das funções disponíveis com a informática e o acesso aos dispositivos de acesso à Internet.

1.3. REDES SOCIAIS VIRTUAIS

Nas redes sociais ocorre a troca de informações pessoais. Em uma plataforma digital, as pessoas revelam detalhes íntimos de suas vidas pessoais, registram seu cotidiano, compartilhando fotos, vídeos e acompanham as novidades na vida das pessoas com quem se relacionam.

Tratando-as como formas de relacionamento na atualidade, Vasconcelos e Brandão[7] dizem:

> As redes sociais da atualidade estão instaladas, principalmente, na Internet devido ao fato de esta proporcionar mais celeridade e eficiência nas formas comunicativas e maior amplitude na divulgação de ideias a serem compartilhadas e absorvidas pelos integrantes da rede na busca constante por algo em comum. Assim, as redes sociais na Internet, a exemplo do Facebook e do Twitter, são formas de relacionamento entre dois ou mais indivíduos na comunicação mediada por computadores conectados à Internet. (VASCONCELOS e BRANDÃO, 2013, p. 134).

Essas relações virtuais não são separadas do mundo real, na verdade, são desdobramentos deste e se devem a influência da evolução tecnológica nas relações humanas.

[7] DE VASCONCELOS, Fernando Antônio; HOLANDA VASCONCELOS BRANDÃO, Fernanda. AS REDES SOCIAIS E A EVOLUÇÃO DA INFORMAÇÃO NO SÉCULO XXI. **Direito e Desenvolvimento**, [S.l.], v. 4, n. 1, p. 125-144, jan/jun. 2013. ISSN 2236-0859. Disponível em: <https://periodicos.unipe.br/index.php/direitoedesenvolvimento/article/view/225>. Acesso em: 14 abr. 2018.

Nas redes sociais virtuais, as pessoas criam perfis para se comunicar com outras pessoas, que também utilizam perfis. Com isso, as relações ocorrem a partir de representações da realidade criadas pelos seus titulares.

Quanto a essas relações, Martins[8] ensina:

> No que concerne às conexões, embora se afirme que a Internet trouxe um enfraquecimento dos laços relacionais, o que ocorre, na verdade, é o surgimento de novas relações humanas, propiciadas e fomentadas pelo ambiente digital, traduzindo formas de convivência diferenciadas, a desafiar os operadores do direito. (MARTINS, 2016, p. 53)

As informações de nome, sobrenome, hábitos, opções religiosas e afetivas geram um capital social de valor econômico. Através da coleta e análise das informações disponibilizadas pelos usuários nesse espaço de *Web* 2.0, são possibilitadas a disponibilização de um conteúdo mais personalizado para cada usuário, assim como as ofertas de publicidade ficam de acordo com suas necessidades e interesses.

Com todo o conteúdo compartilhado, se formam bancos de dados com informações pessoais que ficam a serviço de entidades com caráter privado. Mesmo que a maioria dos serviços sejam gratuitos para o usuário, o fornecedor tem um interesse econômico que é atingido indiretamente.

Dentre as variadas formas de utilização das redes sócias, Shimazaki et al[9] trazem as seguintes:

> As redes sociais podem ser usadas para diferentes funções, dentre elas divertimento, procura de amigos com mesmo perfil, procura de empregos etc. Esta penúltima função, citada anteriormente, está sendo utilizada pelas empresas para ajudar nos processos seletivos, para promover o “primeiro contato” com o candidato, configurando-se a primeira impressão, feita através da procura do seu perfil nas principais ferramentas de comunicação. (SHIMAZAKI et al, 2011, p. 4).

---

[8]MARTINS, Guilherme Magalhães. **Contratos eletrônicos de consumo**. 3. ed., rev. atual. e ampl. São Paulo: Atlas, 2016.

[9]SHIMAZAKI, Vinicius Kenji; PINTO, Maria Márcia Matos. A INFLUÊNCIA DAS REDES SOCIAIS NA ROTINA DOS SERES HUMANOS. **Fasci-tech**: Periódico Eletrônico da FATEC, São Caetano do Sul, v. 1, n. 5, p.171-179, out/dez. 2011. Disponível em: <http://fatecsaocaetano.edu.br/fascitech/index.php/fascitech/article/view/57>. Acesso em: 14 abr. 2018.

As redes sociais mais conhecidas são, por exemplo, Facebook, Twitter, Linkedin e o extinto Orkut. O Orkut, lançado em janeiro de 2004, destinava-se a troca de mensagens entre os amigos adicionados nos perfis, compartilhamento de imagem, vídeos e participação em comunidades para discussão. Em sua época, ela se tornou extremamente popular em território brasileiro. Sua proprietária era a gigante das buscas Google, que após o fim do Orkut, passou a investir em outra rede social chamada Google +, lançado em junho de 2011, que não alcançou o mesmo sucesso. O Facebook, lançado em fevereiro de 2004, ocupou futuramente o lugar do Orkut como rede social mais popular adotando funcionalidades semelhantes, mesmo que sua organização e visual sejam muito diferentes. Esta rede esteve recentemente nos holofotes do noticiário global devido ao escândalo de vazamento de dados, culminando no depoimento de seu fundador Mark Zuckerberg diante do Senado norte-americano. O Twitter, lançado em outubro de 2006, destina-se a publicação de imagens curtas, mensagens e vídeos pelos seus usuários. O Linkedin, lançado em maio de 2003, é uma rede social de negócios onde os profissionais com perfis demonstram suas aptidões.

Todas essas redes envolvem disponibilização e utilização das informações pessoas prestadas voluntariamente pelos seus usuários. O escândalo do Facebook demonstra a importância de se discutir a proteção dos dados pessoais, sendo uma forma de proteger a privacidade, a intimidade e a identidade das pessoas na Internet.

Sendo relevante e influentes na sociedade, as redes sociais também geram impacto nos movimentos sociais e culturais como a luta por direitos humanos, feministas, ambientalistas, etc. São ambientes que permitem a liberdade de expressão e um espaço para dialogar com outros que compartilham ou não das mesmas ideias, sem ter o empecilho da distância geográfica. Quanto a esse papel, Shimazaki et alli[10] destaca que:

> Considerando as afirmações de Afonso, deve-se lembrar o importante papel que as redes sociais tiveram recentemente na articulação dos movimentos políticos contra ditaduras que se estenderam por décadas em países do Oriente Médio e do

[10]SHIMAZAKI, Vinicius Kenji; PINTO, Maria Márcia Matos. A INFLUÊNCIA DAS REDES SOCIAIS NA ROTINA DOS SERES HUMANOS. **Fasci-tech**: Periódico Eletrônico da FATEC, São Caetano do Sul, v. 1, n. 5, p.171-179, out/dez. 2011. Disponível em: <http://fatecsaocaetano.edu.br/fascitech/index.php/fascitech/article/view/57>. Acesso em: 14 abr. 2018.

> Norte da África. Na Tunísia, Egito, Síria, Bahrein, Líbia, entre outros, foi através das redes sociais que os rebeldes conseguiram se unir na expressão dos desejos de liberdade e mudança nas estruturas políticas autoritárias, marcando protestos que tomaram as ruas, levando à derrubada de líderes que se mantinham no poder há anos, como no Egito e na Líbia. (SHIMAZAKI et al, 2011, p 4)

Quanto aos movimentos sociais nas redes sociais no Brasil, Elias[11] traz a seguinte explicação:

> A formação dos movimentos sociais através das redes sociais se dá a partir de uma pequena chama que é o estopim para que as pessoas se juntem virtualmente e logo depois concluam essa junção de forma real e concreta na luta pelo bem comum. Cada pessoa que vai às ruas nesta era digital, previamente mantiveram contatos virtuais com acertos que se consolidaram na busca por dias melhores, sejam eles, educacionais, políticos, na saúde, ou simplesmente por poder transitar de maneira digna e com pouco custo, como foram as manifestações em 2013, vésperas da Copa do Mundo e das eleições presidenciais aqui no Brasil. (ELIAS, 2016, p. 120).

As redes sociais são extremamente populares e são um dos usos mais comuns usos da Internet. Elas permitem o entretenimento e engajamento social entre pessoas a qualquer distância. Contudo, como já mencionado, deve-se atentar as possibilidades de mau uso das informações pessoais fornecidas pelos usuários.

1.4. DADOS PESSOAIS

Com a Internet, surgiram novas formas de relações pessoais e comerciais. As pessoas passaram a criar perfis em redes sociais e fazer compras pela Internet. Com essa cessão voluntária de informações, se abre um campo para discutir como protegê-las, evitar seu uso indevido e permitir que seu titular as altere ou exclua dos servidores onde são armazenadas.

[11]ELIAS, Ednete Morais Costa. A pujança dos movimentos sociais: do Império à formação através das redes sociais virtuais no Brasil atual. **Research, Society And Development**, Logroño, v. 1, n. 2, p.107-126, ago. 2016. Disponível em: <https://dialnet.unirioja.es/servlet/articulo?codigo=6070062>. Acesso em: 15 abr. 2018.

A Diretiva CEE nº 95/46 traz as seguintes definições para dados pessoais e o tratamento desses dados:

> "Artigo 2º. Para efeitos da presente diretiva, entende-se por:
>
> a) 'Dados pessoais', qualquer informação relativa a uma pessoa singular identificada ou identificável ('pessoa em causa'); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social;
>
> b) 'Tratamento de dados pessoais' ('tratamento'), qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registro, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição.

As pessoas ao fornecer suas informações exercem a sua liberdade de expressão nessa nova dimensão da Internet. Por isso devem também ser protegidas sua dignidade e sua identidade em situações nas quais, por exemplo, sua imagem seja ofendida, utilizada indevidamente ou criadas 'comunidades' com conteúdo difamatório. Essa mecânica de 'comunidades' ou 'páginas' é melhor observada em redes sociais como Orkut ou Facebook.

Quanto a essa proteção, Martins[12] traz a seguinte ressalva:

> Neste ponto, porém, deve ser observada a regra pela qual cada provedor, mesmo quando consinta no uso de pseudônimos ou garanta o anonimato na rede, providencie, ainda que no contrato de acesso, a identificação do usuário, mediante a apresentação de documento de identidade válido, como garantia dos imperativos de segurança e lealdade próprios da boa-fé objetiva, valores esses que, balanceados em face da privacidade, devem ser colocados em primeiro lugar. (MARTINS, 2016, p. 57).

Sobre essas informações disponibilizadas, segundo Doneda[13], elas devem possuir um vínculo objetivo com uma pessoa, revelando algo sobre suas

[12]MARTINS, Guilherme Magalhães. **Contratos eletrônicos de consumo**. 3. ed., rev. atual. e ampl. São Paulo: Atlas, 2016.

características e suas ações, sendo o objeto da informação a própria pessoa e, com isso, possam ser caracterizadas como de natureza pessoal, conforme a seguinte explicação:

> A informação pessoal deve observar certos requisitos para sua caracterização como tal. Uma determinada informação pode possuir um vínculo objetivo com uma pessoa, revelando algo sobre ela. Esse vínculo significa que a informação refere-se às características ou ações dessa pessoa, que podem ser atribuídas a ela seja em conformidade à lei, como no caso do nome civil ou do domicílio, ou então que são informações provenientes de seus atos, como os dados referentes, por exemplo, aos seus hábitos de consumo, sobre opiniões que manifesta, à sua localização e tantas outras. É importante estabelecer esse vínculo objetivo, pois ele afasta outras categorias de informações que, embora também possam ter alguma relação com uma pessoa, não seriam propriamente informações pessoais: as opiniões alheias sobre essa pessoa, por exemplo, a princípio não possuem esse vínculo objeto; também a produção intelectual de uma pessoa, em si considerada, não é *per se* informação pessoal (embora o fato de sua autoria o seja). (DONEDA, 2014, p. 62).

Essas informações pessoais ocupam numerosos bancos de dados com grande capacidade de armazenamento e comunicação entre si. Com isso, esse grande volume de informação fica mais organizado e se permite que um número maior de sujeitos tenha acesso a ela.

Considerando que a posição dos titulares dos dados pessoais em relação às entidades que os coletam e processam é completamente desigual, visto que as pessoas tendem a não ter total conhecimento, nem total acesso a manipulação desses dados, é necessário valorizar e aprofundar a discussão sobre como proteger os dados pessoais. Trata-se também de entender este objetivo como um desdobramento da proteção à privacidade.

Quanto à proteção dos dados pessoais, os seguintes princípios devem ser considerados: da publicidade ou transparência, da exatidão, da finalidade, do livre acesso e da segurança física e lógica.

---

[13]DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães et al (Coord.). **Direito Privado e Internet.** São Paulo: Atlas, 2014. Cap. 3. p. 61-78

O princípio da publicidade ou da transparência determina que a existência de um banco de dados pessoais deve ser de conhecimento público, havendo permissão prévia de funcionamento proveniente de uma autoridade.

O princípio da exatidão determina que os dados pessoais armazenados devem ser fiéis à realidade e que devem receber atualizações periódicas.

O princípio da finalidade determina que a utilização dos dados pessoais deve estar de acordo com a finalidade pela qual eles foram cedidos pelos seus titulares, havendo a vedação à transferência desses dados a terceiros.

O princípio do livre acesso determina que o indivíduo deve ter acesso às suas informações armazenadas no banco de dados, de forma que possa obter cópias, controlá-las, corrigir as incorretas e realizar acréscimos de novas. Este princípio está relacionado ao da exatidão.

O princípio da segurança física e lógica determina que os dados armazenados devem ser protegidos do extravio, destruição, modificação, transmissão e acesso não autorizado.

Quanto ao ordenamento jurídico brasileiro, Doneda [14] traz o seguinte panorama:

> No panorama do ordenamento brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma previsão literal e direta, porém da consideração dos riscos que o tratamento automatizado acarreta à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada. (DONEDA, 2014, p. 74).

Sobre este mesmo assunto, o autor continua:

> Não há, no ordenamento jurídico brasileiro, uma normativa genérica sobre a proteção de dados pessoais. A Constituição brasileira contempla o problema da informação inicialmente através das garantias à liberdade de expressão e do direito à informação, que deverão eventualmente ser confrontados com a proteção da personalidade e, em especial, com o direito à privacidade. (DONEDA, 2014, p. 75).

[14]DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães et al (Coord.). **Direito Privado e Internet.** São Paulo: Atlas, 2014. Cap. 3. p. 61-78

Não havendo dispositivo específico e considerando as garantias já previstas na Constituição, como a inviolabilidade da vida privada e da intimidade (art. 5, X); e quanto a interceptação de comunicações telefônicas, telegráficas ou de dados (art. 5, XII), elas devem ser interpretadas conjuntamente, tendo em vista as tecnologias atuais, para proteger a privacidade e os dados pessoais.

1.5. PROBLEMAS ESPECÍFICOS DA INTERNET

Com as novas tecnologias e com a Internet, as pessoas passaram a estabelecer relações no mundo digital. Sejam pessoais ou comercias, há a troca de informações que podem ficar armazenados nos dispositivos ou na Internet. Com isso, surgiram pessoas com conhecimento para manipular essas tecnologias, os chamados *hackers*, e os que o fazem de forma maliciosa com intuito de obter proveito, sendo estes os *crackers*.

O acesso aos computadores pode ser através do contato físico com o dispositivo ou pelo Internet, realizando um acesso remoto. Nessas situações são explorados *bugs*, que são erros no sistema ou demais vulnerabilidades no sistema operacional e nos programas instalados. Existem também as *backdoors* que são programas que permitem que o invasor retorne a manipular o dispositivo invadido após a primeira invasão.

Para invadir os computadores e causar dano e captar informações são utilizados os Malware ou Códigos Maliciosos, que dentre os quais podem ser destacados: os vírus, cavalos de Tróia, *worms*, *spywares*, *keyloggers*, *bots* e *rootkits*.

Os Cavalos de Tróia ou *Trojan Horses*, como na história, invadem o computador e criam uma porta para acesso remoto do invasor, as já mencionadas *backdoors*. Esse *malware* é instalado através da execução de um programa no computador, permitindo a visualização e alteração de arquivos ou a captura de informações como as senhas.

Sobre a atuação do invasor e o dano causado, Martins[15] esclarece:

> Agindo remotamente de qualquer parte do mundo, protegido pela imperceptibilidade do programa em execução, o agente tem total e absoluto controle do computador invadido, podendo visualizar, introduzir, retirar, modificar ou apagar arquivos, ter acesso ao controle dos dispositivos periféricos e ler instantaneamente aquilo que a outra pessoa está digitando, a partir da captura das palavras diretamente do teclado. (MARTINS, 2014, p. 228).

Os vírus são programas que afetam ou danificam outros programas e se reproduzem de forma a aumentar a infecção no mesmo dispositivo e poder alcançar outros. Uma forma de evitar a perda de arquivos é a realização de backups.

Os *worms* são uma fração de código de computador que é compartilhado na Internet e invadem os *hardwares* vulneráveis. Eles podem ser inofensivos ou danosos dependendo da forma que foram programados. Quanto a eles, Martins[16] traz a seguinte explicação:

> Consiste o *worm*, portanto, num "(…) programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferentemente do vírus, o *wor*m não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em computadores (…). (MARTINS, 2014, p. 235/236).

Spywares são programas espiões que enviam informações do usuário do computador a desconhecidos. Com esses programas é possível monitorar o uso de Internet, de arquivos, o que está sendo digitado através de *keylogger*, afetando a privacidade. *Adware* também podem ser assim considerados, pois monitoram os hábitos do usuário de forma a proporciona uma oferta de propagandas mais personalizada.

[15]MARTINS, Guilherme Magalhães. **Responsabilidade civil por acidente de consumo na Internet**. 2. ed. São Paulo: Editora Revista dos Tribunais, 2014.
[16]MARTINS, Guilherme Magalhães. **Responsabilidade civil por acidente de consumo na Internet**. 2. ed. São Paulo: Editora Revista dos Tribunais, 2014.

Os *bots* são programas que se propagam automaticamente e infectam computadores permitindo o acesso remoto. Com isso podem ser formadas *botnets* que são redes de computadores infectados para intensificar os ataques realizados.

Os rootkits são programas que permitem acesso a computador ao mesmo tempo que oculta a sua atividade. Ele se integra a alguma parte do sistema operacional ou se camufla como parte de algum processo do computador, de forma que não possa ser identificado pelas varreduras dos programas de antivírus.

O *spam* é a mensagem eletrônica não solicitada, recebida através da Internet sem a autorização do usuário, geralmente destinada a divulgar produtos ou serviços. Na maior parte das vezes, o problema não é o conteúdo da mensagem, mas a quantidade na qual é enviada. O grande movimento dessas mensagens que não apresentam muita ou nenhuma utilidade aos destinatários ameaça a eficiência e a velocidade da Internet. Quando estas mensagens conduzem a sites falsos ou acionam o download de programas maliciosos, demonstrando um intuito de fraude, são chamadas de *pishing spam* ou *phishing scam*.

Boatos ou *hoaxes* são *e-mails* com conteúdo alarmante ou falso que tem como aparente remetente uma instituição, empresa ou órgão governamental. Seu conteúdo é falso e pode estar acompanhando de *malware*.

Cookies são programas que registram os dados gerados pelo usuário de forma a tornar a navegação na Internet mais personalizada e mais ágil. Registram-se, por exemplo, nomes, senhas, localização, informações de consumo. Mesmo que seu objetivo seja apresentado como a favor do usuário, ele constitui uma violação à privacidade.

Quanto aos *e-mails* enviados, os provedores podem facilmente vasculhar seu conteúdo devido a reduzida segurança nessa forma de comunicação. Por isso, a correspondência eletrônica deve receber a mesma proteção da convencional, conforme a previsão do art. 5, XII, da Constituição.

Uma vez analisado como a Internet mudou os comportamentos sociais na atualidade e o surgimento de diversas formas de causar dano no meio digital, se passa ao foco principal que é entender as novas concepções do direito à privacidade na era da informática e os desafios à legislação para garantir a sua proteção.

2. O DIREITO À PRIVACIDADE

2.1. PRIVACIDADE, UM DOS DIREITOS DA PERSONALIDADE

O Código Civil de 2002 possui um capítulo inteiro dedicado aos direitos da personalidade. Em seus onze artigos (11 ao 21) estão previstos: o direito ao próprio corpo, o direito ao nome, o direito à honra, o direito à imagem e o direito à privacidade. Abandonando a ótica patrimonialista do código anterior de 1916, o atual demonstra seu compromisso com a tutela e a promoção da personalidade humana, estando de acordo com a dignidade da pessoa humana, um dos fundamentos de nossa república, previsto no art. 1º, inciso III da Constituição Federal.

Ao longo da história, se buscou garantir direitos que resguardassem os atributos essências da pessoa humana e a sua dignidade, recebendo diferentes denominações, sejam direitos humanos, direitos fundamentais ou direitos da personalidade. Quanto a isso, Schreiber[17] explica:

> A ampla variedade de termos não deve gerar confusões. Todas essas diferentes designações destinam-se a contemplar atributos da personalidade humana merecedores de proteção jurídica. O que muda é tão somente o plano em que a personalidade humana se manifesta. Assim, a expressão *direitos humanos* é mais utilizada no plano internacional, independentemente, portanto, do modo como cada Estado nacional regula a matéria. *Direitos fundamentais*, por sua vez, é o termo normalmente empregado para designar "direitos positivados numa constituição de um determinado Estado". É, por isso mesmo, a terminologia que tem sido preferida para tratar da proteção da pessoa humana no campo do direito público, em face da atuação do poder estatal. Já a expressão *direitos da personalidade* é empregada na alusão aos atributos humanos que exigem especial proteção no campo das relações privadas, ou seja, na interação entre particulares, sem embargo de encontrarem também fundamento constitucional e proteção nos planos nacional e internacional. (SCHREIBER, 2013, p. 13).

[17] SCHREIBER, Anderson. **Direitos da Personalidade**. 2. ed. São Paulo: Atlas, 2013.

Apesar dos direitos da personalidade já mencionados e previstos no código civil, o rol desses direitos é aberto. Como direitos da personalidade podem ser adicionados também o direito à identidade pessoal, o direito à integridade psíquica e o direito à liberdade de expressão, por exemplo.

Araújo et alli[18] traz a seguinte definição de direitos da personalidade:

> Os direitos da personalidade são prerrogativas individuais, inerentes à pessoa humana. São direitos inalienáveis, que merecem proteção do meio jurídico contemporâneo. Pois, o homem, merece ser protegido em sua essência, e não apenas o seu patrimônio. Os direitos personalíssimos têm por objeto a proteção física, psíquica e moral do homem, e seu convívio em sociedade, ou seja, o objeto de proteção é a sua personalidade, é a sua individualidade que merece proteção, assim, o direito deve tutelar o seu espaço individual. (ARAÚJO et al, 2016, p. 89).

Os direitos da personalidade como essências da condição humana são intransmissíveis, irrenunciáveis, absolutos, ilimitados, imprescritíveis, impenhoráveis, inalienáveis, não sujeitos a desapropriação e vitalícios. Contudo, deve ser considerada a possibilidade de limitação voluntária de seu exercício. Para ser admitida essa autolimitação, deve ser analisado o seu alcance, a duração, a intensidade e a finalidade. Segundo Schreiber[19]:

> [...] a autolimitação ao exercício dos direitos da personalidade deve ser admitida pela ordem jurídica quando atenda genuinamente ao propósito de realização da personalidade do seu titular. Deve, ao contrário, ser repelida sempre que guiada por interesses que não estão própria ou imediatamente voltados à realização da dignidade daquela pessoa. (SCHREIBER, 2013, p. 27).

O direito da personalidade, o qual, será analisado é o direito à privacidade. Este direito está previsto no artigo 21 do Código Civil sob a forma de inviolabilidade da vida privada. Tal definição é insuficiente para a atualidade, onde a privacidade

[18] ARAÚJO, Antônio Carlos da Silva et al. A INDISPONIBILIDADE DA PERSONALIDADE E AS REDES SOCIAIS. **Cadernos de Graduação**: Ciências Humanas e Sociais, Alagoas, v. 3, n. 3, p.85-100, nov. 2016. Disponível em: https://periodicos.set.edu.br/index.php/fitshumanas/article/view/3579>. Acesso em: 27 abr. 2018.

[19] SCHREIBER, Anderson. **Direitos da Personalidade**. 2. ed. São Paulo: Atlas, 2013

também se trata de proteção dos dados e informações pessoais. Sobre o tratamento dado no código, Schreiber[20] comenta:

> A verdade é que o Código Civil brasileiro deu à privacidade um tratamento inadequado. Em primeiro lugar, dedicou um único artigo à matéria, cuja importância se renova a cada dia na sociedade contemporânea. Nesse dispositivo solitário, o legislador limitou-se, como se verá mais adiante, a um enunciado genérico, que não acrescenta rigorosamente nada ao que já se encontrava previsto na Constituição. Perdeu, assim, a oportunidade de oferecer parâmetros para a solução de diversos conflitos concretos ligados à tutela da privacidade. (SCHREIBER, 2013, p.134).

A privacidade, em sua concepção inicial, era entendida como um “direito a ser deixado só”. Ela se relacionava a vida íntima, familiar, pessoal do titular. Buscava-se proteger a intimidade e impor um dever geral de abstenção aos demais. Porém, com as inovações tecnológicas e os novos meios de armazenamento, processamento e utilização da informação, a privacidade passou a abranger também o controle sobre os dados pessoais.

O controle dos dados pessoais por seus titulares se traduz na cessão voluntária ou autorização da inclusão em bancos de dados, a possibilidade de correção, remoção e utilização conforme a finalidade pela qual foram cedidos.

Schreiber[21] divide a problemática da privacidade em duas dimensões: uma procedimental e uma substancial. A dimensão procedimental é sobre o modo de coleta das informações pessoais. A coleta clandestina ou desautorizada se trata de invasão da privacidade. A coleta de informações necessita de autorização prévia do titular. Mesmo que atualmente a coleta de informações mínimas de uma pessoa seja inevitável, a utilização deve ser sempre pautada pela finalidade com a qual as informações foram cedidas. A cessão de informações não pressupõe um livre uso das mesmas. São necessárias medidas que garantam a conferência periódica da veracidade dos dados e a proteção dos mesmos diante de ataques externos, medida necessária quando se trata do ambiente da internet. A dimensão substancial está ligada ao emprego da informação obtida. As pessoas devem controlar a representação de si mesmas que é obtida a partir de seus dados. Dependendo da

[20] SCHREIBER, Anderson. **Direitos da Personalidade**. 2. ed. São Paulo: Atlas, 2013
[21] SCHREIBER, Anderson. **Direitos da Personalidade**. 2. ed. São Paulo: Atlas, 2013

forma de utilização deles, pode conduzir a violação de outros direitos como, por exemplo, a liberdade religiosa, sexual ou de pensamento.

A privacidade é um direito de todas as pessoas, logo mesmo se tratando dos famosos ou estando em local público, ainda há uma expectativa de privacidade. Mesmo que a privacidade seja violada constantemente na vida em sociedade, a proteção jurídica é contínua. Somente se admite o afastamento parcial desse direito quando for a partir de um ato voluntário de seu titular ou quando entrar em conflito com outro direito que, no momento específico, seja mais relevante, como, por exemplo, o direito a segurança ou direito à informação.

Sob a ótica da evolução tecnológica, Schreiber[22] trata do uso de microchips. Pode haver a violação do direito ao próprio corpo, com a implantação de microchips subcutâneos para monitoração de pacientes ou controle de consumo em boates. A utilização pode ser benéfica para o indivíduo ou desnecessária, devendo sempre objetivar o respeito aos direitos fundamentais. O autor também traz o exemplo da utilização de microchips em lixeira no Reino Unido para identificar residência, a quantidade de lixo despejado e guiar as medidas de saneamento. Sobre este modo de violação à privacidade, é feito o seguinte comentário:

> Em particular, a interferência sobre a privacidade alheia não pode ser implementada como efeito natural ou subproduto necessário das inovações tecnológicas que surgem no mercado. São as inovações tecnológicas que devem ser (re)adaptadas para evitar a violação à privacidade. Tal violação somente pode ser admitida quando justificada à luz de uma delicada ponderação com outros interesses igualmente protegidos, como a proteção à saúde, à identidade e assim por diante. Esta é uma constatação a que não apenas os juristas, mas todas as pessoas, devem permanecer atentas. Mesmo porque, com alguma frequência, são os próprios titulares do direito à privacidade os primeiros a promoverem a sua violação. (SCHREIBER, 2013, p. 182-183).

Com a popularização da internet, a privacidade também precisa ser discutida, considerando o *e-mail*, o *spam*, os *cookies* e as redes sociais.

O *e-mail* é utilizado para troca de mensagens entre seus titulares. Seus usuários não precisam estar disponíveis ao mesmo tempo, de forma que as

[22] SCHREIBER, Anderson. **Direitos da Personalidade**. 2. ed. São Paulo: Atlas, 2013

mensagens recebidas e enviadas ficam armazenadas. Um dos problemas dessa forma de comunicação é que um mesmo usuários pode ter inúmeras contas de *e-mail*. A má utilização desta possibilidade pode conduzir a produção de *spam*, que são envios em massa de mensagens não solicitadas, com teor, em regra, comercial. A utilização dos serviços disponíveis na internet pressupõe, na grande maioria das vezes, a disponibilização do e-mail, como, por exemplo, a criação de uma conta em uma rede social ou um site de comércio. Alencar et al[23] demonstra a seguir como se desdobra a violação da privacidade nesse contexto:

> Outro ponto que merece destaque é a consequência de todo o processo explanado previamente: o primeiro passo para que o indivíduo tenha sua privacidade violada é o fornecimento do e-mail como um dado pessoal, pois dessa forma um número indefinido de pessoas podem contatá-lo de maneira inconveniente; após isso, o seu e-mail acaba por tornar-se uma coleção de dados pessoais por conter informações e mensagens que podem ou não serem publicadas; em seguida esse conjunto preciosíssimo de dados é transmitido ou até mesmo comercializado à outras empresas para a construção de perfis de usuários e de anúncios publicitários direcionados. (ALENCAR et al, 2016, p. 10).

Quanto aos *cookies*, eles são dados trocados entre o servidor da página da internet e o computador do usuário. Eles identificam as preferências e tornam a navegação mais personalizada e mais rápida. Também configuram como violação da privacidade e captação de dados, de forma que o titular não tem controle sobre as suas informações que são captadas.

A popularização das redes sociais mudou a forma como as pessoas fazem contato com o mundo e com as outras pessoas. Tornou-se comum ser necessário, principalmente entre os jovens, estar a todo momento atualizando seus amigos ou seguidores sobre aspectos da vida cotidiana, que em outra época, eram privadas e poucos relevantes para comentários. Sobre este novo comportamento, Araújo et al[24] comenta:

---

[23] ALENCAR, Ianara de Sousa; PACHECO, Ludgard Vinicius Andrade; FERREIRA, Rodrigo Leal. A EVOLUÇÃO DO CONCEITO DE PRIVACIDADE DIANTE DAS NOVAS TECNOLOGIAS UTILIZADAS NOS CORREIOS ELETRÔNICOS (E-MAIL). **Revista de Direito Uninovafapi**, Teresina, v. 1, n. 1, p.1-17, 2016. Disponível em: https://revistainterdisciplinar.uninovafapi.edu.br/index.php/revinterdireito/article/view/1106>. Acesso em: 29 abr. 2018.

[24] ARAÚJO, Antônio Carlos da Silva et al. A INDISPONIBILIDADE DA PERSONALIDADE E AS REDES SOCIAIS. **Cadernos de Graduação**: Ciências Humanas e Sociais, Alagoas, v. 3, n. 3, p.85-

> A internet é uma ferramenta que une vários tipos de mídia em apenas um ambiente, e permite uma troca de informações de maneira mais rápida e prática. Porém, apesar de ser tão útil em nossas vidas há de se observar também o outro lado. Com o surgimento das redes sociais a princípio com intuito de aproximar pessoas, compartilhar informações e romper fronteiras, observa-se que, atualmente, estes limites já ultrapassaram os limites, além de serem usadas para conhecer, encontrar e reencontrar pessoas, o foco agora é outro, o intuito é aparecer e mostrar sua vida e algumas vezes a dos outros. (ARAÚJO et al, 2016, p. 94).

O autor continua, ao demonstrar como essa superexposição pode ser prejudicial:

> Tendo em vista os problemas que os usuários possam vir a enfrentar se aspectos da sua vida particular forem expostos, deve ser estendida ao direito de controlar de que forma as informações sobre a sua pessoa serão usadas por terceiros. De fato, dependendo do cruzamento de informações que outrem possa fazer, a pessoa poderá ficar exposta a situações constrangedoras, ou que redundem em violação à sua honra, imagem ou intimidade, deve-se haver o equilíbrio entre a liberdade de expressão e informação e o direito à privacidade e intimidade. (ARAÚJO et al, 2016, p.87).

O direito a ser esquecido, ligado ao direito à privacidade, como um dos direitos da personalidade, tem fundamento na dignidade da pessoa humana. Esse direito se sobrepõe ao direito de imprensa ou a liberdade de expressão quanto a fatos passados que não possuem relevância atual e interesse público para serem relembrados. Dar uma nova atenção injustificada acarreta violação a imagem e a privacidade da pessoa envolvida no assunto. Tal violação não se restringe ao agente principal, mas também se estende aos direitos das demais pessoas que compõem seu núcleo de convívio social. É necessário que fatos pretéritos sejam superados para que a pessoa possa seguir sua vida e construir a sua identidade.

Podendo ser chamado também de direito a ser esquecido, tem a seguinte conceituação conforme Diniz[25]:

100, nov. 2016. Disponível em: https://periodicos.set.edu.br/index.php/fitshumanas/article/view/3579>. Acesso em: 27 abr. 2018.

[25] DINIZ, Maria Helena. Uma visão constitucional e civil do novo paradigma da privacidade: o direito a ser esquecido/A constitutional and civil vision of the new privacy paradigm: the right to be forgotten. **Revista Brasileira de Direito**, Passo Fundo, v. 13, n. 2, p. 7-25, ago. 2017. ISSN 2238-0604. Disponível em: https://ser.imed.edu.br/index.php/revistadedireito/article/view/1670. Acesso em:30 abril 2018.

> O direito a ser esquecido é o direito que a pessoa tem por ex. de opor-se à lembrança de atos verídicos reprováveis, outrora praticados por ela, que perderam, pelo decurso do tempo, a atualidade e que só devem ficar na sua memória por constituir a sua própria história, evitando que sua republicação seja um obstáculo à sua vida presente e ao pleno desenvolvimento de sua personalidade, possibilitando o arrependimento e a pratica de condutas louváveis, mediante a consecução de projetos conducentes a uma vida digna e a uma convivência social como se aquele passado nunca houvesse existido. O direito a ser esquecido consiste no de não ressuscitar informações que o decorrer do tempo sepultou, deixando-as envoltas, como diz Sgroi, nos véus do esquecimento e permitindo à pessoa uma segunda chance de recomeçar a sua vida. Visa, portanto, a tutela da memória individual relativa às recordações íntimas e experiências vividas para possibilitar o desenvolvimento do ser humano, sendo instrumento do direito à identidade pessoal. (DINIZ, 2017, p. 16).

Apesar de, em regra, somente se considerar que fatos negativos seriam desejáveis de ser esquecidos, Diniz[26] contribui ao tema que condutas positivas também podem ser abarcadas pelo direito ao esquecimento, como se percebe na passagem:

> O direito a ser esquecido não tutela apenas pessoa que não deseja rememorar lesão sofrida por fato pretérito de conduta negativa, mas também de condutas positivas, tais como: um ato de coragem, que, ao resistir, por ex., a um estupro, acaba provocando a morte do agressor, ou o desejo de uma celebridade de ficar só e viver em paz. Consiste, portanto, no direito a ser esquecido pela imprensa ou opinião publica e no de apagar dados ou fatos passados sobre a vida das pessoas que não devem ser rememorados. (DINIZ, 2017, p. 11).

Com a internet, tornou-se mais difícil garantir o direito ao esquecimento. Qualquer pessoa pode, atualmente, pesquisar sobre uma notícia datada de anos atrás. Com a grande quantidade de informações disponíveis e a quase impossibilidade de se manter fora da internet, é possível ter informações sobre o passado e o presente das pessoas. O armazenamento digital é muito menos

[26] DINIZ, Maria Helena. Uma visão constitucional e civil do novo paradigma da privacidade: o direito a ser esquecido/A constitutional and civil vision of the new privacy paradigm: the right to be forgotten. **Revista Brasileira de Direito**, Passo Fundo, v. 13, n. 2, p. 7-25, ago. 2017. ISSN 2238-0604. Disponível em: https://ser.imed.edu.br/index.php/revistadedireito/article/view/1670. Acesso em:30 abril 2018.

suscetível a perda permanente de informações do que os armazenamentos físicos de outrora. Sobre essa permanente disponibilidade de informações, Diniz[27] propõe:

> A ordem natural das coisas conduz ao esquecimento de certos fatos passados. Deveras, existem alguns acontecimentos que devem ser olvidados e outros que devem ser sempre lembrados. Se assim é, para que informações, outrora, tornadas públicas não sejam mais divulgadas, dever-se-á dificultar o acesso a elas, restringindo, por ex., o uso de bancos de dados, onde tais informações estiverem armazenadas por um determinado lapso temporal; impor prazo para exibição de fatos ocorridos, de reportagens ou de documentários; vedar sensacionalismo e repetição desnecessárias etc. (DINIZ, 2017, p. 15).

O direito a ser esquecido teve sua origem histórica no campo das condenações criminais onde se buscava permitir a ressocialização do ex-detento. Hoje esse direito se estende a quaisquer fatos passados que possam ser considerados socialmente reprováveis, que quando relembrados geram algum prejuízo ou sofrimento a pessoa que o praticou, seja por estar impelido de uma vontade de transgredir ou um descuido ou a inexperiência. Como já demonstrado acima, condutas positivas também podem merecer ser esquecidas. Com a internet, se tornou ainda mais difícil garantir que alguns acontecimentos permaneçam no passado. Contudo, tal dificuldade não deve impedir o direito de garantir que as pessoas construam a sua identidade, tendo sua privacidade preservada e possibilitando a superação do passado. Somente assim será garantir a realização da dignidade da pessoa humana.

2.2. MARCO CIVIL DA INTERNET – LEI Nº 12.965/14

O Marco Regulatório Civil da Internet Brasileira, ou apenas Marco Civil. É a Lei 12.965 de 23 de abril de 2014, que foi elaborada com consulta pública e pretender ser uma “Constituição da Internet”, de forma a tutelar as novas problemáticas envolvendo questões patrimoniais e existenciais no ambiente da internet.

[27] DINIZ, Maria Helena. Uma visão constitucional e civil do novo paradigma da privacidade: o direito a ser esquecido/A constitutional and civil vision of the new privacy paradigm: the right to be forgotten. **Revista Brasileira de Direito**, Passo Fundo, v. 13, n. 2, p. 7-25, ago. 2017. ISSN 2238-0604. Disponível em: https://ser.imed.edu.br/index.php/revistadedireito/article/view/1670. Acesso em:30 abril 2018.

As questões existenciais estão relacionadas a liberdade de expressão, a proteção da privacidade e controle de dados. As questões patrimoniais dizem respeito as novas formas de comércio realizadas na internet e a grande disponibilização ilegal de conteúdo, afetando direitos autorais, matéria sobre a qual há um polêmico dispositivo nesta lei.

Ao longo de seus trinta e dois artigos, a lei define os fundamentos e princípios do uso da internet no Brasil, trata dos direitos e garantias dos usuários, e dispõe sobre a neutralidade de rede, liberdade de expressão, proteção da privacidade quanto os registros de navegação e os dados pessoais e a responsabilização dos provedores.

A neutralidade da rede significa que os provedores de aplicações e de serviços de internet não podem discriminar os dados que trafegam nas suas estruturas, não importando o conteúdo, origem ou destino.

Recentemente, as principais operadoras de Internet fixa no Brasil buscaram adotar restrições no consumo, de forma que se o consumidor excedesse sua cota mensal, a velocidade da Internet seria reduzida ou suprimida. Tal medida iria de encontro a forma que sempre foi contratada a internet no país, momentos nos quais, era contratada de acordo com a velocidade da internet.

Se essa medida tivesse avançado, haveria grande disparidade entre a disponibilidade de internet entre seus usuários, causando segregação social. Muitas pessoas não poderiam pagar por grandes cotas de uso e teria um acesso ruim e de baixa velocidade ou seriam excluídas da internet.

Mesmo que já ocorra na Internet Móvel utilizada em *smartphones*, essa medida seria um grande retrocesso ao alcançar a Internet Fixa. Sem a neutralidade na rede, o cenário seria o seguinte, conforme Longhi[28]:

> Preconiza-se que a ausência de neutralidade na Rede traria seis grandes possíveis riscos: 1. Filtragem pelos provedores de qual conteúdo é ou não acessado aos usuários; 2. Formação de monopólios verticais entre provedores de conteúdo, acesso e hospedagem com sensível diminuição do poder de escolha dos consumidores acerca do que acessam; 3. Controle de preços e formação de carteis; 4. Diminuição do tempo médio de velocidade para o consumidor final; 5. Restrição à inovação

[28] LONGHI, João Victor Rozatti. Marco Civil da Internet no Brasil: breves considerações sobre seus fundamentos, princípios e análise crítica do regime de responsabilidade civil dos provedores. In: MARTINS, Guilherme Magalhães et al (Coord.). **Direito Privado e Internet.** São Paulo: Atlas, 2014. Cap. 5. p. 109-145

> tecnológica, 6. Diminuição das possibilidades de expressão política na Internet. (LONGHI, 2014, p. 111).

Admitir essa restrição significa restringir a liberdade de expressão e afetar os novos hábitos sociais que foram criados e alterados pela evolução tecnológica e pela internet, interferindo na criação da identidade pessoal.

Quanto à proteção a privacidade, prevista no art. 7º, a lei trata da proteção aos registros, aos dados pessoais e comunicações privadas. A proteção a esse direito é fundamental, pois, os espaços públicos e privados estão muitos relacionados, uma vez que os usuários estão muito mais propensos a voluntariamente dispor de suas informações.

O Marco Civil objetiva evitar práticas de vigilância e, em seu art. 5º, conceitua alguns termos como: internet, terminal, endereço de protocolo de internet (endereço IP), administrador de sistema autônomo, conexão à internet, registro de conexão, aplicações de internet e registros de acesso a aplicações de internet.

Nos arts. 10 a 17 estão os dispositivos que tratam da proteção e guarda dos registros, dados pessoais e comunicações pessoais de forma a pautar a atuação dos provedores intermediários.

Em seu art. 11, a lei determina que os provedores que processam dados pessoais de usuários localizem pelo menos um de seus terminais no Brasil. Com isso, se objetiva evitar situações em que decisões judiciais emitidas no Brasil não possuam efetividade em território internacional devido a diferenças entre a legislação nacional e estrangeira.

A possibilidade de sanções cíveis, criminais e administrativas estão previstas no art. 12.

Quanto a guarda de registros de conexão, o art. 13 prevê que o administrador deve mantê-los por um ano. Tal prazo poderá ser expandido mediante requerimento cautelar da autoridade policial ou administrativa ou o Ministério Público, conforme o parágrafo segundo.

O art. 14 veda o registro de acesso a aplicações de internet pelos provedores.

Do art. 15 ao 17, se trata dos registros de acesso a aplicações de internet na provisão de aplicações. Neste tema, o dever surge quando o provedor de aplicações de internet é pessoa jurídica, que exerça atividade de forma organizada, profissionalmente e com fins econômicos. A guarda dos registros será pelo prazo de

seis meses, o qual poderá ser prorrogado através de requerimento cautelar, conforme hipótese do parágrafo segundo do art. 15. Exige-se determinação judicial para disponibilização dos registros.

Do art. 18 ao 21 é tratada a responsabilidade por danos decorrentes de conteúdo gerado por terceiro. A regra no art. 18 privilegia a neutralidade da rede e a liberdade de expressão ao determinar que o provedor de conexão à internet não será responsabilizado civilmente por dano causado por conteúdo produzido por terceiro como, por exemplo, o *spam*. Quanto a este artigo, Longhi[29] faz a crítica:

> Portanto, o art. 18 é uma decorrência natural da neutralidade, por sua vez um princípio tecnológico estrutural da Rede. Se o provedor de acesso pretende filtrar conteúdo como estratégia de negócios, nada obstaria que fosse responsabilizado pelo conteúdo dos seus consumidores. Faz parte de seu risco-proveito, cabendo ação de regresso contra o causador do dano. (LONGHI, 2014, p. 122).

O provedor de aplicações de internet somente será responsabilizado civilmente se, após ordem judicial, não forem tomadas as providências necessárias para tornar indisponível o conteúdo danoso produzido por terceiro. Além disso, o art. 19 demonstra expressamente o seu intuito de assegurar a liberdade de expressão e impedir a censura.

O parágrafo primeiro do art. 19 diz que a ordem judicial deve indicar claramente a localização do conteúdo infrator que será tornado indisponível. Essa disposição ao evitar uma ordem genérica, não se coaduna com a realidade da internet, onde um conteúdo se espalha em grande velocidade e fica disponível em inúmeros *sites*. Tal medida permite uma proteção insuficiente da vítima que teve lesado seu direito da personalidade e facilita indevidamente a atuação do administrador do *site*, que possui os meios necessários de impedir a propagação do conteúdo.

O parágrafo segundo do art. 19 ao excluir os direitos do autor e conexos do sistema do Marco Civil, onde se condiciona a responsabilização civil à ordem judicial, atende aos interesses da industrial cultural. Esse favorecimento à uma ótica

[29] LONGHI, João Victor Rozatti. Marco Civil da Internet no Brasil: breves considerações sobre seus fundamentos, princípios e análise crítica do regime de responsabilidade civil dos provedores. In: MARTINS, Guilherme Magalhães et al (Coord.). **Direito Privado e Internet.** São Paulo: Atlas, 2014. Cap. 5. p. 109-145

patrimonialista em detrimento da dignidade da pessoa humana, está demonstrado na crítica de Martins[30]:

> Nesse ponto, o Marco Civil, paradoxalmente, consagra a prevalência das situações patrimoniais sobre as existenciais, caso em que a responsabilidade do provedor em face das vítimas depende de um a prévia notificação judicial, o que não se aplica, portanto, ao titular do direito autoral. Conferir aos interesses da indústria cultural, em função da titularidade dos direitos patrimoniais do autor (*copyright*) em face das vítimas de danos sofridos através das ferramentas de comunicação da Internet, como as redes sociais, significa inverter os valores fundamentais contidos na tábua axiológica da Constituição da República. (MARTINS, 2016, p. 260).

No parágrafo terceiro do art. 19, há a possibilidade de conhecimento das ações nos juizados especiais quando se tratar dano à honra, à reputação ou a direitos da personalidade, por conteúdo disponível na internet. O parágrafo quarto do mesmo artigo, permite a antecipação dos efeitos de tutela que consiste em retirada de conteúdo, sendo a verossímil a alegação do autor, com prova inequívoca do fato, considerado o interesse público no conteúdo e o receio de que o dano se torne irreparável ou de difícil reparação.

O uso de tutelas antecipadas já era comum na prática anterior a lei, como indica Longhi[31]:

> Contudo, a prática tem demonstrado que maioria esmagadora de decisões judiciais em ações desta natureza, que determinam a retirada de conteúdo, é oriunda de tutela antecipada (art. 273, CPC) ou de medidas cautelares em que se prescinde do contraditório, *a priori*, para sua determinação. (LONGHI, 2014, p. 124).

O art. 20 determina que o provedor deverá comunicar, quando possível, ao usuário titular do conteúdo indisponível, as razões de tal ato, de forma a possibilitar o contraditório e a ampla defesa. O parágrafo único do mesmo artigo prevê que o titular do conteúdo poderá solicitar que o teor da ordem judicial substitua o local do conteúdo indisponível.

---

[30] MARTINS, Guilherme Magalhães. **Contratos eletrônicos de consumo**. 3. ed., rev. atual. e ampl. São Paulo: Atlas, 2016.

[31] LONGHI, João Victor Rozatti. Marco Civil da Internet no Brasil: breves considerações sobre seus fundamentos, princípios e análise crítica do regime de responsabilidade civil dos provedores. In: MARTINS, Guilherme Magalhães et al (Coord.). **Direito Privado e Internet.** São Paulo: Atlas, 2014. Cap. 5. p. 109-145

Quanto a disponibilização não autorizada de conteúdos contendo nudez ou atos sexuais de caráter privado, o art. 21 traz um tratamento diverso, mais célere e condizente coma realidade atual. A responsabilidade subsidiária do provedor ocorre caso ele não atue de forma diligente para tornar indisponível o conteúdo, após a notificação do participante.

Como se percebe, o Marco Civil traz uma excessiva judicialização das situações em que há infração a direitos na internet. Por mais que se busque uma maior positivação em regras jurídicas, os meios previstos protegem as vítimas na internet de forma menos eficiente. Quanto a essa problemática, Martins[32] destaca:

> Em plena era dos meios alternativos de solução de conflitos, como a mediação e a arbitragem, o Marco Civil judicializa questões que já se encontravam resolvidas por outros instrumentos mais ágeis, como os Termos de Ajustamento de Conduta (TACs). (MARTINS, 2016, p. 258).

No mesmo sentido, Longhi[33] propõe:

> Caso o escopo seja o da promoção de um contraditório prévio à retirada do conteúdo, resguardando a liberdade de expressão do usuário que o produziu, é certo que o texto também elege via inadequada, haja vista que , para evitar um número desenfreado de ações judiciais, nada impede que os tribunais brasileiros disponibilizem um link com o indicativo “denuncie aqui”, criem um “juizado especial de notificações para retirada de conteúdo da Internet” para que, por seu turno, se proceda à notificação eletrônica a qual vise à obtenção de ordem judicial com a assinatura criptografada de magistrado.
> Por essas razões, o sistema da notificação para a retirada por via extrajudicial, consolidado jurisprudencialmente, ainda que dê azo para o retorno da vetusta culpa na seara da responsabilidade civil, desprotege menos a vítima do que aquele proposto pela atual redação do Marco Civil. Mas, conforme se verá, este não é o único objeto de críticas. (LONGHI, 2014, p. 125).

A internet é um ambiente amplo que mudou as formas de socialização das pessoas. Por ser extremamente dinâmica, há a todo momento novas informações. Ao mesmo tempo em que algo se torna disponível, várias pessoas podem fazer com

[32] MARTINS, Guilherme Magalhães. **Contratos eletrônicos de consumo**. 3. ed., rev. atual. e ampl. São Paulo: Atlas, 2016.
[33] LONGHI, João Victor Rozatti. Marco Civil da Internet no Brasil: breves considerações sobre seus fundamentos, princípios e análise crítica do regime de responsabilidade civil dos provedores. In: MARTINS, Guilherme Magalhães et al (Coord.). **Direito Privado e Internet.** São Paulo: Atlas, 2014. Cap. 5. p. 109-145

que o alcance seja aumentado. O direito precisa estar preparado para garantir de forma mais imediata possível a proteção dos direitos da personalidade, para evitar que o dano se torne irreparável. Afinal, a imagem, a honra e a privacidade das pessoas na internet, contribuem para a criação de sua identidade virtual, que gera reflexos em suas relações no mundo real.

2.3. DESRESPEITO AO DIREITO À PRIVACIDADE NA INTERNET

A vida na atualidade é inconcebível sem a internet. É possível estar conectado com fio, havendo todo um cabeamento entre a recepção do sinal do provedor de internet e a conexão para utilização nos aparelhos ou sem fio, através de modems ou roteadores, que permitem um alcance definido conforme a sua potência, facilitando a organização. Dentre os inúmeros aparelhos disponíveis, podem ser citados os computadores, os *tablets*, os *smartphones*, as *smart tv* e os *smart watch*. Deve-se ressaltar que a evolução tecnológica é um movimento presente e atual, o que permite que novas tecnologias sempre surjam modificando mais uma vez as formas como as pessoas estão conectadas a todo momento e em qualquer lugar.

Estar conectado também significa, para muitas pessoas, estar disponibilizando suas informações para seus contatos. Porém, ao mesmo tempo, os serviços utilizados também captam as informações do usuário, mesmo que sem autorização prévia ou de forma oculta, através dos *cookies*. Outra possibilidade é a atuação de pessoas mal-intencionadas, que possuem conhecimento de informática, os chamados *crackers*, que exploram as fragilidades dos códigos que compõem os diversos sites e programas que são acessados na internet, e obtém ilegalmente dados pessoais para proveito próprio.

Com as redes sociais, as pessoas se habituaram a sempre atualizar seus perfis sobre os lugares que conheceram, as coisas que compraram, os filmes e músicas que viram ou ouviram. Voluntariamente, foi formado um banco de dados que permite que redes como o *Facebook*, saibam exatamente o que as pessoas gostam e possam sugerir o que elas poderiam gostar.

Da mesma forma, o popular mecanismo de busca chamado *Googl*e, da empresa de mesmo nome, armazena o que é buscado pelo usuário e torna mais eficiente a sua utilização. Ao mesmo tempo, torna as propagandas na internet melhor direcionadas para o interesse da pessoa.

Tudo isso ocorre através dos *cookies* que armazenam informações nos servidores das empresas e nos computadores dos usuários, de forma a navegação ser mais rápida e direcionada. Comumente, não fica clara a forma de vedar a captação das informações. Com isso, sob o manto de atender ao interesse do internauta, suas informações são utilizadas sem a sua autorização, ferindo de forma contínua a sua privacidade.

Quanto aos *cookies*, Martins[34] faz o seguinte comentário:

> Constituem os cookies verdadeiros bancos de dados nos quais são armazenadas as informações sobre o usuário, na maioria das vezes sem o seu consentimento, afrontando não somente a privacidade, como ainda a autodeterminação informativa do internauta. (MARTINS, 2014, p. 255).

Um constante questionamento é o que as grandes empresas da informática fazem com os dados que elas possuem de seus usuários. Por estarem a sua disposição, eles poderiam ser vendidos. Infelizmente, tal prática, mesmo que considerada ilegal, ocorre de forma oculta e, quando é descoberta, não poderia deixar de ter grande destaque.

O mais recente caso foi o do *Facebook* que vendia os dados de seus usuários para a *Cambridge Analytica*, uma empresa de mineração e análise de dados para campanhas políticas. O vazamento se iniciou em um teste feito pelos usuários da rede social, onde respondiam perguntas sobre personalidade que permitiam construir seu perfil. As pessoas que realizavam esse teste tinham suas informações captadas, algo que era informado pelo aplicativo, porém os amigos dessas pessoas também tinham suas informações alcançadas. Com isso, milhares pessoas realizaram o teste, porém as informações compartilhadas foram de milhões de pessoas. Este acontecimento, afetando usuários de todo o mundo, levou o fundador e presidente-executivo do *Facebook*, Mark Zuckerberg a responder perguntas de deputados na Câmara dos Estados Unidos, no dia 11 de abril de 2018. Na situação,

[34] MARTINS, Guilherme Magalhães. **Responsabilidade civil por acidente de consumo na Internet**. 2. ed. São Paulo: Editora Revista dos Tribunais, 2014.

levantou-se o questionamento da necessidade de regulação para as empresas do setor sobre a forma que elas gerenciam a quantidade maciça de dados pessoais que elas possuem.

Nesse novo ambiente virtual, onde até mesmo as empresas do setor adotam condutas que desrespeitam a privacidade, deve-se atentar aos *crackers*, que se utilizam de seu conhecimento para burlar os sistemas, de forma a captar ilegalmente as atividades de outros usuários, buscando algum proveito.

Com a prática do comércio na internet, devem ser adotadas medidas de segurança adequadas, como a criação de um ambiente seguro pelas empresas, e a utilização de programas de proteção pelos usuários, contra vírus, espiões e demais meios danosos utilizados pelos *crackers*. As pessoas podem ser vítimas de roubo de dados como, por exemplo, o endereço devido a disponibilização da localização geográfica, números de cartões gravados em sites, o que está sendo digitado através *keylogger*.

Inclusive no *email* as pessoas podem ter sua privacidade violada através do *spam*, que são mensagens enviadas em massa com conteúdo geralmente comercial, que não são solicitadas pelos usuários na maioria das vezes.

Mesmo que usuários mais jovens considerem mais tolerável essa insegurança da navegação na internet, é válido considerar a seguinte possibilidade, conforme Moreira[35]:

> Quando alguns consumidores são alertados sobre os perigos da internet, eles acabam desistindo da navegação. Deixam de acessar os sites que vendem livros específicos, optam por não receber emails de certos fornecedores, preferem evitar a compra de certos produtos pela internet, ou acabam voltando às filas dos bancos por temerem a revelação de dados bancários. Ou seja, ocorre um efeito absolutamente lesivo da liberdade do ser humano. (MOREIRA, 2015, p. 54).

Sobre o mesmo ponto, o autor faz as necessárias indagações:

> Por enquanto o interesse tem se voltado para o *e-marketing.* Mas, resta indagar: Até quando será possível garantir que estas informações pessoais (de cada ser humano que habita o planeta Terra) não serão objeto de acesso pelos Estados? Que tipo de incômodos, o conhecimento de certas informações, divulgadas pelos próprios internautas, é capaz de gerar nos

[35] MOREIRA, Adriano Fernandes. A ABUSIVIDADE DAS PRÁTICAS COMERCIAIS E DA PUBLICIDADE NA PRESTAÇÃO DE SERVIÇOS GRATUITOS PELO GOOGLE. **Revista Cereus**, Gurupi, v. 7, n. 1, p.40-59, jan/abr. 2015. Disponível em: <http://www.ojs.unirg.edu.br/index.php/1/article/view/567>. Acesso em: 01 maio 2018.

> seres humanos? Estar-se-á à vontade sabendo que outras pessoas têm conhecimento do que ocorre em sua vida privada?. (MOREIRA, 2015, p.55).

Um caso que chamou a atenção foi o dos aplicativos *Lulu* e *Tubby*, onde homens e mulheres avaliavam a qualidade de uma pessoa específica do sexo oposto. Os perfis eram criados no aplicativo, independentemente da aceitação do avaliado, de acordo com as informações presentes no *Facebook*, situação que gerava danos à privacidade, à honra e à imagem do indivíduo. Com isso, se criou um debate onde se discutia se o aplicativo era uma forma de desrespeito e uso indevido de informação do avaliado ou meramente um meio de diversão. Houve decisão judicial determinando que o aplicativo permitisse a retirada de informações de quem solicitasse e, com a polêmica, culminou com a suspensão de seu funcionamento.

Outra forma de se desrespeitar a privacidade na internet que tem se repetido nos últimos tempos é pornografia de vingança ou *revenge porn*. Trata-se da divulgação, sem o consentimento, de imagens ou vídeos íntimos de um parceiro ou parceira, com o fim de causar dano à vítima. Em regra, as vítimas são mulheres e, quanto a prática deste ato ilegal, destacam Amaral e Chaves[36]:

> Ademais, através de estudo realizado em junho de 2015 com 2.437 brasileiras a partir de 12 anos pela Universidade de São Paulo (USP), os pesquisadores constataram haver seis possíveis explicações para o “revenge porn”, sendo estas: i) geração conectada e livre; ii) educação insuficiente; iii) ambiente competitivo; iv) cultura da pornografia; v) machismo; e vi) julgamento. (AMARAL e CHAVES, 2016, p. 89).

Todo o costume de exposição da vida privada na internet, possibilitou o desenvolvimento de um grupo de pessoas, chamados *stalkers*, que possuem a necessidade de acompanhar e, às vezes, participar da vida alheia. Agem de forma repetida, por algum tempo, causando danos e atrapalhando a vida cotidiana da

[36] DO AMARAL, Ana Beatriz Nunes Paiva; CHAVES, Fernanda Maria de Assunção Furtado. TUTELA DO DIREITO AO ESQUECIMENTO NO BRASIL: CASO FABÍOLA E SUA RELAÇÃO COM O REVENGE PORN. **Revista Pesquisas Jurídicas**, v. 5, n. 1, p. 72-94, fev/jun 2016. Disponível em: < http://www.revistapesquisasjuridicas.com.br/ojs/index.php/RPJur/article/view/127>.Acesso em:02 maio 2018.

vítima. Essa prática, chamada de *stalking*, tem a seguinte definição, conforme Machado e Mombach[37]:

> [...] A prática deste se consubstancia em ações de perseguição, intimidação e ameaças, em que o autor busca aproximação com sua vítima por diversas motivações (amor, ciúmes, idolatria, ódio, inveja etc), atentando contra sua integridade, predominantemente psicológica, mas também física, e vida, intimidade e privacidade. A forma mais usual e prática de perseguição se dá por meio das redes sociais e telefone, mas nada impede que seja também pessoalmente, por exemplo, vigiando a casa de seu alvo ou o seguindo. (MACHADO e MOMBACH, 2016, p. 217-218).

A internet está presente no cotidiano das pessoas. Apresenta inúmeros benefícios e se tornou uma necessidade, porém também é um meio pelo qual as pessoas podem ter sua privacidade e demais direitos infringidos, mesmo sem tomar conhecimento disto. Por essa razão, cabe ao direito definir os limites de atuação dos detentores e desenvolvedores das tecnologias, quanto aos dados pessoais e propor formas de proteger a privacidade e reparar os danos causados pelos infratores.

[37] MACHADO, Jessika Milena Silva; MOMBACH, Patrícia Ribeiro. STALKING: CRIMINALIZAÇÃO NECESSÁRIA SOB A INDUBITÁVEL AFRONTA AO DIREITO FUNDAMENTAL À VIDA PRIVADA. **Revista da Esmesc**, Florianópolis, v. 23, n. 29, p.207-230,. 2016. Disponível em: <https://www.revista.esmesc.org.br/re/article/view/146>. Acesso em: 02 maio 2018.

3. AS DIFERENTES MEDIDAS DE PROTEÇÃO DA PRIVACIDADE

3.1. ASPECTOS DOUTRINÁRIOS

Com a disponibilidade contínua da internet e com o seu uso a qualquer momento e em qualquer lugar, as pessoas estão constantemente disponibilizando voluntariamente suas informações, ou elas são captadas sem o seu conhecimento. Para buscar a proteção da privacidade na internet é necessária a observação de algumas questões.

A privacidade, como um direito fundamental, está prevista na Constituição Federal no art. 5º, incisos X e XII, que tratam da inviolabilidade da intimidade, da vida privada, da honra e imagem das pessoas, assim como quanto as correspondências, comunicações telegráficas, de dados e das comunicações telefônicas. No Código Civil, a proteção a privacidade está no art. 21. Quaisquer interferências nesse direito, necessitam de ordem judicial proveniente do juiz.

Porém, a relativização da privacidade também pode ocorrer de forma voluntária pelo seu titular, devendo sempre ser observada a finalidade pela qual ele admitiu essa limitação.

Uma das formas de se violar a privacidade na internet é através do *spam*. Eles são mensagens eletrônicas não solicitadas que as pessoas recebem em seus correios eletrônicos na internet, cujo conteúdo tende a estar relacionado com propagandas de produtos ou serviços. Eles são utilizados por serem de baixo custo, porém podem causar queda da qualidade da internet para os usuários em geral, em função de seu envio em grande quantidade.

Quanto a limitação das comunicações comerciais indesejadas, Martins [38] destaca:

> Os países da União Europeia dispõem de uma legislação limitativa das comunicações comerciais indesejadas, mediante sistemas de proteção que oscilam entre *opt-out* – que só proíbe o envio de *e-mails* não solicitados no caso de o usuário manifestar-se expressamente em sentido contrário – e o *opt-in* – segundo o qual a

[38] MARTINS, Guilherme Magalhães. **Responsabilidade civil por acidente de consumo na Internet**. 2. ed. São Paulo: Editora Revista dos Tribunais, 2014.

> legitimação do *spam* somente pode ocorrer mediante o prévio consenso do interessado. (MARTINS, 2014, p. 241).

Também sobre os sistemas *opt-in*, *opt-out* e, dentre eles, o adotado pelo Marco Civil da Internet, Lima e Junior[39] explicam:

> Conforme exposto quando da análise do artigo 7.º, da Lei 12965/2014, o sistema adotado pelo nosso ordenamento jurídico é denominado o*pt-in*, neste modelo, o usuário deverá consentir de forma expressa e inequívoca, quanto ao tratamento dos seus dados pessoais. Por outro lado, o sistema *opt-out* (não adotado em nosso sistema) prevê que o usuário deve manifestar de forma expressa o seu interesse em sair, isto porque, o pressuposto é de concordância automática. (LIMA e JUNIOR, 2016, p. 252)

Os autores também explicitam as seguintes condições necessárias para que o consentimento do usuário seja válido no sistema *opt-in* do Marco Civil:

> Por esta razão, para considerar válido o consentimento do usuário é imprescindível que: (i) a informação sobre a coleta dos seus dados ocorra de forma adequada e clara, a permitir a sua inequívoca compreensão; (ii) consentimento prévio e expresso do usuário; (iii) nula de pleno direito a coleta realizada sem a observância dos itens “i” e “ii”. (LIMA e JUNIOR, 2016, p. 253).

Outra forma de se garantir a privacidade é o uso da criptografia, a qual possui o seguinte significado, conforme Teixeira et al[40]:

> A palavra criptografia é formada pelos termos gregos *kryptos*, que significa secreto, oculto, ininteligível, e *grapho*, que significa escrita, escrever. Trata-se da ciência/arte de se comunicar secretamente. O objetivo básico da criptografia é tornar uma mensagem ininteligível para um adversário, que possa vir a interceptar a mensagem. Hoje a criptografia é um

[39] LIMA, Marco Antônio; BARRETO JUNIOR, Irineu Francisco. MARCO CIVIL DA INTERNET: LIMITES DA PREVISÃO LEGAL DE CONSENTIMENTO EXPRESSO E INEQUÍVOCO COMO PROTEÇÃO JURÍDICA DOS DADOS PESSOAIS NA INTERNET. **Revista de Direito, Governança e Novas Tecnologias**, Brasília, v. 1, n. 2, p.241-260, jan/jun. 2016. Disponível em: <http://indexlaw.org/index.php/revistadgnt/article/view/831>. Acesso em: 09 maio 2018.

[40] TEIXEIRA, Tarcísio; SABO, Paulo Henrique; SABO, Isabela Cristina. WHATSAPP E A CRIPTOGRAFIA PONTO-APONTO: TENDÊNCIA JURÍDICA E O CONFLITO PRIVACIDADE VS. INTERESSE PÚBLICO. **Revista da Faculdade de Direito**: Universidade Federal de Minas Gerais, Belo Horizonte, n. 71, p.607-638, jul/dez. 2017. Semestral. Disponível em: <https://www.direito.ufmg.br/revista/index.php/revista/article/view/1882>. Acesso em: 10 maio 2018.

> campo de estudos abrangente, incluindo diversos aspectos da segurança de dados em geral, razão pela qual se tornou alvo de extensas pesquisas científicas. Não só quem manda a mensagem, mas também quem a intercepta, deve possuir um considerável poder computacional. (TEIXEIRA et al, 2017, p. 615).

Para explicar o processo de criptografia, os autores retro mencionados exemplificam com o modelo mais simples, chamado cifra simétrica. Neste o emissor da mensagem cifra a mesma com o uso de uma chave secreta que deverá ser de conhecimento do receptor para que ele possa fazer a leitura. Este procedimento tem menor segurança, pois se um terceiro tomar conhecimento da chave, a mensagem poderá ser lida. Para manter a segurança, a chave deve ser alterada periodicamente. A criptografia é utilizada nos *tokens* para operações bancárias realizadas muitas vezes através dos computadores e smartphones e também no popular aplicativo de conversa, do mesmo titular do *Facebook*, o chamado *WhatsApp*.

Os desenvolvedores do aplicativo *WhatsApp* usam o sistema de criptografia "ponto-a-ponto" (*end-to-end* – E2E) para garantir maior proteção dos dados, das conversas e da privacidade dos usuários. Contudo, essa técnica gerou confrontos com o Poder Judiciários, em razão de ordens judiciais não cumpridas para fornecer mensagens para casos investigatórios. Algumas vezes, o *WhatsApp* sofreu a sanção judicial de bloqueio ou suspensão do funcionamento do serviço por tempo determinado por causa do descumprimento consubstanciado na não colaboração. Tais sanções foram revogadas, pois se mostravam irrazoáveis por afetar milhões de usuários.

Com a referida técnica adotada, somente os usuários em comunicação tem acesso às mensagens e demais conteúdos da conversa. Com isso, a empresa não tem acesso ao conteúdo, de forma que somente oferece a plataforma de conversa e faz o intercâmbio das mensagens, sem fazer nenhum armazenamento permanente das mesmas. O conteúdo das conversas fica armazenado nos aparelhos dos usuários, os quais deverão ser mantidos em local seguro para que não ocorra uma visualização ou acesso não autorizado.

Sobre o funcionamento da troca de mensagens com a criptografia no WhatsApp, Teixeira et al[41] explica:

[41] TEIXEIRA, Tarcísio; SABO, Paulo Henrique; SABO, Isabela Cristina. WHATSAPP E A CRIPTOGRAFIA PONTO-APONTO: TENDÊNCIA JURÍDICA E O CONFLITO PRIVACIDADE VS.

> Segundo a WhatsApp Inc., o conteúdo das mensagens entregues pelo aplicativo WhatsApp não é copiado, mantido ou arquivado pela empresa. Os usuários digitam as mensagens, que são enviadas por algum serviço de acesso à Internet aos servidores WhatsApp, e encaminhadas para o destinatário (que também deve ser um usuário do WhatsApp) se este estiver online. Se o destinatário estiver off-line, a mensagem é armazenada no servidor até que possa ser entregue. Se o destinatário não acessar o aplicativo por 30 (trinta) dias, a mensagem não é entregue e também é excluída do servidor. Logo, sendo entregue uma mensagem, é imediatamente excluída do servidor.
> Desde abril de 2016, a WhatsApp Inc. disponibilizou uma nova versão do aplicativo, agora com criptografia ponto-a-ponto. Criptografia ponto-a-ponto é um termo dado para descrever que mesmo que a mensagem passe por um terceiro ou gerenciador, ela só é decifrada no receptor, ao passo que os gerenciadores da troca de mensagens não possuem acesso às chaves para decifrá-las. (TEIXEIRA et al, 2017, p. 617/618).

O método de criptografia adotado gera efeitos sobre a responsabilização civil do provedor quanto aos danos provocados por conteúdo gerado por terceiros. Na Lei 12.965/2014, o Marco Civil, no art. 19, o provedor será responsabilizado quando, após ordem judicial, não tomar as providências tecnicamente possíveis para indisponibilizar o conteúdo danoso, dentro do prazo fixado; e no art. 21, a responsabilização ocorrerá quando o provedor não indisponibilizar o conteúdo indevido violador da intimidade, após a notificação da vítima.

Com a criptografia ponto-a-ponto, o conteúdo compartilhado pelos usuários já nasce inacessível a empresa. Por não ingressar em seus servidores, não há retenção do conteúdo. Assim se poderia valorizar a não criação de um banco de dados, sem um cruzamento de informações e sem danos a privacidade, mas, por outro lado, também se excluiria a responsabilidade civil da empresa pelo conteúdo de terceiros.

Tal situação se demonstra problemática, pois é necessário garantir a privacidade e também punir as condutas ilícitas. Buscando o aprimoramento da segurança das informações tem se desenvolvido o campo da criptografia, algo que ainda deve alcançar demais serviços disponíveis na internet, podendo conduzir a

---

INTERESSE PÚBLICO. **Revista da Faculdade de Direito**: Universidade Federal de Minas Gerais, Belo Horizonte, n. 71, p.607-638, jul/dez. 2017. Semestral. Disponível em: <https://www.direito.ufmg.br/revista/index.php/revista/article/view/1882>. Acesso em: 10 maio 2018.

uma exclusão da responsabilidade civil. Sobre este cenário e a atuação do Judiciário, Teixeira et al[42] comenta:

> Portanto, diante do estudo realizado, depreende-se que os bloqueios ocorridos por determinação judicial carecem do devido fundamento técnico e jurídico. Inexiste comprovação de que o WhatsApp detém a guarda de todas chaves geradas a cada mensagem compartilhada por milhões de usuários. E, ainda assim, a divulgação seria uma possível afronta à confidencialidade empresarial, além dos custos incomuns que a tarefa geraria, colocando-se em risco a privacidade de diversos indivíduos que comunicam-se via WhatsApp. (TEIXEIRA et al, 2017, p. 631).

Quanto ao tratamento dos dados pessoais, os servidores aonde são armazenados devem ser seguros contra ameaças externas, como ataques empregados por crackers, que buscam a extração para utilização e obtenção de vantagens ilícitas. A proteção dos dados pessoais também envolve alguns deveres em relação aos seus titulares como: a publicidade da existência do banco de dados, a disponibilização voluntária, a utilização conforme o fim, com o qual foi cedido, a possibilidade de controle para permitir a atualização periódica, seja para adição, correção ou retirada de informações.

Possibilitar a retirada de dados ou conteúdo se relaciona com a necessidade de impedir o início ou a continuidade do dano sofrido por uma vítima. Sendo a internet um ambiente com baixo custo para armazenamento e com alto grau de publicidade das informações, a retirada de algo que cause dano à personalidade humana é fundamental para garantir o direito ao esquecimento.

Porém, as ameaças não se resumem a terceiros. Os Estados também podem violar a privacidade. Essas violações se tornaram mais evidentes com as revelações de Edward Snowden em 2013.

Após os ataques terroristas de 11 de setembro de 2001, os Estados Unidos potencializaram seu vigilantismo e deram início ao seu maior esquema de espionagem e vigilância cibernética da história de seu governo, comprovados nos

[42] TEIXEIRA, Tarcísio; SABO, Paulo Henrique; SABO, Isabela Cristina. WHATSAPP E A CRIPTOGRAFIA PONTO-APONTO: TENDÊNCIA JURÍDICA E O CONFLITO PRIVACIDADE VS. INTERESSE PÚBLICO. **Revista da Faculdade de Direito**: Universidade Federal de Minas Gerais, Belo Horizonte, n. 71, p.607-638, jul/dez. 2017. Semestral. Disponível em: <https://www.direito.ufmg.br/revista/index.php/revista/article/view/1882>. Acesso em: 10 maio 2018.

documentos da *National Security Agency* (NSA), a Agência de Segurança Nacional norte-americana.

Em relação a justificativa norte-americana, Favera e Silva[43] apresentam a crítica:

> Ainda que as justificativas para essas práticas sejam o combate ao terrorismo, sabe-se que as estratégias de *big data* associadas à *surveillance* não respondem eficazmente para a proteção da segurança nacional ou internacional, posto que após os atentados terroristas de 11 de Setembro de 2001, muitos outros ataques aconteceram sem que o governo norte-americano conseguisse evitar. (FAVERA e SILVA, 2016, p. 128).

Em nome da segurança, ocorreu a análise, extração e armazenamento por prazo indefinido, de informações de várias pessoas americanas e estrangeiras disponíveis na internet. Desde cidadãos comuns até autoridades e empresas de outros países, inclusive brasileiras, tiveram a privacidade de suas informações violada. Tal violação constitui um atentado a soberania e somente pode ser efetivamente combatida com uma atuação conjunta dos países, num cenário de cooperação combinando os âmbitos nacional e transnacional.

Um parâmetro de atuação conjunta entre países é a Diretiva do Parlamento Europeu sobre a segurança das redes e da informação em toda a União Europeia. O documento reconhece que incidentes de segurança como o ocorrido são uma ameaça ao funcionamento da internet e dos sistemas de informação. Como a Internet não conhece fronteiras, quaisquer perturbações afetam todos os Estados-membros. Por essa razão, cada Estado deve atuar internamente para aprimorar a segurança em seus territórios, ao mesmo tempo em que coopera com os demais para buscar um ambiente de confiança mútua. Tal atuação cooperativa não deve prejudicar a segurança interna dos Estados. Somente com a colaboração entre entes estatais e não estatais, provedores de serviços digitais, fabricantes de *hardware* e desenvolvedores de *software* que se poderá buscar de forma efetiva a segurança na internet.

---

[43] FAVERA, Rafaela Bolson dalla; SILVA, Rosane Leal da. CIBERSEGURANÇA NA UNIÃO EUROPEIA E NO MERCOSUL: BIG DATA E SURVEILLANCE VERSUS PRIVACIDADE E PROTEÇÃO DE DADOS NA INTERNET. **Revista de Direito, Governança e Novas Tecnologias**, Curitiba, v. 2, n. 2, p.112-134, jul/dez. 2016. Disponível em: <http://www.indexlaw.org/index.php/revistadgnt/article/view/1490>. Acesso em: 11 maio 2018.

Quanto a transposição da modalidade de atuação da União Europeia para a nossa realidade, com o Mercosul, Favera e Silva[44] sustentam:

> Sustenta-se que esse tema deve ser incluído na pauta de discussão no âmbito do Mercosul, pois ainda que algumas questões sejam de interesse eminentemente nacional, a fluidez das informações e dados pessoais ultrapassam as fronteiras dos Estados e exigem articulação e colaboração desses. Nesse sentido, a experiência argentina e uruguaia, que já contam com leis específicas de proteção de dados pessoais, poderia ser muito rica para o estabelecimento de políticas e ações coordenadas dentro do bloco, as quais teriam melhores condições de enfrentamento de temas transversais e transnacionais como esse. (FAVERA e SILVA, 2016, p. 129).

A privacidade é um direito de todas as pessoas. Não devem ser admitidas violações de agentes privados, nem do próprio Estado. Por se tratar da internet, uma rede conectada globalmente, as infrações podem ser executadas em um país e causar dano em outro. Somente observando as inovações tecnológicas, como a criptografia e a experiência internacional, buscando a cooperação, que se poderá almejar de forma efetiva, a proteção do direito à privacidade.

3.2. POSIÇÃO DOS TRIBUNAIS

Com a fundamental participação da internet no cotidiano, trazendo inúmeros benefícios, também surgem situações em que direitos são lesados. Nestes momentos, é chamada a atuação do Judiciário de forma a fazer cessar os atos ilícitos e definir meios de se reparar os danos causados às vítimas.

Por esta razão, considerando as legislações aplicáveis, serão analisados alguns acórdãos do Tribunal de Justiça do Estado do Rio de Janeiro, do Superior Tribunal de Justiça e do Supremo Tribunal Federal.

Na apelação cível nº 0028583-76.2010.8.19.0054[45], na fase de cumprimento de sentença, a Terceira Câmara Cível negou, por unanimidade, o provimento aos

[44] FAVERA, Rafaela Bolson dalla; SILVA, Rosane Leal da. CIBERSEGURANÇA NA UNIÃO EUROPEIA E NO MERCOSUL: BIG DATA E SURVEILLANCE VERSUS PRIVACIDADE E PROTEÇÃO DE DADOS NA INTERNET. **Revista de Direito, Governança e Novas Tecnologias**, Curitiba, v. 2, n. 2, p.112-134, jul/dez. 2016. Disponível em: <http://www.indexlaw.org/index.php/revistadgnt/article/view/1490>. Acesso em: 11 maio 2018.

recursos de ambas as partes. Discutiu-se se o Google do Brasil Internet Ltda havia cumprido a determinação da sentença com o simples fornecimento do IP (*Internet Protocol*) do fraudador ou se tinha a obrigação de fornecer a qualificação completa do usuário que criou o perfil falso, expondo a vítima a constrangimentos, de forma a afetar o valor ficado de multa e indenização.

A pretensão do executado, primeiro apelante era que fosse reformada a sentença, reconhecendo que os provedores de aplicações de Internet, como o próprio Google, administrador do Orkut, rede social onde foi criado o perfil falso e realizado o ato ilícito, encontram-se obrigados a armazenar apenas dados de IP, com base no art. 5ª, inciso VIII, da Lei nº 12.965/14, que conceitua registros de aplicações na internet e, por esta razão, haveria justa causa para não armazenar e fornecer outros dados sobre o fraudador, os quais não detém, como o nome completo, endereço pessoal, CPF, RG e outros identificadores.

O relator destacou que a responsabilidade do provedor será subjetiva quando não agir rapidamente para tirar o conteúdo ofensivo ou não adota providência para identificar o autor do dano, conforme entendimento do Superior Tribunal de Justiça, no REsp 1501187/RJ.

Na sentença discutida se entendeu que restou configurado o cumprimento parcial e insuficiente com o mero fornecimento do IP, pois não é informação suficiente para a identificação da pessoa que criou o perfil falso e sobre ser plenamente realizável o fornecimento dos dados utilizados para a abertura da conta na rede social, dados que ao menos deveria estar sob guarda da empresa, a qual responde com base na teoria do risco do empreendimento. Esta teoria está prevista no art.14 da Lei nº 8.078/1990, o Código de Defesa do Consumidor.

O relator decidiu que houve cumprimento parcial da sentença com o fornecimento do IP quando se exigia a qualificação completa do criador do perfil falso, além das alegações apresentadas já estarem atingidas pela coisa julgada. Aduz que a sentença é anterior ao Marco Civil, mas ainda assim os deveres previstos na atual legislação já eram existentes.

---

[45] TJ/RJ. Apelação Cível nº 0028583-76.2010.8.19.0054. Relator: Desembargador Mario Assis Gonçalves. DJe: 15.03.2018. 2018. Disponível em: < http://www1.tjrj.jus.br/gedcacheweb/default.aspx?UZIP=1&GEDID=0004A8B80A791253E1E250EC585F2CF418EEC5075961135F&USER=>. Acesso em: 11 de maio, 2018.

Em análise do Marco Civil, destaca que ele prevê a obrigação de registro dos dados dos usuários pelos fornecedores dos serviços de internet. Em relação aos provedores de conexão à Internet, o prazo é de 1 ano, na forma do art. 13, caput. Em relação aos provedores de aplicações de internet, o prazo é de 6 meses, na forma do art. 15, caput. Para a exclusão de conteúdos violadores é necessária sua identificação clara e específica para que se possa permitir a sua localização inequívoca.

Mesmo que o sigilo das comunicações seja garantido constitucionalmente no art. 5º, inciso XII, da CF/88, o mesmo não pode ser absoluto de forma evitar a impunidade daqueles que praticam atos ilícitos, se aproveitando de seu sigilo e anonimato.

Para aqueles que oferecem serviços de provisão de conexão e de conteúdo na Internet, há o dever de armazenar dados mínimos aptos a identificar os seus usuários, para assegurar a possibilidade de as vítimas prejudicadas pelo uso inapropriado do serviço, sejam também usuárias ou não, obterem informações individualizantes dos autores dos atos ilícitos poder procurar a reparação de seus direitos.

A Décima Nona Câmara Cível do Tribunal de Justiça do Estado do Rio de Janeiro negou provimento, por unanimidade, ao agravo de instrumento nº 0001284-14.2018.8.19.0000[46].

No caso apresentado, a agravada teve conteúdo lesivo a sua privacidade retirado de um blog, a partir da URL indicada. O Google, o agravante, é administrador do Blogger, um dos seus serviços que permitem a criação de blogs, que constituem páginas de internet que permitem atualizações rápidas e constantes com a inclusão de postagens, de forma a atrair pessoas interessadas pelo assunto motivador da criação do blog.

O agravante cumpriu a determinação de retirada do conteúdo, contudo não forneceu os dados do criador do blog onde o conteúdo violador foi postado. Argumentou que a conexão utilizada é oriunda da Espanha e seria impossível

[46] TJ/RJ. Agravo de Instrumento nº 0001284-14.2018.8.19.0000. Relator: Desembargador Juarez Fernandes Folhes. DJe: 22.03.2018. 2018. Disponível em:<http://www1.tjrj.jus.br/gedcacheweb/default.aspx?UZIP=1&GEDID=0004870F68C58D8109BCFC54AE3A825AEFBEC5075E3A2131&USER=>. Acesso em: 11 de maio, 2018.

fornecer dados de conexões estrangeiras, além de haver a limitação da jurisdição do judiciário brasileiro, baseado na norma do art. 11, da Lei 12.965/2014

Nos termos do voto do relator entendeu-se que o provedor deve propiciar meios de identificar o autor de ato ilícito, que não deve ficar impune em razão do anonimato. Este não deve ser pleno e irrestrito, o que não significa uma afronta a liberdade, pois a mesma é necessária a existência e ao desenvolvimento da internet. Identificar a autoria é necessária para preservar a integridade da própria rede. Ademais, o agravante não comprovou a origem estrangeira da conexão e nem mesmo a sua impossibilidade técnica de fornecer os registros de acesso do usuário responsável pelo blog. Considerando que o Google é uma empresa global, a sua extensão brasileira é capaz de fornecer os dados, mesmo que provenientes do exterior.

No acórdão da apelação cível nº 0050120-83.2016.8.19.0001[47], a Décima Oitava Câmara Cível lhe negou provimento sob o fundamento de que as imagens capturadas da apelante no Google Street View não infringiam seus direitos da personalidade, trazendo uma situação ordinária, do cotidiano.

Considerou-se que o Google Street View é integrante do Google Maps e seu serviço gratuito, mesmo que remunerado indiretamente através de publicidade, tem o objetivo de identificar endereços e simular trajetos. Não tem finalidade econômica, tem cunho informativo de interesse público e o registro das imagens dos logradouros leva a uma inevitável captura das pessoas no ambiente.

Ademais de a captura ter sido acidental e a uma distância razoável, o apelado, Google Brasil Internet Ltda., destacou que a usuária não solicitou a distorção ou retirada da imagem, demonstrado que poderia ter sido buscada uma solução consensual.

No Recurso Especial nº 1.698.647/SP[48], discutiu-se o caso em que a recorrida pretendia a remoção de vídeos e comentários postados no YouTube,

---

[47] TJ/RJ. Apelação Cível nº 0050120-83.2016.8.19.0001. Relator: Desembargador Carlos Eduardo da Fonseca Passos. DJe: 20.04.2018. 2018. Disponível em: <http://www1.tjrj.jus.br/gedcacheweb/default.aspx?UZIP=1&GEDID=0004E79F6C6D459860D024EDF2F9583C0C2DC5080A621C28&USER=>. Acesso em: 11 de maio, 2018.

[48] STJ. Recurso Especial nº 1.698.647 SP 2017/0047840-6. Relator: Ministra Nancy Andrighi. DJe: 15.02.2018. 2018. Disponível em: < https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1671167&num_registro=201700478406&data=20180215&formato=PDF>. Acesso em: 13 de maio, 2018.

plataforma de hospedagem de vídeos da Google, cujos conteúdos eram a sua participação em programa de televisão, nos quais se considerou ridicularizada. No acórdão recorrido, o Tribunal de origem concedeu à recorrida a prerrogativa de determinar, mediante simples notificação, a retirada de conteúdo que entendesse lesivo a sua pessoa.

O Ministro Relator deu provimento ao recurso para afastar a obrigação de remover conteúdo, a partir de mera notificação extrajudicial por parte da recorrida. Afirmou que, conforme apontado pelo recorrente, Google Brasil Internet Ltda, deve ser seguido o mandamento do art. 19, § 4º, do Marco Civil da Internet (Lei 12.965/2014), que determina que o comando judicial de remoção de conteúdos de aplicações de internet deve ser específico, com a menção do localizador URL.

Google Brasil Internet Ltda propôs o Recurso Especial nº 1.679.465/SP[49] alegando a violação do art. 19, § 1º, da Lei 12.965/2014, já que a ordem judicial não trazia a identificação específica do conteúdo infringente. O caso era sobre um vídeo íntimo publicado em um site na internet e que aparecia como resultado quando realizada a busca no motor de buscas.

Em seu voto, a Relatora não vislumbrou violação ao dispositivo do Marco Civil, pois a lei não estava em vigor na época dos fatos, nem mesmo poderia se falar em prequestionamento pelo Tribunal de origem. Quanto a situação discutida, mesmo que o recorrente não hospedasse o vídeo íntimo, há a responsabilidade dos provedores de busca, os quais devem contribuir com a não-divulgação de URLs.

Muito importante também é a análise sobre a exposição pornográfica não consentida. O chamado revenge porn ou pornografia de vingança afeta principalmente mulheres adolescentes de doze a dezesseis anos. As consequências podem ser catastróficas levando, muitas vezes, a suicídio ou a depressão severa. Traz também conceitos de Cyberbullying, uma forma de amedrontamento por meio eletrônico com potencial de repetição, havido entre crianças e adolescentes; de *Cyberstalking* ou *cyberharassment,* consistente em perseguição constante e indesejada de uma vítima, com potencial de acarretar medo e constrangimento e; de *Sextortion* ou sextorsão, uma forma de extorsão cibernética, em que se exige

[49] STJ. Recurso Especial nº 1.679.465 SP 2016/0204216-5. Relator: Ministra Nancy Andrighi. DJe: 19.03.2018. 2018. Disponível em: < https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1685789&num_registro=201602042165&data=20180319&formato=PDF>. Acesso em: 12 de maio, 2018.

imagens ou favores sexuais, sob ameaça de distribuição de informações pessoais, imagens pornográficas ou sexualmente explícitas.

O recurso foi conhecido parcialmente e, nesta parte, foi dado provimento no sentido de que se reconheceu que: i) a atividade dos provedores de busca pode causar danos aos direitos da personalidade, em razão de sua capacidade de limitar ou induzir a visibilidade de determinados conteúdos; ii) em medida de urgência, é possível a determinação de retirada de conteúdos indicados em URLs pelos provedores de busca, quando a rápida disseminação agrave os prejuízos da vítima e a remoção do conteúdo em sua origem exija mais tempo; iii) nas medidas de urgência não é possível a determinação de que os provedores de busca façam um monitoramento prévio das informações dos resultados das pesquisas; iv) a pornografia de vingança é uma grave forma de lesão aos direitos da personalidade e também de violência de gênero; v) o art. 21 da Lei 12.965/2014 traz a única exceção a reserva de jurisdição para a retirada de conteúdo infringente da internet quando se tratar de cenas de nudez ou atos sexuais de caráter privado, sendo o provedor subsidiariamente responsável a partir da notificação extrajudicial formulada pelo particular interessado na remoção do conteúdo; e, vi) no caso julgado, em antecipação de tutela, considerou-se cabível a medida de exclusão dos conteúdos indicados por URL dos resultados de pesquisa feitos.

O Recurso Extraordinário 1.037.396/SP [50] foi interposto por Facebook Serviços Online do Brasil Ltda contra acórdão em recurso inominado da Segunda Turma Recursal Cível do Colégio Recursal de Piracicaba/SP, a qual consignou que condicionar a retirada de perfil falso somente após ordem judicial, na forma do art. 19 da Lei nº 12.965/14, fulmina o direito a efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos, do art. 6º, inciso VI, da Lei 8.078/90, o Código de Defesa do Consumidor

O recorrente sustenta que a declaração de inconstitucionalidade do art. 19 da Lei nº 12.965/14 e aplicação da responsabilidade objetiva do Código de Defesa do Consumidor é um golpe a segurança jurídica. O posicionamento adotado possuiria repercussão econômica, pois levaria a mudança de atuação dos provedores, que agiriam como censores, criando um conflito com a vedação a censura, a liberdade

[50] STF. Recurso Extraordinário nº 1.037.396 SP. Relator: Ministro Dias Toffoli. DJe: 04.04.2018. 2018. Disponível em: < http://portal.stf.jus.br/processos/downloadPeca.asp?id=314030456&ext=.pdf>. Acesso em: 15 de maio, 2018.

de expressão e a reserva de jurisdição valorizadas pelo Marco Civil da Internet. A única exceção a reserva de jurisdição está no art. 21 da lei nº 12.965/14.

O Supremo Tribunal Federal reconheceu a repercussão geral por se tratar de questão de contraposição entre valores constitucionais, como a dignidade da pessoa humana, a proteção aos direitos da personalidade, a liberdade de expressão, o livre acesso à informação e a reserva de jurisdição, cabendo decidir se a empresa tem os seguintes deveres: de fiscalização prévia, de retirada de conteúdo ofensivo após notificação extrajudicial e de se responsabilizar legalmente antes da análise pelo Judiciário.

A partir do que foi brevemente analisado, buscou-se demonstrar que a proteção da privacidade e dos demais direitos da personalidade são anteriores e não se resumem ao Marco Civil da Internet. A internet por ser um novo ambiente em constante evolução, traz novas concepções para os direitos, de forma que se produzem novos conflitos, que desafiam os legisladores e o judiciário, fomentando novas leis e novas interpretações. A Lei nº 12.965/14, o Marco Civil, por se tratar de uma legislação consideravelmente recente, ainda se discute quanto aos seus dispositivos, sobre a capacidade de fazer cessar as condutas ilícitas e a propagação de conteúdos lesivos, de forma a garantir a efetiva proteção aos direitos da personalidade e a reparação dos danos, em comparação com as previsões do Código de Defesa do Consumidor e da Constituição Federal.

3.3. PROPOSTAS DE REGULAMENTAÇÃO

Com a rápida expansão da internet e a criação de novas relações sociais e comerciais se necessita a adaptação da legislação para garantir a proteção dos direitos dos internautas, principalmente em relação a sua privacidade e, mais especificamente quanto a utilização dos dados pessoais. A Lei nº 12.965, de 23 de abril de 2014, o Marco Civil da Internet, é a legislação mais recente que busca estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Atualmente, três projetos de lei sobre proteção de dados pessoais estão em tramitação no Congresso Nacional, sendo eles o PL 5276/2016, o PLS 330/2013 e o PL 4060/2012, sobre os quais serão feitas algumas observações.

Para uma breve análise, serão adotados os requisitos elencados pela ARTIGO 19[51], uma organização não-governamental de direitos humanos, fundada em Londres, no ano de 1987, estando no Brasil desde 2007. Seu objetivo é a promoção do direito à liberdade de expressão e de acesso à informação em todo o mundo. Foram elencados quinze aspectos: 1) menção expressa à proteção da liberdade de expressão; 2) exceção à atividade jornalística e outras formas de expressão, como as que possuem fins jornalísticos, artísticos, acadêmicos e literários; 3) menção expressa à lei de acesso à informação, observando as situações em que há interesse público; 4) cuidado com interpretações que possibilitem reivindicações do direito ao esquecimento, evitando a sua banalização; 5) órgão regulatório; 6) mecanismo de participação e controle social; 7) proteção aos dados sensíveis, como os relacionados a saúde, vida sexual, genéticos, biométricos, orientação sexual, ideológica, política, religiosa ou raça; 8) graus de consentimento do titular dos dados, devendo ser livre, informado, inequívoco, específico, determinado e expresso; 9) consentimento do titular para compartilhamento a terceiros; 10) proteção para transferência internacional de dados; 11) proteção de dados em acesso público; 12) adoção de medidas de segurança e de manuseio dos dados pessoais; 13) aplicação ao setor público como um todo, incluindo forças de segurança; 14) delimitação de pesquisa estatística; e 15) prazo para a lei entrar em vigor, tendo em vista a urgência de uma lei que de uma regulação ao tratamento dos dados pessoais.

O PL 4060/2012[52] foi criado pelo deputado federal Milton Monti (PR-SP). Em sua justificativa, declara-se que o projeto de lei tem o objetivo de dar ordenamento jurídico e institucional ao tratamento de dados pessoais, bem como proteção aos direitos individuais das pessoas, com base na Constituição Federal. O deputado baseou-se nas discussões ocorridas no V Congresso Brasileiro da Indústria da

---

[51] Artigo 19. PROTEÇÃO DE DADOS PESSOAIS NO BRASIL: ANÁLISE DOS PROJETOS DE LEI EM TRAMITAÇÃO NO CONGRESSO NACIONAL. p. 17-24. Novembro, 2016. Disponível em: < http://artigo19.org/blog/2017/01/31/protecao-de-dados-pessoais-no-brasil-analise-dos-projetos-de-lei-em-tramitacao-no-congresso-nacional/ >. Acesso em: 18 maio 2018.

[52] BRASIL. Câmara dos Deputados. Projeto de Lei PL 4060/2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066&ord=1>. Acesso em: 18 maio 2018.

Comunicação, evento promovido pela ABAP – Associação Brasileira das Agências de Publicidade e pelo FORCOM – Fórum Permanente de Comunicação. Destacou-se que havia a necessidade de um marco regulatório para disciplinar para o tratamento de dados pessoais, que deveria ser geral e abrangente, devido as constantes evoluções tecnológicas, devendo as questões específicas ficar a cargo de um conselho de autorregulamentação.

Segundo a ARTIGO 19[53], o PL 4060/2012 é o pior avaliado, pois seu teor é mais vago e aborda mais sobre o tratamento dos dados pessoais do que a sua proteção, sem estabelecer padrões mínimos. Seus dispositivos somente tratam de forma satisfatória quanto a exceção à atividade jornalística e outras formas de expressão. Os demais aspectos estão ausentes ou são tratados de forma parcialmente satisfatória ou insatisfatória.

O PLS 330/2013[54] é do senador Antônio Carlos Valadares (PSB-SE). Em sua justificativa, destaca que a insegurança da população e a necessidade da proteção dos dados pessoais ficou evidente com o episódio do acesso aos dados de cidadãos de vários países pelos Estados Unidos. O projeto apresentado é a reapresentação, com algumas modificações do Projeto de Lei do Senado nº 321, de 2004, de autoria do Senador Sérgio Zambiassi. A proteção à privacidade já está presente no art. 12 da Declaração Universal dos Direitos do Homem de 1948 e no art. 5º, incisos X a XII, da Constituição Federal. Foram consideradas também as iniciativas já adotadas pelo Parlamento Europeu com a Diretiva 95/46/CE, por Portugal com a Lei nº 67, de 1998 e pela Espanha com a Lei Orgânica nº 15, de 1999, além de o Brasil ser signatário da Declaração de Santa Cruz de la Sierra, produzida durante a XIII Cimeira Ibero-americana de Chefes de Estado e de Governo, realizada na Bolívia, em novembro de 2003, demonstrando a impossibilidade do Congresso Nacional permanecer inerte frente a evolução da informática e a necessidade de proteção dos dados dos cidadãos brasileiros.

---

[53] Artigo 19. PROTEÇÃO DE DADOS PESSOAIS NO BRASIL: ANÁLISE DOS PROJETOS DE LEI EM TRAMITAÇÃO NO CONGRESSO NACIONAL. p. 39-43. Novembro, 2016. Disponível em: < http://artigo19.org/blog/2017/01/31/protecao-de-dados-pessoais-no-brasil-analise-dos-projetos-de-lei-em-tramitacao-no-congresso-nacional/ >. Acesso em: 18 maio 2018.

[54] BRASIL. Senado Federal. Projeto de Lei do Senado PLS 330/2013. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/113947>. Acesso em: 16 maio 2018.

Segundo a ARTIGO 19[55], o PLS 330/2013, dentre os três analisados, é o intermediário, atendendo a cinco dos 15 aspectos. Suas premissas são semelhantes as adotadas pelo PL 5276/2016. O projeto trata satisfatoriamente quanto a proteção aos dados sensíveis, o grau de consentimento, o consentimento do titular para o compartilhamento a terceiros, a proteção para a transferência internacional de dados e estipula medidas de segurança técnicas e de manuseio durante o período de tratamento dos dados pessoais. Considerou-se disposto de forma parcialmente satisfatória quanto: a exceção a atividade jornalística, porém o projeto não mencionou quanto as outras formas de expressão; o mecanismo de participação e controle social; a utilização para pesquisa estatística, que deve ser delimitada, para evitar uma conservação indevida dos dados pessoais de brasileiros por entes públicos e privados; e o prazo para lei entrar em vigor foi fixado em 120 dias, o qual, deveria ser imediato após a publicação em Diário Oficial. O projeto não trouxe alguns aspectos como: a menção expressa à proteção da liberdade de expressão; a menção expressa à Lei de Acesso a Informação; o órgão regulatório independente e a proteção expressa de dados em acesso público, exigindo consentimento de seus titulares para seu tratamento. Dois aspectos foram tratados de forma insatisfatória, sendo eles: evitar interpretações que possam ensejar reivindicações do direito ao esquecimento e aplicação ao setor público como um todo, inclusive ás forças de segurança.

O que traz mais garantias de proteção aos dados pessoais no seu processo de tratamento pelos órgãos públicos ou privados é o PL 5276/2016[56]. Foi elaborado a partir de reuniões e consultas públicas organizadas pelo Ministério da Justiça, além de passar pela consulta pública online na plataforma e- democracia, no Poder Legislativo. O projeto reconhece a desconformidade da legislação brasileira atual em relação aos padrões internacionais sobre o tema, e foi influenciado pela Resolução da ONU de 25 de novembro de 2013 sobre “Direito à Privacidade na Era Digital”. Devido ao avanço da tecnologia, que amplia enormemente o potencial de coleta de

[55] Artigo 19. PROTEÇÃO DE DADOS PESSOAIS NO BRASIL: ANÁLISE DOS PROJETOS DE LEI EM TRAMITAÇÃO NO CONGRESSO NACIONAL. p. 32-38. Novembro, 2016. Disponível em: < http://artigo19.org/blog/2017/01/31/protecao-de-dados-pessoais-no-brasil-analise-dos-projetos-de-lei-em-tramitacao-no-congresso-nacional/ >. Acesso em: 18 maio 2018.

[56] BRASIL. Câmara dos Deputados. Projeto de Lei PL 5276/2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 >. Acesso em: 17 maio 2018.

dados, o estabelecimento de regras é necessário para proteger o titular dos dados e favorecer a sua utilização lícita, condicionada a garantia de segurança, transparência e boa-fé.

Segundo a ARTIGO 19[57], o PL 5276/2016 atende plenamente a oito dos quinze aspectos, sendo eles: menção expressa à proteção da liberdade de expressão; exceção jornalística e outras formas de expressão; menção expressa à Lei de Acesso à Informação; proteção aos dados sensíveis; graus de consentimento; consentimento do titular para o compartilhamento a terceiros; proteção para a transferência internacional de dados e adoção de medidas de segurança e de manuseio dos dados pessoais. O projeto trata de forma parcialmente satisfatória quanto ao órgão regulatório, ao mecanismo de participação e controle social, a proteção de dados em acesso público, a falta de delimitação sobre pesquisa estatística e o prazo para a lei entrar em vigor, que é o mais longo dentre as três, sendo de 180 dias. Quanto aos aspectos de evitar interpretações que possam ensejar reivindicações do direito ao esquecimento e a aplicação ao setor público como um todo, incluindo forças de segurança, seus dispositivos são insatisfatórios.

A proteção aos dados pessoais, como uma forma mais específica de proteção à privacidade é fundamental, considerando a alta capacidade de troca e utilização dos mesmos através da Internet. Por esta razão, após o Marco Civil da Internet, é necessária e urgente uma regulação para os dados pessoais em nosso país.

[57] Artigo 19. PROTEÇÃO DE DADOS PESSOAIS NO BRASIL: ANÁLISE DOS PROJETOS DE LEI EM TRAMITAÇÃO NO CONGRESSO NACIONAL. p. 25-31. Novembro, 2016. Disponível em: < http://artigo19.org/blog/2017/01/31/protecao-de-dados-pessoais-no-brasil-analise-dos-projetos-de-lei-em-tramitacao-no-congresso-nacional/ >. Acesso em: 18 maio 2018.

CONSIDERAÇÕES FINAIS

A sociedade está conectada através da internet. Seja em casa, no trabalho ou em qualquer lugar com conexão fixa ou móvel, utilizando os variados dispositivos, as pessoas podem ter acesso às informações disponíveis na internet. Com a mudança dos hábitos, passamos a uma sociedade de exposição, onde quase tudo sobre nós está na internet. Entender como se chegou ao atual cenário, os atores que atuam diariamente na internet e como garantir a proteção da privacidade é o que se pretendeu ao longo desta monografia.

No primeiro capítulo buscou-se demonstrar como a internet surgiu e evoluiu, se tornando indispensável na atualidade. Se tornou instrumento de participação na vida pública e exercício da transparência, democracia e da cidadania. Refletiu também na formação dos relacionamentos entre as pessoas, permitindo que cada um construa a sua identidade, ao ceder suas informações criando um perfil nas redes sociais virtuais. Com isso, se desenvolveram bancos de dados pessoais em formato digital, que diferente dos formatos físicos anteriores a popularização dos computadores e da internet, estão muito menos sujeitos a deterioração e perda de dados com o decurso do tempo e permite o cruzamento de dados entre diferentes servidores de armazenamento. Contudo, essa considerável perpetuidade também é negativa, devendo ser garantido aos titulares dos dados, o controle sobre os mesmos, através da sua adição, correção ou retirada. Deve se dar atenção também a necessária segurança dos dados e da navegação na internet, pois apesar de seus benefícios para a sociedade, também surgiram problemas específicos desse ambiente.

O segundo capítulo tratou da privacidade, das formas de desrespeito a esse direito e do Marco Civil da Internet. O direito a privacidade é um dos direitos da personalidade e está previsto no Código Civil. Mesmo que intransmissível, irrenunciável, absoluto, ilimitado, imprescritível, impenhorável, inalienável, não sujeito a desapropriação e vitalício, deve ser admitida a possibilidade de limitação voluntária de seu exercício, desde que temporária e conforme a finalidade pretendida por seu titular. A privacidade não deve ficar desprotegida, mesmo que a internet seja um espaço público. Esse novo ambiente exige uma evolução do conceito de proteção a privacidade, de forma que englobe também a proteção dos

dados pessoais e a garantia do direito ao esquecimento, permitindo que a pessoa afaste fatos que atrapalhem a continuidade e/ou recomeço de sua vida, desde que tais informações não sejam de interesse público. Para cumprir esse objetivo, combatendo práticas ilícitas de usuários como o *revenge porn* e a de captação e utilização de dados não autorizada expressamente, tendo em vista a disparidade na relação entre provedores e usuários, foi criado o Marco Civil da Internet. Essa lei busca conciliar a liberdade de expressão com a proteção da privacidade e o controle de dados, privilegiando também a neutralidade da rede.

No terceiro capítulo foram apresentadas medidas de proteção a privacidade como o sistema *opt-in* e *opt-out* quanto ao *spam*, o uso da criptografia de forma a garantir a proteção do conteúdo das conversas entre usuários de alguns serviços, a proteção dos dados pessoais armazenados em bancos de dados, permitindo o acesso de seus titulares. Contudo, para a proteção ser efetiva, é necessária a cooperação entre os países, visto que a internet sendo uma rede conectada globalmente, atos ilícitos podem ser praticados em um lugar e produzir resultados em outro. Também foram analisados acórdãos do Tribunal de Justiça do Estado do Rio de Janeiro, do Superior Tribunal de Justiça e do Supremo Tribunal Federal. A partir deles se extrai o entendimento que as questões sobre a privacidade na internet envolvem a dignidade da pessoa humana, a proteção aos direitos da personalidade, a liberdade de expressão, o livre acesso a informação, devendo buscar soluções céleres para cessar rapidamente as violações, considerando a alta velocidade de propagação dos conteúdos na internet. Para a proteção dos direitos das vítimas, nesses casos, baseia-se no Marco Civil da Internet, no Código de Defesa do Consumidor, no Código Civil e na Constituição Federal. Contudo, o Brasil ainda necessita de uma legislação específica sobre a proteção dos dados pessoais estando, no momento, três em tramitação no Congresso Nacional: o PL 5276/2016, o PLS 330/2013 e o PL 4060/2012.

Quanto aos objetivos constantes da introdução desta monografia, conclui-se que eles foram alcançados. A flexibilização do direito a privacidade não deverá ser permanente, nem integral, devendo sempre decorrer da autonomia do seu titular e estar de acordo com as finalidades pretendidas. Na internet, mesmo que a privacidade seja constantemente flexibilizada voluntariamente ou violada ilicitamente, é inegável o papel fundamental deste ambiente no desenvolvimento da

personalidade da pessoa humana, merecendo destaque as redes sociais com a criação de perfis, baseados na visão de seu titular sobre si mesmo, para interagir com outros perfis que representa outras pessoas. Quanto as violações à privacidade na internet, podem ser exemplificadas com o envio de *spam*, o *revenge porn*, o uso não autorizado de dados que podem ser enfrentados com os dispositivos da Constituição Federal, do Código Civil, do Código de Defesa do Consumidor e do Marco Civil da Internet. Contudo, mesmo com as várias previsões para se garantir a privacidade, ainda cabe questionar quanto a efetividade dessas soluções, pois para combater uma violação na internet, deve-se considerar a necessária celeridade na atuação do judiciário e do provedor e a característica particular deste ambiente que é rápida repercussão com o amplo compartilhamento dos conteúdos. Mesmo o Marco Civil da Internet, sendo a lei mais específica dentre as mencionadas, recebe críticas quanto a forma como balanceou a liberdade de expressão e a proteção da privacidade. Considerando todo o arcabouço jurídico atual, o Brasil ainda necessita de uma lei que trate da proteção dos dados pessoais, sendo essa uma vertente mais específica da proteção a privacidade. No Congresso Nacional está em tramitação três projetos de lei sobre o assunto, sendo o PL 5276/2016 o mais promissor.

A partir de toda a análise realizada se depreende que a internet se tornou parte inseparável das relações sociais e comerciais na atualidade. Através dela, as pessoas conhecem e mantém contato umas com as outras, armazenam suas fotos e vídeos sobre suas recordações e se expõem para os demais nas redes sociais, fazem compras, preenchem seus dados e permitem que eles sejam usados pelas empresas para o que poderia ser, supostamente, a sua maior comodidade. Constantemente, os titulares admitem que sua privacidade seja violada e seus dados sejam utilizados. O papel do Estado ao formular as legislações é garantir que essas situações estejam sempre de acordo com as finalidades pretendidas pelos titulares que embasaram a relativização de seu direito à privacidade e definir meios de fazer cessar quaisquer danos causados e garantir a reparação.

Somente atualizando a lei para que ela esteja de acordo com as novas práticas sociais motivadas pelas inovações tecnológicas, que se poderá manter um ambiente saudável para o desenvolvimento da personalidade humana, sendo esta uma condição para a continuidade e confiabilidade da internet.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBERTIN, Alberto Luiz; DE MOURA ALBERTIN, Rosa Maria. A internet das coisas irá muito além as coisas. **GV-executivo**, v. 16, n. 2, p. 12-17, mar/abr 2017. Disponível em: < http://bibliotecadigital.fgv.br/ojs/index.php/gvexecutivo/article/download/68668/66258 >. Acesso em: 10 abr 2018.

ALENCAR, Ianara de Sousa; PACHECO, Ludgard Vinicius Andrade; FERREIRA, Rodrigo Leal. A EVOLUÇÃO DO CONCEITO DE PRIVACIDADE DIANTE DAS NOVAS TECNOLOGIAS UTILIZADAS NOS CORREIOS ELETRÔNICOS (E-MAIL). **Revista de Direito Uninovafapi**, Teresina, v. 1, n. 1, p.1-17, 2016. Disponível em: https://revistainterdisciplinar.uninovafapi.edu.br/index.php/revinterdireito/article/view/1106>. Acesso em: 29 abr. 2018.

ARAÚJO, Antônio Carlos da Silva et al. A INDISPONIBILIDADE DA PERSONALIDADE E AS REDES SOCIAIS. **Cadernos de Graduação**: Ciências Humanas e Sociais, Alagoas, v. 3, n. 3, p.85-100, nov. 2016. Disponível em: https://periodicos.set.edu.br/index.php/fitshumanas/article/view/3579>. Acesso em: 27 abr. 2018.

ARAÚJO, Marco Antônio Pereira. A Inclusão Digital como Estratégia para Resgate da Cidadania e Diminuição da Exclusão Social e Econômica. **Revista Interdisciplinar de Direito**, v. 6, n. 1, p. 375-382. 2017. Disponível em: < http://revistas.faa.edu.br/index.php/FDV/article/download/50/32>. Acesso em: 11 abr. 2018.

Artigo 19. PROTEÇÃO DE DADOS PESSOAIS NO BRASIL: ANÁLISE DOS PROJETOS DE LEI EM TRAMITAÇÃO NO CONGRESSO NACIONAL. Novembro, 2016. Disponível em: < http://artigo19.org/blog/2017/01/31/protecao-de-dados-pessoais-no-brasil-analise-dos-projetos-de-lei-em-tramitacao-no-congresso-nacional/ >. Acesso em: 18 maio 2018.

BATISTA, Nadine Victor; BATISTA, Gisele Victor; GOMES, Nicole Victor. A TRANSPARÊNCIA PÚBLICA E OS DESAFIOS DA ACESSIBILIDADE: A INTERNET ENQUANTO INSTRUMENTO DE APROXIMAÇÃO ENTRE ESTADO E CIDADÃO NA ERA DA SOCIEDADE DA INFORMAÇÃO. **V Seminário de Ciências Sociais Aplicadas**, Criciúma, v. 5, n. 5, p.1-17, maio 2016. Disponível em: <http://periodicos.unesc.net/seminariocsa/article/view/2786>. Acesso em: 13 abr. 2018.

BRASIL. Câmara dos Deputados. Projeto de Lei PL 4060/2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066&ord=1>. Acesso em: 18 maio 2018.

BRASIL. Câmara dos Deputados. Projeto de Lei PL 5276/2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 >. Acesso em: 17 maio 2018.

BRASIL. Constituição da República Federativa do Brasil de 1988. DOU: 05.10.1988. 1988. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 10 de abril, 2018.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. DOU: 11.01.2002. 2002. Disponível em: < http://www.planalto.gov.br/CCivil_03/Leis/2002/L10406.htm >. Acesso em: 10 de abril, 2018.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. DOU: 24.04.2014. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 20 de abril, 2018.

BRASIL. Senado Federal. Projeto de Lei do Senado PLS 330/2013. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/113947>. Acesso em: 16 maio 2018.

DE VASCONCELOS, Fernando Antônio; HOLANDA VASCONCELOS BRANDÃO, Fernanda. AS REDES SOCIAIS E A EVOLUÇÃO DA INFORMAÇÃO NO SÉCULO XXI. **Direito e Desenvolvimento**, [S.l.], v. 4, n. 1, p. 125-144, jan/jun. 2013. ISSN 2236-0859. Disponível em: <https://periodicos.unipe.br/index.php/direitoedesenvolvimento/article/view/225>. Acesso em: 14 abr. 2018.

DINIZ, Maria Helena. Uma visão constitucional e civil do novo paradigma da privacidade: o direito a ser esquecido/A constitutional and civil vision of the new privacy paradigm: the right to be forgotten. **Revista Brasileira de Direito**, Passo Fundo, v. 13, n. 2, p. 7-25, ago. 2017. ISSN 2238-0604. Disponível em: https://ser.imed.edu.br/index.php/revistadedireito/article/view/1670. Acesso em:30 abril 2018.

DO AMARAL, Ana Beatriz Nunes Paiva; CHAVES, Fernanda Maria de Assunção Furtado. TUTELA DO DIREITO AO ESQUECIMENTO NO BRASIL: CASO FABÍOLA E SUA RELAÇÃO COM O REVENGE PORN. **Revista Pesquisas Jurídicas**, v. 5, n. 1, p. 72-94, fev/jun 2016. Disponível em: < http://www.revistapesquisasjuridicas.com.br/ojs/index.php/RPJur/article/view/127>.Acesso em:02 maio 2018.

ELIAS, Ednete Morais Costa. A pujança dos movimentos sociais: do Império à formação através das redes sociais virtuais no Brasil atual. **Research, Society And Development**, Logroño, v. 1, n. 2, p.107-126, ago. 2016. Disponível em: <https://dialnet.unirioja.es/servlet/articulo?codigo=6070062>. Acesso em: 15 abr. 2018.

FAVERA, Rafaela Bolson dalla; SILVA, Rosane Leal da. CIBERSEGURANÇA NA UNIÃO EUROPEIA E NO MERCOSUL: BIG DATA E SURVEILLANCE VERSUS PRIVACIDADE E PROTEÇÃO DE DADOS NA INTERNET. **Revista de Direito,**

Governança e Novas Tecnologias, Curitiba, v. 2, n. 2, p.112-134, jul/dez. 2016. Disponível em: <http://www.indexlaw.org/index.php/revistadgnt/article/view/1490>. Acesso em: 11 maio 2018.

LIMA, Marco Antonio; BARRETO JUNIOR, Irineu Francisco. MARCO CIVIL DA INTERNET: LIMITES DA PREVISÃO LEGAL DE CONSENTIMENTO EXPRESSO E INEQUÍVOCO COMO PROTEÇÃO JURÍDICA DOS DADOS PESSOAIS NA INTERNET. **Revista de Direito, Governança e Novas Tecnologias**, Brasília, v. 1, n. 2, p.241-260, jan/jun. 2016. Disponível em: <http://indexlaw.org/index.php/revistadgnt/article/view/831>. Acesso em: 09 maio 2018.

MACHADO, Jessika Milena Silva; MOMBACH, Patrícia Ribeiro. STALKING: CRIMINALIZAÇÃO NECESSÁRIA SOB A INDUBITÁVEL AFRONTA AO DIREITO FUNDAMENTAL À VIDA PRIVADA. **Revista da Esmesc**, Florianópolis, v. 23, n. 29, p.207-230,. 2016. Disponível em: <https://www.revista.esmesc.org.br/re/article/view/146>. Acesso em: 02 maio 2018.

MARTINS, Guilherme Magalhães. **Contratos eletrônicos de consumo**. 3. ed., rev. atual. e ampl. São Paulo: Atlas, 2016.

MARTINS, Guilherme Magalhães. **Direito privado e internet.** São Paulo: Atlas, 2014.

MARTINS, Guilherme Magalhães. **Responsabilidade civil por acidente de consumo na Internet**. 2. ed. São Paulo: Editora Revista dos Tribunais, 2014.

MARTINS JUNIOR, Joaquim. **Como escrever trabalhos de conclusão de curso**: instruções para planejar e montar, desenvolver, concluir, redigir e apresentar trabalhos monográficos e artigos. 7. ed. Rio de Janeiro: Vozes, 2013.

MORE: **Mecanismo online para referências**, versão 2.0. Florianópolis: UFSC Rexlab, 2013. Disponível em: ‹ http://www.more.ufsc.br/ ›. Acesso em: 21 out. 2017.

MOREIRA, Adriano Fernandes. A ABUSIVIDADE DAS PRÁTICAS COMERCIAIS E DA PUBLICIDADE NA PRESTAÇÃO DE SERVIÇOS GRATUITOS PELO GOOGLE. **Revista Cereus**, Gurupi, v. 7, n. 1, p.40-59, jan/abr. 2015. Disponível em:

<http://www.ojs.unirg.edu.br/index.php/1/article/view/567>. Acesso em: 01 maio 2018.

SCHREIBER, Anderson. **Direitos da Personalidade**. 2. ed. São Paulo: Atlas, 2013.

SHIMAZAKI, Vinicius Kenji; PINTO, Maria Márcia Matos. A INFLUÊNCIA DAS REDES SOCIAIS NA ROTINA DOS SERES HUMANOS. **Fasci-tech**: Periódico Eletrônico da FATEC, São Caetano do Sul, v. 1, n. 5, p.171-179, out/dez. 2011. Disponível em: <http://fatecsaocaetano.edu.br/fascitech/index.php/fascitech/article/view/57>. Acesso em: 14 abr. 2018.

SILVA, Vivian Duarte da. COMUNICAÇÃO PÚBLICA NA INTERNET E CIDADANIA. **Ii Interprogramas – Xv Secomunica**: COMUNICADORES E MUTAÇÕES: CENÁRIOS E OPORTUNIDADES, Brasília, p.325-335, set. 2016. Disponível em: <https://portalrevistas.ucb.br/index.php/AIS/article/download/7869/4881>. Acesso em: 14 abr. 2018.

STF. Recurso Extraordinário nº 1.037.396 SP. Relator: Ministro Dias Toffoli. DJe: 04.04.2018. 2018. Disponível em: < http://portal.stf.jus.br/processos/downloadPeca.asp?id=314030456&ext=.pdf>. Acesso em: 15 de maio, 2018.

STJ. Recurso Especial nº 1.679.465 SP 2016/0204216-5. Relator: Ministra Nancy Andrighi. DJe: 19.03.2018. 2018. Disponível em: < https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1685789&num_registro=201602042165&data=20180319&formato=PDF>. Acesso em: 12 de maio, 2018.

STJ. Recurso Especial nº 1.698.647 SP 2017/0047840-6. Relator: Ministra Nancy Andrighi. DJe: 15.02.2018. 2018. Disponível em: < https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1671167&num_registro=201700478406&data=20180215&formato=PDF>. Acesso em: 13 de maio, 2018.

TEIXEIRA, Tarcisio; SABO, Paulo Henrique; SABO, Isabela Cristina. WHATSAPP E A CRIPTOGRAFIA PONTO-APONTO: TENDÊNCIA JURÍDICA E O CONFLITO PRIVACIDADE VS. INTERESSE PÚBLICO. **Revista da Faculdade de Direito**: Universidade Federal de Minas Gerais, Belo Horizonte, n. 71, p.607-638, jul/dez. 2017. Semestral. Disponível em: <https://www.direito.ufmg.br/revista/index.php/revista/article/view/1882>. Acesso em: 10 maio 2018.

TJ/RJ. Agravo de Instrumento nº 0001284-14.2018.8.19.0000. Relator: Desembargador Juarez Fernandes Folhes. DJe: 22.03.2018. 2018. Disponível em:<http://www1.tjrj.jus.br/gedcacheweb/default.aspx?UZIP=1&GEDID=0004870F68C58D8109BCFC54AE3A825AEFBEC5075E3A2131&USER=>. Acesso em: 11 de maio, 2018.

TJ/RJ. Apelação Cível nº 0028583-76.2010.8.19.0054. Relator: Desembargador Mario Assis Gonçalves. DJe: 15.03.2018. 2018. Disponível em: < http://www1.tjrj.jus.br/gedcacheweb/default.aspx?UZIP=1&GEDID=0004A8B80A791253E1E250EC585F2CF418EEC5075961135F&USER=>. Acesso em: 11 de maio, 2018.

TJ/RJ. Apelação Cível nº 0050120-83.2016.8.19.0001. Relator: Desembargador Carlos Eduardo da Fonseca Passos. DJe: 20.04.2018. 2018. Disponível em: <http://www1.tjrj.jus.br/gedcacheweb/default.aspx?UZIP=1&GEDID=0004E79F6C6D459860D024EDF2F9583C0C2DC5080A621C28&USER=>. Acesso em: 11 de maio, 2018.